UNIVERSITY OF PÉCS

Faculty of Law, Doctoral School of Law

Ph.D. Thesis summary

Risks of Big Data and Artificial Intelligence in light of data protection – an examination of the existing legal framework with a focus on the General Data Protection Regulation

Supervisor: Dr. Gergely László Szőke

Author: Branka Mania

Date: October 25, 2021

Table of Contents

PART 1: **Summary of the research task**

The question behind this Thesis is how Big Data and data protection relate to each other in the sense of if, and to which extent, current data protection laws address risks of Big Data applications. To examine this issue, it first must be clarified what lies behind the buzzword Big Data, and what exactly is protected by data protection laws, especially because new technology may involve new risks, and because data processing nowadays in many cases is rarely limited to national borders or a single service provider. To complete the picture about this matter, the Thesis examines how the existing legal framework and the General Data Protection Regulation in particular capture Big Data and potential risks involved in its applications.

In fact, Big Data involves algorithmic data processing as well as automated decision-making systems which can operate with little human intervention: from a business perspective, the use of algorithmic systems is very attractive as it leads to time and cost efficiency and allows for better analytics and forecasting as well as real-time insights. However, from an individual`s perspective, the use of Big Data, automated decision-making that results in so-called Artificial Intelligence may lead to serious consequences: the challenge already starts with errors that may occur during the design of algorithms, owing to underlying datasets being incorrect or due to wrong interpretation of outcomes which may lead to undesirable results.

The problem from a data protection perspective are effects like data aggregation and maximization, unpredictable as well as secondary (indefinite) use of personal information and the fact that complex data processing operations which are performed by self-learning machines and solely based on data-driven predictive models may not be transparent and explainable anymore. Any such processing is thus potentially opaque and may lack human oversight and control, meaning that basic data protection principles like accountability or transparency, lawfulness and fairness may be affected. Ditto for individual`s rights, because privacy self-management seems hard to achieve when there is information mismatch between data subjects and operators. In addition, the use of algorithmic technology is also criticized for having the potential for (secret) profiling and scoring or even surveillance and discrimination, which shows that there are various implications that go with the use of algorithmic technology.

This in turn leads to the question whether the current legal framework for data protection offers sufficient protections for the individuals behind data protection laws. To answer this question, the following has been examined: what is Big Data; what is Artificial Intelligence; what are the relevant legal (GDPR) definitions; what is the scope of applicable laws; what do data protection and data privacy protect; what is the current (international, EU, national, sectoral) data protection framework; which other relevant sources of law such as product, liability, data-specific rules exist; which risks come with the use of Big Data, automated decision-making or profiling and the use of algorithms and Artificial Intelligence; do existing regulatory conditions and legal concepts capture these risks; which legislative, regulatory or non-governmental proposals and expert guidelines have been suggested for a future-proof AI regulation; which conclusions can be drawn.

PART 2: **Description of examinations and analyses**

The examination starts with the history of privacy and the development of data protection laws and furthermore covers the emergence of Big Data, automated decision-making and Artificial Intelligence. The historical context is important to distinguish various terms that are used interchangeably, for example, privacy and data protection, and to explain legislator objectives in recent decades. The next section deals with the emergence of Big Data, automated decision-making and Artificial Intelligence describes data processing as we know it today and shows the foundations of these technologies as well as their dependency on the development of computer science, the needed speed of processing and infrastructure.

The examination continues with relevant definitions such as personal, anonymous, pseudonymous and identifiable as well as special categories of data, processing, profiling and automated decision-making or consent, and explains the challenges with existing legal definitions and (inconsistent) terminology or translation issues, which is especially true for the definition of (the right to) privacy. Definitions are an important starting point as they clarify the overall scope and the applicability of laws to certain use cases such as profiling. Given the fact that the General Data Protection Regulation has a broad definition of personal data, some speak of the General Data Protection Regulation as "the law of everything" since literally everything seems covered because everything may be regarded as personal data, because anonymization is technically hard to achieve or cannot be applied to certain data-sets where "real data" is needed as opposed to "synthetic data" or dummy data.

Rather than defining Artificial Intelligence, the next section deals with the characteristics of Big Data and Artificial Intelligence, including the most relevant use cases, for example analytics and forecasting, fraud prevention as well as data-driven products and services. It covers the "Vs" of Big Data (volume, variety, velocity, veracity, variability, volatility, value) and describes various types of Artificial Intelligence such search and planning Algorithms, symbolic AI, Robotics, computer sensing and vision, Machine Learning and Deep Learning, Natural Language Processing, Knowledge Engineering or Neural Networks to name some.

Further on, the analysis focuses on relevant sources of law, which is a substantial part of the Thesis as it provides an overview over the existing legal framework for processing of personal data and the protection of individuals' rights such as the respect for private life. The overview starts with rules at international level: the United Nations Universal Declaration of Human Rights, the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the Council of Europe Data Protection Convention 108+, OECD's Privacy Guidelines as well as further conventions and resolutions. All these conventions and charters also deal with rights related to data protection and privacy, and some explicitly mention principles that are well-known for privacy practitioners, e.g., the principle of data minimization and purpose specification. The fact that conventions that deal with fundamental rights also deal with data protection and privacy matters shows the human rights dimension of data protection issues. Regarding superior law, it should not be forgotten that legally binding global trade agreements also play a role in the context of data processing and trans-border data flows: these agreements set forth certain standards, including norms of non-discrimination that require protections against unjustified data localization requirements.

From a data protection perspective, many immediately think of the General Data Protection Regulation as a major piece of legislation, and despite the fact that the General Data Protection Regulation was a milestone in the history of data protection laws, it is by far not the only relevant regulation. At EU-level only, a variety of other regulations and directives have to be taken into consideration when processing of (personal) data, automated decision-making, profiling, Big Data or Artificial Intelligence are in question – be it from a security, database, know-how protection, compliance or product safety perspective, for example: the privacy and e-communications directive, the directive on trade secrets, the NIS-Directive, the Cyber-Security Act, the directive on the free flow of non-personal data, the directive on general product safety, the database directive as well as directives on equal treatment and against discrimination and equal opportunity in the employment context, and rules applicable to EU institutions and bodies or the police and justice sector.

