Algorithmic Governance and Governance of Algorithms: An Introduction

Marta Cantero Gamito and Martin Ebers

Contents
1 The Promise and Perils of Algorithm-Based Technologies ............................................. 2
2 From Algorithmic Governance to Governance of Algorithms ............................................. 5
   2.1 The Current Legal Landscape ................................................................................. 5
   2.2 Existing Initiatives to Regulate AI and Robotics in a Nutshell ................................. 6
3 The European Union’s AI Strategy .................................................................................... 8
   3.1 The EU as the Global Regulatory Standard-Setter .................................................. 8
   3.2 The European Parliament’s Resolution of February 2017 ........................................... 9
   3.3 The European Commission’s AI Strategy and the Work of the High-Level Expert
       Group on AI ........................................................................................................... 10
   3.4 The European Commission’s White Paper on AI .................................................... 12
4 Overview of This Book .................................................................................................... 14
5 The Way Forward ............................................................................................................. 17
References ............................................................................................................................. 18

Abstract The use of algorithms is more than ever replacing human decision-making. Naturally, this raises concerns about how to govern AI-powered technologies. This chapter introduces the potential as well as the threat(s) posed by decision-making by algorithms (algorithmic governance) and provides an up-to-date overview of the state of art and the existing legislative initiatives in this field (governance of algorithms).

Sections 1–3 written by Martin Ebers; Sections 4 and 5 written by Marta Cantero Gamito.

M. Cantero Gamito
CUNEF, Law Department, Madrid, Spain
University of Tartu, School of Law, Tartu, Estonia

M. Ebers (*)
Humboldt University of Berlin, Law Faculty, Berlin, Germany
University of Tartu, School of Law, Tartu, Estonia
e-mail: martin.ebers@ut.ee

© The Editor(s) (if applicable) and The Author(s), under exclusive licence to
Springer Nature Switzerland AG 2021
M. Ebers, M. Cantero Gamito (eds.), Algorithmic Governance and Governance of Algorithms, Data Science, Machine Intelligence, and Law 1, https://doi.org/10.1007/978-3-030-50559-2_1
1 The Promise and Perils of Algorithm-Based Technologies

Algorithm-based technologies\(^1\) such as artificial intelligence (AI)\(^2\) and smart robotics\(^3\) are increasingly pervading our lives. They are deployed in many sectors ranging from retail and production, finance and transport to healthcare and security.\(^4\) They come in different forms and shapes, as personal assistants on our smartphones, search engines, translation apps, data-mining programs, scoring systems, medical diagnosis systems, price algorithms, expert trading systems, and in physical manifestations, such as self-driving cars, drones, unmanned underwater vehicles, surgical robots, personal robots and social robots.

Many of these systems have the potential to improve our lives as well as the overall economic and societal welfare. AI-powered systems can lead to better healthcare services,\(^5\) safer and cleaner transport systems,\(^6\) better working conditions,\(^7\) higher productivity\(^8\) and new innovative products, services and supply chains.\(^9\) They can also benefit the public sector in a number of ways;\(^10\) for example, by automating repetitive and time-consuming tasks, or by providing public agencies with more accurate and detailed information, forecasts and predictions, which in turn might lead to personalized public services tailored to individual circumstances. AI-powered systems may even help to respond to key global challenges, such as the climate change\(^11\) and the novel coronavirus pandemic.\(^12\)

However, as with every disruptive technology, AI and smart robotics come not only with benefits but also with substantial risks, raising a broad variety of ethical

---

\(^{1}\)Generally speaking, an algorithm can be understood as “sets of defined steps structured to process instructions/data to produce an output”; Kitchin (2017).

\(^{2}\)Popular definitions of AI are equally unrefined. For different definitions cf. Samoili et al. (2020), High Level Expert Group on AI (AI HLEG) (2019a), McCarthy (2007), Russell and Norvig (2011), pp. 1 et seq.

\(^{3}\)There is currently no generally accepted definition of the term “robot” either. The AI HLEG describes robotics as “AI in action in the physical world”, but points out that robots cannot be equated with AI systems, since robotics also uses technologies that lie outside of artificial intelligence; cf. AI HLEG (2019a), p. 4.

\(^{4}\)For an overview on different use-cases cf. OECD (2019a), pp. 47 et seq.; International Electrotechnical Commission (IEC) (2018), pp. 45 et seq.

\(^{5}\)Abu-Nasser (2017) and Gray (2018).

\(^{6}\)Anderson et al. (2016), pp. 9 et seq.; OECD (2019a), pp. 48 et seq.

\(^{7}\)Arntz et al. (2016) and OECD (2019b).

\(^{8}\)Autor and Salomons (2018).

\(^{9}\)Charalambous et al. (2019) and World Economic Forum (2017).

\(^{10}\)Freeman Engstrom et al. (2020).

\(^{11}\)Vinuesa et al. (2020).

\(^{12}\)Kritikos, European Parliamentary Research Service (EPRS) (2020), pp. 1–2; Dumbrava, European Parliamentary Research Service (EPRS) (2020).
and legal challenges. Algorithmic systems can unpredictably harm people’s life, health, and property. They can also affect fundamental values on which western societies are founded, leading to breaches of fundamental rights, including the rights to human dignity and self-determination, privacy and personal data protection, freedom of expression and of assembly, non-discrimination, or the right to an effective judicial remedy and a fair trial, as well as consumer protection.

Automated or algorithmic decision making (ADM) systems are particularly of concern. Many important decisions, which were historically made by people, are now either made by machines or at least prepared by them. We live in a “scored society” in which citizens, consumers and legal entities are increasingly subject to actions and decisions taken by or with the assistance of AI systems. AI increases the possibilities to track and score the daily habits of people. Companies from various industries collect, analyze, acquire, share, trade, and utilize data on billions of people in order to discern patterns, predict the likely behavior of people through scoring systems, and act accordingly. As a result, there is not only the danger that AI systems—in violation of data protection law—are used by state authorities or private companies for mass surveillance. Rather, the widespread use of algorithms for preparing or even making decisions is also criticized on the grounds of discrimination. A number of examples show that ADM procedures are by no means neutral but can perpetuate and even exacerbate biases in various ways. Compared to human decision-making, ADM systems pose a particular challenge: while it is true that human decision-making is not immune to mistakes and biases, algorithmic decisions can have a much larger effect, as the software not only decides dozens or hundreds of cases, but rather tens of thousands or more.

AI systems can also unintentionally or intentionally lead to manipulation. Social media platforms and search engines use AI systems to channel, prioritize and filter information—with potentially detrimental effect on the right to freedom of information, the right to freedom of expression, media pluralism, and the political discourse in general. Moreover, the insights gained by AI powered systems can be used by companies or political parties to exploit or trigger irrational behavior—a practice which in the end led to the well-known Cambridge Analytica scandal.

