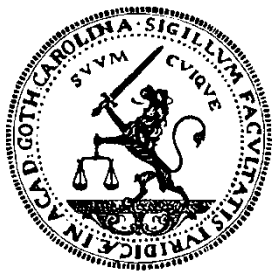

FACULTY OF LAW
Lund University

C hinara Gasimova

Privacy and Transparency in an AI-driven world: Does algorithmic transparency fit on data privacy under GDPR?

JAEM03 Master Thesis
European Business Law
30 higher education credits

Supervisor: Petra Gyöngyi
Term: Spring 2023

TABLE OF CONTENT

SUMMARY

The quick advancement of AI technology has changed how we relate to our environment. AI is reshaping almost every business nowadays. Data privacy issues have surfaced as AI algorithms are increasingly employed in decision-making processes. Algorithmic transparency has become essential for preserving data privacy in an AI-driven world. Understanding how an algorithm generates decisions and the elements that go into those decisions is referred to as algorithmic transparency. Algorithmic transparency can guarantee that the use of AI technology does not violate people's rights to privacy by encouraging transparency and accountability.

A review of existing AI technologies and their effects on data privacy is given at the outset of this thesis. Then, algorithmic transparency and how it contributes to data privacy are explored under the given topic. The GDPR and the AI Act that regulates data processing and controls the usage of AI technology are examined in the thesis and look at the relationship between privacy and transparency under the GDPR. Besides, it analyses how AI affect privacy and transparency. It questions whether the GDPR can cover AI-related issues and where the AI Act stays with respect to privacy and transparency. To do so, various industrial fields are touched on throughout the thesis, offering a thorough knowledge of the benefits and drawbacks given by the usage of AI technology.

The thesis also stresses the importance of limiting transparency considering "Black Box" algorithms, sensitive information, trade secret and other Intellectual Property. Finally, emphasising the legal and regulatory frameworks controlling the use of AI technology, it explicitly explores the impact of algorithmic transparency on data privacy. Thus, this study intends to evaluate how well the GDPR protects privacy and transparency in a world powered by AI and how effective is the transparency requirement under the AI Act.

PREFACE

This thesis is the result of weeks, months, or even years of effort, devotion, and academic study. I have had the honor of delving deeply into a subject that fascinates me and exploring it from a variety of perspectives, learning new information. This thesis aims to add to the body of information already known about the issue by providing a unique contribution that illuminates it in a fresh way. I have used various techniques throughout the study process to reach my results, including literature reviews, empirical analysis, and critical thinking.

Writing my thesis has given me the chance to consider the importance of the subject, its wider ramifications, and the gaps in the existing literature that I have attempted to address. In addition to academics working in the subject, I hope my results will also be helpful to the general public, who might gain from the information provided.

I want to sincerely thank everyone who contributed to the success of the Lund University master's program in European Business Law. I am grateful to my supervisor Petra Gyöngyi, who helped me with the research process for their crucial advice and assistance. She helped me learn more about my research topic and assisted me in making my thesis' content and structure better, and supported me during the whole research process. I would also like to thank all of the staff at the Faculty of Law at Lund University, Julian Nowag, Xavier Groussot, Eduardo Gill-Pedro, Ana Nordberg, and others, for their wonderful assistance during my master's program.

Besides, I would like to express my gratitude to the Swedish Institute (SI) team for all the assistance and possibilities they provide for studying at Swedish institutions as a holder of the SI Scholarship for Global Leaders. Finally, I want to express my gratitude to my colleagues, family and friends for their support and tolerance throughout this challenging but ultimately fulfilling journey.

Thank you!
Chinara Gasimova
Lund, May 2023

ABBREVIATIONS

AG	Advocate General
AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
AILD	AI Liability Directive
CJEU or ECJ	Court of Justice of the EU
Commission	European Commission
DSA	Digital Services Act
DMA	Digital Markets Act
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
MSs	Member States
WP29	Article 29 Working Party
XAI	Explainable AI

1. INTRODUCTION

As the technology and the role of Artificial Intelligence (AI) develop more rapidly, the regulatory framework governing it inevitably becomes more complex and comprehensive. The impact of AI on all aspects of our society, businesses, and life, in general, is undeniable. Today, AI systems are making decisions that affect people's lives in many aspects, and this impact is expected to grow even more in the future. Both individuals and organizations can benefit from profiling and automated decision-making, which can result in enhanced productivity and resource savings.[1] Transportation, healthcare, education, medicine and many other fields can all gain from these processes.[2] However, despite all the benefits, the increasing role of AI also raises some issues to consider, such as guaranteeing privacy, transparency, and compliance of existing legislation to rapid change in an AI-driven world.

General Data Protection Regulation (the GDPR) is the most comprehensive piece of legislation on data protection presently in effect that preserves business transparency and extends data subjects' rights to privacy.[3] However, as Kalliopi Spyridaki, Chief Privacy Strategist at SAS Europe, said, the GDPR only directly addresses a few critical issues related to AI, which Article 22 of the GDPR contains a number of these, such as automated decision-making and profiling.[4] Therefore, narrowly covered Article 22 clearly cannot cover and answer all matters related to AI with respect to privacy and transparency issues. For example, the GDPR does not provide a detailed guide for algorithmic explanation and transparency in relation to automated decision-making, including profiling, which causes different interpretations that become the subject of debate. Thus, some discussions on practices for data gathering and the privacy of users, and transparency of AI tools go beyond the GDPR.

[1] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, (2017), 17/EN WP251rev.01, 5.
[2] Ibid.
[3] Michael Kretschmer, An Pennekamp and Klaus Wehrle, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web', (2021), ACM Transaction on the Web, Vol. 15, No. 4, Art 20, 1, 21.
[4] Kalliopi Spyridaki, 'Chief Privacy Strategist, SAS Europe, "GDPR and AI: Friends, foes or something in between?', sas.com, https://www.sas.com/en_us/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html#, accessed 31 January 2023.

Furthermore, the EU's Artificial Intelligence Act[5] (the AI Act) answers the questions regarding AI systems. Specifically, the AI Act requires transparency from AI tools, including those under Articles 13, 14, and 52. However, under the Act, it is still not clear enough what data subjects' needs and expectations of the AI disclosure process are. Besides, the transparency duty in the AI Act creates another concern about privacy. It is because AI processing requires numerous data sets, which may also contain sensitive personal data, and it needs strong algorithm protection. For example, suppose companies do not comply with privacy requirements under the GDPR, abuse the transparency duty under the AI Act, or cannot create a safe environment for data. In that case, it poses a severe threat to privacy. The privacy concerns that ChatGPT brings to the table can be one of the relevant examples in this regard.[6] Thus, there is a need for detailed regulation in this respect to make a balance between privacy and transparency in an AI-driven world.

Thus, this thesis will analyse privacy and transparency under the GDPR and examine the impact of AI on privacy and transparency. The connection between both AI and privacy and AI and transparency will be discussed under the given topic.

1.1. The purpose of this research and the research questions

One of the primary purposes of this study is to assess the effectiveness of the GDPR in ensuring privacy and transparency in an AI-driven world. Besides, it aims to critically discuss the AI Act in the light of transparency and privacy and stress the concerns arising from it. Thus, the following research questions will be addressed to achieve the goal of the thesis:

1. What do privacy and transparency mean in GDPR?
2. How does AI affect privacy and transparency?
3. How does the algorithmic transparency requirement of the AI Act affect privacy?
4. Is GDPR adequate in ensuring privacy and transparency in an AI-driven world?

[5] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act (AI Act)) and Amending Certain Union Legislative Acts (Brussels, 2021) COM(2021) 206 final.
[6] Politico, 'ChatGPT is entering a world of regulatory pain in Europe', (2023), https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/, accessed 10 May 2023.

1.2. Research methodology and sources

The legislative framework for data protection and privacy in the European Union (the EU) is examined in this thesis and uses a mixed-methodologies that includes legal dogmatic, descriptive, and analytical legal research methods with a focus on the GDPR and the AI Act. First, examining legal texts and principles to comprehend their application and implications entails legal dogmatic research. Accordingly, the thesis will employ this method to explore the legal frameworks. It will be used legal sources by legal scholars to describe tools and approaches created for identifying and interpreting the legal framework, namely, the GDPR and AI Act. Followingly, the thesis will discuss the GDPR and AI Act's implementation and its efficacy in regulating AI systems in this context. Besides, descriptive research focuses on describing and recording occurrences or issues as they occur in an AI-driven world.

In addition, in order to better understand complicated concepts and information, analytical research requires disassembling them into simpler components. The GDPR and AI Act's numerous provisions and their effects on data privacy and the advancement of AI will be examined in this research by involving an examination of legal arguments, scholarly opinions, and judicial reasoning to evaluate the strengths and weaknesses of legal positions. Thus, the goal of the study is to present a thorough analysis of the GDPR and the AI Act utilizing several research methods to comprehend their rules and effects on privacy, transparency, and the advancement of AI.

Besides, when it comes to the legal sources in this thesis, both primary and secondary legal sources are analysed to highlight the situation for data protection and privacy in the EU, focusing on the GDPR and the AI Act. As primary sources, the EU's law, other legal publications on the subject area, the Court of Justice of the EU (CJEU), and the EU's Member States' (MSs') national case law concerning privacy and transparency in AI will be used. Accordingly, the GDPR and the AI Act, as the main pieces of law, control data protection and privacy in the EU, and they will be in-depth examined to determine some provisions and consequences for AI systems. Moreover, a selection of case law will be included to demonstrate the difficulties and opportunities of regulating AI systems to guarantee compliance with data protection and privacy legislation in order to obtain more profound knowledge of the interpretation and practical consequences of the GDPR and the AI Act.

With regard to the secondary sources of law, books, scholarly articles, research papers, journals, official legal blogs, commentary on the pertinent issue, reports, and publications pertaining to the provided topic from the EU authorities are examples of secondary sources. These documents will be evaluated to find new trends, challenges, and best practices in the relevant filed and to better grasp the theoretical and practical elements of privacy and transparency issues in AI.

1.3. Delimitation

This thesis examines the legal ramifications of AI systems for data processing and the protection of personal data under the legal framework of the EU. The GDPR and the AI Act are discussed explicitly as the primary legislative instruments controlling data protection and privacy in the EU. In order to ensure compliance with the GDPR and the AI Act, the research will look at the potential problems associated with regulating AI systems. This thesis does not cover the Digital Services Act (DSA) and the Digital Markets Act (DMA), which are close to AI Act, and additional legislative initiatives to regulate the AI environment.

Besides, the relevance of algorithmic transparency in preserving data privacy in an AI-driven environment will be the core topic of this thesis. However, it will adopt a broad approach that touches various industries rather than concentrating on a single field or business. This is due to the fact that possible threats and difficulties to data privacy are a universal issue in the context of AI technology rather than being specific to any one industry. With an emphasis on its use across several areas and industries, this thesis seeks to thoroughly understand the significance of algorithmic transparency in preserving data privacy in an AI-driven world.

2. PRIVACY AND TRANSPARENCY UNDER GDPR

GDPR is designed to safeguard the personal data and privacy of EU citizens and residents. To achieve so, the GDPR grants people more control over their personal data and obliges businesses and data controllers to disclose more information about how they collect, process, and store that data. The GDPR includes several principles and provides several rights to data subjects aimed at protecting individuals' privacy rights and promoting responsible data practices by businesses. Besides, the GDPR under Article 23 ("data protection by design and by default") requires companies to apply necessary organisational and technical measures to put data protection principles into practice while designing their systems, products, and services.[7]

Furthermore, one of the key requirements of the GDPR is transparency. According to Recital 26, in relation to the natural persons involved, any processing of personal data must be "lawful, fair and transparent".[8] Under the GDPR, there is a general requirement for transparency that covers three key areas: 1) how data subjects are educated about the fair processing of their data; 2) how data controllers interact with data subjects regarding their GDPR rights; and 3) how data controller make it accessible for data subjects to exercise their rights under the GDPR.[9] In other words, regarding transparency, the GDPR mandates that businesses use clear and plain privacy policies on how users' personal data will be handled.

Furthermore, Articles 12, 13 and 14 of the GDPR outline what information data subjects have a right to know about the processing of their data. In addition, Recital 58 of the GDPR stresses the importance the transparency and provides guidelines to data controllers on how to achieve this requirement.[10] Besides, without access to data, it is difficult to achieve transparency, followingly, Articles 15 and 34 of the GDPR require access to data.

Thus, the GDPR aims to strike a balance between safeguarding individuals' privacy and enabling companies to use their personal data in a transparent manner for legal purposes.

---

[7] General Data Protection Regulation (hereinafter "GDPR"), (Regulation (EU), 2016/679), Art 25(1), (2).
[8] Ibid, Recital 26.
[9] Data Protection Working Party, 'Guidelines on transparency under Regulation' (2016/679), 17/EN WP260, Art 29, 5.
[10] GDPR (n 7), Recital 58.

2.1. Deriving privacy from the legal framework: GDPR

Privacy constitutes a key value of individuals and democratic societies. Several legal frameworks have been adopted to protect privacy both at international and regional levels. For example, the European Convention on Human Rights under Article 8[11], the Universal Declaration of Human Rights under Article 12[12], and the International Covenant on Civil and Political Rights under article 17[13] enshrine privacy as a fundamental right. In addition, the Charter of Fundamental Rights of the EU, under Articles 7 and 8, protects the interests of data and privacy.[14] Besides, the GDPR, as a regional human rights instrument, also safeguards privacy as a fundamental right under certain provisions, which will be addressed below. The GDPR lays out standards and requirements to protect the privacy of individuals while gathering, utilising, and processing their personal data by organisations.

