

Perception of privacy and data protection in the context of the development of artificial intelligence

Grzegorz Mazurek & Karolina Małagocka

To cite this article: Grzegorz Mazurek & Karolina Małagocka (2019) Perception of privacy and data protection in the context of the development of artificial intelligence, Journal of Management Analytics, 6:4, 344-364, DOI: [10.1080/23270012.2019.1671243](https://doi.org/10.1080/23270012.2019.1671243)

To link to this article: <https://doi.org/10.1080/23270012.2019.1671243>



Published online: 02 Oct 2019.



Submit your article to this journal [↗](#)



Article views: 4582



View related articles [↗](#)





View Crossmark data [↗](#)



Citing articles: 41 View citing articles [↗](#)

Perception of privacy and data protection in the context of the development of artificial intelligence

Grzegorz Mazurek ^{*} and Karolina Małagocka 

Marketing Department, Kozminski University, Warsaw, Poland

(Received 30 June 2019; accepted 19 September 2019)

Customer privacy perception and the principles of its regulatory protection determine how the tech sector is operating, striking a new balance between economic winners and losers. Nevertheless, not all countries that are leaders in the latest technologies are strongly in favor of flexible and pro-business regulations. This can be clearly seen in the field of artificial intelligence (AI). Self-regulation as a key strategic approach to AI may be seen as an essential factor of broader implementation of AI solutions. The purpose of this paper is to present approaches to AI while indicating the differences that result from the understanding of privacy, increasing customers privacy concerns and regulations related to data privacy which come together with official administrative strategies. The impact of AI implementation on relationships between customers and companies has been emphasized and analyzed in the context of regulations and customer perception of privacy.

Keywords: artificial intelligence; online privacy; data privacy; data protection

Introduction

In the modern economy, data represents a certain monetary value. From growing sets of unstructured, seemingly disconnected data, one can extract information that can not only identify a given person, but also determine their demographic, socio-geographical, behavioral or mental characteristics, learn their shopping preferences, track their daily schedules or habits. Data processing and storage methods are evolving quickly. At the same time, the methods of aggregating and analyzing data, as well as the methods of making business decisions based on this data, are becoming more complex. Meanwhile, artificial intelligence feeds on data, as large sets of information are its main driving force. One may ask whether companies will be able to collect patterns necessary for effective machine learning.

The starting point for perceiving data as a productive factor is the techno-economic paradigm describing a “shift from a technology based primarily on cheap inputs of energy to one predominantly based on cheap inputs of information derived from advances in microelectronics and telecommunications technology” (Castells, 2007). Here, information is a resource, a type of fuel, and it is processed with the use of technologies. Drawing on this paradigm, data may be seen as a currency in the digital world, and even compared to oil, gold or nowadays to labor.

*Corresponding author. Emails: gmazurek@kozminski.edu.pl; www.kozminski.edu.pl

Although the field of AI research dates back to the end of the Second World War, for many decades its progress has failed to keep up with expectations. From the 50's to the 70's, it was assumed that AI would be developed within a few months or years at most (Castro & New, 2016). Nothing like this has happened. Progress has finally accelerated with the development of statistical and probabilistic methods and, what is also very important, the availability of large amounts of data together with increasing capabilities of gathering, processing and analyzing them via enormous computational power (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016).

The free flow of data across borders is crucial to every stage of the AI life cycle, from its development to deployment and use within various services. It is clear that the data used for AI purposes often originates from multiple geographically distant sources, which makes large and easy movement of data across borders more imperative. Regulations which at any point limit cross-border transfers may reduce competitiveness and the pace of development of AI technology. From the existing economics it is known that if the cost of purchasing raw materials required for production increases, in the absence of other regulatory variables, the price of the final product usually increases as well. The situation with AI is no different. Policies, often resulting from the privacy concerns expressed by customers, that artificially increase the costs of acquiring the data used to train systems will ultimately increase the costs of these technologies for customers. Thus the motivation to develop a new technology and use it widely may be potentially reduced with the detriment to the general consumer welfare.

This paper addresses a central research question of how the perception of data privacy and its protection shapes the legal and economic situation for the development of AI. To provide an answer, we start with presenting various concepts in the understanding of privacy and privacy concerns (Section one), which then leads to considerations regarding the perception of data (Section two). The third part of the text is devoted to the analysis of legal regulations and strategies for the development of AI adopted by public administration (Section three). The most extensive part of Section three is the analysis of solutions adopted within the European Union, as they are a benchmark for other regions. The law reflects the mood of consumers in this respect, which spans the continuum from techno optimism to techno defeatism, as described in the following part (Section four). At the same time, we discuss the adverse and beneficial impacts of AI on data protection.

Understanding privacy: from the right to be left alone to the genes of defense against predators

Nowadays, privacy issues are most often linked to the Internet, technological giants, algorithms and the general, growing demand for data. While privacy concepts initially included physical separation from others, there is now more emphasis on the possibility of separating or sharing information about oneself in order to limit the impact that others may have on one's behavior. Privacy has traditionally been recognized as a prerequisite for the use of human rights such as freedom of expression, association and choice. Due to the growing economic interest in personal data in recent years (Bédard, 2016), privacy has become increasingly important in the daily lives of both individuals and businesses. Private information is collected, stored and processed on an unprecedented scale as a result of rapid technological progress. One of the notions is artificial intelligence, for which data is like oxygen and which requires

huge amounts of data to progress, while most of its processes are usually hidden. At the same time, the use of AI technology is now visible in almost every area of life. This raises additional questions about privacy and transparency. The majority of internet users have privacy concerns and feel a strong need to protect their personal data.

Although the concept of privacy is much older than modern technologies, it is still quite young compared to human rights. It was one of the first concepts of privacy that determined its perception in terms of the law, which for a long time has not been, or at least has not become, the subject of separate regulations. Until today, the way of thinking about privacy is dominated by Brandeis and Warren's (1890) definition of privacy as the right to be left alone. In a similar way as back then, today the direct impulse for reflection is the intrusiveness of technology, which in the nineteenth century was about photography and the dynamic development of media. Nevertheless, one should recognize the separation of areas of life – private and public – as a timeless element of this theory. At that time, it was already considered unacceptable to reveal information concerning the private life if it was not connected with the public interest. Nowadays, a similar approach determines the use of data for learning algorithms. The concept then evolved towards human dignity and the ability to control information about the individual. In particular, the extent to which information is made available to others has taken the center stage (Westin, 1967). Control of access to such information should always be considered in a specific social context – which information, to whom, when and in what situation can be provided (Nissenbaum, 2004).