Particularly troublesome is the fact that not only private companies, but also governmental institutions are increasingly relying on algorithmic systems to analyze and predict behavior in order to make decisions. Tax offices have started using

---

13 For an in-depth analysis cf. Ebers (2020). According to the Stanford AI Index 2019, the ethical challenges most mentioned across 59 ethical AI framework documents were: fairness; interpretability and explainability; transparency, accountability; data privacy, reliability, robustness and security; Perrault et al. (2019), p. 149.
14 Cf. Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET) (2017), Raso et al. (2018).
15 Cf. AlgorithmWatch (2019).
16 Keats and Pasquale (2014).
17 Pariser (2011), Sunstein (2017) and Epstein (2014).
18 Cf. Nix (2016); moreover Rubinstein (2014).
algorithms to predict abuse and fraud in tax returns and to allocate cases for human review.\textsuperscript{19} In social welfare systems, algorithms are used to determine whether a citizen should be flagged because of an increased risk of irregularities, or potential fraud.\textsuperscript{20} In the field of public security, many agencies use AI systems to detect terrorists,\textsuperscript{21} to screen people at the border,\textsuperscript{22} and to predict and respond to crime (predictive policing).\textsuperscript{23} In the US, algorithmic prognosis instruments are even used by courts to calculate the likelihood of an accused person committing another crime while on parole.\textsuperscript{24} In China, the government has implemented a Social Credit System which is intended to standardize the assessment of citizens’ and businesses’ economic and social reputations.\textsuperscript{25}

The risks associated with AI systems and smart robotics are further intensified and amplified by the specific characteristics of many of these technologies, including opacity (black box-effect),\textsuperscript{26} complexity, unpredictability and partially autonomous behavior—all of which may make it hard to verify compliance with the existing legal rules. Due to these characteristics, both enforcement authorities and affected persons might lack the means to verify how a given algorithmic decision was taken and whether the relevant rules were respected.

\textsuperscript{19}DeBarr and Harwood (2004).
\textsuperscript{20}For Austria see https://algorithmwatch.org/en/story/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm/; for Finland, https://www.tieto.com/en/success-stories/2018/the-city-of-espoo-a-unique-experiment/; for the Netherlands https://bijvoorbaatverdacht.nl/; for Spain https://algorithmwatch.org/en/story/spain-legal-fight-over-an-algorithms-code/; for Sweden https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/. Accessed 29 Apr 2020.
\textsuperscript{21}In the EU, the European Commission is funding the DANTE experiment, an anti-terrorism project (Detecting and analysing terrorist-related online contents and financing activities), aimed at using automated decision-making against terrorism, https://www.h2020-dante.eu/. Accessed 29 Apr 2020.
\textsuperscript{22}In the EU, many countries use “iBorderCtrl”, a system tested in Hungary, Greece and Latvia to screen non-EU nationals at EU borders, using automated interviews with a virtual border guard, based on “deception detection” technology; https://www.iborderctrl.eu/The-project. Accessed 29 Apr 2020.
\textsuperscript{23}Barrett (2017), Ferguson (2012), p. 317; Rich (2016) and Saunders et al. (2016).
\textsuperscript{24}Such processes are used at least once during the course of criminal proceedings in almost every US state; Barry-Jester et al. (2015). More than 60 predictive tools are available on the market, many of which are supplied by companies, including the widely-used COMPAS system from Northpointe.
\textsuperscript{25}Hvistendahl (2017), Botsman (2017). Chen et al. (2018), pointing out that the Social Credit System has not—at least for now—employed AI technologies, real-time data or automated decisions, despite foreign media reports to the contrary.
\textsuperscript{26}The notion of black-box AI refers to such scenarios, where we can see only input data and output data for algorithm-based systems without understanding exactly what happens in between. Burrell (2016), Leese (2014), Mittelstadt et al. (2016), p. 6; Pasquale (2015).
2 From Algorithmic Governance to Governance of Algorithms

2.1 The Current Legal Landscape

There is currently not a single country (or supranational organization) in the world with legislation that explicitly takes into account the problematic characteristics of algorithmic systems in general.

Apart from a few exceptions, there are also no special rules for AI systems and smart robotics in particular. Admittedly, special regulation exists for self-driving vehicles, drones, and high-frequency trading. Moreover, in the European Union, the General Data Protection Regulation (GDPR) contains rudimentary provisions for fully automated decisions. In addition, the EU Consumer Rights Directive 2011/83/EU, as amended by the “New Deal for Consumers”, includes an obligation to provide information on the use of automatically generated personalised prices. Moreover, the so-called P2B (Platform-to-business) Regulation 2019/1150 requires providers of online search engines to “set out the main parameters, which individually or collectively are most significant in determining ranking and the relative importance of those main parameters, by providing an easily and publicly

27 In the US, most of the states have either enacted legislation or executive orders governing self-driving vehicles; cf. National Conference of State Legislatures, Autonomous Vehicles State Bill Tracking Database, http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx. Accessed 29 Apr 2020. In 2017, the House of Representatives passed a bill for a “Self Drive Act” which was supposed to lay out a basic federal framework for autonomous vehicle regulation but, ultimately, failed to be considered on the Senate floor. For the EU, see Expert Group on Liability and New Technologies—New Technologies Formation (2019).

28 In the EU, the Regulation on Civil Aviation 2018/1139 addresses issues of registration, certification, and general rules of conduct for operators of drones—however, without regulating civil liability directly; cf. Bertolini (2018).

29 See esp. Art. 17, Art. 48(6) MiFID II (Directive 2014/65/EU on markets in financial instruments) and Commission delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements of investment firms engaged in algorithmic trading, OJ 31 March 2017 L 87/417.

30 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, OJ L 119, 4 May 2016. Art. 22 GDPR prohibits fully automated decisions; for those decisions, Art. 13 (2) lit. f and Art. 14 (2) lit. g GDPR establish moreover a special obligation for data controllers to provide information. However, these provisions have a rather limited scope of application, because they only apply to decisions “based solely on automated processing” of data. Since most algorithmically prepared decisions still involve a human being, the majority of ADM procedures is not covered by the aforementioned provisions; cf. Martini (2019), pp. 10 et seq.

31 According to Art. 6(1) (ea) Consumer Rights Directive 2011/83/EU as amended by Directive 2019/216/EU, the trader may have to inform the consumer “that the price has been personalised on the basis of an automated decision making process”.
available description”. \(^{32}\) Furthermore, some countries have issued rules for automated algorithm-based administrative decisions, such as Canada with its “Directive on Automated Decision-Making”. \(^{33}\) In France, the Digital Republic Act (Loi no. 2016-1321 du 7 octobre 2016 pour une République numérique), provides that, in the case of state actors taking a decision “on the basis of algorithms”, individuals have a right to be informed about the “principal characteristics” of the decision-making system. \(^{34}\)

However, all these rules deal only with individual aspects without providing a satisfactory answer to the problems described above. Certainly, many countries and sometimes also international and supranational organizations have laws, norms and rules that are relevant for AI and robotics—ranging from constitutional principles (rule of law, democracy), \(^{35}\) human rights, \(^{36}\) and (international) humanitarian law, \(^{37}\) to administrative and criminal law protecting inter alia fair procedures; \(^{38}\) to special laws that could help to mitigate the described problems such as data protection law, cybersecurity law, product safety and product liability law, competition law, consumer law; and many other fields. These laws, however, were not made with AI and smart robotics in mind.

Accordingly, it is difficult to gauge to what extent existing legislation sufficiently regulates the undesirable implications of AI.