2.1.1. Privacy requirements under the GDPR

To start with, the GDPR under Article 4(1) defines "personal data" term as any information that relates to an individual that identifies or may identify them.[15] GDPR contains many requirements and legal bases for privacy protection, such as obtaining express and informed consent before gathering, processing, and storing the personal information of individuals, as required by Article 6(1) of the GDPR. It is worth mentioning that consent is only one of the legal bases to collect, handle and/or store individuals' personal data, along with five further justifications listed in Article 6.[16]

While it may appear simple, the GDPR has severe requirements regarding consent. So, such consent must be freely given, in other words, individuals must clearly know what they are consenting to when giving their consent.[17] Besides, organisations must offer persons a simple and easy way to withdraw such consent.[18] Thus, on the one hand, these requirements can be

[11] The European Convention on Human Rights (ECHR), 213 UNTS 221 (1950) (entered into force 3 September 1953).
[12] Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810 (1948).
[13] The International Covenant on Civil and Political Rights (1966), 999 UNTS 171 (entered into force 23 March 1976).
[14] Charter of Fundamental Rights of the European Union, 2012/C 326/02.
[15] GDPR (n 7), Art 4(1).
[16] See in more detail: GDPR (n 7), Art 6(1).
[17] GDPR (n 7), Recital 32.
[18] GDPR (n 7), Art 7(3).

challenging for companies, and on the other hand, it provides individuals with more power over their personal information.

Furthermore, the GDPR includes several principles, obligations and limitations on data processing to safeguard privacy. For instance, the GDPR outlines 'purpose limitation' in Article 5(1)(b), which mandates that personal data must only be gathered and processed for clear, unambiguous, and legitimate purposes and must not afterwards be treated in a way that is inconsistent with those purposes.[19] Since 'purpose limitation' prevents the exploitation of individuals' personal information and promotes the appropriate use of personal data, this means that the purpose limitation is what makes data protection work. Notably, as a core of data protection, purpose limitation permits the implementation of the other GDPR criteria outlined in Article 5(1), including data minimisation, integrity and confidentiality, accountability, storage limitation, and accuracy.[20]

Moreover, to come to data minimisation, Article 5(1)(c) of the GDPR restricts data collecting, keeping and use to only that which is essential and pertinent to achieve the purpose that should be acquired.[21] Besides, as this GDPR requirement also limits data storage to a predetermined amount of time,[22] it may not be compatible with big data and can go against data minimisation. It is because big data mining needs to analyse large amounts of data to be effective,[23] on the other hand, data minimisation leads to a lower risk of data breaches and safeguards privacy rights. On the grounds of that, figuring out which data is necessary for a given purpose and complying with data privacy laws, specifically with the GDPR, can be challenging for companies. Thus, they must carefully strike a balance between data analysis and the requirement to respect individuals' privacy and adhere to data protection laws.

In addition, Article 5 of the GDPR requires organisations to take adequate technical and organisational measures to provide appropriate data security.[24] Thus, personal data's integrity and confidentiality must be guaranteed to safeguard individuals' privacy rights. Integrity and

[19] GDPR (n 7), Art 5(1)(b).
[20] See in more detail: GDPR (n), Art 5(1).
[21] GDPR (n 7), Art 5(1)(c).
[22] See in more detail: GDPR (n 7), Art 5(1)(c).
[23] Nils Gruschka, Vasileios Mavroeidis, Kamer Vishi and Meiko Jensen, 'Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR', *Research Group of Information and Cyber Security*, (2018), University of Oslo, Norway, arXiv:1811.08531v1 [cs.CR], 2.
[24] See in more detail: GDPR (n 7) Art 5(1)(f).

confidentiality appear to be the aspects of cybersecurity that are most related, but it is not just about how organisations store and transfer data but also covers how to access, modify, and remove the data.[25] Thus, integrity and confidentiality are crucial for protecting privacy rights. For example, the Maximilian Schrems v Facebook Ireland Limited cases (Schrems 1[26] and Schrems 2[27]) could be a good example to emphasize the requirement for strict data protection laws, transparency, and responsibility in AI systems, all of which are necessary to protect individuals' privacy. Although the Schrems cases focused especially on data transfers between the EU and the US, and they do not particularly deal with privacy in AI applications, however, the fundamental ideas of data protection, privacy, and reasonable safeguards also apply to AI systems.

Besides, Article 5(2) and 24 of the GDPR establish accountability requirement, which demands organisations process personal data in a proactive and comprehensive manner in order to achieve GDPR compliance.[28] According to this principle, organisations carry responsibility and create responsible practices to ensure that they follow all principles and respect data subjects' rights regarding processing their personal data. In other words, accountability symbolises the shift of duty for preserving personal data towards data controllers (the supposed strong party) and data subjects (the supposed weak party), therefore, it is an essential requirement within the current EU data protection legislation[29] to ensure the privacy of individuals.

Additionally, Articles 5(1)(b) and (e) of the GDPR regulate storage limitation, the idea behind storage limitation is that data should not be kept around for any longer than is absolutely essential.[30] The data should be deleted as soon as it has been used for the intended purpose and is no longer required.[31] However, it is worth stating that GDPR provides exemptions for both purpose and storage limitations in regard to personal data processing for purposes of research

[25] Peyo Hristov, William Dimitrov, 'SIMPRO 2018: Challenges and opportunities for sustainable development through quality and innovation in engineering and research management', (2018), University of Petrosani, 8th International Multidisciplinary Symposium, 3.
[26] *Maximilian Schrems v Facebook Ireland Limited* (Case C-498/16), Judgment of the Court (Third Chamber) [2018] ECLI:EU:C:2018:37.
[27] *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* (C-311/18) [2020] ECLI:EU:C:2020:559.
[28] See in more detail: GDPR (n 7) Arts 5(2), (24).
[29] Zhasmina Radkova Kostadinova, 'Purpose limitation under the GDPR: can Article 6(4) be automated?' (master thesis, Tilburg University, the Netherlands), 20.
[30] GDPR (n 7), Art 5(1)(b), (e).
[31] Ibid.

under Article 89.[32] What is more, the controller is responsible for ensuring the accuracy and update of the data, as required in Article 5(1)(d) of the GDPR. Apparently, there is also a logical connection between storage limitation and accuracy. Thus, assuming the accuracy principle is not followed, then personal information would be deemed incompatible with the purpose limitation.

Since the relevant principles are mentioned, it is appropriate to state data subject rights apply when dealing with organisations that process their personal data. Subsequently, data subjects have the following rights to privacy and protection of their personal data based on Chapter 3 of the GDPR ("Rights of the data subject):[33]

i) Right to transparent information, communication and modalities to exercise rights;
ii) Right of access one's personal data;
iii) Right to rectification;
iv) Right to erasure;
v) Right to restrict of processing;
vi) Right to data portability;
vii) Right to object;
viii) Right to know that they are/were subject to automated decision-making.

Hence, the GDPR has a variety of provisions, including principles and data subjects' rights, designed to uphold individuals' privacy rights. By invoking these principles and rights, it is possible to ensure privacy and encourages organisations to create secure data practices for protecting the personal data of individuals.

2.1.2. Privacy by Design and Default in IT systems

The GDPR also mandates the application of Privacy by Design and Default to some extent.[34] "Privacy by Design and Default" requires all systems must be created, set up, and managed with data protection as their main objective.[35] Thus, the requirements related to the design of

[32] See in more detail: GDPR (n 7) Art 89.
[33] See in more detail: GDPR (n 7) Art 12-23.
[34] See in more detail: GDPR (n 7) Art 25 and Recitals 74-7.
[35] Ibid.

products and services, such as privacy by design and privacy by default, are essential tools for safeguarding the right to privacy.

First, according to the "privacy by design" approach, data protection and privacy are integrated into all stages of technology development, from the initial stages of conceptualisation to deployment, use, and eventual disposal.[36] Accordingly, privacy by design includes not only encryption but also protocols for anonymous communications, attribute-based credentials, and private database searches, in addition to various methods that businesses can use.[37] Thus, to determine compliance with the GDPR, system designers should carefully examine all systems' algorithms, internal data structures, and configuration settings from beginning to end.

Then, another notion that the GDPR introduces is "privacy by default", which guarantees that personal data are automatically protected in any given IT system or business activity.[38] Even if a person does nothing, their privacy is still protected as a system or service is designed to safeguard privacy by default, so an individual does not need to do anything to protect their data.[39] For instance, the default setting should not gather data like location, contacts or other shared information online through social networking platforms unless the user distinctly permits it. Hence, Privacy by Design mandates that the system uses privacy-respecting settings by default in order to achieve the highest level of privacy.

While privacy by design emphasises the significance of taking data privacy into account at the first stage by focusing on incorporating privacy protections into systems and processes, privacy by default gives consumers particular tools to regulate how their personal data is gathered, processed, and shared. Thus, privacy by design and default is a proactive measure to identify and resolve potential privacy issues. Organisations can contribute to ensuring that personal data is processed in a fair, transparent, and secure manner by integrating privacy into the design of systems and processes and by making privacy the default setting.

[36] Anna Romanou, 'The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise', Computer law & Security review, (2018), Vol 34, Issue 1, 99-110. (Article)
[37] Roslyn Layton and Simone Celant, 'How the GDPR compare to best practices for privacy, accountability and trust', (2017), 2017/TPRC45, 19
[38] Ann Cavoukian, Jules Polonetsky and Christopher Wolf, 'SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation', Springerlink.com, (2010), IDIS 3:275–294 DOI 10.1007/s12394-010-0046-y, 290
[39] Ibid.

Nowadays, almost all businesses moved to online channels, and when it comes to online businesses, they should consider Privacy by Design and Default principles while developing and implementing their services. Thus, without denying the role of other principles, it is no exaggeration to claim that Privacy by Design and Default is the core of the GDPR for online businesses. However, it is not an easy task for all online businesses as they should be aware of many risks considering data collection, encryption, privacy and transparency. Because depending on the activity and size of the company, not all online businesses are set a limit to receive information that they may need, which is a requirement under Articles 5(1)c and 25 of the GDPR.[40]

Moreover, as there are no standards or exact methods for encryption and other security measures under GDPR, it can be problematic to avoid data breaches and misuse or unauthorized access to personal data. Hence, companies should prioritize privacy and data protection in their design and development processes to overcome these issues. In addition, as the GDPR provides data subjects a right to control over their personal data, including the ability to delete, modify and other rights under Articles 12-23 of the GDPR[41], businesses have to follow requirements. However, some companies might make it challenging for customers/data subjects to access or manage their data, which may leave them open to privacy concerns.

Besides, when it comes to AI-powered privacy systems, AI systems are trained by the amount of data, thus, it is protected by data protection and privacy laws. Accordingly, as the GDPR applies to AI-powered privacy systems, they must comply with all the GDPR requirements, including data privacy and transparency. However, AI algorithms and procedures can be difficult to ensure data privacy. It is because as AI algorithms include a large amount of data processing, it can be challenging to verify that privacy controls are enforced adequately at every level of the data process. Apart from the complexity of AI algorithms, it is also not easy to have full control over AI-powered privacy systems to monitor or guarantee that privacy requirements are always followed.

[40] See in more detail: GDPR (n 7) Arts 5(1)c and 25.
[41] See GDPR (n 7) Arts 12-23.

2.2. View of transparency in the GDPR

The concept of transparency has been of significant importance, especially in the context of governance and data sharing throughout history. Technological developments and the growing significance of data in the digital era have influenced the development of transparency. Consequently, transparency has grown more crucial in recent years when it comes to privacy and data protection. Businesses are now responsible for fostering an environment of openness and respect for their customers' data. In light of this progresses, some countries have passed data protection legislation with provisions with respect to transparency. The growth of transparency has also been considerably influenced by the GDPR. As transparency has an impact on many crucial areas, it is worth mentioning that the fundamental tenet of the GDPR is transparency.

According to Article 5(1)(a) of the GDPR, personal data must be processed fairly, legitimately, and transparently in regard to the data subject.[42] Moreover, many provisions in the GDPR address transparency in data processing, which focuses on educating data subjects better about how their personal data is processed and giving them more control over it. For instance, Articles 12, 13 and 14 of the GDPR are the main provisions addressing the transparency requirements that derive the responsibility for organisations to be transparent under the right to be informed.[43] In addition, the notion of transparency is addressed explicitly in Article 58, which also offers guidance on how to put this principle into practice.[44] Besides, the requirements under Articles 15 and 34 of the GDPR promote transparency since they require data controllers to give data access to data subjects.[45]

2.2.1. The right to be informed (transparency): Articles 12, 13 & 14 GDPR and Recital 58

Article 12 of the GDPR is a general provision particularly relating to transparency, and it provides the requirements for "transparent information, communication, and modalities" with data subjects, accordingly, Article 12 mandates that controllers[46]

[42] See in more detail: GDPR (n 7) Art 5(1)(a).
[43] See in more detail: GDPR (n 7) Arts 12-14.
[44] See GDPR (n 7) Art 58.
[45] See GDPR (n 7) Art 15, 34.
[46] See in more detail: GDPR (n 7) Art 12(1-3).

i) give data subjects clear and explicit information with easy-to-understand language about how their personal data is processed;
ii) create an accessible environment for individuals to exercise their rights mentioned in the GDPR; and
iii) ensure availability when the data subject has requests regarding their personal information.