There are numerous national data protection laws and laws with specific provisions pertaining to the processing of personal data, even within the European Union as the General Data Protection Regulation has dozens of "opening clauses" that either provide or allow for national rules: for certain areas (e.g., processing of personal data in the employment context, see GDPR Art. 88) or for certain types of data (e.g., processing of national identification numbers, see GDPR Art. 87). It should also be considered that, for example, Brazil's data protection law LGPD has a territorial scope that extends outside of Brazil, meaning that as a result, global companies to which these laws apply must comply with a multitude of laws. And depending on the use case in question, further laws may be applicable such as consumer protection and e-commerce or competition laws for marketing activities or labor, equal opportunity, and industrial constitution laws in the employment context. The same is true for products or "connected devices" with a particular focus on information and cyber-security provisions and rules that apply to the so-called "Internet of Things".

In terms of existing rules and regulations, it is important to take note of the fact that already at present, various sector / industry specific (e.g., banking: high frequency algorithmic trading), or product specific (e.g., medical devices) as well as purpose (e.g., facial recognition, autonomous driving, autonomous weapons) and data specific (e.g., biometric data, genetic data, health information) laws exist which must be obeyed when Big Data applications and algorithmic systems are used. In this context, it must furthermore be noted that some states within the U.S.A. either already introduced or are working on laws that specifically deal with algorithm-based data processing and automated decision-making, and several states introduced specific provisions for facial recognition technology that is based on Artificial Intelligence. It can generally be said that the legal framework in the U.S.A. is lively in this area of law; the US privacy landscape became so dynamic that specialized law firms started providing weekly updates about the status of state privacy legislation: California alone, to only name one example, introduced the following laws relating to privacy: the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), or the California Online Privacy Protection Act (CalOPPA). Many states introduced their own privacy bills with requirements that are similar to those set forth in the GDPR and which grant consumers various rights such as access, portability, correction, deletion, and the right to object to the processing of their data in certain circumstances; other laws requires opt-out for targeted advertising and profiling decisions that produce legal or similarly significant effects and foresee that mandatory data protection impact assessment must be carried out for certain processing activities including profiling. Documentation requirements and data subject rights often sound familiar, however, the scope is not the same as these laws are

rather concerned with consumers than individuals. This underlines the relevance of the historical context, because in the U.S.A., data protection was and is connected to consumer protection whereas in Europe, the focus of first-generation data protection laws was the public sector and public authorities. The "European approach" is traditionally focusing on individual`s rights, whereas the approach in the U.S.A. is traditionally focusing on harms: considering how difficult the exercise of individual rights and privacy-self management in today`s Big Tech "David vs. Goliath" data processing environment is, a harm-based approach may be more of a future-proof concept. Finally, as regards existing sources of law that complete the current legal framework relevant to the research topic, apart from "hard law", there is also guidance at authority level, be it at EU or national level or provided by de-facto-regulators like the Federal Trade Commission in the U.S.A. There are moreover private (including self-certification) sector initiatives by companies like IBM, Microsoft and numerous telecommunications companies.

The next part of the paper deals with recommendations and initiatives that specifically address issues that arise in the context of the use of algorithmic systems and technology that uses Artificial Intelligence. In this regard, it shall first be noted that, despite the fact that some consider that the codification and regulation of systems and applications that use some sort of Artificial Intelligence to be in its infancy, there is already a variety of (non-binding) recommendations and guidelines that specifically address the development, design and responsible use of Artificial Intelligence. This is not surprising since such technology is already being used across the board, for example, in production (robotics), operations (forecasting), marketing (analytics), finance (scoring), healthcare (diagnostics), in "smart cities," "smart homes," and "smart devices" and as well as for (behavioral, online, location) tracking and targeting purposes. The use of Artificial Intelligence in biometrics is probably the best example that the point is already reached where some call for a ban of certain technology that uses Artificial intelligence. Facial recognition may lead to serious threats from an individual's perspective since it could be used for unlawful or at least undesired data processing as the case of ClearView showed. In addition, facial recognition has the potential for discrimination and could also be used for surveillance purposes, and that is why many raised concerns from a human rights point of view and call to limit the use of this technology. The case of Cambridge Analytica demonstrated that the use of Artificial intelligence has a political dimension as well: Influencing voters is traditionally at the core of any campaign, but the problem is that there is little transparency and awareness of how sophisticated this technology is and how cleverly it can be used.

At international level, the paper OECD's AI principles as well as the G20, G7 and World Economic Forum recommendations on AI. Ditto for various initiatives and declarations the United Nations provided, e.g., UNESCO, UNICRI, UNICEF or UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. As for guidance and recommendations at European level, the following initiatives are examined (non-exhaustive): the European Commission's White Paper on Artificial Intelligence, the Ethical Charter on the Use of AI in Judicial Systems, the Resolution on Civil Law Rules on Robotics, Council of Europe Recommendations as well as ethics guidelines for trustworthy AI – the latter is also a good example that the majority of these initiatives focus on ethics, including UNI Global Union's Principles for Ethical Artificial Intelligence or IEEE's Ethically Aligned Design. The same is true for various expert guidelines, civil society and multistakeholder recommendations such as the Toronto and the Montreal Declaration or papers published by the Future of Life Institute and the Centre for Information Policy Leadership