### 2.2 Existing Initiatives to Regulate AI and Robotics in a Nutshell

Since the beginning of 2017, many governments in the world have begun to develop national strategies for the promotion, development, and use of AI systems. Still, as Tim Dutton—a Canadian Senior Policy Advisor who regularly updates a summary of different AI policies—observes, no two strategies are alike. \(^{39}\) Instead, national (and international) initiatives focus on a wide variety of aspects such as research and development programs, skills and education, data and digital infrastructure,

---

\(^{32}\) Art. 5(2) Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services (P2B Regulation), OJ L 186, 11 July 2019.

\(^{33}\) Government of Canada, ‘Directive on Automated Decision-Making’, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592. Accessed 29 Apr 2020.

\(^{34}\) For more details see Edwards and Veale (2018).

\(^{35}\) Cf. for example Council of Europe, European Commission for the Efficiency of Justice (CEPEJ) (2018).

\(^{36}\) Cf. Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET) (2017); Raso et al. (2018).

\(^{37}\) Margulies (2018).

\(^{38}\) On AI and administrative law cf. Oswald and Grace (2016), Cobbe (2018) and Coglianese and Lehr (2017).

\(^{39}\) Dutton (2018). Cf. also the overview by Thomas (2018).
technical standardization, AI-enhanced public services, ethics and inclusion, and sometimes also legal standards. Whereas some countries have laid down specific and comprehensive AI strategies (e.g. China, the UK, France), some are integrating AI technologies within national technology or digital roadmaps (e.g. Denmark, Australia), while still others have focused on developing a national AI R&D strategy (US).\(^{40}\)

In the US, most notably, the government already relied heavily under the Obama administration on the liberal notion of the free market.\(^{41}\) In its report “Preparing for the Future of Artificial Intelligence”, published in October 2016,\(^{42}\) the White House Office of Science and Technology Policy (OSTP) explicitly refrains from a broad regulation of AI research and practice. Instead, the report highlights that the government should aim to fit AI into existing regulatory schemes, suggesting that many of the ethical issues related to AI can be addressed through increasing transparency and self-regulatory partnerships.\(^{43}\) The Trump administration, too, sees its role not in regulating AI and robotics but in “facilitating AI R&D, promoting the trust of the American people in the development and deployment of AI-related technologies, training a workforce capable of using AI in their occupations, and protecting the American AI technology base from attempted acquisition by strategic competitors and adversarial nations”—thus maintaining US American leadership.\(^{44}\) In January 2020, the White House published a draft memorandum outlining ten principles which federal agencies should consider when devising laws and rules for the use of AI in the private sector, but stressed—again—that a key concern was limiting regulatory “overreach”.\(^{45}\)

By contrast, the European Union focusses in its AI strategy (published in April 2018) and its Whitepaper on AI (published in February 2020) not only on the potential impact of AI on competitiveness but also on its social and ethical implications, underpinning that compliance with European ethical norms, legal requirements and social values is essential to create “an ecosystem of trust”.

Beyond the European Union, several international organizations have also taken the initiative to reflect on the future legal framework for AI and robotics, such as the Organisation for Economic Cooperation and Development (OECD) with its principles on AI, adopted in May 2019,\(^{46}\) and the new AI Policy Observatory which aims

\(^{40}\)Delponte (2018), p. 22.

\(^{41}\)For a detailed discussion of the various AI strategies in the US, the EU, and the UK, see Cath et al. (2018).

\(^{42}\)Executive Office of the [US] President—National Science and Technology Council Committee on Technology (2016). The report followed five workshops and a public request for Information, cf. Executive Office of the [US] President—National Science and Technology Council Committee on Technology (2016), p. 12.

\(^{43}\)Executive Office of the [US] President—National Science and Technology Council Committee on Technology (2016).

\(^{44}\)Trump (2019). Cf. also Shepardson (2018).

\(^{45}\)Office of Management and Budget (OMB), the White House (2019).

\(^{46}\)OECD (2019c).
to help policymakers to implement the AI principles;\(^4\)the United Nations (UN) with its several activities on AI;\(^8\) and the Council of Europe with its “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment’’, adopted at the end of 2018,\(^9\) and its ad hoc committee on AI (CAHAI) with the specific task to examine the possibility of creating a legal framework for the development, design and application of artificial intelligence, based on Council of Europe’s standards on human rights, democracy and the rule of law.\(^5\)

Apart from these initiatives, hundreds of different ethical AI guidelines have emerged during the past years. The number of ethical guidelines developed by governments, tech companies, and industry has grown exponentially in recent years—so much that researchers had to develop special tools to provide an overview.\(^6\) However as laudable as this work may be, it should be clear that soft law as such will not suffice. The work on ethical principles and guidelines can lay the groundwork for subsequent legislation, providing orientation on the possible content of legal rules. However, the main problem is that ethical guidelines and self-regulatory initiatives by industries are non-binding.\(^7\) In addition, these principles are often too abstract to provide sufficiently detailed guidance. As it has been pointed out, “[m]uch of the debate about ethics seems increasingly focused on companies avoiding regulation. Unable or unwilling to properly provide regulatory solutions, ethics is seen as the ‘easy’ or ‘soft’ option which can help structure and give meaning to existing self-regulatory initiatives.”\(^8\) Indeed, ethical guidelines and self-regulation should not be used as an escape from (hard) regulation.

3 The European Union’s AI Strategy

3.1 The EU as the Global Regulatory Standard-Setter

The regulatory efforts of the EU are particularly noteworthy. The EU is widely acknowledged to be the regulatory standard-setter,\(^9\) especially in the field of data protection and its respective flagship, the General Data Protection Regulation.\(^10\) Although it has been argued that the GDPR puts European companies at a competitive disadvantage compared with firms in countries such as China and the US by

\(^4\)https://oecd.ai/. Accessed 29 Apr 2020.
\(^8\)https://www.itu.int/pub/S-GEN-UNACT-2018-1. Accessed 29 Apr 2020.
\(^9\)Council of Europe, European Commission for the Efficiency of Justice (CEPEJ) (2018).
\(^5\)www.coe.int/cahai. Accessed 29 Apr 2020.
\(^7\)See Fjeld et al. (2020).
\(^7\)Saurwein et al. (2015).
\(^8\)Wagner (2018), pp. 108 et seq.
\(^9\)Bradford (2020), Cremona and Scott (2019).
\(^10\)Smuha (2019).
imposing restrictions on the collection and use of personal data, which is especially relevant in the context of AI systems.\textsuperscript{56} this criticism did not alter the fact that the GDPR has been one of Europe’s most successful regulatory export products. Since its entry into force in May 2018, the GDPR has had a significant impact on data protection policy and enforcement beyond the EU in many jurisdictions, including California and Brazil.\textsuperscript{57}

With regard to AI, the European Union also seems to be willing to take the lead in developing regulatory standards. In 2019, the new president of the European Commission, Ursula von der Leyen, announced that in her first hundred days in office, she “would put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence”,\textsuperscript{58} thereby building on existing protective regulation as well as on the work of the High Level Expert Group on AI that published AI Ethics Guidelines in April 2019. In the same vein, German Chancellor Angela Merkel announced in June 2019 at the G20 summit in Japan, that “it will be the job of the next Commission to deliver something so that we have regulation similar to the General Data Protection Regulation that makes it clear that artificial intelligence serves humanity”.\textsuperscript{59}

Clearly, the European Union has not been the only regulatory power to claim a leading role in the governance of AI and robotics. However, no other country has taken a stance as strong as the EU’s promise to bring forth new binding legislation in this field. Against this background, the following observations focus solely on the political efforts of the EU to regulate algorithms, AI and robotics, while initiatives from other states and international organizations are not taken into account.