Westin's considerations in the publication called "Privacy and Freedom" refer to a study of animal behavior, which shows that all species exhibit the need for distinctiveness and intimacy in certain periods of time. In the natural sciences, this is known as territorial protection, which consists in the designation of a particular area by a living organism as its own, regardless of whether it is water, earth or air. Access to the territory is protected. In case of its violation, animals are willing to kill even the representatives of their own species. Westin compared these behaviors to the human need for privacy, which he defined as a state of varying intensity depending on the situation. Presenting rather liberal views, he emphasized that while the need to protect information about oneself is a measurable state, there is no need to create regulations imposing a rigid framework for the manifested need for privacy (Moore, 2003; Westin, 1967). Similar references to the behavior of mammals are used by biologist Peter Watts, who considers the need for privacy to be innate and compares the response to spying or watching as a physical threat because it is predators in the natural environment that trace their prey. He stresses that the invigilated person behaves as under threat from a natural enemy, loses confidence, has a strong escape syndrome that prevents normal functioning (Schneier, 2015). With regard to the Internet, we can talk about data manipulation, lack of trust in e-services or the virtual world as such. Transferring this concept to the AI, it means an unwillingness to adopt the offered solutions, the expressed suspicion of intentions of the creators and application.

People who have reason to believe that they may be spied on by companies operating on the Internet or by technology with extraordinary computing power are increasingly concerned about privacy, which can lead to behavioral changes. Assuming that privacy-related behaviors are context sensitive, deciding what data to disclose and what to protect from disclosure seems to be a universal dilemma in societies over time. Decades ago, Altman (1975) postulated that people should manage privacy by pushing boundaries between personal and private sides of their lives. An important

premise, in this case, is the belief that individuals have the knowledge of the circumstances and are able to comply with the rules they set before they take on any action. Navigation in the delimitation seems to be a particularly difficult task in the era of the increasing complexity of activities carried out in a virtual channel. The significant influence of technology on everyday life may cause these instinctive actions to be inadequate. Disclosure of information, like the use of the Internet, has become a permanent feature of social life, and thus most people have learned to accept the requirements associated with it (Zafeiropoulou, Millard, Webber, & O'Hara, 2013). Uncertainty and context dependence means that individuals are unable to make decisions based on their own welfare. Researchers analyzing the decision-making process tend to appreciate non-rational factors over making rational calculations by the clients. The rationale for this view lies in the particular context and situation of disclosure (Barth & De Jong, 2017). Companies can build trust when they prioritize customer security and privacy. Meanwhile, the government is responsible for better enforcement.

Ironically, this modern concept of privacy, as an inherent right to protection, has emerged with the development of new technologies that have threatened to undermine it. At the end of the nineteenth century, it was "instant photography and tabloid gossip". Today it is the Internet. The nineteenth century was dominated by the involvement of individuals versus the state, and the twentieth century saw a new aspect or clash with bureaucracy and companies that massively benefit from the knowledge of the citizen or the client. The twenty-first century brings a new dimension to the relationship between man and algorithm. It is illusory to expect to retain control over information in the Internet. If it has been placed once in a virtual environment, it will remain there, regardless of whether its original owner has withdrawn or remained in the network. The digital mark left by customers, i.e. information about themselves, can be collected, processed and stored not only by many institutions, but also for a long time. In his works and speeches, Kosiński (2015), a social psychologist associated with Stanford University, announces the end of privacy, the cause of which he sees in the number of digital data left by Internet users every day.

The sense of honesty and justice in the long-term exchange of information resulting from the theory of social contract has been disturbed. Clients do not feel safe, because they communicate information not only through intentional filling out of forms, but also by being followed and observed, and their behavior seems to be subject to continuous analysis. Growing privacy concerns have resulted in an outflow of trust. The term privacy refers to concerns about the possible loss of privacy as a result of self-disclosure (Xu, Dinev, Smith, & Hart, 2008). Information privacy concerns, a subset of the overall concept of privacy (Bélanger & Crossler, 2011), refer to the ability of individuals to personally control information about themselves. People do not exactly know whether and to what degree they should be concerned about privacy (Acquisti, Brandimarte, & Loewenstein, 2015), mainly because their everyday lives now include countless daily compromises between the needs and facilities of the Internet and the development of algorithms and the private details they need to disclose in order to access it. Increasingly sophisticated aggregation of information – often without people's consent or even knowledge – causes more and more privacy concerns. They evolve from their main focus, which was data control, to the purely biological needs of protection against continuous

surveillance seen as a threat equated with that which our brains associate with the activities of predators.

With the emergence of advanced data exploration opportunities, privacy has become an important social topic. Identifying, profiling and directly influencing people's lives without their consent has become extremely low-cost and easy. With the appearance of increasingly sophisticated artificial intelligence systems, these privacy concerns have only increased. In this context, AI means an increased ability to collect, analyze and combine vast amounts of data from different sources, thus enhancing the capabilities of technology owners. Finally, Artificial Intelligence can perform designated tasks without supervision, which greatly improves analysis performance. These features of artificial intelligence enable it to influence privacy in various ways. AI can use advanced machine learning algorithms to deduce or predict confidential information from non-sensitive data forms. For example, someone's typing patterns on the keyboard can be used to deduce their emotional states, such as nervousness, self-confidence, sadness and anxiety. Even more worrying are the possibilities to analyze political views, sexual orientation and even general health based on data such as activity logbooks, location data and similar data.

The level of privacy concerns is quickly increasing. The topic itself is a constant subject of academic research in various aspects, as well as reports and analyses conducted by state institutions and companies. In the Microsoft survey, concerning the impact of technology on everyday life, privacy concerns have been identified as persistent and widespread. The majority of respondents argued that current protection is insufficient and that the rights of Internet users should be subjected to local regulations of the country of residence of the particular users. The highest percentage of respondents who considered the current level of privacy protection to be insufficient was in Japan (80%), followed by Germany (76%), with 68% US citizens agreeing with this statement. Similar trends are also observed in China, which traditionally is associated with a low level of privacy concerns, however, a high acceptance of the compromises resulting from a large amount of data available to companies and the state. Meanwhile, a survey of 8000 respondents conducted by China Central Television (CCTV) and Tencent Research as part of CCTV's China Economic Life Survey (2019) indicates that 3 in 4 Chinese people are concerned about privacy, which challenges the perception of the Chinese not caring about their data. At the same time, the survey indicates that nearly 77% think of certain forms of AI as a threat to their privacy, even though they believe that AI holds much development potential and will permeate different industries.

Data as oil, as gold, as labor – data as a central asset for AI

Data has become one of the most important factors of growth in all sectors of the economy, however, the inherent value of each piece of data is rather small. It is only when there is a real possibility to use data as an input to other value-added services, such as improvement of customer management or experience processes, assessment of market purchasing power or AI, understood as a field of computer science that performs operations similar to human learning and decision-making processes. A well-known saying that money is today's king should rather state that data is today's king. Majority of companies around the world nowadays have to deal with a huge amount of data collected from a huge number of sources: websites, blogs, social

media accounts and others. The data is also obtained from third parties. As mentioned above, the acquisition and processing of data is the subject of growing privacy concerns. Simultaneously with technological development, different concepts of data perception appear, shaping thinking about algorithms that process them. Data collection, analysis and processing are mainly perceived as a threat to privacy. This regularity brings the considerations about data and their relationship with privacy closer to AI, especially if it is taken into account that that AI systems are trained by ingesting enormous volumes of data. They are implicitly very dependent not only on quantity but also on the quality of the data that is available for training.