(non-exhaustive). There is also considerable intergovernmental cooperation with regards to Artificial Intelligence, for example, OECD's Network of Experts on AI, UNESCO's Ad Hoc Expert Group, EU's High-level Expert Group on Artificial Intelligence, or the Global Partnership on AI. As regards to expert / multistakeholder / NGO guidelines, it can be said that these initiatives have in common that they intend to provide useful recommendations for the use of Artificial Intelligence, however, they vary insofar that some guidelines focus on the ethics and responsible use of AI including the future of work, whereas other recommendations are concerned with the classification of AI systems. Most of these papers underline the importance of awareness raising and emphasize the relevance of a human-centered approach to AI and the need for the protection of privacy and intimacy, as well as human control and oversight. Notwithstanding differences as regards strategy and methods, these initiatives show certain parallels which could be summarized as follows: a new kind of transparency that exceeds existing standards and ranges from the explicability and replicability of decisions, failure transparency as well as making "true operators known" to public consultation and/or public registries for high-risk AI use cases. Some of these guidelines discuss a new kind of accountability which shall include "all players" in the data value chain (onward responsibility) and suggest specific audits for AI applications, further independent oversight bodies and public safety obligations. The papers furthermore deal with new requirements such as mandatory human rights impact assessments and termination obligations in the event a system gets out of control. Some of the statements recommend advanced individual rights such as general the right to human intervention and determination as well as enhanced access and redress mechanisms, and others discuss the introduction of further principles such as non-discrimination and inclusion, equality and diversity that should be applied whenever algorithmic processing is in question. These initiatives also address judicial and societal implications of AI applications and elaborate on how to best ensure fair trial and access to justice and welfare how to best protect the freedom of expression, assembly and association, and the right to work in an era of growing automatization and digitalization. Finally, some papers propose the strict prohibition of certain AI uses, for example secret profiling and unitary scoring or facial recognition. In contrast, other opinions stress the relevance and application of existing principles and (enforcement) mechanisms like the fairness, accountability, transparency, data quality, accuracy and provenance, privacy by design and by default, joint controllership, the need for (explicit) consent or technical and organizational requirements which constitute substantial part of most data privacy and data security laws. Last but not least, there are also interesting alternative approaches to issues that arise with the use of Algorithms and Artificial Intelligence such as the call for a Hippocratic oath for data scientists or initiatives that deal with the question how privacy bills should (not) be written: these authors question the concept of rights-based governance where individual rights function as the primary mechanism for governing the collection and processing of personal data since that puts the burden of privacy controls on the individual rather than the controller as such a conventional approach might not be appropriate in an era of more and more "surveillance-based business models".

As a matter of fact, the "AI arms race" has long started and resulted in numerous national AI initiatives and strategies around the globe, all pursuing the same goal – to become a leader in Artificial Intelligence: the U.S.A. is home to world-famous Big Tech companies and innovation; the fact that numerous laws that specifically deal with AI such as the Artificial Intelligence Act, the Algorithmic Accountability Act, the AI in Government Act, the Future of AI Act, the Artificial Intelligence Reporting Act, the National Artificial Intelligence Initiative Act, the Advancing AI Research Act, the Growing Artificial Intelligence Through Research Act show the nation's

strong wish to shape the American AI policy. China is also heavily engaged in AI, the nation released an "Artificial Intelligence Development Plan" and established an AI Governance Expert Committee as well as AI-focused industrial parks. Similar developments can be observed in many countries, throughout various jurisdictions, and business sectors. A noteworthy development in this context is that the UK, which has well-established tech landscape and is traditionally strong in the area of research, announced that it intends to take advantage by the opportunity afforded by the UK's exit from the European Union to reform the UK's data protection regime, including plans to revisit the nation's AI strategy: this might have implications for data protection as there are discussions around softening the conditions around (re-)use of personal data and considerations if data protection legislation and the ICO is the right forum and regulator for determining "fairness" in profiling and automated decision-making.

Before elaborating on the possible future legal framework for Artificial Intelligence, the Thesis covers further relevant developments as regards international data transfers. Big Data and AI are complex processing operations, and many of them are unimaginable without a multitude of vendors and multiple data handling and (cloud?) storage locations, which leads to further issues, e.g., regarding alternative transfer mechanisms, data localization requirements or potential technical solutions such as encryption. The invalidation of the "Privacy Shield" by the European Court of Justice in summer 2020 is probably the most remarkable development: despite the confirmation of the validity of (renewed) Standard Contractual Clauses and regardless of the fact that numerous authorities came up with guidance (on transfer impact assessments and the like), companies are left with a certain degree of uncertainty when it comes to considerations for international data transfers, because many questions are unanswered – be it with regards to possible derogations in accordance with GDPR Art. 49, or with regards to California, the home of many Tech Giants, having an adequate level of data protection (GDPR Art. 45 III refers to a third country or *territory*), or regarding possible technical solutions like encryption or data trustee models to on the one hand, allow for data transfers, but on the other hand, avoid undesired (government) access to personal information. The factual problem is that some promising data trustee models have been discontinued, and the legal problem is that government access to personal information is neither novel nor unique to the U.S.A. It is a given in the U.S. and in the EU, the difference being that there is little public awareness of regulations like the E-evidence Regulation that allows for cross-border access to electronic evidence. The situation for globally active corporations is further complicated by the fact that there are dozens of national laws that foresee local storage of personal information. Such data residency requirements do not necessarily do privacy a favor: principles like data minimization, data integrity and confidentiality may not be met if companies must establish and defend multiple versions of its systems across continents with additional hardware, additional vendors and additional staff having access to that data. One author commented as follows on forced localization: "*technically speaking, physical access to a server or device containing data is neither a necessary nor a sufficient condition for access to information, and logical access is both necessary, and may be sufficient to provide access to data in an intelligible form, regardless of geographic location".*

Another core element of the Thesis deals with the future legal framework, i.e., which rules and regulations are currently discussed / will be implemented in the near future and which might have an intersection with AI, algorithmic processing and decision-making. In this context, it shall first be noted that the least of these initiatives are focusing solely or directly on data privacy issues, data subject rights or potential concerns around