3.2 The European Parliament’s Resolution of February 2017

In the European Union, it was above all the European Parliament (EP) that first developed a strategy for an EU-wide regulation of AI and robotics. In February 2017, the EP passed a Resolution “with recommendations to the Commission on Civil Law Rules on Robotics”.\textsuperscript{60} The resolution called for the creation of a “European Agency for Robotics and AI” consisting of regulators and external technical and ethical experts who could provide the “technical, ethical and regulatory

\textsuperscript{56}On the frictions between Big Data Practices based on AI and the GDPR see Zarsky (2017) and Humerick (2018).

\textsuperscript{57}For a review of 24 jurisdictions cf. https://theword.iuslaboris.com/hrlaw/whats-new/the-impact-of-the-gdpr-outside-the-eu. Accessed 29 Apr 2020.

\textsuperscript{58}Von der Leyen (2019), p. 13.

\textsuperscript{59}Kayali (2019).

\textsuperscript{60}European Parliament, ‘Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051’. The resolution does not include unembodied AI. Instead, AI is understood as an underlying component of “smart autonomous robots”. Critically, Cath et al. (2018).
expertise needed to support the relevant public actors, at both Union and Member State level, in their effort to ensure a timely, ethical and well-informed response to the new opportunities and challenges,” 61 and could monitor robotics-based applications, identify standards for best practice and, where appropriate, recommend regulatory measures, define new principles, and address potential consumer protection issues. 62 Moreover, the Resolution recommended introducing an EU-wide registration system for specific categories of advanced robots. 63

Apart from that, the EP proposed to develop a Charter on robotics consisting of a code of ethical conduct for researchers and designers to “act responsibly and with absolute consideration for the need to respect the dignity, privacy and safety of humans”. 64 In addition, the EP asked the European Commission to clarify the liability of industry and autonomous robots when harm or damages occur and to adopt new rules on liability if necessary. 65

3.3 The European Commission’s AI Strategy and the Work of the High-Level Expert Group on AI

On 25 April 2018, the European Commission published its Communication “Artificial Intelligence for Europe”. 66 The document—complemented by another communication of 7 December 2018 67—outlined three pillars as the core of the proposed strategy: (i) boosting the EU’s technological and industrial capacity and AI uptake across the economy, (ii) preparing for socio-economic changes brought by AI, and (iii) ensuring an appropriate ethical and legal framework based on the Union’s values in line with the Charter of Fundamental Rights of the EU.

To support its implementation, the Commission established the “High-Level Expert Group on Artificial Intelligence” 68 (AI HLEG) and mandated it with the drafting of two documents in particular: (i) AI Ethics Guidelines that build on the work of the European Group on Ethics in Science and New Technologies 69 and of the European Union Agency for Fundamental Rights, 70 and (ii) Policy and

---

61European Parliament, Resolution, No. 16.
62European Parliament, Resolution, No. 17.
63European Parliament, Resolution, No. 2.
64European Parliament, Resolution, p. 19.
65European Parliament, Resolution, Nos. 49 et seq.
66European Commission (2018a).
67European Commission (2018b).
68https://ec.europa.eu/digital-single-market/en/high-level-group-artificial-intelligence. Accessed 29 Apr 2020.
69European Group on Ethics in Science and New Technologies (2018).
70The European Union Agency for Fundamental Rights (FRA), an independent EU body funded by the EU budget, started a new project on ‘Artificial Intelligence, Big Data and Fundamental Rights’
Investment Recommendations. At the same time, the European AI Alliance, an open multi-stakeholder platform with over 2700 members, was set up to provide broader input for the work of the AI HLEG.

At the end of 2018, the AI HLEG presented its first draft, “Ethics Guidelines for Trustworthy AI”.72 After an open consultation which generated feedback from more than 500 contributors, the AI HLEG published the final version at the beginning of April 2019, followed in June 2019 by the “Policy and Investment Recommendations for Trustworthy AI”.74 The ethics guidelines are neither an official document from the European Commission nor legally binding. They are also not intended as a substitute for any form of policy-making or regulation, nor to deter from the creation thereof.75 Rather, the ethics guidelines should serve as a “living document” and starting point for the discussion about “Trustworthy AI for Europe”.76

One of the main goals of these guidelines is to ensure that the development and use of AI follows a human-centric approach, according to which AI is not seen as a means in itself but as a tool to enhance human welfare and freedom. To this end, the AI HLEG propagates “trustworthy AI” which is (i) lawful, complying with all applicable laws and regulations; (ii) ethical, ensuring adherence to ethical principles and values; and (iii) robust, both from a technical and social perspective. The document aims to offer guidance on achieving Trustworthy AI by setting out in Chapter I fundamental rights and ethical principles AI should comply with. From those fundamental rights and principles, Chapter II derives seven key requirements (human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental wellbeing; and accountability), which then lead in Chapter III to a concrete but non-exhaustive assessment list to apply the requirements of Chapter II, offering AI practitioners guidance. During a piloting phase, organizations had the possibility to test the assessment list for trustworthy AI artificial intelligence.77

The work of the AI HLEG is accompanied by evaluations of the current EU safety and liability framework. To this end, the Commission set up the “Expert Group on Liability and New Technologies”, which published at the end of 2019 its findings on how liability regime should be designed—and, where necessary changed—in 2018 with the aim of helping create guidelines and recommendations in these fields. Cf. https://fra.europa.eu/en/about-fra/introducing-fra. Accessed 29 Apr 2020.

71https://ec.europa.eu/digital-single-market/en/european-ai-alliance. Accessed 29 Apr 2020.
72AI HLEG (2018).
73AI HLEG (2019b). Moreover, AI HLEG (2019a) published the document ‘A Definition of AI: Main Capabilities and Disciplines’.
74AI HLEG (2019c).
75AI HLEG (2019b), p. 3.
76AI HLEG (2019b), p. 3.
77European Commission (2019), p. 7.
78European Commission (2018a), p. 16.
order to rise to the challenges emerging digital technologies bring with them.\textsuperscript{79} Another paper of early 2020, prepared by the Joint Research Center (JRC) of the European Commission, deals with the topic “Robustness and Explainability of Artificial Intelligence”.\textsuperscript{80}

3.4 The European Commission’s White Paper on AI

On the basis of this preparatory work, the Commission published on 19 February 2020 its long-awaited White Paper “On Artificial Intelligence - A European approach to excellence and trust” to launch a public consultation on the future legal framework for AI.\textsuperscript{81} The White Paper on AI is supplemented by two other documents, namely a report on the safety and liability implications of new technologies,\textsuperscript{82} and the European data strategy.\textsuperscript{83} In addition, the Commission announced in its current work program that binding legislation on AI will be proposed in Q4 2020, in particular regarding safety, liability, fundamental rights and data aspects.\textsuperscript{84}

The White Paper highlights, first of all, possible adjustments to the existing EU legislative framework to AI.\textsuperscript{85} The specific characteristics of many AI systems—such as the already mentioned black box effect, complexity, unpredictability and semi-autonomous behaviour—could lead to new safety risks and liability gaps and could make effective enforcement of EU legislation more difficult, as algorithmic decisions cannot be traced and therefore cannot be checked for legal compliance.\textsuperscript{86} The European Commission is therefore considering an evaluation, and if necessary, adjustment of the current legal framework with regard to “the protection of fundamental rights and consumer rights” and with regard to “existing EU product safety and liability legislation”.\textsuperscript{87}

In addition to possible adjustments, the White Paper considers that new legislation specifically on AI may be needed “in order to make the EU legal framework fit for the current and anticipated technological and commercial developments”. Taking into consideration potential future regulation of AI, the White Paper takes a risk-based approach: as any regulatory intervention should be targeted and proportionate, the Commission does not want to introduce new mandatory legislation for all AI

\textsuperscript{79}Expert Group on Liability and New Technologies—New Technologies Formation (2019).