Article 12 of the GDPR is crucial to encourage transparency and engagement with data subjects. It provides general information on the direct dialogue between the controller and the data subject. Then, Articles 13 and 14 define more specific obligations for data controllers regarding processing personal data before data subjects.

Followingly, per Article 13 of the GDPR, controllers are obliged to give specified information to data subjects when personal information is obtained from them. This includes information about the purposes of data processing, the legal basis for processing, the categories of personal data being processed, and the recipients or categories of recipients of the data.[47] Besides, Article 14 of the GDPR has very similar content to Article 13.

To come to Article 14, while Article 13 is applicable when personal data is taken directly from the data subject, Article 14 is applicable when personal data is received from external sources rather than directly from the data subject. Accordingly, when personal data is not obtained directly from the data subject, Article 14 of the GDPR requires the data controller to give information to the data subject about such processing.[48] Thus, regardless of whether the data was obtained directly from the data subject or other third parties, Articles 13 and 14 combined to ensure that the data subject has access to appropriate information concerning the processing of their data.

Thereby, Articles 12-14 of the GDPR set out numerous steps relevant to the obligations to provide information to the data subject about the processing of their data. In other words, data subjects have the right to be informed under the GDPR about why, where and for how long their personal data is collected, how they will be used and with whom they will be shared. Thus,

[47] See in more detail: GDPR (n 7) Art 13.
[48] GDPR (n 7) Art 14.

no records should be kept in secret by data controllers regarding individuals' data processes. Moreover, one of the essential aspects of Articles 13 and 14 is the controller must carry out the obligations outlined under these Articles without the data subject's request.[49] Hence, Articles 13 and 14 seek to inform users instantly of the intended data collection without requiring them to do anything, such as reading long privacy notices or policies.[50]

Furthermore, Recital 58 of the GDPR emphasises how crucial it is for controllers and data subjects to communicate transparently and clearly regarding processing data subjects' information. It underlines the necessity for controllers to give data subjects clear, accessible, and intelligible information about how their personal data is processed in order to guarantee that data subjects are fully informed about how their personal data is handled and can exercise their rights enshrined under the GDPR.[51]

Thus, Articles 12, 13 and 14 of the GDPR are essential with respect to transparency. These provisions give data subjects more transparency and control over their personal data and ensure data security in turn. Along with the Articles, Recital 58 also provides guidance on their application and stresses the importance of transparency. In addition, since mentioning transparency, it is also appropriate to state about access to information, specifically Articles 15 and 34 of the GDPR, because they are important to ensure transparency.

2.2.2. Access to information: Articles 15 and 34 of the GDPR

Under the GDPR, transparency and access to information are closely associated since transparency makes it possible for individuals to exercise their right to access their personal data and see how their personal data is being handled. Individuals have the right to access their personal data and information about how it is being processed under Article 15 of the GDPR.[52] While the GDPR protects individuals' personal data and gives them the right to be informed about their data, then it is also worth notifying individuals about the data breaches that have

[49] Armin Gerl and Dirk Pohl, 'Critical Analysis of LPL according to Articles 12 - 14 of the GDPR', (ARES 2018, Hamburg, Germany), DOI: 10.1145/3230833.3233267, 3.
[50] Sandra Wachter, 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', Oxford Internet Institute, University of Oxford and The Alan Turing Institute, British Library, (London, United Kingdom, 2018), 18.
[51] GDPR (n 7) Recital 58.
[52] GDPR (n 7) Art 15.

occurred. Accordingly, Article 34 of the GDPR requires data controllers to warn persons who have been affected by personal data violations.[53]

The two most crucial facts are that Article 15 of the GDPR governs the right to access personal data and that specific information must be made available upon request. Nevertheless, it is not clear whether this right applies to data that has been recombined with other data, for instance, scoring or profiling.[54] Besides, other concerns are how to get access to automated decision-making, which Article 15, together with Articles 13 and 14 of the GDPR, provides this right and some intellectual property rights, specifically trade and business secrets.[55] The concerns here are about balancing the right to access data and protecting some other rights, such as privacy and making a clear assessment to give individuals the right to access and use such data. Furthermore, since data subjects have a right to access data, the question arises whether they can use such data in an unrestricted way or whether there are restrictions in this regard.

Because the GDPR does not provide a clear and exact answer to these questions, such uncertainty leads to other issues to consider. For example, when data subjects use their right to access data, the outcome of such data processing may not always be related to the data subject, meaning they might get more information. Moreover, when it comes to getting information about automated decisions, it is not clear whether it is enough to be informed about the technology used in automated decisions or whether an explanation of the precise decision-making method is also included. In other words, the right of data subjects to obtain under Article 15 'meaningful information about the logic involved'[56] is open to interpretation and questions how deep data subjects can go to get information concerning automated decision-making. Besides, the information data subjects obtain when exercising their rights to access data may include trade and business secrets, then it may jeopardise the controller's trade and business secrets or may harm such interests.[57]

[53] GDPR (n 7) Art 34.
[54] Indra Spiecker genannt Döhmann, 'The legal framework for access to data from a data protection viewpoint – especially under the GDPR', Nomos eLibrary, (2023), https://doi.org/10.5771/9783748924999-175, http://www.nomos-elibrary.de/agb, 189.
[55] Ibid 189-191. See also Andrew D. Selbst and Julia Powles, 'Meaningful information and the right to explanation', International Data Privacy Law, (2017), Vol. 7, No. 4, 235, 242.
[56] GDPR (n 7) Art 15.
[57] Döhmann (n 54) 189-190.

Besides, as Article 15 of the GDPR grants data subjects access to their personal data, there is a connection between Articles 15 and 22 of the GDPR. Article 22 of the GDPR also emphasises the value of transparency in the use of personal data and grants people the right to know and be in control of how their data is used.[58] However, while addressing AI, Article 22 is the first GDPR article worth mentioning, as it discusses the application of automated decision-making in particular. Together, these two articles, Articles 15 and 22, make sure that data subjects have control over their personal data, including the right to know how it is handled, additionally, Article 22 provides the ability to challenge automated decisions making processing.

Moreover, another issue worth discussing since mentioning transparency under the GDPR is the notification requirement in Article 34, which requires the controller to notify the affected individuals to increase transparency in dealing with data breaches.[59] Interestingly, notification obligations under Article 34 only apply to data breaches that pose a "high risk to the rights and freedoms of natural persons".[60] However, the concern here is that the term 'high risk' is not defined under the GDPR, therefore, it is not apparent which industries or specific data are regarded as being the most concerning data breaches.

Hence, while exercising data subject rights with respect to their data process, it is necessary to ensure measures regarding transparency and privacy and other relevant interests. While promoting transparency, data protection and privacy laws must be taken into account; proper measures should be taken to maintain balance and not violate data protection and privacy laws. It is important because transparency, specifically in AI systems, has the potential to violate privacy when personal data that is not intended or permitted to be shared is disclosed to third parties. The concerns are mainly related to re-identification, sensitive data, lack of control and out-of-date security and privacy control while disclosing data to ensure transparency.

[58] GDPR (n 7) Art 22.
[59] GDPR (n 7) Art 34.
[60] GDPR (n 7) Art 34.3(b).

3. PRIVACY AND TRANSPARENCY IN AI

When it comes to AI, two significant concerns in the field of AI are privacy and transparency. By delivering personalized services and enhancing decision-making, AI significantly impacts people's lives in a good manner. However, despite its positive effects, AI also prompts worries concerning privacy breaches and a lack of transparency in profiling and automated decision-making. Besides, it is not always AI systems developers, experts or organizations but consumers themselves can be an obstacle to guaranteeing privacy and achieving transparency. For example, consumers frequently misunderstand or disregard less technical disclosures like terms and conditions or privacy statements, according to prior experimental studies.[61] This study indicates that the average people are less likely to comprehend technology as it develops fully. Since privacy and transparency concerns in AI are about the protection of individuals, it raises a question whether they are aware of what the regulation in this respect is capable of and how it can affect them.

The protection of personal data that is gathered, stored, and analyzed by AI systems is referred to as privacy in AI. This may include private data, such as financial information, health records, personal preferences and so forth. All AI applications, notably those involving sensitive data, take place in a complicated, multi-stakeholder conflict environment, private data exploitation, particularly when motivated by financial gain, is certainly more common than previously thought and will undoubtedly continue to rise[62] given constant development of AI and the difficulty of controlling it. AI systems must protect this data from unauthorized access, usage, and disclosure. Strong security safeguards, including encryption and access limits, are necessary as legal frameworks strengthen privacy.

The transparency principle in AI refers to the capacity to comprehend how AI systems decide when it comes to automated decision-making. Concerns about transparency are related to failures to disclose when AI is used to make decisions and to provide an explanation of how it

[61] Adam S. Chilton & Omri Ben-Shahar, 'Simplification of Privacy Disclosures: An Experimental Test' (CoaseSandor Working Paper Series in Law and Economics No. 737, 2016), 2.
[62] Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert. *et al*, 'Secure, privacy-preserving and federated machine learning in medical imaging', Nat Mach Intell 2, 305–311 (2020). https://doi.org/10.1038/s42256-020-0186-1, 309.

does so.[63] Several AI systems employ challenging to understand machine learning models and complicated algorithms. Lack of transparency in AI systems can raise issues regarding discrimination, bias and uncertainty in profiling and automated decision-making. To avoid and solve this, AI systems should be created to clearly explain their decision-making processes, open about the data, the algorithms used and the rationale for making decisions. This will ensure that AI systems are used in a fair and open manner.

Moreover, since due process and freedom of information are well-known institutions, transparency has long been seen as the obvious first step to obtaining redress and vindication of rights.[64] It is now being adopted as the primary answer to algorithmic problems like unfairness and discrimination.[65] While it seems logical and simple to protect individuals' personal data and achieve algorithmic transparency in AI systems, however, since these principles are not absolute, some issues should also be considered, such as "Black Box" algorithms and trade secrets of organizations. It is because it is challenging to interpret Black Box decisions.[66] Besides, under the GDPR, a trade secret is considered an exemption from the right to information access and transparency.[67]

Transparency plays a crucial role in assessing the fairness and morality of an algorithm[68] and achieve privacy protection. The questions such as why an algorithm makes a decision, how it was done, what steps can be accounted for in the decision-making process, what were the determining elements that led to the choice, and what alternatives could have been made must be answered when discussing transparency in AI systems.[69] Thus, designers and developers of AI systems must prioritise data privacy and transparency in their systems as critical concerns in the creation and application of AI include privacy and transparency.

[63] Pauline T. Kim and Matthew T. Bodie, 'Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy', Journal of Labor and Employment Law Vol 35, 2 (2021), , Saint Louis U. Legal Studies Research Paper No. 2021-26, 291.
[64] Lilian Edwards, Michael Veale, 'Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You are Looking For', 16 DUKE L. TECH. REV (2017), 21-2.
[65] Ibid.
[66] Eirini Ntoutsi, Pavlos Fafalios, Ujwal Gadiraju, Vasileios Iosifidis, Wolfgang Nejdl, Maria-Esther Vidal, Salvatore Ruggieri, Franco Turini, Symeon Papadopoulos, Emmanouil Krasanakis, et al, 'Bias in data-driven artificial intelligence systems—An introductory survey' Wiley Interdisciplinary Reviews: Data Mining and Knowledge 2020), e1356., 8.
[67] Madalina Busuioc, 'Accountable Artificial Intelligence: Holding Algorithms to Account', Public Administration Review', (2020), https://doi.org/10.1111/puar.13293, 879.
[68] Marianna Anagnostou, Olga Karvounidou, Chrysovalantou Katritzidaki, *et al*, 'Characteristics and challenges in the industries towards responsible AI: a systematic literature review', *Ethics Inf Technol* Vol 24, 37 (2022). https://doi-org.ludwig.lub.lu.se/10.1007/s10676-022-09634-1, 37.
[69] Ibid.

Legal frameworks should also support the development of AI systems fairly, safely, and transparently to address privacy and transparency in AI systems.

3.1. What is AI?

"Everyone has had or will soon have an AI moment."[70] Since it is difficult to describe precisely, the terms AI, machine learning, algorithmic decision-making, and automated decision-making are frequently used interchangeably.[71] AI, as a field, was used initially in the 1950s, and has been going through numerous waves of development throughout the years.[72] Although there is not a single, widely accepted definition of AI, however, European Commission's (the Commission's) proposed AI Act defines AI as "software that is developed with one or more of the techniques and approaches … and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[73]

Besides, Technopedia describes AI as follows: "[AI], also known as machine intelligence, is a branch of computer science that aims to imbue software with the ability to analyze its environment using either predetermined rules and search algorithms, or patternrecognizing machine learning models, and then make decisions based on those analyses".[74] AI gives technical systems the ability to comprehend their surroundings, deal with what they observe, solve issues, and take action to reach a particular objective. Remarkably, "[t]he theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[75] To achieve so, AI systems use training data that is either provided by humans or is gathered by the machine itself.[76]

---

[70] Ajay Agrawal, Joshua Gans, Avi Goldfarb, 'Prediction Machines: The Simple Economics of Artificial Intelligence', Harvard Business Review Press, (2018).
[71] Kim (n 63) 290.
[72] European Commission, 'AI Watch Historical Evolution of Artificial Intelligence, Analysis of the three main paradigm shifts in AI', Joint Research Centre, Italy, (EUR 30221, 2020), doi:10.2760/801580, 4.
[73] AI Act (n 5) Art. 3(1).
[74] Technopedia, 2020 'Definition of AI', https://www.techopedia.com/definition/190/artificial-intelligence-ai. accessed 10 April 2023.
[75] *Artificial Intelligence*, Eng. Oxford Living Dictionaries, https://perma.cc/B22X-KZAD (accessed 18 April 2023).
[76] David Touretzky, Christina Gardner-McCune, Fred Martin, Deborah Seehorn, 'Envisioning AI for K-12: What Should Every Child Know about AI?', *Association for the Advancement of Artificial Intelligence* (www.aaai.org), (2019), The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19), 9797.