AI and ADM. But transparency, security or documentation, evaluation and oversight requirements and the like are topics that are relevant to data privacy and may be covered by regulations that govern online content, electronic communications, the Internet of Things or the (re-) use of public sector information. This part of the Thesis examines whether legislative proposals which, at first glance, do not suggest having provisions on consumer and / or data protection, in fact have rules that are relevant from a data subject perspective. A variety of legislative proposals qualify in this regard, for example, the proposal for a Regulation on electronic evidence in criminal matters or the proposal for a review of the Directive on the re-use of public sector information, the Machinery Regulation or the Digital Services and Digital Markets Act and the Data Governance Act. The proposal for a Regulation on Artificial Intelligence immediately attracted a lot of attention and has received numerous comments. But the proposal for a Regulation on privacy and electronic communications alone is probably the best example of how hard it is to assess the situation appropriately: there is controversy around the draft E-Privacy regulation for many years now, and it is possible that the same could happen to the draft AI regulation owing to the high business significance of this initiative. Therefore, at this stage, only an overview and outlook on potential developments in the legal landscape relevant to Big Data and AI applications can be given.

The next part of the Thesis deals with typical effects and potential risks of Big Data and Artificial Intelligence. This is a substantial part of the Thesis as it shows what kind of risks may result out of the application of Big Data and AI systems, algorithmic processing or automated decision-making and profiling, and there is good reason why data protection laws traditionally foresee that impact assessments or similar documentation is necessary as a first step when new technology is used, or when systems are deployed that allow for systematic / extensive / large-scale processing of personal information, or when the processing may involve high risks for the rights and freedoms of individuals or lead to decisions that may have significant (negative, legal) effects on individuals.

The first two types of risk, data aggregation and data maximization, can be considered a common effect of most Big Data and AI applications, simply because large (training) datasets are needed for the majority of use cases – Big Data is about turning volume to value, but that may conflict with GDPR's principle of data minimization, and it may pose a threat to individuals insofar as there is a risk of (re-)Identification: the more datasets grow, and the more data is attributed to a person, the easier it gets to identify the person behind the dataset: a study of credit card records showed that only four spatiotemporal points are enough to uniquely re-identify 90 percent of individuals; knowing the price of the underlying transaction further increased the possibility of re-identification by 22 percent. The usual practice of constant "enrichment" of datasets also raises questions with regards to profiling and identity: if one and the same person is "constantly analyzed and scored" this may result in detailed profiles and (online) "identities" the person is not aware of. Another problem of Big Data and AI applications is that, quite often, external (collateral) data are processed. The upload of address books to social media platforms is a simple example of this risk: whenever a user uploads his individual contacts to a social media platform, the platform receives a full set of contact information of other individuals, and these individuals may not have been informed nor did they consent to such data collection.

One further effect of Big Data, ADM and AI is the secondary use of personal information: compatible re-use of personal data is admissible to the extent the conditions of GDPR Article 6 (4) are met, i.e. considering the nature of the data in question, the context in which the data were collected, the relationship between the purposes for which the data have been collected and the purposes of further processing, the impact of the envisaged data processing on the data subjects, and the safeguards applied by the controller. Since a major characteristic of many AI applications is a certain degree of autonomy with systems being able to perform in an unsupervised manner, it is questionable whether such data processing operations meet all these requirements or if that may lead to indefinite re-use of personal data which could also render purpose limitation obsolete.

Further potential risks of AI applications are opaqueness and lack of human oversight: a challenge with Artificial Intelligence is that quite often, important factors are unknown, e.g., details of the processing operations, and the "true operators" behind those algorithms in the sense of who exactly is responsible for which part of the processing. In many cases, input and output are known, but the workings in between are not, is also known as the "black box effect". Some argue that there are three distinct types of opaqueness which can be distinguished: intentional opacity when the inner workings of the system are deliberately concealed, illiterate opacity when the inner workings are opaque since only those with expert knowledge understand how it works, and intrinsic opacity due to a fundamental mismatch between how humans and how algorithms understand the world. The ability of AI to act autonomously and in unforeseeable ways adds to the fear that certain types of AI systems may be considered a "Kafkaesque system of unreviewable decision-makers", and that explains why human oversight may be at risk when algorithms are used for the processing of personal information.

Closely connected to the issue of oversight are question of responsibility and liability: while accountability is established as a privacy principle and rated as an important value in literally all publications, fewer texts deal with the fact that AI has the potential to challenge the traditional notions of legal responsibility (and legal personality). In this regard, the European Parliament and the European Commission provided various publications, for example on liability issues in respect of autonomous robots, liability (and safety) implications of Artificial Intelligence and the Internet of Things, or a report on liability for other emerging technologies. In their papers, the EC and EP explain their key findings with regards to new duties of care, strict and vicarious liability, the burden of proof as well as insurance issues. From an individual's perspective, the question would probably primarily be whom to turn to: a court or a regulator or a company, and if so, which one: from a GDPR perspective, there are controllers, processors and joint controllers, but the problem is that and more laws introduce more "players": the DGA, for example, mentions, amongst other things, "data holders" and "data users", and looking at the categorization of relevant players within the draft AI regulation, the situation becomes even more complex as there are providers, manufacturers, distributors, importers – how should an average person without corresponding expertise be able to tell who is responsible for which part and under which conditions. This clearly shows the complexity has greatly increased, and this is far from mere terminology problems.