\textsuperscript{80}Hamon et al. (2020).

\textsuperscript{81}European Commission (2020d).

\textsuperscript{82}European Commission (2020c).

\textsuperscript{83}European Commission (2020b).

\textsuperscript{84}European Commission (2020a), Annex I.

\textsuperscript{85}European Commission (2020d), pp. 13 et seq.

\textsuperscript{86}European Commission (2020d), p. 12.

\textsuperscript{87}European Commission (2020d), p. 13.
systems, but only for so-called “high-risk AI systems”, whereas “low-risk AI systems” should be subject to a voluntary labelling scheme.\textsuperscript{88}

For high-risk cases, the White Paper identifies the following requirements that could be included in the regulatory framework:\textsuperscript{89}

- Requirements regarding the \textit{quality of training data} to guarantee representative and comprehensive data-sets in compliance with privacy and data protection rules
- \textit{Record and data keeping requirements} to enable a regulatory review and enforcement by allowing AI decisions to be traced back and verified
- \textit{Adequate information and transparency requirements} regarding the use, limitations and capabilities of high-risk AI systems
- \textit{Requirements on robustness and accuracy} of high-risk AI systems by avoiding and minimizing the different risks it may be vulnerable to
- \textit{Human involvement}, ranging from human oversight before a decision is implemented, to the possibility of human intervention in real time or afterwards
- \textit{Specific requirements for remote biometric identifications} such as facial recognition.

In order to ensure compliance of high-risk AI applications with these mandatory requirements, the European Commission envisages the creation of prior conformity assessments, which could include procedures for testing, inspections or certification—and “checks of the algorithms and of the data sets used in the development phase”.\textsuperscript{90}

Should the risk-based approach favoured by the Commission prevail, it is essential from the point of view of legal certainty, that the criteria for “high risk AI applications” are clearly defined. In this respect, however, the Commission’s statements remain rather vague. On the one hand, the Commission is of the opinion that AI applications should be considered high-risk only if both the sector \textit{and} the intended use involve significant risks.\textsuperscript{91} In this regard, the Commission plans to exhaustively list these high-risk sectors, as for instance healthcare, transport, energy and parts of the public sector. On the other hand, the Commission acknowledges that the use of AI may in exceptional circumstances be considered as a high-risk by itself, irrespective of the sector concerned and where the above mentioned requirements would still apply. As examples, the White Paper mentions the use of AI for recruitment purposes and remote biometric identification, as well as “specific applications affecting consumer rights”.\textsuperscript{92} However, it remains open which AI applications the Commission has specifically in mind.

For the future discussion, it will therefore be important first to identify the shortcomings of the current (national and European) legal framework for the use

\textsuperscript{88}European Commission (2020d), p. 17.
\textsuperscript{89}European Commission (2020d), pp. 18 et seq.
\textsuperscript{90}European Commission (2020d), p. 23.
\textsuperscript{91}European Commission (2020d), p. 17.
\textsuperscript{92}European Commission (2020d), p. 18.
of AI systems, and to determine the corresponding regulatory requirements for specific risks. For the time being, as the White Paper signals, both high-risk and non-high-risk existing AI applications remain entirely subject to already existing rules. Accordingly, the chapters of this volume provide an examination from different legal backgrounds, enriching the legal debate on the governance dimension of AI technologies.

4 Overview of This Book

In view of the different and fast-evolving developments of AI technologies manifold questions emerge. Some of these questions have been discussed above. As noted, the most pressing issue concerns the power of algorithms. There is no doubt that the expansion of AI is changing our world. The emergence of this new technological reality allows algorithms to make or influence decisions (algorithmic governance). Most of the online services we use nowadays rely on algorithms. Not only individuals and corporations, but also public authorities are delegating decision-making to algorithms, resulting in potential threats to privacy, non-discrimination, consumer protection, freedom of expression or the right to a fair trial among others. Certainly, this phenomenon is impacting how law is designed, applied and interpreted. The massive diffusion of algorithms is indeed fueling debates on how to govern this power adequately; there is an unrelenting urge to address the governance of algorithms.

This book brings those two dimensions together. The different contributions discuss the impact of algorithms and the different possibilities of forthcoming regulation. This volume combines some of the key topics and the challenges posed by algorithms, namely transparency and due process in automated decision-making, liability, privacy, consumer protection and copyright. 

Niklas Eder focuses on the increasing use of algorithms for individual profiling and its implications for privacy, non-discrimination and equal treatment. In his chapter, the key question revolves around how to address the challenges of profiling without individually undermining the fundamental rights involved. Eder argues that, in finding solutions, scholars have disregarded the boundaries between different categories of fundamental rights, which may ultimately undermine the relevance and essence of these rights. The chapter critically engages in the reasons why we, as lawyers, should care about establishing a proper definition and delimitation of the fundamental rights concerned; a proper definition and delineation of fundamental rights will significantly shape the normative choices to be made. Eder also provides a useful discussion on the existing trade-off between fundamental rights and the actual value-added of services relying on machine learning based data analysis innovations. The chapter concludes by suggesting a narrow interpretation of the potential fundamental rights affected by profiling, as the means to fully exploit the potential benefits of machine learning algorithms.
Francesca Palmiotto examines the consequences of the increasing use of algorithms for the purposes of collecting evidence and decision-making in criminal proceedings. More often than not, algorithms used for such purposes are not disclosed, making it very difficult to assess whether the process transforming the input into output respects fair trial rights. Specifically, Palmiotto focuses on the possibility for these algorithms to contain miscodes, and how these miscodes, which can be technical, scientific or legal, remain invisible as a result of algorithmic opacity. She uses the Harm Assessment Risk Tool (HART)—a software used by the UK police for supporting custody decisions and for assessing the risk of future offending by arrestees—as a use case, and shows how potential miscodes may remain hidden as a result of the opacity of the algorithms involved in the software. She discusses how the identified miscodes may impact fair trial rights and due process, such as preventing the contestability of the decision. Palmiotto concludes that the use of algorithms in criminal proceedings should be aligned with existing procedural guarantees. The risk is otherwise a dysfunctional system of criminal justice where fundamental rights are impaired.