The starting point for perceiving data as a productive factor is the techno-economic paradigm describing a “shift from technology-based primarily on cheap inputs of energy to one predominantly based on cheap inputs of information derived from advances in microelectronics and telecommunications technology” (Castells, 2007, p. 10). Here, data is a resource, a type of fuel, and it is processed with the use of technologies. Drawing on this paradigm, information is seen as a currency in the digital world, and even increasingly often compared with oil, while analytic tools are likened to the role that the steam engine once fulfilled in human development. The authorship of oil metaphor is attributed to Clive Humby, the British mathematician who established the Tesco’s Clubcard loyalty program. It referred to the value resulting from the very nature of the resource, and the need to process it before producing the final product. The comparison has long been criticized due to differences in the availability of resources, the possibility of repeated use of data as opposed to oil, as well as various costs of their exploitation. It is true, however, that a parallel can be created considering how data is used to power technology that has significant potential to change the world. In the context of technological development and artificial intelligence, perhaps the biggest difference is the exhaustiveness of the resource. While oil deposits are decreasing with their exploration, data is increasing. They are even renewable and replicable, i.e. from the analysis of one data set, it is possible to obtain more. The data as oil metaphor was established in 2006, a bit later is the reference to gold, which appeared around 2012. Both combine data with the possibility of earning huge money and treat data as natural resources, which despite being extracted from the common space belong to only a few (Dean, 2016). At this point, reference is made to technological giants and their profits from data-driven economics. Ultimately, the leaders in the acquisition and processing of data, such as Facebook or Google, will completely close the access to the data collected from the outside world. In conclusion, the data can be used for generating value. At the same time, due to changes in the perception of privacy and cases such as the use of Facebook’s mechanisms by Cambridge Analytica to manipulate public opinion during the presidential election in the US or voting on Brexit, exclusivity in their possession is sanctioned. Changes in the law have already strengthened the role of first parties while limiting the possibilities of obtaining data or the value resulting from their analysis for other entities. If we refer to a situation in which AI needs the largest possible data resources to improve performance, then it may mean that wealth created from all resources will actually be concentrated in the hands of a few.

Data comes from the community, as if from everyone, but it is not perfectly comparable to natural resources such as gold. However, it is often referred to as money. Data can be paid for services that are not payable in other ways, such as e-mail accounts or social media. Researchers have called such a barter as the creation of

free online culture, where data is a currency, although it is not always noticed by users (Lanier, 2013). When using free services, customers often treat the possibility of profiting from private information as a way of recycling by-products. They underestimate their role in generating value in a data-driven economy (Arrieta-Ibarra, Goff, Jiménez-Hernández, Lanier, & Glen Weyl, 2018). Data is being treated as free land for tech companies to discover and sweep up from our online footprints. This leaves users, in the absence of any bargaining power, destitute of a way to meaningfully negotiate overpayments for their data and completely unprotected from the invasion to their privacy. This way, the majority is being denied a share in the economic value of the production our data empowers (Posner & Weyl, 2018). Thinking of data as labor rather than capital may increase the productivity gains from the AI revolution simply because of the respectability and meaning that comes from labor. What is more, workers respond to incentives to work harder and produce higher quality goods and services. This perception can be particularly justified in a situation where data is collected from people who are increasingly worried about their privacy.

The free flow of data across borders is crucial to every stage of the AI life cycle, from its development to deployment and use within the services that sustain global commerce, health care, financial systems and the technologies of the future, just to mention a few. It is clear that the data used for AI purposes often originates from multiple geographically distant sources, which makes large and easy data movements across borders more imperative. Regulations which may at any point limit cross-border transfers may reduce the insights and other benefits from AI technology. From the existing economics it is known that if the cost of purchasing raw materials required for production increases, in the absence of other regulatory variables, the price of the final product usually increases as well. The situation with AI is no different: policies that artificially increase the costs of acquiring the data used to train systems will ultimately increase the costs of these technologies. Thus the motivation to develop new technology and use it widely should be balanced with the general consumer welfare. Observable trends in the world strive to maintain equilibrium between the need to secure customer privacy, reduce concerns about consumer privacy and the needs of the market driven by the possibilities offered by AI.

Different approaches to regulating online privacy and data protection combined with their impact on the development of AI

AI tools are used widely by both private and public sectors around the world. Governments have expressed a commitment to AI's continued development. However, policy-makers and human rights watchdogs emphasize existing tensions between data privacy, data protection and implementing AI technology. A need is expressed for a more nuanced, detailed understanding of the opportunities and the issues presented by AI and of practical ways of addressing these challenges, in terms of both legal compliance and ethical issues that AI raises. Many scholars and market analytics highlight an obligation to develop principles, best practices and other accountability tools to encourage responsible data management practices and respect data protection in the future development of these innovative technologies. We focused primarily on UE regulations, as they seem to be the most intrusive with regard to the AI field, while serving as an example for other regions. Clarifying the application of existing data protection law on AI will be essential to ensuring that limited resources are not wasted on

protecting data that does not impact individuals' privacy rights or otherwise create a risk of harm.

European Union – law against the machine

General Data Protection Regulation (GDPR), the new European Union data protection legislation, came into force on 25th May 2018. The GDPR applies to EU and non-EU organizations that use or process personal data about people living in the EU. The place the data is processed is irrelevant. It is a legislative response to the changing realities where individuals may function both as citizens and customers. The regulations are adapted to changes in the scope of technologies and groups of information used to trade in the virtual channel, as well as taking into account the cross-border nature of collecting, processing and using databases. Providing of a single digital market within Europe is a central matter to the concept. The main task is to strengthen the rights of individuals, allowing them to express their informed consent to disclose private information to companies, with the option of withdrawing it.

The common digital market and the positioning of the individual in the center seem to be important from the economic and social development perspectives. The regulation aims to increase trust in digital services and standardize the flow of money. It is worth emphasizing that the regulations came at the time when companies around the world aggressively competed for the development and use of artificial intelligence, seen as a technological capability of computers to perform tasks in a manner similar to human, but with much more precision and speed resulting from their computing power.

The GDPR regulates the rules of personal data processing applicable to everyone living within the European Economic Area, which includes the EU countries, as well as Switzerland and Norway. The regulations apply to residents and there is no dependence on the place where the data is collected, processed or analyzed. What is important, the new regulation takes into consideration only personal data, which means that an essential part of the AI system does not necessarily have to be affected. However, as already mentioned before, these systems are trained using large datasets. In addition, such services as automated query handling, recommendations (appropriate for the Amazon or Netflix business model, for example), streaming, automatic responses (chat bots) will certainly be subject to restrictions if they include in any way the data of residents of the European Economic Area. It is worth underlining that the regulation came into force at a time when companies and countries realized that the technology sector is the area of intense competition. Economic development is to be driven by computers that performs tasks in a manner similar to human but faster and in a more precise way. There is less and less talk of replacing people, but more and more about improving decision-making processes and executive methods through human-machine relations.