Big Data and AI applications in many cases raise further concerns, which is a situation literature describes as the information mismatch: companies must be transparent about the processing of personal data, but even GDPR itself sets limits to transparency obligations: Article 13 (2) lit. f limits the obligation to information about "*the*

existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". Details about the significance as well as envisaged consequences of the processing are relative insofar as dynamic processing may simply not allow to foresee all relevant consequences; details about the underlying logic are relative insofar as meaningful information is simply not the same as comprehensibility or reproducibility of decisions. Companies may moreover argue with trade and businesses secrets to avoid having to disclose underlying algorithms they use. Another factor that adds to the mismatch is the dilemma of information asymmetry between users and (Internet, online) service providers, and the situation is worsened by the fact that this often goes hand in hand with a concentration of power within the so-called "Industry 4.0". One author's situational analysis is that "*Alphabet controls our search and much of our mobile experience, Apple controls the remainder of our mobile and much of our content experience, Amazon controls a large portion of our content experience and much of the Internet of Things, and Microsoft essentially sweeps up everything else*." As a result, a small number of companies has the power to control a large part of what we do – perhaps rather based on their own corporate terms and conditions and less on privacy laws, and the phenomenon is so significant that it this has put the antitrust authorities on notice.

The above circumstances lead to the next problem, the issue of privacy self-management. Even if lack of transparency is not the problem, transparency as such is problematic since the ineffectiveness of transparency requirements seems to be proven by now: people are as badly informed as they are overtaxed with long and complex privacy notices; people routinely turn over their data for small benefits; people care much more about price-sensitive information than about data protection information; people are much more concerned about social privacy than about institutional privacy, and if people are about to decide about their privacy preferences, they tend to make their lives easy and accept all default settings instead of taking their time to really decide on relevant settings. Even worse, certain Apps take advantage of psychological (behavioral) patterns that can reinforce loss of user control, and legislation on such dark patterns is just in the process of being created.

Some authors describe the afore-mentioned challenges around information obligations as the transparency paradox. They compare interactions with Big Data platforms with a poker game "where one of the players has his hand open and the other keeps his cards close". The controversy around the use of cookies and similar technologies showed that transparency and consent are difficult to achieve and that privacy self-management in many instances is only about a take-it-or-leave-it-approach, a mere click-mechanism. This leads to the next issue, the control paradox, i.e. the problem that affording more control to users does not help them to better protect their privacy. It seems that the opposite is true: affording more control to users does not necessarily lead to a better protection of their data – this may even induce them to reveal more information: if people feel that they have control over their data, they tend to provide more data about themselves. Similar effects are known from other fields, for example in the framework of the introduction of the safety belt legislation as people felt more secure with safety belts and drove less carefully; ditto for the introduction of "COVID apps": the fact that there is technology that can track cases of infections does not replace other necessary measures to prevent infections such as hygiene, distance rules or masks. The control paradox is connected to another problem, the security paradox. Data protection and data security are inseparable, and that is why security measures such as access controls are principally indispensable. But any such measures require the processing of personal data such

as log-in data, and the general risk is that the more data are processed, the larger the risks that data are somehow compromised. More and more often, users are required to provide a fingerprint in the framework of the authentication process, and that may lead to further risks: nowadays, many devices require the use of biometric data, but the problem is that, unlike a password, there is no reset process for a unique fingerprint, and what is worse, such data can be manipulated very easily, because access to a used object is sufficient to reproduce a fingerprint, and if fingerprints are a mandatory part of official ID-documents, then the individual concerned has a serious problem. Another effect that is connected with the security paradox can be described as the trust paradox: a growing number of people are so used to relying on all kinds of Apps as their "single source of truth" that there does not seem to be any more room left for own decision making, and that has an impact on how they handle their data.

Another point to consider as regards security is the risk of malicious use of AI, because much more attention has been paid to beneficial applications of AI than the ways in which Artificial Intelligence could be used maliciously, which is why some authors claim that AI has a dual-use character. Some predict that the growing use of AI systems will change the landscape of threats, because adequate defenses to potential security threats from malicious uses of AI are not yet developed. A recent report surveyed potential security threats in the area of Artificial Intelligence and came to the conclusion that the use of AI will expand existing threats and change the typical character of threats, because AI may simply lower the costs of attacks since AI is scalable and can complete tasks that would ordinarily require human labor, intelligence and expertise. The use of AI for malicious purposes could be especially effective because it could be finely targeted, difficult to attribute, and thus likely to exploit vulnerabilities (e.g., by using speech synthesis for impersonation), and complete tasks that would be otherwise be impractical for humans (e.g., labor intensive attacks). In addition, AI can be used in novel ways, for example by exploiting human vulnerabilities (e.g., through using speech synthesis for impersonation), by exploiting existing software vulnerabilities (e.g., through automated hacking) or the vulnerabilities of AI systems (e.g., through data poisoning or by introducing training data that causes a learning system to make mistakes or by inputs designed to be misclassified by machine learning systems. The latter is a particularly interesting aspect insofar as AI itself may be vulnerable as well – if AI systems can exceed human performance, they may also fail in ways that a human never would.

Since AI helps with the transformation of businesses, AI will consequently also have an impact on workforce. We have come to a point where not only monotonous tasks in production lines or computer-assisted customer care operations care can be automated by robots or chatbots. Complex operations can be automated as well, and even the legal profession may be severely impacted by this new kind of virtual workforce, because tasks like document classification, summarization, comparison, knowledge extraction, discovery and retrieval are more and more based on technology, and less on human work. Against this background, discussions around potential negative employment effects of AI commenced, including ideas like specific taxes on AI-performed tasks or the introduction of an unconditional basic income to secure livelihoods. At the same time however, some say that the lack of access to new technologies in less developed countries will further increase inequalities between individual populations and countries. The impact on AI on the digital economy was also raised by numerous international institutions who stress that AI shall, amongst other things, respect internationally recognized labor rights. Fact is that today, even getting a job starts with AI because resume screenings and background checks are

very often being automated, and the draft AI Regulation addresses employment and recruitment issues and classifies AI applications used for such purpose / in this sector as high-risk applications.