In their chapter, Seili Suder and Merle Erikson explore the consequences of a dystopian phenomenon that is closer to reality than what we might think, microchipping employees. This practice is added to a wide array of mechanisms for controlling labour, namely computer screen recording, video surveillance, key-stroke monitoring, location tracking and social media monitoring, inter alia. The pervasive nature of microchipping, most notably constant surveillance, outweighs the possible benefits associated with its use. The risks of escalating beyond merely monitoring employee’s activities poses significant threats to privacy. Hence, the chapter carefully examines the privacy implications of microchipping in light of GDPR. The authors conclude that the collection of employee information triggers the application of the GDPR and that the employee’s consent is not a sufficient legal ground for the processing of personal data. As a result, the authors require the existence of a legitimate interest of the employer. However, they argue, this alone is not enough. Suder and Erikson propose the creation of specific national rules protecting microchipped employees, esp. by prohibiting the compulsory use of microchipping, which should be restricted only to those occupations where monitoring employee’s activities is critical for the job.

Tomás García-Micó offers an extensive overview of issues related to the liability of autonomous devices. Using the example of surgical robots, the chapter explores different implications of granting electronic personhood to autonomous goods. The questions to be addressed in this regard have sparked a scholarly debate on the capacity of existing civil rules to address the problems posed by robotics. For the most part, the current EU product safety framework already covers some of the risks posed by autonomous devices. Yet, for the purposes of legal certainty, concrete rules are still required to govern new emerging realities. García-Micó provides a careful analysis of current proposals, such as the European Parliament Resolution containing recommendations to the Commission on Civil Law Rules on Robotics also discussed above. The chapter concludes that granting legal personhood to autonomous devices, as suggested by the European Parliament Resolution, is
unnecessary and inadequate. Instead, it recommends strengthening other existing measures such as a mandatory insurance scheme for producers, which would facilitate compensation for persons having suffered harm caused by these devices.

Previous chapters have already shown that algorithms generally do not operate in an unregulated environment. In most cases, existing frameworks can accommodate the challenges posed by their increasing use. However, such accommodation requires a proper scrutiny and a serious assessment to identify whether new rules are needed. **Federico Galli** provides a detailed evaluation of the capacity of GDPR and the Unfair Commercial Practices Directive (UCPD) to properly cope with the problems arising from behavioral advertising; e.g. manipulation. This granular analysis reveals that the UCPD appears to be the most suitable instrument to address behavioral advertising. The article concludes with a call for a re-examination of the consumer policy approach embedded in the UCPD, and points at the insights offered by behavioral economics for the much-needed revision of the standard ‘average consumer’ in the twenty-first century.

**Jasper Siems** explores the suitability of the legal solutions offered by intellectual property (IP) rules to protect artificial neural networks (ANN). ANN are critical for deep learning. The chapter illustrates how existing IP regimes, such as copyright and patent protection are inadequate to protect ANN. As explained in the chapter, copyright and patent protection are generally anthropocentric. This largely rules out the possibility of protecting the intellectual creation of ANN by copyright or patent laws. Siems turns to trade secret protection rules as an alternative for the protection of the works by neural networks. The result is inconclusive; trade secret rules would have to be refined to accommodate ANN. It is argued however, that the application of trade secret rules is, despite its limitations, preferred to a rushed and potentially underdeveloped instrument that would inadequately address data ownership.

The last chapter deals with the legal status of computer-generated works (CGWs). **Ying Ye** and **Mike Adcock** provide an analysis of the Chinese copyright framework to explore how copyrightability and authorship operate in the case of CGWs. The chapter offers interesting illustrations of the possibilities of AI technologies to develop creative output, so far exclusively attributed to humans. Examples include the Xiaoice application, a poem generator, or Alibaba’s Luban, an AI-based graphic design tool. The analysis focuses on the application of copyright rules through the examination of the scope of Chinese copyright law to cover CGWs. Unlike the UK copyright law that explicitly defines CGWs, Chinese legislation, similarly to other countries, has not yet incorporated this development. By proposing a separation between authorship and ownership, Ye and Adcock conclude that Chinese copyright law may extend protection to CGWs under existing rules which allow “work for hire” and the “work of legal person or entity”.

5 The Way Forward

The continuous development and increasing use of AI technologies has created significant governance challenges. However, the legal and political implications of the use of algorithms for decision-making go beyond governance questions, triggering a social debate on the meaning and reach of algorithms in our future life. A proper prognosis should consider the challenges of scalability as well as the potential benefits of AI-powered systems for business and society. In this light, any (serious) legislative initiative should consider the possibilities and limitations of providing a legal framework sufficiently flexible to fit the purpose. From a legal perspective, potential threats to fundamental rights triggered by the pervasive use of algorithms are particularly pressing.

While a ‘wait-and-see’ approach is suitable for fast-pace emerging technologies, a clear regulatory roadmap such as the one provided in the European Commission’s latest White Paper is a sensible starting point. The significance of the issues involved, i.e. potential fundamental rights violations, favors a short-term strategy. Therefore, the proposed EU regulatory plan based on a risk-based approach, if executed appropriately, would ensure a much-needed democratic scrutiny and legal certainty for the ongoing development of AI. Moreover, the EU’s strategy and political vision on AI is set to influence an international discussion. The proposed EU framework will most likely have extraterritorial implications, similarly to the GDPR and other sectors. The Commission attempts to assert a distinctive European position on AI regulation for a trustworthy ecosystem. Two issues would require a closer look here.

First, the European Commission aims at establishing a framework for excellence and trust in which it is “paramount” that the requirements are applicable to all relevant economic operators providing AI-enabled products or services in the EU, “regardless of whether they are established in the EU or not”. This means that some non-EU operators will be subject to the abovementioned prior conformity assessment to verify that AI is trustworthy, secure and in line with European values and rules. This is important with regard to fundamental rights protection. The Commission clearly points at risks to fundamental rights and specifically mentions the need to ensure effective judicial redress for parties negatively affected by AI. In order to monitor and facilitate compliance, the White Paper mentions the role of standards. Standards might also contribute to specify future mandatory requirements. In this regard, it will be important to examine which values underpin the standard-setting process.

Secondly, a closer look should be paid to the coordination of global compliance. Regulation is also currently being drafted outside of the EU. In January 2020, the US

93 Cf. Cremona and Scott (2019) and Bradford (2020).
94European Commission (2020d), p. 22.
95European Commission (2020d), p. 23.
96European Commission (2020d), p. 18.
has published a set of principles which US agencies must meet when drafting AI regulations.\textsuperscript{97} This initiative is complemented by the proposal for an Algorithmic Accountability Act of 2019,\textsuperscript{98} currently under discussion. Given that many AI applications are built through a complex supply chain, it is expected that any legislative initiative will most likely have a global impact.

In conclusion, while fueling debates around the world, the EU Commission’s White Paper is certainly welcome and can be considered a sensible path towards the development of legislation for AI as well as to guide the global development of AI applications. However, the EU approach should not be rushed into a regulatory race. The concrete proposals expected towards late 2020 will provide some apparent regulatory relief, but the legislator cannot, and should not, overlook the fact that AI is constantly evolving. The expected evolution of AI will require a flexible regulatory approach that could make the EU framework a long-lasting one.

The rapid technological breakthroughs and the complexity of the sector make it particularly challenging for scholars and policymakers, who seek to understand and evaluate this phenomenon and its multifaceted implications. This volume contains a thoughtful analysis of some of the key legal topics that arise with regard to AI, framing the discussions questions and challenges to be faced in upcoming days.