Opinion-makers, experts and at least some scholars believe that the GDPR will have a negative impact on the development and use of AI in Europe, putting EU companies at a competitive disadvantage compared to their competitors from other parts of the globe (Wallace & Castro, 2018). The sources of expressed concerns can be found in several articles of the new regulation. The purpose of this paper and the discussion is not a detailed analysis of all articles, which is the reason why the main focus is placed on those with the wider and significant impact on AI. This includes article 22 about the

requirement to manually confirm decisions based on algorithms. Experts agree that this will increase AI's total costs, among others, because companies will need to have employees responsible for reviewing algorithms. The reason for concern is not only labor costs, but also limitation of this technology in its obvious advantages such as speed, efficiency (cost and production) as well as ease of use. Article 17 in turn provides the right to repair the potential damage that AI systems may cause. As already mentioned, the essence of this technology is machine learning and self-improvement of algorithms. The assumption is that no external intervention should be needed or desirable, and the only requirement is data for learning. At the same time, the technology works in such a way that it remembers the data which formed the basis of the training and on this basis builds the rules that it uses later. There is no possibility of removing any particular data at the moment when the customer wants to be forgotten or reports the necessity to remove his records. It is like starting from a complicated multi-level construction, to take one brick out of the foundations. One can imagine that regardless of the finesse of the building, it will collapse anyway. At the beginning of the article, the differences between data and oil were described. One of them is the possibility of using the same data multiple times for different purposes. Meanwhile, Article 6 requires the use of data only for the purpose for which they were collected, which may limit the ability of companies to develop or use AI to experiment with new functions (Press Club Brussels, 2018).

Only a few examples of regulatory provisions are discussed above and GDPR itself is very complex and difficult to follow. Each and every company using AI (developing technology or applying its in business) will need specialized personnel to make sure they comply with regulation, which obviously raises costs, but also does not encourage investment in this area (Siegele, 2018). There is also a growing body of evidence that a large amount of small and medium companies have problems with understanding and applying the regulation. Thus they may be resistant to take advantage of AI when facing the risk of finding themselves the unwitting targets of legal action (Meulen, 2017). It is worth to note here that in the opinion of many lawyers, this is one of the few regulations with such imprecise provisions and such high penalties. Fines the GDPR imposes, up to 4% of a company global turnover (in disputes, this will always be a mother company in order to avoid setting up small marketing companies) or €20 million, constitute a strong element that is terrifying and explicitly pointing to the policy maker's determination to penalize behaviors that affect the sphere of data privacy. At the same time GDPR provides relatively little clarification to certain articles; it contains, among others, one on how to define *meaningful information about the logic involved*, which may be understood as a way a particular algorithm generally makes a decision or as a precise explanation on how it arrived at the particular conclusions. This leaves companies, especially the ones that plan to develop innovations extensively, in highly uncertain circumstances.

However, GDPR is not the only regulation in EU. Shortly before the new regulation's coming into force, on 10th of April 2018, 25 European countries (24 EU countries and Norway) signed the Declaration of Cooperation in the sphere of Artificial Intelligence. They declared to engage in building a European approach to key issues and development challenges, which included increasing technological and industrial capacity, modernizing education and training in view of changes in the labor market and providing an ethical and legal framework based on core values (Digital Single Market, 2019). The declaration was the basis for an official EC

Communication, issued less than a month later, which assumes the use of the European Fund for Strategic Investments in order to raise the region's competitiveness and attract the private sector's investment.

Nevertheless, it is worth emphasizing that the Commission clearly indicated it will follow the development and use of technology-based on automated processing of personal data (in which the so-called profiling is included). Individuals whose data is processed have the right to obtain information on the logic of making decisions. This is a clear reference to the Regulation of articles 13–15 of GDPR, which impose on companies an obligation to inform about the exact course of decision making by algorithms (Goodman & Flaxman, 2016). This is yet another signal, following the GDPR record, for the potential wide use of technology, because AI algorithms learn specific behaviors using mechanisms that are not entirely transparent to humans. At the moment, the discussion often concentrates on explanation how intra-machine learning is initiated and what exactly starts the whole process. The road to make it fully understandable for people appears to be long. Notwithstanding, the creators of this technology may be forced by regulators from the European Union to reproduce any AI decision path or to achieve an identical effect by another method. For now, programmers do not offer a clear and unambiguous answer whether it is feasible at all. From the technical side, there are studies going in this direction, but most of them lead to the conclusion that the need for transparent decision-making algorithms at the same time will limit the freedom of their development (Microsoft, 2017).

Another important element for using AI on a large scale is the access to large amounts of data. In order to develop AI, it is necessary to use large amounts of data that are processed and form the basis for learning algorithms. The types of data vary depending on the application of a particular artificial intelligence. It may therefore be such data as images that may or may not contain information about specific people, which is difficult to control fully. It must be assumed that there is a strong need for both access and data protection. The regulation of personal data protection raises concerns that the development of AI will be limited or slowed down. To this end, the Commission intends to take a number of initiatives to increase the availability of data in the EU. This is a particularly important issue for small and medium-sized enterprises and entities that are starting their business operations. According to the European Commission, in 2016 the European data-based economy was worth EUR 300 billion. This value is expected to increase to over EUR 700 billion by 2020, which will constitute 4% of European GDP (Digital Single Market, 2019).

Another approach reflects the position of the UK. Year 2016 seems to be the very year when a number of official statements in the area of AI and technology was taken into account. It was then that both the United States and the European Union prepared and published their reports. However, a separate position was taken by the UK, which is related to the Brexit procedure. A report released by the House of Commons' Science and Technology Committee expressed an alarming tone when it came to the development of new technology and its impact on economy and society, not different from other parts of the world, while emphasizing the significant role of the research and academia. Apart from the EU, the need for a minimum regulation of areas directly related to AI was highlighted. The lack of legal barriers was mentioned as London's main chance to remain the leading center of development of AI-sector in Europe. The risk of losing research funding from the common funds of the European Union was underlined as one of Brexit's disadvantages. In spite of

considerable confusion in companies such as DeepMind that have their headquarters in the capital, it was positioned well enough to use little resources to maintain a competitive advantage based on domestic resources ([5th Report on Robotics and Artificial Intelligence](#)).