Artificial Intelligence is also used in the area of welfare, public administration and in the field of jurisprudence, which is why some object to the use of AI applications in such areas as this may pave the way or strengthen injustices or even restrict the legal process, and this way limit access to justice. Further risks that have been discussed in the context of Artificial Intelligence are the potential for discrimination for surveillance: the probabilistic nature of individual decision-making and profiling is highly desired from a business perspective, but their inherent opacity together with their potential for discrimination and discrimination is problematic from an individual's perspective, and that is why many believe that these two risks are probably the most important dangers from the point of view of those affected. There consequences of such risks are far-reaching: employers may turn down job candidates based on social media information without providing candidates with an opportunity to comment on their findings, and this explains the problem of information injustice and information inequality. The problem is that individuals unlike companies do not dispose of enough information to defend themselves not just against the data processing as such (which may be legitimate under GDPR Article 6 (1) lit. f, but against being sorted in the wrong bucket. More dramatic examples such as facial recognition bias, bias in recidivism scoring systems, or bias in healthcare show that the data protection rights do not necessarily help against certain risks of the new economy, and they also show that AI risks affects individuals and society: facial recognition technology may be deployed across the board for mass surveillance purposes; Artificial Intelligence could be used in a political context, for example, by creating targeted propaganda or to manipulate photos and videos with the help of deepfakes and this way, pose a threat to democracy. AI may even threaten physical security, e.g., by using drones or by subverting systems. In consequence, a new quality of malicious actors may emerge, which reinforces the conclusion some make that, certain types of Artificial Intelligence should be treated as dual-use technology, which shall result in a corresponding (appropriate) legal framework as is the case for weapons or dangerous goods.

PART 3: Brief summary of results

This part of the Thesis deals with findings as well as ideas for improvement, ranging from general observations and developments in the field of data protection, challenges within the existing and envisaged future legal framework, up to GDPR and AI specific issues and new approaches that suggest enhancement of existing mechanisms or avoidance of undesirable phenomena.

The history of (the right to) privacy and the fact that privacy and the respect for the private life are mentioned in a variety of international conventions shows that privacy is considered a fundamental right. As such, protective mechanisms are traditionally directed against the state. The problem is that there seems to be a shift of protections of fundamental rights to the private sector: some argue that, because GDPR allows for processing based on legitimate interests, as well as compatible processing (secondary use of personal information), this may lead to a self-regulatory regime.

Data protection laws as we know them today have been introduced some decades ago, but the Internet (of things), the growing digitalization, new technologies and new phenomena like social media platforms, together with the growing connectivity of devices, and the overall exponential growth of (user, sensor, behavioral, etc.) data leads to the emergence of a well-known problem, the fact that the development of (appropriate) laws takes too much time: in this context, "cookies" are a good example – debates are still focused around the use of cookies, but fact is that regulators took a lot of time to come up with guidance and enforcement, and legislators took too much time with controversial discussions around accompanying legislation like the draft E-Privacy Regulation. However, there is already new technology that can replace cookies and provide for the same results.

The enforcement of existing laws is also a challenge: while we have seen several multi-million dollars fines in the last two years, there has also been a series of fine failures (for example, drastic reductions of penalties of up to 90 %) which showed that imposing administrative fines under GDPR might not be easy, because administrative, procedural as well as commercial criminal laws must be taken into consideration as well. Plus, the more laws are applicable to a specific processing activity, the more there is risk for enforcement overlap if both, data protection and competition or further supervisory authorities are called to action.

On the one hand, it is good news is that data protection laws are on the rise; Brazil or China adopted data protection laws, and the U.S.A. is also a good example of an emerging legal landscape with numerous (state-level) laws on (consumer) privacy or specific rules on the use of sensitive data like biometric or genetic information. On the other hand, it is bad news that this adds to the complexity, which starts with seemingly simple issues like terminology, including translation issues. The scope and application of laws depend on clarity as regards relevant definitions, and there are indeed challenges due to inconsistent use of terms, potentially non-future-proof definitions, and the introduction of new terms in new relevant laws like the draft AI regulation. It is moreover important to follow that Big Tech players who process personal information at large scale define types of data in a way that is unknown to data protection laws. In their data processing agreements, they distinguish between data entered by users and data generated by systems or otherwise accessed, which shows that there is awareness about the de-facto predominance of indirect data collection. This explains that very often, there is

little room left for the individual to control what happens to their data, and that questions viability of traditional concepts of data protection laws such as privacy self-management, and that is also why some authors argue to expand the development of privacy-enhancing and privacy-preserving technologies that need to leverage on device data.

Another factor to consider is the different approach the legislators take. The EU is rights-based, the U.S.A. is harm-based, and China pursues a control-based approach, and different jurisdictions focus on different things, for example the U.S. legal landscape is mostly concerned customers, not all individuals (including employees). Probably the greatest difference between the U.S. and the EU approach to data protection is that European law is permission-based, meaning that a legal basis is always required for the processing of personal data, whereas in the US, the contrary is true, because data can generally be processed unless a law forbids such an activity.

Fragmentation and lack of harmonization are further problems that can be best explained in the area of marketing activities as well as employment law, both of which are areas of high importance to businesses: GDPR only mentions marketing in one of its Recitals but does not explicitly cover such activities; GDPR also has dozens of "opening clauses" with either allow or foresee for national provisions, even in such important areas like employee data protection. As a result, depending on the case in question, companies must consider various regulations on top of data protection rules. In the area of marketing, that would be consumer protection, E-commerce or competition laws; in the area of employment, that would be co-determination or legislation concerning health at work – the recent COVID crisis has shown how significant the intersection of different areas of law can be.