3.1.1. Historical development of AI: How AI revolution did start vs How is it going?

To come to the historical development of AI, the philosophy of AI started to discuss in 1950, after Alan Turin published the famous paper "Computing Machinery and Intelligence".[77] In this early AI research era, the 1950s and 1960s, AI researchers mostly worked on the development of neural computers and artificial neural networks maintained, developed an anti-logical outlook about the representation of knowledge and reasoning, and primarily focused on developing generic strategies for tackling diverse classes of issues to replicate the complex thinking process.[78] At the beginning of AI, they were many questions, concerns, and issues to be solved, however, they were great expectations for AI and computers were expected to be capable of much more. Conceivably, for this reason, the period can also be called "the era of great expectations".[79]

However, expectations from AI did not become a reality, and in the 1970s and 1980s, early systems failed to deliver on their promises,[80] as a result, government funding support and general interest in this new field decreased.[81] Moreover, this dramatic slowing down period in AI is also known as the "AI winter" in publications on this topic. Besides, some also acknowledge the late 1980s extending to the early 1990s as a second winter because of the extreme expense of creating and maintaining expert digital information databases.[82] Nevertheless, as it was said: "No winter lasts forever", machine learning took off in the 1990s, and after a while, it gained popularity and success, which has been largely attributed to the availability of faster technology and larger datasets.[83] Along with, the advancement of deep learning in this period led to the rise of AI technology and the spring of the 2010s in AI.[84]

---

[77] James H. Moor, 'The Turing Test: The Elusive Standard of Artificial Intelligence', Kluwer Academic Publisher, (2003), Vol. 30, p. ISBN: 978-1-4020-1205-1.
[78] Michael Negnevitsky, 'Artificial Intelligence A Guide to Intelligent Systems', (Pearson Education, England, 2005), Second Edi, ISBN 0-321-20466-2, 6-7.
[79] Ibid.
[80] Shashi Shekhar Vempati, 'India and the Artificial Intelligence Revolution', *Carnegie Endowment for International Peace*, (2016, Washington), 19.
[81] Wim Naudé, 'The Race against the Robots and the Fallacy of the Giant Cheesecake: Immediate and Imagined Impacts of Artificial Intelligence', IZA Discussion Papers, (2019), No. 12218, Institute of Labor Economics (IZA), Bonn, 3.
[82] Vivek Kaul, MD, FASGE, Sarah Enslin, PA-C, Seth A. Gross, MD, FASGE, 'History of artificial intelligence in medicine', *American Society for Gastrointestinal Endoscopy, (*New York, 2020), Vol 92, No. 4 : 2020, 806-7.
[83] François Chollet, 'Deep Learning with Python', *Manning Publications Co, (*the USA, 2018), ISBN 9781617294433, 6.
[84] Proposal for a Regulation laying down harmonised rules on artificial intelligence, European Commission 2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence accessed 22 April 2023, 3.

The massive amount of data and improvements in computing power have been the driving forces behind the rapid evolution of deep learning in the early 2010s.[85] Neural natural language processing systems have gained popularity and have been extensively used for a variety of language processing applications in 2010s, in part because of the advent of effective deep learning and representation learning techniques.[86] Undoubtedly, the development that took place during this period laid the groundwork for future developments in natural language comprehension and communication and was paving the way for further advances and to reach the current level in AI.

Hence, significant progress has happened from the birth of AI until today. Now, it has been difficult to talk about AI systems "currently", it is because they are constantly updated, and continuously, something is happening and changing around us. The AI development that started with the chess-playing computer program[87] is currently at a rapid pace, and systems and machines are emerging that can replace humans. The historical development of AI, which began with a downward trend, has now reached such a stage of development that perhaps exceeds initial expectations.

In general, the development of AI has been a long and complex process, and although there were doubts and uncertainties about it in the early stages, however, somehow but certainly, AI is already in our lives, and it looks like it always will be. Extensively, AI is everywhere, and it should not be exaggerated to claim that it is impossible to imagine our future without it. In the modern world, AI is used in numerous applications, from conversational interfaces, such as chatbots and virtual assistants to self-driving automobiles and predictive analytics in the financial, healthcare and many other sectors.

3.1.2. What does AI development bring to the table?: Opportunities and risks of using AI systems

AI has an impact on how we live, and this impact is getting more and more every day. Although the development of AI makes people's lives easier and has many advantages, including

[85] François Chollet, Joseph J. Allaire, 'Deep learning with R, Shelter Island', NY: Manning, Book review, Biometrics (2020) 76:361–2, DOI: 10.1111/biom.13224.
[86] Milad Moradi and Matthias Samwald, 'Deep learning, natural language processing, and explainable artificial intelligence in the biomedical domain', arXiv:2202.12678, 3.
[87] The first software capable of playing a full game of chess was published by Alan Turing. See H. Moor (n).

increased efficiency and productivity and improved decision-making, however using AI systems also raises many concerns, such as lack of transparency and privacy risks.

On the one hand, AI-powered systems give opportunities to both individuals and businesses: AI may benefit individuals through health care, safer transport systems, individualized products and services, access to information, education and training, and workplace safety by using robots to perform hazardous tasks and by creating new job opportunities as AI-driven sectors develop and adapt; besides, AI can facilitate the creation of a new generation of goods and services, boost sales, improve equipment maintenance, and save energy.[88] Moreover, AI has the ability to boost human welfare and well-being, sustainably grow the global economy, promote innovation and productivity, assist in addressing major global concerns,[89] such as global health issues, climate changes and so forth, and in turn, it is expected to result in positive effects on society as a whole.

On the other hand, despite the number of benefits and opportunities of AI, using AI-powered systems can also create some severe risks in many aspects. They include, for instance, the growing possibilities for control over people's preferences, manipulation, bias and discrimination, inequality, unemployment, social isolation, and surveillance, besides, they may expose humans to danger, which emerges from technical failures or failure to give sufficient attention to individual rights and social values.[90] Besides, AI could threaten privacy, data protection and transparency. For example, face recognition technology can be used for online tracking and profiling, moreover, as AI systems can be used to create fake video, audio and images, which are incredibly convincing, deep fakes can pose financial hazards and damage reputations[91] in case it is used in bad faith. Moreover, among the others, one of the greatest challenges is transparency, for example, in case of lack of explanation, algorithmic decision-making for medical diagnoses in healthcare can be problematic.

[88] European Parliament, 'Artificial intelligence: threats and opportunities, News, www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities accessed 2 April 2023.
[89] OECD, 'Recommendation of the Council on Artificial Intelligence', (2022), OECD/LEGAL/0449, 3, 6.
[90] Mihalis Kritikos, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence', European Parliamentary Research Service, Scientific Foresight Unit (STOA) (EPRS), (2020), 1.
[91] European Parliament, News (n 88).

Furthermore, AI can lead to polarisation and manipulation of elections by fostering online echo chambers, spreading disinformation, and lacking media trust, which may threaten democracy.[92] One of the relevant examples in regard to the impact of profiling on elections is the Cambridge Analytica case, which is about the 2016 presidential election in the United States, and the UK Brexit referendum, it indicates how potential abuses of personal data in a digital age can be dangerous in regard to affecting peoples' voting behavior.[93]

Thus, while AI can present both opportunities and risks, it is crucial to remember that humans ultimately have the responsibility for ensuring that AI is created and used in a responsible and lawful manner and that legal regulations in this regard are sufficient and updated enough.

3.2. The connection between AI and privacy

While technologies, machines and AI systems are being driven forces behind today's businesses, more and more data is being and needed to be produced, collected, proceed and stored every day. There is no doubt that analysis becomes more powerful and sophisticated as more data is available. Hence, as large volumes of personal data are frequently necessary for AI to operate efficiently, certainly, Big Data has become increasingly important in AI. Since AI is transforming the world, new instruments create new risks and issues to be considered in addition to new opportunities. So, the connection between AI and privacy: obtaining and processing the data, brings up the legal dilemma of protecting user privacy while using AI-powered systems. Thus, privacy and protecting individuals' data become important issues that must be adhered to in an AI-driven world.

To learn and produce reliable predictions, AI algorithms must gather large amounts of personal data, such as names, locations and other directly or indirectly identifying information.[94] Besides, AI-powered systems may also use sensitive data, including personal information that reveals a person's racial or ethnic origin, political views, religious beliefs, genetic and biometric information and others as defined under the GDPR.[95] Organizations can understand human

[92] Dubois, Elizabeth, Sara Minaeian, Ariane Paquet-Labelle, and Simon Beaudry, 'Who to trust on social media: How opinion leaders and seekers avoid disinformation and echo chambers', *Social media+ society* 6, no. 2 (2020): 2056305120913993, 2, 6.
[93] EPRS (n 90) 23.
[94] GDPR (n 7) Art 4(1).
[95] GDPR (n 7) Arts 4(13-15), 9 and Recitals 51-56.

behaviors and preferences when data is correctly collected, processed and kept, and such information is useful for creating and modifying goods and services to fulfil the needs and interests of persons.[96]

The gathered data can be used in various ways, such as for personalized content, targeted advertising, and predictive analytics. These kinds of actions make consumers' life easier and help them save time finding their needs quickly, for example, Netflix for films or Amazon shopping suggestions. But, on the contrary, the ways in which this data is gathered, stored and used can significantly affect privacy. Hence, there are certain issues with respect to data AI-powered systems that need to be considered. The main risks in this regard are AI biases in algorithms, discrimination, unauthorized surveillance by third parties or data violations caused by system errors.

If training data is wrong or biased, then the result and the outgoing of such data will also be inaccurate or biased.[97] Furthermore, bias may cause discrimination, which may occur for various reasons by an AI system, for example, certain protected groups may face discrimination if the training data set does not represent the intended audience.[98] Besides, suppose the training data set includes sensitive information enshrined in the GDPR[99]. In that case, the AI system may learn to discriminate based on one or more of those variables, which is prohibited by law.[100]

Followingly, one of the relevant examples is the famous Amazon recruitment incident, where Amazon was using an AI-powered system to assist in recruiting new employees, but the system discriminated subject to the gender of candidates, so it discriminated against women and hired men more.[101] The problem, in this case, was about gender unbalanced training data set, so that the organization collected a data set of CVs over a ten-year period - those accomplished period, men performed the majority of technical jobs over women - and the algorithm discovered trends

[96] Chang, Younghoon; Wong, Siew Fan, and Lee, Hwansoo, 'Understanding Perceived Privacy: A Privacy Boundary Management Model', PACIS, Proceedings. 78. (2015), http://aisel.aisnet.org/pacis2015/78, 3.
[97] Huang, MH., Rust, R.T., 'A strategic framework for artificial intelligence in marketing'. J. of the Acad. Mark. Sci. 49, (2021), 30–50. https://doi-org.ludwig.lub.lu.se/10.1007/s11747-020-00749-9, 46.
[98] Richard Benjamins, 'A choices framework for the responsible use of AI', AI Ethics 1, (2021), 49–53, https://doi.org/10.1007/s43681-020-00012-5, 51.
[99] See GDPR (n 7), Arts 4(13), (14) and (15) and 9 and Recitals (51-56).
[100] Benjamins (n 98).
[101] Jeffrey Dastin, 'Amazon scraps secret AI recruiting tool that showed bias against women', (2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G, Accessed 10 April 2023.

that resulted in successful hires, which the AI system identified patterns that were unfavorable to women.[102] Thus, in this case, it appears that some groups of candidates were discriminated against by the AI system that used biased data or algorithms to make employment decisions, potentially limiting their possibilities and violating their privacy. Apparently, unwanted or even illegal discrimination in AI systems may result from biased algorithms.

Moreover, since mentioning privacy and AI, it is also worth stating "surveillance capitalism". Considering that over the past ten years, the development and application of data-intensive digital technology have accelerated, it creates discussions over data protection, secrecy, and privacy in the era of "surveillance capitalism".[103] For Shoshana Zuboff, professor of law at Harvard, a new economic system known as "surveillance capitalism" claims human experience as free raw material for behavioral data, which is used to predict future behavior.[104]

Accordingly, the impact of AI-enabled surveillance technologies and data analysis on human behavior when they know that they are being followed or checked, as well as a possible chill effect on behaviour in connection with agencies; social interaction, physical activities, use of public space and communications may be affected.[105] For instance, AI is used to decide whether news stories, social media posts, YouTube videos, or the types of search engine results are shown to people individually or in groups as recommendations. As a result, AI has the capacity to affect the forms of information and the reference of people where they would consider in order to make their decision. Thus, because large volumes of data from numerous sources, such as cameras, sensors, and other monitoring devices, are frequently gathered and analyzed by AI systems, so some AI systems know even more about us. In our daily lives, we are being "tracked" and "traced" in unprecedented ways by a wide range of players, which could lead to manipulation. For this reason, in case these AI-powered systems are used other than for legitimate purposes or without consent of data subjects as regulated under the GDPR[106] or unauthorized surveillance, it may create a significant risk for privacy in AI.