It will not come as any surprise that the private sector is interested in acquiring as much information about their customers as possible. It is also not so difficult to understand that the state and inter-governmental intuitions meant to protect an individual's right to manage their own personal data impose straight rules on companies seeking to profit by using them (Drezner, 2007). Nevertheless, analyzing the various manifestations of activities undertaken in Europe, it is worth asking why the regulations on privacy protection with serious fines came into effect when investments in the area of AI were planned and the governments of various countries expressed a significant interest in the development of AI systems. Scholars have long characterized the EU lobbying system as the elite pluralism, where especially in Brussels many different business interests groups have an advantage over citizens (Berkhout et al., 2015; Berkhout & Lowery, 2008; Broscheid & Coen, 2007; Mazey & Richardson, 1997; Wonka, Baumgartner, Mahoney, & Berkhout, 2010). Of course there was an extensive pressure around GDPR consultations, however, examination of the dataset consists of lobbying positions taken by nearly 280 individual interest groups over years 2009–2011 reveals surprising key findings (Atikcan & Chalmers, 2016). A clear evidence linking IT companies to either support or opposition was not found. Only anecdotal and media stories linking tech companies and their disapproval for new regulations were published. Newspapers and magazines were full of articles kept in an alarming tone. Jan Philipp Albrecht commented these publications for ePrivacy Regulation portal: *It's the death of the press, it's the death of all apps and free services online, it will be shutting down the internet, it is the end of the telcos, we will lose everything. This is really very radical lobbying with regard to the tone, and in my view it is completely over-exaggerated* (Inside the e-Privacy, 2017). Despite the tone, there were some hints that big players, like Google or Facebook, have been publicly quite discreet on the subject, but there were other organizations, especially involved in online advertising, that were really acting in the interests of those companies. The amount of suspicions and rumors that have arisen around the topic forced organizations like the Computer & Communications Industry Association (CCIA) to formulate official statements about their lack or very little engagement in privacy topics in Europe. One may ask at this point who was the biggest opponent at that time. As evidenced by recent studies, the financial and retail industry were the most involved, due to the fact they host a vast amounts of sensitive information; they are also at risk of cyber attacks and data breaches (both penalized and requiring special, expensive actions). Both sectors are also the ones who may be the most interested in AI systems (Long, 2014).

US – letting a thousand flowers bloom

After an extensive description of the situation in Europe, it is now time to discuss the U.S. approach. It has been shaped by a long tradition of self-regulation and small government interventionism. This is fundamentally different from the European view, which, due to the nature of the interstate agreements and the need to reconcile different interests, is often in a situation of a significant degree of regulation. The American view at AI is well characterized by one word, which is innovation. The White House

Office of Science and Technology Policy (OSTP) defined AI as one of the major factors of economic growth, good for society, as it addresses social issues. It is not a big surprise that the US government's vision of its own role is very limited (OSTP, 2016). Self-regulatory partnership may be seen as a staple of the US approach to AI.

Obama's administration saw the important role of research, which has not been changed by their successors. The pivotal objective was not only to develop technology, but also monitor on-going works, focus its efforts on ensuring accountability and transparency of AI. The key role of the private sector in the development of AI in the US, especially technological giants with global reach, means that the federal government does not have to focus on stimulating the domestic market or commercializing technologies being developed. Instead, the goal of public administration is to ensure optimal development and expansion opportunities for technology companies, through financing basic research, the lack of strict regulations and adapting the education system to the market needs.

The second administration of Barack Obama (2013–2016) definitely had the most active policy towards AI. It launched a number of initiatives, created dedicated working groups and published reports that were the beginning of the debate on the role of the state in the stimulation and regulation of AI. The key narrative of the presidential administration was that the free market was the best stimulant and promoted technological innovation, and any regulation or interference could only disturb and limit the potential of the American AI sector. The government was promoting an approach to the lack of new regulations that could delay the emergence of new AI applications (Swanson, 2017).

Current administration (President Donald Trump) recognizes blocking of buyouts of US technology companies by entities from other countries, especially from China, as a pivotal obligation. AI and autonomous systems, for the first time in history, were included on the official list of priorities of the federal budget (as part of the expenses proposed by the President Donald Trump for 2019). At the same time, the main axis of the narrative and undertaken initiatives assumes organically a minimum of regulatory and standardization activity of the state, underlining the key role of the free market and the private sector (Presidential Executive Order, 2017).

Explanation for a different approach in the U.S. can also be seen in a special market circumstances. The US is the country of origin for the key technology companies shaping the global AI environment such as Alphabet (Google), Apple, Amazon, IBM, Microsoft, Nvidia, as well as the largest startup ecosystem. According to the latest research from 2018, there are 1393 startups in the US, which is 40% of the entire global market of startups developed artificially. For comparison's sake, the second country in the ranking – China – can boast only 383 young companies from this sector, and the third – Israel – 362 companies (Berger, 2018). American technology companies are also a source of many groundbreaking research in the field of artificial intelligence. Microsoft and Google are currently the most active companies, while IBM in turn dominated the US patent market in terms of the number of registered AI solutions (MIT, 2017). Provided examples may serve as a proof of the advantage of America on many fronts. If we add the domination of American companies in social media and streaming services connected with the power of culture, the European policy makers may find themselves in very precarious situations when it comes to protect their citizens' rights.

Today there is no clear evidence regarding factors having the greatest impact on the development of AI in the US. Certainly favorable market conditions, business culture and large research centers were important. However, we should remember that AI learns on large amounts of data. This is why societies with huge populations have the biggest chances in this race. Access to data is not just a technical problem; it is also a policy issue. People who use smartphones, social media, wearable devices as well as connected cars in their daily routines leave more and more digital footprints. In pro-AI market and legislative conditions, where data can be processed into patterns and algorithms, there will be a really strong push to develop and implement new technology into business and national security, as indicated by the example of the US in contrary to the EU.

China – Cherry and technology-blooming country

China, has virtually unlimited amounts of data, which have recently become a decisive factor in developing powerful AIs. China currently generates 13% of all digital data in the world, and it should be around 20–25% by 2020 (Report of the Artificial Intelligence, 2018, p. 9, 39). The country is rapidly building up its cloud-computing capacity. In the sheer volume of research on AI, Chinese academics surpass their American peers, for example AI-related patent submissions in China almost tripled between 2010 and 2014 compared with the previous five years. Chinese startups are attracting billions in venture capital. Above all, China has over 700 m smartphone users, more than any other country in the world. They are consuming digital services, using voice assistants, paying for stuff with a wave of their phones while generating vast quantities of data. That gives local businesses such as Alibaba, Baidu and Tencent the opportunity to concoct best-in-class AI systems for everything from facial recognition to messaging bots. The government in Beijing is convinced of their potential.

The AI strategy adopted by the China State Council in July 2017 does not create anything from scratch. Its goal is to accelerate activities already undertaken by the private sector. The Chinese market today is dominated by three players: Baidu, Alibaba and Tencent (referred to as “BAT”). Each has a strong technological base and its own AI research centers and invests in startups dealing with artificial intelligence. The scale of their operation and the resulting data play a significant role in the current and future successes of these companies in the area of AI. Alibaba is the largest online shopping platform. During the 2017 Chinese Singles’ Day, which is celebrated on November 11, Alibaba sold goods for a total of \$25 billion. For comparison, the U.S. Cyber Monday, which falls on 27 November, brought only \$6.59 billion to all sellers in 2017. Huge sales mean a huge amount of data which Alibaba uses, e.g. for developing machine learning to personalize the purchase offers. Alibaba has its own cloud resources which it sells externally, thus competing with Amazon. Baidu, the Chinese counterpart of Google, has been exploring the potential of AI since 2014. The company is a leader in voice recognition and autonomous car research. When Microsoft created a system able to recognize voices with better efficiency than a human in 2016, hardly anyone knew that Baidu had already done it a year earlier.