References

Abu-Nasser B (2017) Medical expert systems survey. Int J Eng Inf Syst 7:218
AlgorithmWatch (2019) Automating society. Taking stock of automated decision-making in the EU. https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf. Accessed 29 Apr 2020
Anderson JM et al (2016) Autonomous vehicle technology. A guide for policymakers. RAND, Santa Monica California. https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf. Accessed 29 Apr 2020
Arntz M et al (2016) The risk of automation for jobs in OECD countries: a comparative analysis. OECD Social, Employment and Migration Working Papers, No. 189. OECD Publishing, Paris. https://doi.org/10.1787/5jlz9h56dvq7-en. Accessed 29 Apr 2020
Autor D, Salomons A (2018) Is automation labor-displacing? Productivity growth, employment, and the labor share. NBER Working Paper, No. 24871. https://doi.org/10.3386/w24871. Accessed 29 Apr 2020
Barrett L (2017) Reasonably suspicious algorithms: predictive policing at the United States border. N Y Univ Rev Law Soc Change 41(3):327
Barry-Jester AM et al (2015) The new science of sentencing. The Marshall Project, 4 Apr 2015. https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing#.xXEp6R5rD. Accessed 29 Apr 2020

\textsuperscript{97}Office of Management and Budget (OMB), the White House (2019).
\textsuperscript{98}www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf. Accessed 29 Apr 2020.
Bertolini A (2018) Artificial intelligence and civil law: liability rules for drones. Study commissioned by the European Parliament’s Policy Department for citizens’ rights and constitutional affairs at the request of the JURI Committee, PE 608.848

Botsman R (2017) Big data meets Big Brother as China moves to rate its citizens. Wired UK, 21 Oct 2017. https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion. Accessed 29 Apr 2020

Bradford A (2020) The Brussels effect: how the European Union rules the world. Oxford University Press, Oxford

Burrell J (2016) How the machine “thinks”: understanding opacity in machine learning algorithms. Big Data Soc, January-June, 1

Cath C et al (2018) Artificial intelligence and the “Good Society”: the US, EU, and UK approach. Sci Eng Ethics 24(2):505

Charalambous E et al (2019) AI in production: a game changer for manufacturers with heavy assets. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/ai-in-production-a-game-changer-for-manufacturers-with-heavy-assets. Accessed 29 Apr 2020

Chen Y et al (2018) “Rule of Trust”: the power and perils of China’s social credit megaproject. Columbia J Asian Law 32(1):1. https://ssrn.com/abstract¼3294776. Accessed 29 Apr 2020

Cobbe J (2018) Administrative law and the machines of government: judicial review of automated public-sector decision-making. A pre-review version of a paper in Legal Studies, Forthcoming. https://ssrn.com/abstract¼3226913. Accessed 29 Apr 2020

Coglianese C, Lehr D (2017) Regulating by robot: administrative decision making in the machine-learning era. Georgetown Law J 105:1147. https://ssrn.com/abstract¼2928293. Accessed 29 Apr 2020

Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET) (2017) Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. DGI(2017)12. https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a. Accessed 29 Apr 2020

Council of Europe, European Commission for the Efficiency of Justice (CEPEJ) (2018) European Ethical Charter on the use of artificial intelligence in judicial systems and their environment. Strasbourg, 3-4 Dec 2018. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Accessed 29 Apr 2020

Cremona M, Scott J (2019) EU law beyond EU borders. Oxford University Press, Oxford

DeBarr D, Harwood M (2004) Relational mining for compliance risk, presented at the Internal Revenue Service Research Conference. http://www.irs.gov/pub/irs-soi/04debar.pdf [https://perma.cc/Y9F8-RWNK]. Accessed 29 Apr 2020

Delplonte L (2018) European Artificial Intelligence (AI) leadership, the path for an integrated vision, Study requested by the ITRE Committee of the European Parliament. PE 626.074. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf. Accessed 29 Apr 2020

Dumbrava C, European Parliamentary Research Service (EPRS) (2020) Tracking mobile devices to fight coronavirus. PE 649.384. http://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf. Accessed 29 Apr 2020

Dutton T (2018) An overview of national AI strategies. Medium, 28 June 2018. https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70e66edf. Accessed 29 Apr 2020

Ebers M (2020) Regulating AI and robotics: ethical and legal challenges. In: Ebers M, Navarro S (eds) Algorithms and law. Cambridge University Press, Cambridge, pp. 37–99

Edwards L, Veale M (2018) Enslaving the algorithm: from a “right to an explanation” to a “right to better decisions”? IEEE Security & Privacy, May/June 46

Epstein R (2014) How Google could end democracy. U.S. News & World Report, 9 June 2014. https://www.usnews.com/opinion/articles/2014/06/09/how-googles-search-rankings-could-manipulate-elections-and-end-democracy. Accessed 29 Apr 2020

European Commission (2018a) Communication ‘Artificial Intelligence for Europe’. COM(2018) 237 final
European Commission (2018b) Communication ‘Coordinated plan on Artificial Intelligence’. COM (2018) 795 final
European Commission (2019) Communication ‘Building trust in human-centric Artificial Intelligence’. COM(2019) 168 final
European Commission (2020a) Communication ‘Commission Work Programme 2020. A Union that strives for more’. COM(2020) 37 final
European Commission (2020b) Communication ‘European strategy for data’. COM(2020) 66 final
European Commission (2020c) Report on the safety and liability implications of artificial intelligence, the Internet of Things and robotics. COM(2020) 64 final
European Commission (2020d) White Paper ‘On Artificial Intelligence – A European approach to excellence and trust’. COM(2020) 65 final
European Group on Ethics in Science and New Technologies (2018) Statement on artificial intelligence, robotics and “autonomous” systems. Brussels, 9 Mar 2018. https://ec.europa.eu/info/news/ethics-artificial-intelligence-statement-ege-released-2018-apr-24_en. Accessed 29 Apr 2020
Executive Office of the [US] President - National Science and Technology Council Committee on Technology (2016) Preparing for the future of artificial intelligence (OSTP report). https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Accessed 29 Apr 2020
Expert Group on Liability and New Technologies – New Technologies Formation (2019) Liability for artificial intelligence and other emerging technologies. https://doi.org/10.28385/573689. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199. Accessed 29 Apr 2020
Ferguson AG (2012) Predictive policing and reasonable suspicion. Emory Law J 62:259
Fjeld J et al (2020) Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for AI. Berkman Klein Center Research Publication No. 2020-1, 15 Jan 2020. https://doi.org/10.2139/ssrn.3518482. Accessed 29 Apr 2020
Freeman Engstrom D et al (2020) Government by algorithm: artificial intelligence in federal administrative agencies, Report submitted to the administrative conference of the United States. https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf. Accessed 29 Apr 2020
Gray A (2018) 7 amazing ways artificial intelligence is used in healthcare. World Economic Forum, 20 Sep 2018. www.weforum.org/agenda/2018/09/7-amazing-ways-artificial-intelligence-is-used-in-healthcare. Accessed 29 Apr 2020
Hamon R et al (2020) Robustness and explainability of artificial intelligence – From technical to policy solutions. Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/57493 (online), JRC119336. Accessed 29 Apr 2020
High Level Expert Group on AI (AI HLEG) (2018) Draft “Ethics Guidelines for trustworthy AI”, Working Document for stakeholders’ consultation. Brussels, 18 Dec 2018. https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai. Accessed 29 Apr 2020
High Level Expert Group on AI (AI HLEG) (2019a) A definition of AI: main capabilities and disciplines. Brussels, 9 Apr 2019. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341. Accessed 29 Apr 2020
High Level Expert Group on AI (AI HLEG) (2019b) Ethics Guidelines for trustworthy AI (Ethics Guidelines). Brussels, 8 Apr 2019. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477https://ec.europa.eu/futurium/en/ai-alliance-consultation. Accessed 29 Apr 2020
High Level Expert Group on AI (AI HLEG) (2019c) Policy and investment recommendations for trustworthy AI. Brussels, 26 June 2019. ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343. Accessed 29 Apr 2020
Humerick M (2018) Taking AI personally: how the E.U. must learn to balance the interests of personal data privacy & artificial intelligence. Santa Clara High Technol Law J 34:393
Hvistendahl M (2017) Inside China’s vast new experiment in social ranking. Wired, 14 Dec 2017. https://www.wired.com/story/age-of-social-credit/. Accessed 29 Apr 2020
International Electrotechnical Commission (IEC) (2018) White Paper ‘Artificial Intelligence across industries’. https://basecamp.iec.ch/download/iec-white-paper-artificial-intelligence-across-industries-en/. Accessed 29 Apr 2020