[102] Benjamins (n 98) 52.
[103] James Wright, David Leslie, Charles Raab, Fumi Kitagawa, Florian Ostmann, Morgan Briggs, 'Privacy, agency and trust in human-AI ecosystems: Interim report (short version)'. The Alan Turing Institute, (2021), 11.
[104] Shoshana Zuboff, 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power', Public Affairs, (2019), 14.
[105] Wright (n 103) 11.
[106] GDPR (n 7) Arts 5.1(b), 7.

In addition, another remarkable risk related to privacy vulnerabilities in AI-powered systems is about system errors. System errors, as in biased cases in data sets, will affect outcomes. Because of a lack of expert knowledge, the complexity of AI algorithms and the black-box nature of AI systems[107] severe or even small errors may occur in AI systems, which may significantly impact privacy. These system errors may include incorrect misidentification, "adversarial attacks" and other errors from incomplete data. For example, a person may become the focus of surveillance if an AI system incorrectly misidentifies them in a security camera feed, leading to a violation of privacy. Another example, if the databases are used for AI algorithms contain errors, this may cause inaccurate re-identifications, such as if the patient's name was incorrectly recorded, it can pose a significant risk for the person with respect to personal health information in case the person was subject to re-identifications or unauthorized access to data.

Besides, adversarial attacks are one of the examples that may cause system errors. As a type of cyber-attack, adversarial attacks in a practice where the attacker intentionally modifies data or inputs into an AI system in order to influence the system.[108] Principally, "Adversarial perturbations" are deliberately engineered modifications to the input that are either invisible to humans or irrelevant, but that cause the system to commit errors.[109] In addition, errors in AI systems may be caused by not updating or not being safe enough systems. For instance, AI systems might be able to identify a person who, according to the input dataset, was not identifiable, however, as a result of the AI computation, such re-identification may occur even unintentionally, subjecting the concerned person to unanticipated outcomes.

Moreover, despite anonymising the personal data of data subjects, an individual can be reidentified in a dataset by converting anonymized data back into personal data via data matching or other similar methods, known as re-identification,[110] which may expose the personal data of an individual. It is because in AI systems if the model's predictions are connected to other data sources that contain personal information, they may expose anonymized

[107] Bernd W. Wirtz, Jan C. Weyerer, Ines Kehl, 'Governance of artificial intelligence: A risk and guideline-based integrative framework', Government Information Quarterly, (2022), Vol 39, Issue 4, 101685, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2022.101685, 10.
[108] Ali Sayghe, Junbo Zhao, Charalambos Konstantinou, 'Evasion attacks with adversarial deep learning against power system state Virtual Conference'. IEEE Power & Energy Society General Meeting (PESGM), (2020), 1.
[109] Melanie Mitchell, 'Why AI is harder than we think', (2021). *arXiv preprint arXiv:2104.12871*, 3.
[110] AEPD-EDPS joint paper on 10 misunderstandings related to anonymization, (2021), https://edps.europa.eu/, 3.

data of the person. As a result, the anonymized data of individuals is not anonymized anymore, which poses to breach of privacy.

Hence, the relationship between AI and privacy is complex and needs to be aware of the potential risks and careful consideration to prevent data breaches and other security threats while developing and deploying AI systems. Due to its complexity, lack of transparency, a possibility for bias, lack of control, data security threats, and the requirement to adhere to rules, AI algorithms can be challenging to secure data privacy in AI. However, the GDPR already protect individual privacy. Therefore, even though the GDPR does not have a separate article addressing AI, its rules for handling and protecting personal data also apply to using personal data in AI systems. In principle, specifically, Articles 5, 22 and 25 of the GDPR, which deal with handling personal data, can be considered while using AI systems.

3.3. The importance of algorithmic transparency in privacy: Challenges in achieving algorithmic transparency for ensuring privacy

Since mentioning privacy, it is worth stating algorithmic transparency, as a key concept in privacy, especially when it comes to AI-powered systems. As was said by American privacy law expert Marc Rotenberg, "at the core of modern privacy law is a single goal: to make transparent, the automated decisions that impact our lives."[111] Understanding and explaining how an AI algorithm generates decisions or predictions that have an impact on people's lives, such as determining a person's eligibility for a job, loan, insurance or even health conditions and treatments relying on AI systems, are referred to as algorithmic transparency.

People might not comprehend why they were rejected or authorized for anything if these decisions or predictions are not made transparently, which could result in damage and discrimination. As a result, algorithmic transparency is essential to uphold people's rights to privacy and data protection. It enables people to check and understand if their data is using or used in a discriminatory or unlawfull manner by AI algorithms. In other words, transparency allows the data subject to have complete authority over their data and perceive how AI systems are using their data.

[111] 'Privacy expert argues "algorithmic transparency" is crucial for online freedoms', https://www.unesco.org/, News, (2015), https://www.unesco.org/en/articles/privacy-expert-argues-algorithmic-transparency-crucial-online-freedoms-unesco-knowledge-cafe, Accessed 10 April 2023.

Furthermore, transparency is also important with respect to guaranteeing the fair and accurate processing of data, if there is no transparency in AI algorithms, then it is challenging to make an automated decision, measure fairness, assess risk, and create truth for AI applications.[112] By altering individuals' perceptions of an AI system's credibility, transparency can either strengthen or weaken their faith in it.[113] Transparency also makes algorithmic bias simpler to find and assists in understanding an AI-powered system's incorrect decisions, allowing individuals and organizations to fix the algorithm's errors and prevent bias by carefully selecting the input variables.[114] Hence, algorithmic transparency is essential for safeguarding data subjects' right to privacy and ensuring that AI systems function fairly and accurately. To establish trust with its users and prevent any harm or discrimination, companies should make an effort to make sure that their algorithms are open and understandable for users.

However, while algorithmic transparency is a key aspect of ensuring privacy, providing it is not always easy. So, transparency became one of the concerns to reaching privacy in an AI-driven world. The main concerns with respect to achieving algorithmic transparency for ensuring privacy are about "Black Box" algorithms and trade secrets.

3.3.1. "Black Box" algorithms

The technical difficulties posed by the interpretability of "black box" algorithms complicate the interaction between the terms "transparency" and "algorithmic systems". Due to the potential for black-box algorithms to render biased decisions, it is noteworthy to state black-box concerns in AI systems regarding achieving algorithmic transparency for guaranteeing privacy. The main issue is that complex AI systems evaluate enormous volumes of data in humanely impenetrable ways, leading to choices with unknowable biases, known as "black box" algorithms.[115] Hence, machine learning models and other algorithms with opaque decision-making processes, an

[112] Osonde A Osoba and William Welser IV, 'An intelligence in our image: The risks of bias and errors in artificial intelligence'. Rand Corporation, (2017), 3.
[113] René F Kizilcec, 'How much information?: Effects of transparency on trust in an algorithmic interface', In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, (2016), ACM, 2390–2395, 1.
[114] Starke, G., De Clercq, E. & Elger, B.S, 'Towards a pragmatist dealing with algorithmic bias in medical machine learning', Med Health Care and Philos, (2021), Vol 24, 341–349, https://doi.org/10.1007/s11019-021-10008-5, 343.
[115] Kashyap Haresamudram, Stefan Larsson and Fredrik Heintz, 'Three Levels of AI Transparency', Computer, (2023), Vol. 56, no. 02, pp. 93-100, doi: 10.1109/MC.2022.321318, 96.

inability to accurately evaluate and comprehend the behavior and results of AI systems, are referred to as "black box" algorithms.[116]

By way of explanation, when AI algorithms are not able to properly explain how they make decisions, then the AI systems may be referred to as "black box" algorithms. For example, there are many significant examples of black-box algorithms that have generated biased decisions that were not intended by their developers, as in the Amazon recruiting case, where unintended discrimination against women arose from the biased dataset.[117] However, sometimes it is challenging to recognize what is causing the problem, one of the difficulties in overcoming such bias is that AI systems are "black box" that lack transparency in how they make decisions.

The existence of the "black box" problem and the inability to defend the system's output make this situation even more unfavourable with respect to combating unconscious bias in automated decision-making and achieving transparency. Thus, achieving algorithmic transparency and protecting privacy in AI systems is difficult due to "black box" algorithms' potential for discrimination and difficulty in discovering and fixing errors, which may lead lack of trust. It is because it can be challenging to assume whether an algorithm is biased or making decisions that are not compliant with privacy laws without transparency which assists in understanding how the algorithm generates decisions. This may reduce data subjects' ability to control and regulate algorithmic decisions, although they are entitled under the GDPR. Since black box algorithms make explaining the reasoning behind a decision more challenging, organizations need to take relevant actions to ensure that their rights are exercised.

Accordingly, a new research area known as Explainable AI (XAI) proposes different ways of opening these black boxes and explaining the decisions made by those algorithms.[118] In response to AI's growing "black box" dilemma, there is now a desire for transparency and XAI, which aims to give stakeholders in a machine learning model insights into the results and display them in qualitative, clear language or visuals.[119] "Explainability is associated with the notion of explanation as an interface between humans and a decision maker that is, at the same

[116] Laurie A. Harris, 'Artificial Intelligence: Background, Selected Issues, and Policy Considerations', Congressional Research Service Report R46795, (2021, Washington, DC: U.S. Congress), summary.
[117] Haresamudram (n 115), See also Dastin (n 101).
[118] Haresamudram (n 115), 95-96.
[119] Julie Gerlings, Millie Søndergaard Jensen, Arisa Shollo, 'Explainable ai, but explainable to whom? An exploratory case study of xai in healthcare', Springer, (2022), 4.

time, both an accurate proxy of the decision maker and comprehensible to humans".[120] Thus, by comprehending data subjects what goes on inside AI systems, XAI techniques aim in reducing AI's "black box" effect.

Nevertheless, although XAI models focus on providing data subjects with information regarding a decision made through "Black Box", whether these models can provide accurate information is debatable. Considering that such information can also be regarding health or other vitally important decisions, it is expected to give well-explained and precise information. Considering that even the algorithms are not Black Box, such algorithms' explanations themselves can be so confusing and complex, so how can the explanations of "Black Box" not be complex and difficult to explain? Besides, it raises another concern regarding trade secret revealing.

3.3.2. A balance with trade secrets

The requirement to access data and transparency should not negatively affect the rights or freedoms of others, including intellectual property, in particular, the copyright protection and trade secrets of AI systems.[121] Given the commercial significance of these frequently delicate business procedures, any attempt more than intended and necessary to explain algorithms may expose trade secrets. In addition, based on conflicts with other people's rights and freedoms, such as trade secrets, organizations are free to limit the information they provide under Article 15(4) and Recital 63 of the GDPR.[122] Therefore, if data subjects exercise their right of access to understand what data is being processed and how, data controllers must disclose this information unless there are overriding interests, like trade secrets.[123]

Accordingly, trade secrets can be considered as a particular type of opacity, a means of corporate secrecy or proprietary protection which is largely deliberate and motivated by a company's desire to preserve its competitive advantage, extract valuable information from its data, and defend itself against the "growing and persistent threat" posed by individuals,

[120] Alejandro Barredo Arrieta, Natalia D´ıaz-Rodr´ıguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador Garc´ıa, Sergio Gil-Lopez, Daniel Molina, Richard ´ Benjamins, et al., 'Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible AI'. Information Fusion, (2020), 5.
[121] Kritikos (n 90) 57.
[122] See GDPR (n 7) Art15(4), Recital 63.
[123] Wachter (n 50) (2018) 30-1.

competitors, and other governments that intend to edge some of its most valuable intangible assets.[124] In consequence, it can be challenging to achieve transparency into how algorithms generate decisions, what data is being used, and if they adhere to privacy standards due to the need to protect trade secrets. Thus, "trade secrets are a core impediment to understanding automated authority like algorithms" and analyzing how the algorithm makes decisions since they attempt to hide information in order to gain an advantage.[125]

Besides, despite the fact that automated decision-making is not specifically addressed in the SCHUFA decisions, however, since this case is a good example to show the balance between the interests of data subjects and the legitimate owner of trade secrets, it is noteworthy to state the SCHUFA case.[126] This interpretation of the right of access as being limited to system functionality in order not to contradict trade secrets is also reflected in German jurisprudence.[127] According to several authors, the German SCHUFA judgments show that data subjects do not have a right to investigate the accuracy of automated processing systems fully, as the underlying formulas are protected as trade secrets.[128] So, on the one hand, the rights of individuals to obtain information and, on the other hand, the rights of companies to keep trade secrets conflict.