An AI boom in the world’s most populous place enabled wide possibilities as no other country could generate such a volume of data to enable machines to learn patterns indicative of rare diseases, just to mention a one example. The development of new technologies ought to happen more rapidly just because typing Chinese

characters is awkward, voice-recognition services are more popular than in the West which may result in their faster improvement. Systems to adjust traffic lights automatically in response to footage from roadside cameras are already being tested. According to the McKinsey Global Institute (2018), a research arm of the consultancy, AI-driven automation could boost China's GDP growth by more than a percentage point annually.

The AI is also a new mechanism to drive economic growth in China. It can support many areas of the economy, such as manufacturing, distribution and consumption. Thus, investments in this area can enable China's economy to grow faster. However, it is problematical to discuss the usage of consumer consent in the context as in China, decisions on obtaining data, as well as their use, are made at the central level without the voice of individuals. AI should also have a positive impact on China's social development. The State Council sees potential in such areas as education, health care, environmental protection, urban development or access to state and judicial administration. Therefore, the AI that China is betting on should also improve the quality of citizens' lives. Yet the country's AI plans also give cause for concern. One worry is that the benefits of Chinese breakthroughs will be muted by data protectionism. A cyber-security law that came into force in June requires foreign firms to store data they collect on Chinese customers within the country's borders; outsiders cannot use Chinese data to offer services to third parties. Worth to underline that if data cannot be pooled, the algorithms that run autonomous cars and other products may not be the most efficient.

The role of technology is under attack with customers questioning the abuse of their private data

In just the last year investment in AI exploded: rising from 25% to nearly 70% of early adopters according to the Constellation 2018 AI Study (Sato & Wang, 2018). Data collection, aggregation and increasing analytical capabilities together with AI development are infamously providing corporations and governments with the means to know us "better than we know ourselves." From medicine and mobility to marketing and finances, significant progress has been made in using AI methods. The application of AI is progressively expanding from the commercial and service industries to the manufacturing and agricultural fields, which make the general technology and basic technical features of AI more prominent and spread (Doshi-Velez & Kim, 2017; Kaplan & Haenlein, 2019; Russell & Norvig, 2016). Larger companies and industries that adopted digital technologies in the past are more likely to adapt AI. For them, AI is the next wave of digitization. This implies that, at least in the near future, AI deployment is likely to accelerate at the digital frontier.

AI is being implemented and received with enthusiasm in many areas, starting with areas such as healthcare, transportation, the environment, criminal justice, and economic inclusion. Recent examples of a smart car, smart city and autonomous drone applications are very much welcomed. At the same time, the methodology of algorithms remains in the shadows, often undisclosed. AI enthusiasts and its widest possible application seem to underestimate its value as the next step towards digitization beyond the potential harmfulness caused, for example, by subjectivity biases. Obtaining full knowledge of how the AI works is a challenge in terms of competitiveness in this area as well as the "black box" of what we are dealing with. While most basic

research on artificial intelligence is now carried out by scientists and commercial laboratories that work together to announce and publish their findings, it is likely to change in the near future. Increasing commercial applications resulting from the passion for technology and its implementation almost everywhere possible may result in increased competition, especially among commercial entities. It will then become impossible to track progress in the development of AI. Thus, the same negative scenario assumes increased use of private data to develop and improve algorithms, as well as the temptation to use potentially harmful but profitable solutions.

At this point, the market implementation of AI can be metaphorically compared to the high popularity and versatility of asbestos, which, as in the case of AI, was directly related to the unique properties of this mineral and its availability and decreasing costs. The use of asbestos in the industry has been accompanied by great optimism, even euphoria, and the belief that it is the best material in the history of mankind, which reminds us of today's enthusiastic, mostly in terms of artificial intelligence. There are more than 3000 described technologies using asbestos, which harmonizes with a wide range of applications of AI in almost every area of life presented in the publications. The range of applications for asbestos was also very diverse, ranging from traditional insulation products to building materials, textiles and filtration. The confirmed harmful and carcinogenic effects of asbestos on human health as a consequence of exposure to prolonged inhalation have been proven during its highest industrial use (1975–1985) and have led to the gradual introduction by individual countries of relevant legislation and restrictions on its use (Virta, 2006). The question may, therefore, be asked whether, with relatively little knowledge of the potentially harmful effects of algorithms, although publications highlighting the risk of biases and discrimination are already described today, humanity will not repeat the mistake made with asbestos being implemented with power and then removed on the mass scale.

However, if one looks at the issue of AI privacy concerns and the introduction of legal restrictions, the process seems to repeat itself even geographically. In response to confirmed reports of the harmfulness of asbestos fibers to human health, numerous pieces of legislation have emerged which, since the 1970s, have gradually started to regulate the issues related to this material. From the outset, a great deal of activity in regulating the handling of asbestos has been observed in Europe. The European Economic Community in 1983 regulated the marketing, use and labeling of products containing asbestos. Subsequent restrictions led to a final ban on the use of asbestos throughout the European Union, in force since 2005. Excluding the European Union, asbestos legislation varies greatly from one country to another. It is understandable that developed countries have a higher level of awareness of the harmful effects of asbestos on human health, although this is not always reflected in restrictive legislation. However, in many regions of the world where the population is large and there is equally high demand for cheap and effective solutions, for example in China, India, Russia and Brazil, asbestos is still being used. A geographical comparison with the implemented legal restrictions on data protection, which also started in Europe and functions here in its most restrictive form, is rather illustrative, whereas areas with a significant population are less regulated, such as China. In addition, the extraordinary properties of asbestos also make it impossible to eliminate this mineral completely, despite the prohibitions and restrictions in force. A futuristic diagnosis can be

made that the most likely once AI tools have been used, it would also be difficult to eliminate them completely, as their practical value is considerable.

According to the statement used by E. O. Wilson, the father of sociobiology, “The real problem of humanity is that we’ve got palaeolithic emotions, medieval institutions, and god-like technology”. Through the development of artificial intelligence, it has been possible to create solutions with so much power that it can manipulate the behavior of 2 billion people, so it seems crucial to have the certainty that it works in our interest. A comparison to asbestos, the enthusiasm that accompanied the wide use of the mineral and its harmful consequences can only be metaphorical if the transparency of AI processes can be implemented and the ethical codes find practical and not only theoretical application.

Consideration of the impact on people’s lives, the perception of privacy, the use of data of ourselves to influence behavior and decisions beyond many different directions can also be divided into techno-optimists and techno-defeatists. Many techno-optimists believe in the coming of a technological peculiarity, followed by good and powerful artificial intelligence to serve societies in their well-understood interests. A special form of technological optimism is solutionism described in Evgeny Morozov’s works (2013). He defines this phenomenon as a belief that in order to solve all human problems, appropriate tools and sufficient computational power would be enough. It is a fascination with simple solutions to extremely complicated problems. Umberto Eco’s maxim can be considered the shortest summary of solutionism: “Every complicated problem has a simple solution and it is wrong”. Today, however, many AI enthusiasts do not seem to notice that the solutions proposed by technology for almost every need, from diagnosing diseases through voice commands to devices, without mentioning the coming era of General Artificial Intelligence, carry a whole spectrum of threats and potential abuses, especially since most of the technology remains completely incomprehensible.