Kayali L (2019) Next European Commission takes aim at AI. Artificial intelligence will be the next GDPR. Politico, 18 July 2019. https://www.politico.eu/article/ai-data-regulator-rules-next-european-commission-takes-aim/. Accessed 29 Apr 2020

Keats D, Pasquale FA (2014) The scored society: due process for automated predictions. Washington Law Rev 89:1

Kitchin R (2017) Thinking critically about and researching algorithms. Inf Commun Soc 20 (1):1–14

Kritikos M, European Parliamentary Research Service (EPRS) (2020) Ten technologies to fight coronavirus. PE 641.543

Leese M (2014) The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. Secur Dialog 45(5):494

Margulies P (2018) The other side of autonomous weapons: using artificial intelligence to enhance IHL compliance. Roger Williams University Legal Studies Paper No. 182, 12 June 2018. https://ssrn.com/abstract=3194713. Accessed 29 Apr 2020

Martini M (2019) Fundamentals of a regulatory system for algorithm-based processes. Speyer. https://www.vzbv.de/sites/default/files/downloads/2019/07/19/martini_regulatory_system_algorithm_based_processes.pdf. Accessed 29 Apr 2020

McCarthy J (2007) What is artificial intelligence? www-formal.stanford.edu/jmc/whatisai/. Accessed 29 Apr 2020

Mittelstadt BD et al (2016) The ethics of algorithms: mapping the debate. Big Data Soc, July-September, 1

Nix A (2016) Speech at the 2016 Concordia annual summit in New York. https://www.youtube.com/watch?v=n8Dd5aVXLCc. Accessed 29 Apr 2020

OECD (2019a) Artificial intelligence in society. OECD Publishing, Paris. https://doi.org/10.1787/eedfied77-en. Accessed 29 Apr 2020

OECD (2019b) Going digital: shaping policies, improving lives. OECD Publishing, Paris. https://doi.org/10.1787/9789264312012-en. Accessed 29 Apr 2020

OECD (2019c) Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Accessed 29 Apr 2020

Office of Management and Budget (OMB), The White House (2019) Draft Memorandum for the Heads of executive departments and agencies, Guidance for regulation of artificial intelligence applications. www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. Accessed 29 Apr 2020

Oswald M, Grace J (2016) Intelligence, policing and the use of algorithmic analysis: a freedom of information-based study. J Inf Rights Policy Pract 1(1). https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/16. Accessed 29 Apr 2020

Pariser E (2011) The filter bubble: what the internet is hiding from you. Penguin Press, New York

Pasquale F (2015) The black box society: the secret algorithms that control money and information. Harvard University Press, London

Perrault R et al (2019) The AI Index 2019 Annual Report. AI Index Steering Committee, Human-Centered AI Institute. Stanford University, Stanford, Dec 2019. https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf. Accessed 29 Apr 2020

Raso F et al (2018) Artificial intelligence & human rights: opportunities & risks. Berkman Klein Center Research Publication, No. 2018-6, 25 Sep 2018. https://doi.org/10.2139/ssrn.3259344. Accessed 29 Apr 2020

Rich M (2016) Machine learning, automated suspicion algorithms, and the fourth amendment. Univ Pa Law Rev 164:871

Rubinstein I (2014) Voter privacy in the age of big data. Wisconsin Law Rev:861

Russell S, Norvig P (2011) Artificial intelligence: a modern approach. 3rd ed. Pearson Education, London
Samoili S et al (2020) AI Watch. Defining artificial intelligence. Towards an operational definition and taxonomy of artificial intelligence. EUR 30117 EN. Publications Office of the European Union, Luxembourg. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC118163/jrc118163_ai_watch_defining_artificial_intelligence_1.pdf. Accessed 29 Apr 2020

Saunders J et al (2016) Predictions put into practice: a quasi-experimental evaluation of Chicago’s predictive policing pilot. J Exp Criminol 12:347

Saurwein F et al (2015) Governance of algorithms: options and limitations. Info 17(6):35

Shepardson D (2018) Trump administration will allow AI to “freely develop” in U.S.: official. Technology News, 10 May 2018. https://www.reuters.com/article/us-usa-artificialintelligence/trump-administration-will-allow-ai-to-freely-develop-in-u-s-official-idUSKBN1IB30F. Accessed 29 Apr 2020

Smuha NA (2019) From a “race to AI” to a “race to AI regulation”: regulatory competition for artificial intelligence. https://doi.org/10.2139/ssrn.3501410. Accessed 29 Apr 2020

Sunstein CR (2017) #Republic. Divided democracy in the age of social media. Princeton University Press, Princeton

Thomas V (2018) Report on artificial intelligence: Part I - the existing regulatory landscape. Howtoregulate.com, 14 May 2018. https://www.howtoregulate.org/artificial_intelligence/. Accessed 29 Apr 2020

Trump D (2019) Executive order on maintaining American leadership in artificial intelligence. 11 Feb 2019. https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/. Accessed 29 Apr 2020

Vinuesa R et al (2020) The role of artificial intelligence in achieving the sustainable development goals. Nat Commun 11:233. https://doi.org/10.1038/s41467-019-14108-y. Accessed 29 Apr 2020

Von der Leyen U (2019) Political Guidelines for the next European Commission 2019-2024, A Union that strives for more: my agenda for Europe. 19 July 2019. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf. Accessed 29 Apr 2020

Wagner B (2018) Ethics as an escape from regulation: from ethics-washing to ethics-shopping? In: Hildebrandt (ed) Being profited: cogitas ergo sum. Amsterdam University Press, Amsterdam, pp. 84–89

World Economic Forum (2017) Impact of the fourth industrial revolution on supply chains. October 2017. http://www3.weforum.org/docs/WEF_Impact_of_the_Fourth_Industrial_Revolution_on_Supply_Chains_.pdf. Accessed 29 Apr 2020

Zarsky TZ (2017) Incompatible: the GDPR in the age of big data. Seton Hall Law Rev 47(4):995