Moreover, due to the fact that once algorithms are revealed, they no longer qualify as trade secrets, it is even more crucial to maintain their confidentiality regimes. On the contrary, strict trade secrecy rules may prevent individuals from learning about how their data is used, and stored, if there is an error or breach with respect to their data and if there is discrimination against them. As a result, information protected as trade secrets reduces the control of individuals over information. The matter can become even worse and more complicated when it is about more vital issues, such as health. For example, employers may be more inclined to create complex scoring systems based on electronic medical records to identify potential high-

[124] Merle Temme, 'Algorithms and Transparency in View of the New General Data Protection Regulation', 3 Eur. Data Prot. L. Rev. 473 (2017) / European Data Protection Law Review (EDPL), Vol. 3, Issue 4 (2017), 479.
[125] Nicholas Diakopoulos, 'Algorithmic Accountability Reporting: On the Investigation of Black Boxes, Columbia Journalism School: Tow Center for Digital Journalism, (2014), 12.
[126] Judgment of the German Federal Court, BGH, Bundesgerichtshof 28 January 2014 – VI ZR 156/13 (SCHUFA).
[127] Sandra Wachter, Brent Mittelstadt, Luciano Floridi, 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation', International Data Privacy Law Vol 7 (2), (2017), 87.
[128] Ibid.

risk and high-cost employees if their use of these records cannot be investigated.[129] This may lead to undermining trust in electronic health record systems.[130] Consequently, there is a need to strike a good balance between trade secrets and transparency.

Despite the literature identifying several technical challenges in explaining AI-generated decisions and legal issues surrounding a so-called "right of explanation", there is not enough evidence or studies to claim with certainty upon the connections between XAI and trade secret protection.[131] Thus, relying on some pieces of literature, trade secrets can be protected by using the XAI method for an explanation of AI decision-making, however, there is no great detail about the scope and nature of the issue or how it might be solved.[132] While the EU has rules laying down a minimal level of protection for its MSs, they still have the power to control and regulate the disclosure of information to the public or public authorities.[133] This means that in addition to what is required by the GDPR, national laws may also impose additional restrictions or requirements on the processing and disclosure of personal data. The Slovak case can be one suitable example examined in this thesis below.[134]

Moreover, Trade Secrets Directive[135] permits MSs to specify exceptions to the right to information when disclosing the information may jeopardize a trade secret's protection. For example, according to Finnish law, confidential information is generally protected, however, since it is not an absolute right, it is considered that the right to effective remedies in public procurement overrides any private interest concerning confidentiality and requires a competitor to be granted access to all tender data.[136] In addition, based on the EU's Public Procurement Directive, public bodies must be transparent about their procurement procedures, including the standards used to award contracts.[137]

---

[129] Frank Pasquale, 'Restoring Transparency to Automated Authority', Journal on Telecommunications & High Technology Law, Vol 9, (2011), 242.
[130] Ibid.
[131] Rita Matulionyte, Ambreen Hanif, 'A call for more explainable AI in law enforcement', IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), pp. 75–80. IEEE (2021), 76
[132] Ibid.
[133] See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
[134] See the Slovak case (n 230).
[135] Directive (trade secrets) (n 133).
[136] Kirsi-Maria Halonen, 'Disclosure rules in EU public procurement: Balancing between competition and transparency', Journal of Public Procurement, Vol. 16 No. 4, pp. 528-553, (2016), doi: 10.1108/JOPP-16- 04-2016-B005, 531.
[137] See Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

Followingly, although there are some rules on the EU level to ensure that MSs strike a proper balance between transparency and the preservation of trade secrets, however, the EU Courts' decisions demonstrate that the European Court of Justice (the CJEU) has so far largely disregarded the provisions on the protection of confidentiality and the withholding of strategically important information (trade secrets) and have failed to understand the ramifications of such a high level of commercially sensitive information disclosure.[138] For instance, the Cosepuri v EFSA case[139], which is about tender evaluation, can be a good example, although the court, in this case, displayed a more balanced approach than in earlier judgments addressing transparency, the case law in this area still encourages excessive disclosure and does not guarantee a proper balance between transparency and the protection of business secrets.[140]

Furthermore, the principles of privacy and transparency are not absolute, the necessity to safeguard trade secrets and sensitive information of both public and private enterprises is an exception to the principle of transparency. Besides, considering the complexity of AI algorithms, it can also be tricky for experts to understand or explain them, the existence of "Black Box" algorithms and the possibility that the data can constitute confidentiality, it is not always possible to achieve transparency. Since AI algorithms may contain Black Box algorithms or trade secrets, employing explanation approaches for AI algorithms may not always be effective. Trade secret protection is, therefore, likely to prevent access to information needed for AI explanation purposes when it is necessary to access particular information that is protected by trade secrets or when it contains Black Box algorithms.

Hence, it is challenging to strike a balance between trade secrets and transparency in AI-powered systems, to achieve this, a deliberate and cautious approach is necessary. Utilizing XAI and anonymization methods, involving an independent audit to explain AI algorithms, specifically if explanations are related to sensitive data, can help to ensure privacy and transparency by making a balance with trade secrets. Besides, since Black Box algorithms are

[138] Albert Sánchez Graells, 'The Difficult Balance between Transparency and Competition in Public Procurement: Some Recent Trends in the Case Law of the European Courts and a Look at the New Directives' (University of Leicester School of Law Research Paper No. 13-11), (2013), 23.
[139] Judgment of 29 January 2013 in Joined Cases T-339/10 and T-532/10 Cosepuri Soc. Coop. pA v European Food Safety Authority (EFSA) [2013].
[140] Graells (n 138) 17.

a reality of AI-powered systems and there in no established standard to explain them, it is better to create AI explainability degree in this respect.

4. IS GDPR ADEQUATE IN ENSURING PRIVACY AND TRANSPARENCY IN AN AI-DRIVEN WORLD?

The EU's GDPR is already in place to provide general data and privacy protection and sets out rules for transparency. Privacy and transparency were outlined as general criteria for handling personal data in the GDPR. Since the GDPR does not contain AI-related articles or it does not have explicit reference to AI, it creates an open debate about whether GDPR can completely guarantee privacy and transparency in an AI-driven world. However, some provisions such as Article 5(1)(a) ('lawfulness, fairness and transparency') and Article 22 (Automated decision-making, including profiling) of the GDPR are pertinent to the usage of AI.[141] Besides, the GDPR also contains a provision regarding profiling under Article 4.

Along with, it is worth noting that the guideline published by Article 29 Working Party (WP29) outlines the relationship between AI and automated decision-making and profiling.[142] Under this guideline, it is stating that big data analytics, AI, and machine learning have made it simpler to develop profiles and make automated decisions, which have the potential to impact people's rights and freedoms substantially.[143] The most prevalent AI language may be automated decision-making, the GDPR sets out rules and defines termination in this regard, and WP29 guides how the rules will apply. Although the GDPR does not answer all questions regarding AI privacy and transparency and WP29 does not have a direct legal effect, however, they are both good to have as starting points when addressing privacy and transparency in an AI-driven world.

Accordingly, since there was no exact legal framework addressing AI, the European "Commission has proposed the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally".[144] It is also assumed that the AI Act will ensure that Europeans can trust the AI they are utilizing doing this.[145] Certainly, the discussion about privacy and transparency is extensive and complicated in itself, and when it comes to AI, the issue is undoubtedly even more complex. No matter challenging, AI must be subject to appropriate regulation and control to guarantee that it is created and utilized in a way

[141] See in more detail: GDPR (n 7), Arts 5(1)(a), 22.
[142] Guidelines on Automated individual decision-making and Profiling (n 1).
[143] Ibid 5.
[144] European Commission Proposal (n 84).
[145] Ibid.

that respects individual rights to privacy and ensures transparency. The AI Act is the first endeavour by any significant global economy to develop a general legal framework for AI.[146] As a new attempt at this continuously evolving field, it is not easy to expect it to cover everything in this field and find answers to all questions.

A risk-based approach (establishing four risk categories (top-down) to privacy is used in the GDPR and the AI Act.[147] When it comes to differences between the GDPR and the AI Act, the first notable difference is that the AI Act seeks to establish a single definition of the term "AI".[148] Moreover, compared to the GDPR, the AI Act requires new standards for AI system providers, prohibits some high-risk AI systems, and specifies particular requirements for high-risk AI systems.[149] Besides, the AI Act sets out rules regarding transparency requirements on AI systems, accordingly, Al systems that communicate with people, identify emotions, and produce or modify images, sounds, or videos (such as 'deep fakes') are subject to transparency obligations under the AI Act.[150] Thus, while the GDPR offer some protection for individuals from privacy issues and exposes transparency requirement for AI systems, the AI Act lays out more detailed and focused rules in this respect.

In all efforts for the development of more trustworthy AI systems which is relevant to markets and society, transparency has a crucial role to play.[151] Therefore, it is foremost to consider AI's transparency as balancing interests and governance issues, which require adequate attention to multidisciplinary development.[152] However, it should be marked that there is not always a "one-size-fits-all" approach, followingly, not everyone needs free access to every piece of information[153], or there is no need to disclose all the information either since they may consider trade secret. Besides, sometimes, for various reasons, information cannot be disclosed, for

[146] Jakob Mökander, Maria Axente, Federico Casolari, Luciano Floridi, 'Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation', Minds & Machines, Vol 32, 241–268 (2022). https://doi.org/10.1007/s11023-021-09577-4, 241.
[147] Giovanni De Gregorio, Pietro Dunn, 'The European risk-based approaches: Connecting constitutional dots in the digital age', (2022), 59, Common Market Law Review, Issue 2, pp. 473-500, https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/59.2/COLA2022032, 477.
[148] See AI Act (n 5), Art 3.
[149] Marijn Storm & Alex van der Wolk, 'Privacy and the EU's Draft AI Regulation: What's New and What's Not?' (2021) 4 The Journal of Robotics, Artificial Intelligence & Law (Fastcase), 456.
[150] AI Act (n 5) Art 52.
[151] Stefan Larsson, Fredrik Heintz, 'Transparency in artificial intelligence', Internet Policy Review, Vol 9, Isssue 2 (2020), https://doi.org/10.14763/2020.2.1469, 9.
[152] Ibid 10.
[153] Thomas Wischmeyer, Timo Rademacher, 'Regulating Artificial Intelligence', Springer: Cham, Switzerland (2020), https://doi.org/10.1007/978-3-030-32361-5, 86.

example, if training data contains "Black Box" algorithms, as mentioned in the different part of this Thesis.

Hence, as it was stated by the European Data Protection Board (the EDPB), "the GDPR is built in a technologically neutral manner in order to be able to face any technological change or revolution".[154] Since the GDPR protects individual's right to privacy and ensures transparency the questions may arise that how can businesses guarantee that AI-based automated decision-making procedures are fair, transparent, and understandable? What details and explanations should be given to data subjects to ensure transparency when decisions based on AI are made?

4.1. GDPR provisions that regulate AI in the light of privacy (Articles 24; 25; and 28 of the GDPR) and transparency (Article 5(1)(a) of the GDPR; automated decision making (Article 22 of the GDPR))

"Any processing of personal data through an algorithm falls within the scope of the GDPR".[155] It means the GDPR covers all technologies intended to process personal data, including AI. The GDPR has requirements that govern the use of AI in terms of privacy and transparency, as indicated in Chapter 2 of this Thesis. For example, more specifically, Article 24 of the GDPR mainly addresses the rights to privacy and data protection,[156] which states that controllers' responsibility for the security of all personal data.[157] Followingly, according to Article 25, all systems must be created, set up, and managed with data protection as their top priority.[158] Then, Article 28 precludes the controllers from using any processors that do not meet the requirements of the GDPR.[159]

Thus, AI systems must put these GDPR criteria into practice and ensure that the systems are built and run to protect individuals' right to privacy and prevent discrimination based on personal information while still enabling the use of AI for its intended purposes. Ensure that AI systems continue to comply with GDPR standards, this will necessitate a combination of

[154] EDPB, Response to the MEP Sophie in't Veld's letter on unfair algorithms, (2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf, 2.
[155] Ibid.
[156] Ibid 4.
[157] See GDPR (n 7), Art 24.
[158] See GDPR (n 7), Art 25.
[159] See GDPR (n 7), Art 28.

technological, organizational, and legal safeguards as well as regular monitoring and review, which is not straightforward.

Besides, Article 5(1)(a) of the GDPR explicitly enshrines that "Personal data shall be processed lawfully, fairly and in a transparent manner…".[160] Thus, 'lawfulness, fairness and transparency' is a requirement for the processing of personal data.[161] The question may arise, "How to guarantee lawfulness, fairness, and transparency in AI systems?". First, lawfulness is defined as "identifying the purpose of a system and how this relates to law".[162] Accordingly, with respect to AI, it expects AI systems to comply with all applicable laws and regulations in order to ensure trust.[163] For example, the GDPR's legal basis includes consent, which must be "free, unambiguous, and able to withdraw", the fulfillment of a contract, a legal obligation, legitimate interests, and automated decision-making, each including requirements linked to AI.[164] Since GDPR, as a legal basis, regulates the data processing of individuals, however, it is not always an easy task to stick to it and ensure compliance with the GDPR in AI.