At the same time, there is a group of technological defeatists who emphasize the negligible influence of man on technology and especially on the possibility of predicting its wide usage. They highlight that history teaches us cases when at least one more technological progress has been unstoppable and not heading in the right direction. Ronald Wright in his book “A short history of progress” popularized the term “a development trap” (2004). It means a situation when society chasing progress creates new problems that it cannot solve because it lacks resources or political will. An example of a development trap is the use of fossil fuels such as oil and coal. For a long time, we have been benefiting from this, yet at some point the border was crossed and a process of global warming began, which could lead to the collapse of the entire human civilization. According to the opinion of techno defeatists, the only way to respond to new technology is to change the law and adapt to society.

Those are just a few of the complaints leveled against technology. For most of human history, however, technology was mostly seen as a force for good. More people would live because of technical progress, from refrigeration to vaccination. Today a “tech-lash” is underway. The atmosphere around new technologies has changed. Information about ethically questionable business practices, data leaks and social and economic side effects caused the tech industry to lose its innocence and unambiguously positive image in the public opinion. The “Global Risk 2017 Report” indicates that artificial intelligence is one of those technologies that require precise legislative regulations. Experts point out in the document that a very high

risk for humanity is the fact that software and machines operating due to artificial intelligence will, perhaps soon, have greater intellectual potential than we as humanity. For years, however, specialists, scientists and business people have been arguing about the direction and effects of such an intensive and dynamic development of AI in the present time. Stephen Hawking, professor of physics and one of the most prominent minds of modern times, warned against the uncontrolled development of artificial intelligence. According to him, the emergence of the first independent artificial intelligence may be the first step towards the extinction of the human species, because when AI obtains a certain kind of self-awareness and becomes decisional, mankind will never be able to predict the effects of its actions. A further worry is that such technologies might operate outside the transparency and accountability.

AI is also a threat directly related to having large data sets. Yuval Harari, who sees the danger in this area in machine learning systems. Powered by huge data sets, accessible only to selected entities, they use vague procedures to detect unexplained patterns, which are then used as assumptions for autonomous decision-making systems. At the same time, the world has already been divided into technological giants from both the US and China, who have an overwhelming amount of information about the preferences, intentions and actions of customers and the rest of the world, which for them is a passive recipient of the technology they use. At the same time, all the rest feeds their systems with data without having any influence on how they are used. Harari sees a possible way out into regulation of data ownership while emphasizing repeatedly that this is the most important political and social issue. It is one of the most powerful voices calling for a discussion about what people should really expect from artificial intelligence data analysis, alongside ethical-legal theorists related to AI. When it comes to short-term regulatory and political activity, the focus on all direct governance, security and privacy issues remains crucial.

Conclusion

Digital technologies such as AI have made substantial contributions to many areas of our life. The vast quantities of information that we are able to gather and analyse through the use of these tools allow us to tackle social ills that previously had no solutions. Unfortunately, the same technologies can also be used against its users and community as such by various social actors, from individuals to corporations, to government agencies. Loss of privacy is just one example of how technologies such as AI can work to our detriment. However, if we manage to properly understand these technologies and their impact on our daily life, we will acquire the means to defend ourselves from exploitation by those that wield them with malicious intent.

The collection, usage and processing of personal data is big business nowadays and a significant stimulus of growth. The fit among big data, artificial intelligence and data privacy standards is complex and one in which a dynamic balance must be maintained in order for new digital business models at the intersection of these emerging norms to ward off regulatory and consumer backlash. At some point ongoing changes in regulations can be seen as a manifestation of consideration of the privacy as a fundamental human right to be protected by the state. However, as communities increase their scrutiny over profits extracted from personal data to be transparent about their business models, the noticeable demand expanded to offer consumers a fair and transparent trade for data about them, and to innovate in privacy. Nevertheless, adoption of a

tight jacket of EU rules, in many places from Old Continent to populated China, will impose a high regulatory tax not only on European private sector but also on companies around the world.

The legal framework may allow for the implementation of new solutions, but it will also limit or even inhibit them. Their role should be to find a balance in a changing society, but also to protect participants of the fast-changing world, including people, and in the future maybe also self-conscious machines. Countries that are leaders in the newest technologies are strongly in favor of flexible and pro-business regulations. In regions with a restrictive legal regime, it may be possible to create geographically separated areas (similar to special economic zones) where other legal standards apply.

On the other hand, while self-regulation is a key-strategic approach to AI, there is a need of bolder strategy, which would empower the government role in reacting to the full spectrum of challenges (ethical, privacy-related and more), which AI brings to society. Is there no contradiction in the pursuit of success in the field of AI while perceiving this goal through the prism of ethical principles? Antoine Petit, head of the CNRS (French National Center for Scientific Research), at the #AIForHumanity conference commented: “Let us not be specialists in ethics, while the Chinese and Americans become specialists in the business. Let’s not pretend that there are equal ethical chances on the global level!” (Oury, 2018). As the ethical matters should not be given lower priorities in thinking about AI, it is the contradiction of intentions to participate in the competition for artificial intelligence, and at the same time putting into force such regulations as the GDPR, which creates a barrier that prevents keeping pace with the biggest giants in the field of technology industry.

To conclude it should not be forgotten that artificial intelligence relies heavily on the collection of huge data sets; this is one of the main factors that allowed market leaders from the US and China to get ahead. It is practically impossible to remain a world leader in the digital industry without a large and homogeneous customer base. In this respect, individual European countries are too small and the market is too fragmented. Therefore, AI systems may not die because of too little data, but they certainly will not develop as quickly as their competitors in places where data are abundant. Also, one of the significant development factors is always a practical application in business. As we have begun teaching machines how to understand humans, AI involvement is growing rapidly. All this is possible as a result of the growing appreciation of data. Access to the right data in massive amounts is a necessary but not sufficient condition. Publicly available algorithms, smart content creation, voice search, programmatic media buying, chatbots, voice bots and a lot more, are not only available but are also becoming cheaper. The market application of the possibilities offered by technology becomes more and more important. Customers’ perception of privacy, legal regulations and the discussion about technology adoption influence the scale of AI implementation. Any limitations in its use to build a competitive advantage will constitute the development of not only a data-driven economy but also technology itself. In the age of AI promoting ethical data processing seems to become critical. Protecting individuals and their data in all regulatory initiatives should be comprehensive but also technology neutral. Legal interventions should be complemented by the countervailing power of civil society, both consumer unions and individuals.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Grzegorz Mazurek  <http://orcid.org/0000-0002-0047-6944>