In addition, historically different legal traditions, deviations with respect to the maturity of privacy laws or with regards to transposition into national law, differences in the interpretation as to the scope of data privacy laws and in particular data subject rights – the right to information and the right to copy are perfect examples – as well as the inconsistent application of privacy laws at regulator level resulted in privacy being far less uniform than generally assumed, and GDPR did thus not result in a full harmonization of privacy laws. Given its definitions and its very broad material and territorial scope, some raised concerns that GDPR or similar privacy laws may become "the law of everything" which may lead to an extensive application of data protection rules which can hardly be prevented, because anonymization is hard to achieve and pseudonymization leaves personal information identifiable, and this way, privacy laws remain relevant. Since the use of encrypted or synthetic data does not work for certain processing operations, data protection laws may indeed govern most of what happens with (customer, employee) data within a business, leaving very little room for the avoidance of the application of laws that govern personal information and allow for data subject rights.

In the context of possible risks of Big Data and AI applications, many authors commented on the potential of Big Data and AI applications to conflict with a variety of basic privacy principles such as purpose limitation or fairness and transparency which seem to be rendered obsolete. Others underline that they observed that there is a risk of trade-offs between different data protection principles. Such tensions may arise between the principles of accuracy, fairness and privacy, for example: more data may lead to more accuracy, but at the expense of individual's privacy; if AI is tailored to avoid discrimination (if certain indicators are removed to that AI is fair),

this may have an impact on accuracy; if AI is tested to see if it may be discriminatory, it needs to be tested by using data that is labeled by protected characteristics, but that may be restricted under privacy laws that govern the processing of special category data.

As a reaction to the above-mentioned issues, there have been controversial discussion on how to address these risks. While some predict that new approaches are needed, others stress that existing legal framework shall be exploited, e.g., starting with well-established standards like accountability and joint controllership, which is particularly important as Big Data and AI applications in many cases involve more than just one controller, more than just one service provider, and more than just one location where data are processed and stored, on the contrary, data is being transferred internationally.

As for the existing legal framework, the problem is not only fragmentation and lack of harmonization, but also opposing legislative aspirations: a technical example is encryption which is desirable under privacy laws but may be legally prevented for reasons of crime prevention. This is both, a legislative and a provider trend as recent discussions around certain provider's filter functions show. A legal example is data localization: many countries around the globe already introduced data localization requirements, either for selected industries or for public service providers or for certain types of data (for example, government data, health records, payment information). Data localization has also been discussed as a reaction to the invalidation of the EU-US Privacy Shield, but there seems to be little awareness that global trade and investment agreements, which are legally binding, in fact address the issue of international data transfers and set forth (minimum) standards, including protections against unjustified data localization requirements. Therefore, any future legislation which foresees data localization may be challenged owing to the existing overarching trade law framework. Finally, it is worthwhile mentioning that specific risks of AI have been addressed in specific legislation, e.g., for autonomous vehicles or for facial recognition technology.

As regards factual difficulties, errors may occur at any stage, during the design of algorithms, or owing to underlying datasets being outdated, incomplete, incorrect or noisy, or due to wrong interpretation of results – this "relativity of results" is a human (awareness, training), not a technical problem. But another defiance is that the outcome of AI applications is based on statistical correlations, not causality, and this is quite often overlooked when AI is used.

In terms of GDPR-specific challenges and the question whether GDPR addresses specific risks of processing with the help of Big Data, ADM and AI, it can generally be said that GDPR's fundamental principles like accountability, transparency, data accuracy and quality, fairness, purpose specification as well as its permission- and risk-based approach (accompanied by appropriate technical and organizational measures) together with a dedicated set of individual rights form a sound foundation for data privacy. GDPR is also not silent on various topics that are highly relevant for Big Data, ADM, and AI, for example: consent, profiling, automated decision-making, data subject rights, admissible re-use of personal information, international data transfers, transparency, data security or special categories of personal information. But this is also an example of areas in which the framework might have failed: GDPR (definitions) are concerned with "original data", not "derived data", but that seems needed as the minority of data that is being processed in Big Data and AI applications has been

collected directly form the individual. These circumstances raise further questions from a business and an individual's perspective, e.g., with regards to copyrights database rights and legal personhood of robots, or regarding the idea of data ownership.

GDPR itself has numerous ambiguities and uncertainties. On the one hand, data subject rights are strengthened but on the other hand, there is also an emphasis on legitimate interests. GDPR Art 6 IV is another example, and some fear that compatible processing may lead to unlimited processing. There is also controversy about whether profiling under GDPR Art 22 shall be interpreted as a prohibition or a data subject right, and there is very little case law to explain GDPR Art 21, the "*right to object, on grounds relating to his or her particular situation*". It is also not always clear what has the quality of a decision (or similar legal effect): does that only apply to a final (job candidate selection, credit or housing application, etc.) decision or should this rather be regarded as a constant criterion for the design of Big Data and AI applications, and thus be applicable at every relevant processing phase. GDPR is perhaps not as far-reaching or future-proof in terms of data subject rights. Some U.S. laws already introduced "do not sell" as an individual's right, and if that is taken seriously, then this is more than what GDPR Art. 12 to 18 and 19 want – not just a "notification obligation regarding rectification or erasure of personal data or restriction of processing" in the sense of an onward duty, but preventing that an individual's personal information is provided to other (unknown, unlimited number of) entities and monetized. The fact that the standard of GDPR Art. 22 is only applicable if the decision is "*based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*" sounds like a guarantee, but it also shows that there is a limit to this right. Fully automated means that there is no human intervention at all, but this can be circumvented quite easily by implementing spot checks.

One of the most important observations is that many approaches have failed in practice, and that makes the viability of traditional data protection (i.e. rights based) concepts questionable: consent and privacy self-management does not seem to afford the desired individual protections, and it not the same like comprehensibility or replicability of individual decisions or the demand for making "true operators" known, which would be especially important as many controllers and processors may be involved in processing operations, but this is not what the front-end user of (online, mobile, etc.) applications gets to know. Consent is another well-established concept in privacy, but consent can factually hardly work given the information mismatch, and psychologically, privacy self-management does not work given the inconsistency between peoples' opinions on the relevance of privacy and their actual behavior which tells a different story.