Furthermore, when it comes to fairness, despite its significance, the concept of fair processing has not been officially or consistently defined, it is still challenging to define fairness in terms of AI and other areas like privacy and data protection.[165] However, fairness is described as an overarching principle by the EDPB in its Guidelines on Data Protection by Design and by Default as follows: "Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject".[166]

Followingly, to achieve fairness in data processing, all people, regardless of their disability, should have access to AI systems and involve relevant stakeholders throughout their lifetime.[167] Considering that in general concept, fairness seems to be a vague, context-specific term that is

[160] GDPR (n 7), Art 5(1)(a).
[161] Ibid.
[162] Philip Treleaven, Jeremy Barnett, Andrew Knight and Will Serrano, 'Real Estate Data Marketplace', AI Ethics (2021) DOI: 10.1007/s43681-021-00053-4, 18.
[163] European Commission, Shaping Europe's digital future, Ethics guidelines for trustworthy AI, Report, (2019), https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, accessed 24 April 2023.
[164] Emre Kazim, Danielle Mendes Thame Denny, Adriano Koshiyama, 'AI auditing and impact assessment: according to the UK information commissioner's office', AI and Ethics, Vol 1, 301–310 (2021), 304.
[165] Centre for Information Policy Leadership (CIPL), 'Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice', (Second Report, 2020, Hard Issues and Practical Solutions), 6.
[166] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, (2019), 16.
[167] European Commission, Report (n 163).

influenced by numerous social, cultural, and legal aspects[168], it can be demanding to assess whether the data has proceeded in a fair manner. For example, since fair processing necessitates bias-free AI systems, if "[d]ata sets used by AI systems (both for training and operation) may suffer from the inclusion of inadvertent historical bias, incompleteness and bad governance models. The continuation of such biases could lead to unintended (in)direct prejudice and discrimination".[169] Thus, even unintentionally biased datasets may cause damage to the AI systems, meanwhile, may cause the failure of achieving fairness in data processing. As a consequence, it requires a careful approach to trained datasets in AI systems to avoid such failure of fairness.

In addition, when it comes to transparency, there is no doubt that to achieve privacy in AI systems and to follow all obligations maintained under the GDPR, transparency in AI systems is a core. It is because "lawfulness and fairness" as stated in Article 5(1)(a), overlap with the demand for transparency with regard to AI systems. Thus, without ensuring transparency in AI systems, neither privacy can be ensured nor established rights can be enforced. The most common term can be automated decision-making and/or profiling when it comes to AI. Accordingly, due to Article 22 of the GDPR, "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling…".[170]

Furthermore, "AI is associated with what a system uses, profiling is associated with what a system does, and automated decision-making is associated with what a system is used to do".[171] Consequently, these terms are connected to each other, and AI can be considered an automated decision-making or profiling method. There is no exact definition of automated-decision making under the GDPR, but Article 22 guidelines for the automated decision-making process. However, guidelines on automated individual decision-making and profiling outline automated decision-making as "the ability to make decisions by technological means without human involvement".[172] AI systems use training data to make automated decisions based on information gathered through a data subject, third party or various actions and sources.

---

[168] EDPB (n 166), 7.
[169] European Commission, Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, (2019), 18.
[170] GDPR (n 7), Art 22.
[171] Michelle Seng Ah Lee, Jennifer Cobbe, Heleen Janssen, & Jatinder Singh, 'Chapter 16: Defining the scope of AI ADM system risk assessment', In Research Handbook on EU Data Protection Law. Cheltenham, UK: Edward Elgar Publishing (2022), https://doi-org.ludwig.lub.lu.se/10.4337/9781800371682.00025, 414.
[172] Guidelines on Automated individual decision-making (n 1), 8.

Specific requirements for automated decision-making, including profiling, are provided under Article 22 of the GDPR. Thus, as per Article 22, individuals must have the right to be free from decisions that are exclusively the result of automated processing, such as profiling, legal or other significant outcomes, and if that is the case, then the individuals have the right to request human involvement in these situations, to voice their opinions, and to challenge the decision.[173] For example, one relevant case can be the Uber case[174], where some of the company's drivers inquired about the reasoning behind the algorithm used to match drivers and passengers in meaningful ways. Uber claims that the automated allocation of available trips has no legal consequences and does not materially affect the data subject, indicating that no automated decision-making as defined by Article 22 GDPR occurs.[175] As a result, the court denied the data subjects' request for disclosure regarding this algorithm, concluding that no automated decision-making occurs as defined by Article 22 of GDPR.[176]

Moreover, in another Uber case, some of its drivers inquired about the reasoning behind an algorithmic decision resulting in their contracts' termination due to fraud.[177] According to the company's privacy statement, such decisions are made entirely automatically, however, contrary to what Uber claimed, such decisions are not completely dependent on automated decision-making in the EU and the UK.[178] Ultimately, the court reached the same conclusion in this case as in the other Uber case. These two examples indicate that there are consequential limits to the explanation of algorithmic decision-making.

Another interesting case that was adopted by the same court contrary to these decisions is related to the Ola drivers' case.[179] In this case, the court acknowledged that the GDPR grants such a right, but only under very specific circumstances, and it states that "Automated decision-making is permitted, …, if the decision in question is necessary for the conclusion or performance of an agreement between the data subject and a controller or is based on the express consent of the data subject".[180] Hence, the court stated that the provisions of the GDPR forbid any company to have data subjects affected by such algorithmic decisions, which would

[173] See GDPR (n 7), Art 22(1), (3).
[174] Uber drivers v. Uber B.V. C/13/687315 / HA RK 20–207, District Court, Amsterdam (2021).
[175] Ibid, para 4.66 (translated from Dutch to English).
[176] Ibid, decision.
[177] Uber drivers v. Uber B.V. C/13/692003 / HA RK 20–302, District Court, Amsterdam (2021).
[178] Ibid.
[179] Ola drivers v. Ola Netherlands B.V. C/13/689705 / HA RK 20–258, District Court, Amsterdam (2021).
[180] Ibid, para 4.39 (translated from Dutch to English).

only be permitted if it was necessary for the implementation of a contract or had obtained explicit consent before doing so. The court ruled specifically that Ola had failed to get the drivers' valid agreement for using their personal data and had not adequately informed them about how their data would be used.[181] Hence, the cases stipulate that there is no standard structure for ensuring transparency.

Besides, the fact that data subjects must take action in order to learn about their rights and subsequently exercise them diminishes the effectiveness of 22 of the GDPR.[182] Thus, in some literatures, it is called "a double transparency barrier".[183] Followingly, it requires asking if Article 22 is effective enough to inform individuals. The CJEU takes into account the right not to be subject to automated decisions for the first time in the SCHUFA (scoring) case, where the applicant, after receiving a rejection for credit score, asked SCHUFA to provide more information about the logic involved in this decision, significance and consequences of such processing, and to remove any errors from data that they have about that person.[184] However, SCHUFA provided an overview of how their system operated in general but did not provide detailed information because those are covered by trade secrets.[185] Under this case, it is questioning how Article 22 of the GDPR should be interpreted, and since it is still a pending case, it is interesting how the CJEU will judge this case. However, the Advocate General (AG), in its opinion, cites the goals of the GDPR, particularly the protection of data subjects' rights.[186] According to the AG, the requirement to offer 'meaningful information about the logic involved' must be taken to mean that the process used to determine the score and the justifications for a particular conclusion must be appropriately explained.[187]

Thus, in light of the rapid rise of algorithms and AI, the opinion and decision, in this case, will set a precedent for applying Article 22 GDPR. After the ruling of this case by the ECJ, it will be more explicit if Article 22(1) GDPR can be read extensively. If so, it will also be a clear sign

[181] Ibid, decision.
[182] Alexander J. Wulf and Ognyan Seizov, 'Please understand we cannot provide further information: evaluating content and transparency of GDPR-mandated AI disclosures', AI & Soc (2022), https://doi.org/10.1007/s00146-022-01424-z, 3.
[183] Alexander J. Wulf and Ognyan Seizov, 'Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU', European Business Law Review, (2020), 624.
[184] Case C-634/21, *SCHUFA Holding and Others*.
[185] Ibid.
[186] CJEU, Advocate General's (AG) Opinion in Case C-634/21, AG Pikamäe.
[187] Ibid, see also Press Release No 49/23, (2023), 2.

that the transparency requirement under the GDPR and AI Act can be applied sufficiently. Otherwise, GDPR would leave a legal gap for exercising data subjects' rights under the GDPR.

4.2. The future of privacy and transparency: AI Act

Considering rapid development and changes in technology and AI systems, it can be claimed that the futures of privacy, transparency, and AI are extremely linked. The more technology and AI involve people's life, the more rapidly advancing laws in this regard are required to protect individuals' privacy and ensure transparency in an AI-driven world. It is because the possibility of misusing and abusing AI systems increases as they get more complex and are able to process and analyze enormous volumes of data. In order to prevent this, it is crucial to think about how new technologies will affect the security and privacy of individual's data in the future.

The EU's strategy for managing AI is not straightforward, so a legal framework on AI at the EU level is varied. For example, Initiatives like the EU Cybersecurity Strategy, DMA, the Data Governance Act, and the DSA seek to expand business and research capacity while preserving security and fundamental rights.[188] Besides, a potential AI Liability Directive (AILD) could also be crucial, since the Commission responded to the White Paper's goals and the request of the European Parliament on September 28, 2022, with the Proposal AILD.[189] For instance, the DSA, which was enacted in November 2022, requires large platforms to describe how its AI recommends content to users, give meaningful explanations for the reasoning behind it, including instances where it is based on profiling, such as filling news feeds, and to provide users with an alternative recommender system that is not dependent on sensitive user information.[190]

[188] European Commission, Shaping Europe's digital future, A European approach to artificial intelligence, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, (accessed 4 May 2023).
[189] European Commission, Liability Rules for Artificial Intelligence, The European approach to artificial intelligence (AI) will help build a resilient Europe for the Digital Decade where people and businesses can enjoy the benefits of AI, https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en (accessed 4 May 2023).
[190] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), Recital 68, 69, Art. 26(3).

However, the laws stated in this paragraph are not principally about AI, these laws clearly indicate the EU's willingness to regulate AI that is incorporated into extremely complex systems. All for that, the AI Act is a proposed legislative framework for the creation, implementation, and application of AI within the EU.[191] The AI Act intends to guarantee that AI systems are created and utilized in a way that respects fundamental rights and values, such as privacy and data protection, and is transparent and accountable.[192] Regarding how it clarifies the GDPR, the AI Act is similar to the DSA and the DMA.

Besides, AI Act may be inconsistent with the GDPR and can lead to possible conflict with it since both laws cover matters relating to the handling of personal data. Thus, it is controversial how these laws will work together without inconsistency. In case there is no detailed guide which law applies in what situation, these laws may overlap with the AI Act and create confusion regarding transparency and privacy issues in AI. In addition, due to the interconnection of supervisory authorities' competencies,[193] to avoid conflict, their tasks and powers are required to be divided clearly. Otherwise, this is not only creating a risk for the sake of legal clarity, but also jeopardizing the fundamental right to personal data protection, guaranteed by Article 16 of the TFEU and Article 8 of the Charter.[194]

When it comes to AI Act concerning privacy and transparency, it suggests a number of measures to guarantee transparency in the use of AI. For example, Article 52 of the AI Act enshrines the mandatory transparency criteria for AI systems, which requires developers to provide details that guarantee people can comprehend AI systems affect on them.[195] Besides, the AI Act mandates mandatory human oversight, which means that AI systems are under human control, ensuring that decisions made by AI systems are explicable and that errors can be fixed.[196]

[191] AI Act (n 5).
[192] Ibid, Explanatory memorandum, 1.1.
[193] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (2021), 14.
[194] Ibid 16.
[195] See AI Act (n 5), Art 52.
[196] Ibid, Art 14.

The AI Act follows a risk-based approach and distinguishes between uses of AI that pose an unacceptable, high, and low or minimal risk.[197] In this sense, high-risk AI systems are those that pose considerable threats to people's health, safety, or fundamental rights.[198] Since the transparency requirement also applies to high-risk AI systems,[199] which include ethnic origin, sexual orientation or disabilities[200] that consider "sensitive data" under the GDPR,[201] it indicated that the AI Act approaches sensitive data differently from the GDPR. Thus, in contrast to the GDPR, the AI Act permits the processing of "sensitive data", an AI system's algorithm can now process this kind of data.

Furthermore, since AI Act also provide transparency requirement on emotion recognition and biometric data[202], as a result of providing information that a person may not demand to give, exposure to emotion detection systems may pose several concerns to privacy and data protection. Understanding how to identify emotions can help data processors and controllers understand a person's mental state and reveal sensitive information about that individual. Thus, the AI Act plan seeks to encourage transparency and responsibility in creating and applying AI systems, which is a step in the right direction toward ensuring that AI is created and applied responsibly. However, it is also true that the AI Act may occasionally compromise data security and privacy, particularly in light of the mandated transparency requirement and the gathering and processing of personal data.

4.3. Does GDPR protect individuals from privacy risks produced by AI: the position of the AI Act?

AI is especially relevant for privacy to some extent. For example, the first is that the AI systems can decide for themselves, and the second is that the system grows by learning from experience. People's privacy may be significantly impacted by the possibility of automated decision-making processes, profiling, and how AI systems need more data to find a solution to see its mistakes and to be kept updated. Thus, to do so, AI systems frequently need a lot of data, some of which may be sensitive and personally identifying. As a result of their frequent use of

[197] Ibid, 5.2.2 Explanatory Memorandum.
[198] Ibid, 3.
[199] Ibid, Recital 43.
[200] Ibid, Recital 33.
[201] See (n 95).
[202] AI Act (n 5), Art 1(2).

sophisticated algorithms and machine learning techniques to evaluate vast volumes of data and find patterns, AI systems are also capable of making decisions based on considerations that are not immediately apparent and obvious to humans.

Followingly, taking the Amazon case as an example: an AI system used to evaluate applications for jobs may be trained on a large dataset of successful and unsuccessful candidates, males and females in this case.[203] The fact that successful candidates tend to be males in the system, so while the AI system used this pattern to make predictions about the likelihood of success for future job applicants, this pattern might not be immediately obvious to people. Thus, because the patterns may not always be accurate or fair, it may be challenging for people to comprehend why certain decisions are being made about them.