Karolina Małagocka  <http://orcid.org/0000-0003-2544-2094>

References

- 5th Report on Robotics and Artificial Intelligence. Retrieved from <https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Altman, I. (1975). *The environment and social behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Pub., Co., Belmont.
- Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J., & Glen Weyl, E. (2018). Should we treat data as labor? Moving beyond 'free'. *Proceedings of the American Economic Association*, 1(1), 1–5. Retrieved from www.aeaweb.org/conference/2018/preliminary/paper/2Y7N88na
- Atikcan, E., & Chalmers, A. (2016). *Explaining patters of lobbying alignment in case of the EU's general data protection regulation*. Presentation prepared for the SGEU conference, Trento.
- Barth, S., & De Jong, M. D. (2017). The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058.
- Berger, R. (2018). *Artificial intelligence - a strategy for European startups. Recommendations for policy makers*. Retrieved from www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf
- Berkhout, J., Carroll, B. J., Braun, C., Chalmers, A. W., Destrooper, T., Lowery, D., & Rasmussen, A. (2015). Interest organizations across economic sectors: Explaining interest group density in the European Union. *Journal of European Public Policy*, 22(4), 462–480.
- Berkhout, J., & Lowery, D. (2008). Counting organized interests in the European Union: A comparison of data sources. *Journal of European Public Policy*, 15(4), 489–513.
- Bédard, M. (2016). *The underestimated economic benefits of the internet*. Montreal: Montreal Economic Institute.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041.
- Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law Review*, 4(5), 193–220.
- Broscheid, A., & Coen, D. (2007). Lobbying activity and fora creation in the EU: Empirically exploring the nature of the policy good. *Journal of European Public Policy*, 14(3), 346–365.
- Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication*, 1(1), 29.
- Castro, D., & New, J. (2016, September). *The promise of artificial intelligence*. Center for Data Innovation. Retrieved from <http://www2.datainnovation.org/2016-promise-of-ai.pdf>
- China Economic Life Survey. (2019). Retrieved from <https://technode.com/2018/03/02/almost-80-chinese-concerned-ai-threat-privacy-32-already-feel-threat-work/>
- Dean, J. (2016). Big Data: Accumulation and Enclosure. *Theory & Event* 19(3). Retrieved from <https://www.muse.jhu.edu/article/623988>.
- Digital Single Market. (2019). *Final results of the European Data Market study measuring the size and trends of the EU data economy*. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy>
- Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.

- Drezner, D. W. (2007). The new new world order. *Foreign Affairs (Council. on Foreign Relations)*, 86, 34–30.
- Goodman, B., & Flaxman, S. (2016, June). *European Union regulations on algorithmic decision-making and a 'right to explanation'*. Presented at ICML workshop on human interpretability in machine learning (WHI 2016), New York, NY. Retrieved from http://adsabs.harvard.edu/cgi-bin/bib_query?arXiv:1606.08813
- How can Europe Unleash its untapped data held. (2018, June 26). By Press Club Brussels. Retrieved from <https://www.pressclub.be/event/how-can-europe-unleash-its-untapped-data/>
- Inside the e-Privacy Regulations furious lobbying war. (2017, October 31). Retrieved from <https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/>
- Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25.
- Kosiński, M. (2015). *End of privacy*. Retrieved from <https://www.gsb.stanford.edu/insights/michal-kosinski-end-privacy>
- Lanier, J. (2013). *Who owns the future?*. New York, NY: Simon and Schuster.
- Long, W. (2014). Significant impact of new EU data protection regulation on financial services. *Global Banking and Finance Review*, 1.
- Mazey, S., & Richardson, J. (1997). Policy framing: Interest groups and the lead up to 1996 inter-governmental conference. *West European Politics*, 20(3), 111–133.
- McKinsey Global Institute. (2018, September). *Outperformers: High-growth emerging economies and the companies that propel them*. Retrieved from <https://www.mckinsey.com/~media/mckinsey/featured20insights/innovation/outperformers20high20growth20emerging20economies20and20the20companies20that20propel%20them/mgi-outperformers-full-report-sep-2018.ashx>
- Meulen, R. (2017, June). *Top 5 priorities to prepare for EU GDPR*, gartner. Retrieved from <https://www.gartner.com/smarterwithgartner/top-five-priorities-to-prepare-for-eu-gdpr/>
- Microsoft Research Podcast. (2017). *Making intelligence intelligible with Dr. Rich Caruana*. Retrieved from <https://www.microsoft.com/en-us/research/blog/category/podcast/>
- MIT Technology Review. (2017, June 27). *Who is winning the AI race?* Retrieved from <https://www.technologyreview.com/s/608112/who-is-winning-the-ai-race/>
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*. doi:10.1177/2053951716679679
- Moore, A. D. (2003). Privacy: Its meaning and value. *American Philosophical Quarterly*, 40(3), 215–227.
- Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. New York, NY: Public Affairs.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 101–139.
- OSTP. (2016, October). *Preparing for the future of artificial intelligence*. Retrieved from <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/OSTP-AI-RFI-Responses.pdf>
- Oury, J.-P. (2018, April). *Europe trapped in the artificial intelligence paradox*, European Scientists. Retrieved from <https://www.europeanscientist.com/en/editors-corner/europe-trapped-in-the-artificial-intelligence-paradox/>
- Posner, E. A., & Weyl, E. G. (2018). *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton, NJ: Princeton University Press.
- Presidential Executive Order. (2017, June). *Donald J. Trump, presidential executive order expanding apprenticeships in America*. Retrieved from <https://www.whitehouse.gov/presidential-actions/3245/>
- Report of the Artificial Intelligence Task Force. (2018). p. 9, 39. Retrieved from <http://dipp.nic.in/whats-new/report-task-force-artificial-intelligence>
- Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: A modern approach*. Malaysia: Pearson Education Limited.
- Sato, C., & Wang, R. (2018, June). *Constellation research 2018 artificial intelligence study*. Retrieved from <https://www.constellationnr.com/research/constellation-research-2018-artificial-intelligence-study-0>
- Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. London: WW Norton & Company

- Siegele, L. (2018). New EU data rules will get tough on privacy. *The Economist: The World in 2018*. Retrieved from <http://www.theworldin.com/edition/2018/article/14563/new-eu-datarules-will-get-tough-privacy>
- Swanson, A. (2017, September). Trump blocks China-backed bid to buy U.S. chip maker. *New York Times*. Retrieved from www.nytimes.com
- Virta, R. L. (2006). *Worldwide asbestos supply and consumption trends from 1900 through 2003*. Reston, VA: U.S. Geological Survey.
- Wallace, N., & Castro, D. (2018, March 27). *Center for data innovation, the impact of the EU's new data protection regulation on AI*. Retrieved from <https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/>
- Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, 7, 431–453.
- Wonka, A., Baumgartner, F. R., Mahoney, C., & Berkhout, J. (2010). Measuring the size and scope of the EU interest group population. *European Union Politics*, 11(3), 463–476.
- Wright, R. (2004). *A short history of progress*. Toronto: House of Anansi.
- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.
- Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013, May). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions?. In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463–472). ACM