The principle of accountability is a common thread running through data protection regulations, but the question is whether accountability as set forth in existing data privacy laws goes far enough to guarantee responsibility, liability, contestability, safety, and fairness together with an approach to data processing that includes sound risk assessment and human oversight and human intervention if need be. Even if certain requirements have already been laid down in law, they are still too weakly implemented in practice, for example, joint controllership does not seem to cover all relevant players which are involved in the data processing, and that in turn weakens accountability as such. That is why in summary, many believe that traditional rights-based concepts no longer fit the era of Artificial Intelligence.

Another factual problem is that it seems that certain mechanisms have simply not been used in practice, for example GDPR Art. 80, the representation of data subjects which allows the "*data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law*."

The above findings show that it is worthwhile investigating if algorithmic (autonomous) decision-making implies that (data protection) laws need adjustment. As a reaction to the emergence of Big Data and AI as an economic and societal given lead to a variety of initiatives that dealt with the issue of addressing risks of Big Data and AI. A common feature of many approaches is that they focus on established principles like accountability, purpose specification, collection and use limitation as well as data quality, security, but also stress the need for enhanced transparency and individual participation which they claim shall be taken more seriously and enforced correspondingly. However, the nuances within call for "enhanced transparency" and "individual participation" goes beyond existing standards, and these two demands show that what is at stake here is the desire for further development of existing conditions which would result in new standards. The right to participation is more than the right to information, and if "enhanced transparency" includes the need for public registries for (audited) AI apps, this is also more than a mere public-facing privacy notice with a brief explanation of the underlying logic.

Recently, there has been a significant increase of initiatives that deal with the issue of addressing risks of Big Data, ADM and AI at international, intergovernmental, EU as well as local / national level. Numerous proposals address the matter from different perspectives, e.g., from a regulatory, governance, assessment, data subject rights perspective. As for the latter, there are debates about data ownership to fight data monetization, the right to human intervention, enhanced redress mechanisms including rights of association action, the right to participation or the right not to be subject to a discriminatory decision and secret profiling. Moreover, in the context of individual's rights, the idea of having personal information replaced rather than the processing restricted has been suggested because that might be a more effective way to avoid re-identification.

Some authors ask for additional (specific) AI laws, for example in the area of employee data protection, for the "Internet of Things" or to facilitate the handling of research data; other proposals discuss the introduction of new duties such as a termination obligation in the event a system gets out of control or underline the need for enhanced transparency, including making true operators known. Further initiatives deal with the idea of labeling and the introduction of specific liability regime in accordance with product liability regulations which should cover all involved providers. Certain recommendations for the future regulation of AI call for the strict prohibition of certain technology such as facial recognition. Some suggest the use of anonymized and synthetic data where appropriate while others stress the importance of certifications and the need for external control mechanisms such as audits including DPIAs being conducted by external auditors or call for the establishment of AI specific oversight bodies and technical standardization. Further propositions deal with the introduction of

mandatory public archives; others reference antitrust law in view of the market power of GAFAM and the like. Given that mass application of Big Data, AI and automated decision-making not only affect individuals, but society, many initiatives elaborated on embedding ethics into Big Data, ADM, and AI, and focused on a human-centric approach that does not harm, but which serves society.

Despite the fact that there are already laws applicable to certain use cases, certain processing activities or certain types of data, or certain businesses (covered entities), and notwithstanding the regulation on Artificial Intelligence the European Union drafted, an overarching analysis of propositions relating to AI applications shows that a majority of proposals suggest that any future AI regulations or AI principles shall take the following into consideration: accountability and responsibility, human control of technology, safety and security, transparency and explicability, fairness, non-discrimination as well as privacy and the promotion of human values.

For the above reasons, the following conclusions which also form the main hypotheses underlying this work, can be drawn. It can first be determined that privacy self-management as a rights-based concept failed, for a variety of reasons, for example considering that data subject rights do not lead to the desired protections, taking into consideration that valid consent is difficult to imagine given the existing information asymmetries, owing to admissible or secondary use of personal information, or due to transparency obligations being restricted. Second, transparency therefore needs to be further developed, moving from mere notice-level summary-format information which addresses individuals in the direction of meaningful information on underlying algorithms for all data subjects concerned as well as public registries allowing the public to access relevant information such as details on risk evaluations, mitigation measures and information on sub-processors. This may increase the chances for the needed social debate for this important technology that has the potential to shape our lives, and it could also allow to better exercise individual's rights and foster individual engagement, which is a factor that should not be underestimated as a single activity has brought down an entire data transfer mechanism. The success of such initiatives can be compared to the functioning of the fourth pillar of the state which, in addition to the executive, legislative and judicial branches, can influence developments through reporting and public discussion. This idea forms the transition to the next conclusion and leads to the third hypothesis, which is that new controls are needed that are based on public debate and include new values which are not only judged from an individual's perspective, but consider the societal perspective since issues AI's dual use character, its potential for surveillance and potential impact on human rights and democracy as well as digital workforce aspects show that there is an important intersection between individuals rights and societal values.

PART 4: List of publications

The following publications are relevant to the research topics:

"*New approaches to Big Data and Artificial intelligence regulation*" published in STUDIA IURIDICA Essays of Faculty of Law University of Pécs, Yearbook of 2019-2020, pp. 87-107 (https://journals.lib.pte.hu/index.php/studiaiuridica/issue/view/495/125).

„*Datenschutzrechtliche Probleme und mögliche Lösungsansätze bei Big-Data-Anwendungen aus bisheriger und neuer deutscher Perspektive*" published in JURA 2019, pp. 239-254 (https://jura.ajk.pte.hu/JURA_2019_2.pdf).

"*The Role of Data as Potential Entry Barriers*" published in STUDIA IURIDICA Essays of Faculty of Law University of Pécs, Yearbook of 2017-2018, pp. 43-58 (https://journals.lib.pte.hu/index.php/studiaiuridica/issue/view/496/126).