For the processing of personal data, the GDPR lays down some principles and criteria and provides rights to data subjects and liabilities for data controllers and data processors to support people in exercising more control over their personal data and protecting their privacy, as stated in different parts of the thesis. What is more, the GDPR applies to all types of personal data regardless of how it is obtained or handled. It also covers data processing by AI systems.

Although the GDPR is the strictest privacy and security law in the world,[204] obviously, it provides strict rules for protecting personal data in the EU, however, the privacy cases brought on by AI highlight the challenges in addressing privacy issues in AI systems. For example, the Cambridge Analytica case is one instance that highlights the difficulties in implementing the GDPR for AI systems, where Cambridge Analytica utilized the information to produce targeted political advertising for the 2016 US presidential election and the 2016 UK Brexit referendum.[205] Thus, the scandal highlighted the potential privacy risks posed by AI systems. Furthermore, while the GDPR mandates that companies obtain data subjects' consent before processing their personal data, and transparency in processing data, when data is collected and processed by opaque and complicated AI systems, it might be challenging to get meaningful consent and provide meaningful data.

[203] See (n 101).
[204] https://gdpr.eu/, What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/ (accessed 6 May 2023).
[205] See (n 93).

Accordingly, since the GDPR does not offer a clear framework for addressing the possible harms that can come from the misuse of personal data, it alone might not be enough to address all of the privacy concerns raised by AI, though, the AI Act, which the Commission proposed in 2021, aims to address these issues by defining explicit guidelines and standards for the creation and application of AI in the EU, including obligations for accountability, transparency, and data protection.[206] The GDPR and the AI Act are compatible, and the latter will be enhanced by adding a set of unified guidelines for creating, developing, and applying specific high-risk AI systems.[207]

Followingly, AI Act requires "to comply with a set of mandatory horizontal requirements for trustworthy AI … to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle".[208] Thus, to ensure that AI systems are used in ways consistent with fundamental freedoms and human rights, they are subject to the proper regulation and control. Hence, the AI Act is not intended to undermine the position of the GDPR, but to work with it together to offer a more complete legal framework for addressing the particular privacy issues that AI systems present. According to the AI Act, the GDPR must be followed while processing personal data for use in AI systems. However, what is more, beyond those outlined in the GDPR, the AI Act provides additional requirements for the development and use of AI, such as obligations for transparency and accountability. Followingly, the AI Act mandates that AI systems be transparent and accountable, which means that people must be informed when engaging with AI systems and given explicit explanations of how the AI system functions, what data is utilized to make decisions, and how it makes decisions.[209]

The recent case law indicates the importance of proper data management methods in reference to algorithms and how automated decision-making goes beyond Article 22 of the GDPR. Accordingly, the cases such as the Deliveroo case, in which the riders' manifested availability during key times (Friday, Saturday, and Sunday evening) and their dependability regarding their manifested availability, this algorithm automatically ranked and assigned riders to specific

[206] Tambiama Madiega, 'EU Legislation in Progress: Artificial Intelligence Act', EPRS, PE 698.792 (2022), EPRS, Briefing.
[207] AI Act (n 5) 4-5.
[208] Ibid, 3.
[209] See AI Act (n 5), Arts 13-14, 52.

delivery slots[210], and the Foodinho case, that automated data processing system that it utilized to allocate riders to certain food and goods delivery based on their "score", which were determined by taking into account comments from consumers and merchants as well as the history of service requests made by riders (such as how many requests they had accepted and how quickly they completed deliveries),[211] can be good examples indicate improper data management methods in reference to algorithms under Article 22 of the GDPR.

Although these are not stated criteria under GDPR's Article 22, the Italian Data Protection Authority penalized the controllers for not confirming the accuracy and correctness of their automated rider-management decisions and underlying datasets.[212] Thus, the AI Act aims to fill the gaps and intends to create a strong transparency requirement by providing the data subject with clear and understandable reasoning for making decisions, the implications and the expected consequences for the data subject of this processing shall be taken into account. However, this can be controversial whether the AI Act establishes higher standards of transparency that are unachievable in reality.

4.4. Limits of transparency for AI: Is there a need for a new set of transparency duties for companies?

The combination of trustworthiness and transparency is often taken into account. "Transparency is the currency of trust, [i]t offers clarity and certainty".[213] In case of a lack of transparency, it is challenging to pinpoint and establish potential legal violations, particularly those that safeguard fundamental rights, assign responsibilities and fulfill requirements for compensation claims.[214] In order to help us understand our world and predict the future, more and more advanced algorithms are emerging every day.[215] Since AI processing requires numerous data sets, having complete control over it and ensuring compliance with the legislation is becoming challenging.

---

[210] Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l., (2021) (Deliveroo case) [9685994].
[211] Garante, Ordinanza ingiunzione nei confronti di Foodinho s.r.l., (2021) (Foodinho case) [9675440].
[212] Ibid, Deliveroo and Foodinho cases (n 210 and 211).
[213] Ida Varošanec, 'On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI', International Review of Law, Computers & Technology, Vol. 36, No 2, pp. 95–117, (2022), https://doi.org/10.1080/13600869.2022. 2060471, 95.
[214] White Paper 'On artificial intelligence - A European approach to excellence and trust', Brussels, 19.2.2020 COM(2020) 65 final, 14.
[215] Bernard Marr, 'Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results', 1st Edit, (Chichester, UK: Wiley, 2016), 3.

Big technology companies that need Big Data, such as Google or Facebook, heavily rely on enormous volumes of personal data from people who frequently lack knowledge and awareness of what precisely happens to their data. Thus, the usage of AI does necessitate transparency, it may be required to amend or clarify current law or introduce new legislation to guarantee its efficient application and enforcement. The recent case law, which some mentioned under this thesis, brings out that Article 22 of the GDPR is not enough to cover all questions that arise from the usage of AI systems with respect to automated decision-making, followingly, AI Act sets out new obligations in this regard. However, what is in writing and what is in reality should coincide, so it creates a question of whether the transparency demand required by the AI Act might not be realistic or impossible to fulfill.

A new set of transparency obligations for businesses using AI is required, which the AI Act is a promising legal source that sets out specific transparency requirements precisely, under Articles 13, 14 and 52 for AI systems. For instance, it mandates that developers of high-risk AI systems give documentation on the system's operation and decision-making process.[216] In some circumstances, while transparency is crucial to building confidence and ensuring accountability, there are limitations in how much transparency can or should be achieved.

Accordingly, information systems may intentionally or unintentionally be opaque:[217] i) When a system purposefully withholds information from users or other systems, it may be done to safeguard trade secrets, and other intellectual property rights, protect user privacy, or maintain security and prevent unlawful access, among other things; ii) On the other side, accidental opacity might be caused by the user's lack of technological literacy or inadequate knowledge, for instance, when the system's documentation or user interface is not sufficiently clear or user-friendly, making it challenging for the user to comprehend how the system operates or what data it is gathering.

Moreover, some AI models are so complex and opaque that even their developers cannot fully understand what they are dealing with when making a decision or recommendation. It is

[216] AI Act (n 5) Art 52.
[217] Heike Felzmann, Eduard Fosch Villaronga, Christoph Lutz, Aurelia Tamo`Larrieux, 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns', Big Data & Society, (2019), 10.

because of the complexity of AI algorithms, and some AI systems contain Black Box algorithms which are stated in different parts of this thesis. This kind of limitation raises questions about the limits of explanation and trade-offs between accuracy and interpretation in AI. Considering all the limitations stated, it can be argued that transparency requirements may be deemed unreasonable and difficult to achieve.

Besides, it has been argued that transparency depends solely on its instrumentality to attain many further important values, such as trust and that it is primarily based upon achieving these more fundamental values.[218] Furthermore, "transparency should not be elevated to an intrinsic value"[219], means the right amount of transparency should be carefully considered in relation to other aspects in order to guarantee that all pertinent values and interests are fairly balanced and taken into consideration. In addition, it is argued that a growing degree of transparency can cause a flood of unsorted information and misinformation, which is only confusing if it cannot be separated and evaluated, which it may lead to uncertainty rather than trust.[220] It is because people those do not want to be shared may be less honest when they are aware that everything they say or write will be made public.[221] Thus, balancing transparency with the protection of privacy and other fundamental values is essential to ensure trust.

However, imposing strict legislative measures which are not realistic to achieve is just in vain, for this reason, setting realistic requirements that can be enforced will be more effective in ensuring transparency with protecting privacy. Thus, it is crucial to approach the way that the AI Act does not mandate perfect disclosure or total comprehension of AI systems in its transparency requirements. Instead, it strives to guarantee that AI developers offer the highest level of transparency to support oversight and accountability. To achieve this, users need to be cautious when making decisions about what constitutes untrustworthy, opacity and reasonable in their expectations of transparency.[222]

On the other side, the existing law in this respect has to be also clear and plain, and it may be necessary for businesses and policymakers to come up with innovative methods of transparency

[218] Ibid, 9.
[219] David Heald, 'Transparency as an instrumental value', In C. Hood & D. Heald (Eds.), Transparency: the key to better governance? (pp. 59–73). Oxford: Oxford University Press, (2006), 70.
[220] Onora O'Neill, O., 'A Question of Trust. The BBC Reith Lectures', Cambridge: Cambridge University Press, (2002), 19.
[221] Ibid.
[222] H. Felzmann, 10.

that go beyond conventional ideas of disclosure and concentrate on fostering trust via increased stakeholder participation, cooperation, and accountability. When it comes to AI Act, although having transparency requirements is essential, the AI Act is silent on the level of transparency that will be expected of AI systems and what exactly will be meant by their "interpretability" for users. For example, when Article 13 of the AI Act requires "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent… and [a]n appropriate type and degree of transparency",[223] it does not specify the required level of transparency.

Besides, in relation to Article 14 of the AI Act, it slightly narrows the degree to what is required transparency, and it states that the AI system must be designed and developed in a manner that it can be effectively controlled by individuals during its use, sufficient to achieve transparency.[224] Thus, it seems that this requirement should not be too heavy to achieve transparency, and the transparency requirement by the AI Act is not at a level that cannot be fulfilled, and since the GDPR also has that requirement,[225] the AI Act does not create a new, unusual requirement. In addition, since Article 52 of the AI Act imposes "transparency obligations for certain AI systems",[226] this calls into question whether the AI Act is sufficiently flexible.

Taking into account the rapid development of AI systems, it would be more appropriate for the new legislation to be in line with the rapid development and to keep up with it in order to ensure transparency and safeguard privacy. For example, since "ChatGPT is entering a world of regulatory pain in Europe", as it is stated, suspected violations by ChatGPT "should be discussed at [the] European level."[227] Besides, at least two complaints were filed against ChatGPT with France's data protection body, CNIL, alleging privacy infractions, including those in violation of the GDPR.[228] Thus, ChatGPT already sheds light on enough problems, and it raises unanswered questions about how to strike a balance between ensuring transparency and privacy on ChatGPT.

[223] AI Act (n 5), Art 13.
[224] AI Act (n 5), Art 14.
[225] GDPR (n 7), Art 22(1).
[226] AI Act (n 5), Art 52.
[227] Politico (n 6).
[228] Ibid.

The fact that some countries banned ChatGPT's use and others expressed their concerns regarding possible breaches through using it, such as Italy and France,[229] accordingly, indicates a lack of confidence in the MSs in legislation to ensure privacy and data protection within the EU. Since AI is very unpredictable, new AI systems may emerge, and that in itself may present new challenges concerning privacy and transparency. Hence, there can be consistent if AI legislation be more flexible and prepared for all future challenges, the more advanced legislation on privacy and transparency, the more prepared for IA systems-related concerns. For example, the Slovak Constitution mandates additional legal safeguards be put in place to protect people when automated assessments by State agencies are involved, including making sure that (i) the criteria, models, or linked databases used in that context are current, trustworthy, and non-discriminatory; (ii) people are aware of the existence, scope, and impact of their automated assessment; and (iii) evaluating the system's quality, including its error rate; (iv) enshrining transparency for people to defend themselves against the system's flaws effectively.[230] Thus, it indicated that the requirement of the Slovak Constitutional Court exceeds that of Article 52 of the AI Act, which again shows that the AI Act did not go very far, and it is even possible to go more beyond.

[229] Euronews, 'Which countries are trying to regulate artificial intelligence?', (2023), https://www.euronews.com/next/2023/05/03/which-countries-are-trying-to-regulate-artificial-intelligence, accessed 10 May 2023.
[230] Ústavného súdu Slovenskej republiky, Case 492/2021 Z. z., (2021), available at https://www.slovlex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217, see also Sebastião Barros Vale and Gabriela Zanfir-Fortuna, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities', the Future of Privacy Forum, (2022), 11.

5. CONCLUSION

As AI technologies continue to transform many industries and have become and continue to be an integral part of our lives, it brings some issues to be considered. The quick development of AI technology has transformed data gathering, processing, and analysis. In addition to bringing certain benefits, potential risks and challenges to data privacy are also increasing. Thus, the rise of algorithmic transparency has become essential for preserving data privacy in an AI-driven world.

Through the thesis, the significance of algorithmic transparency in data privacy, particularly in the context of GDPR and the AI Act, has been studied. The findings demonstrate that algorithmic transparency is essential for improving data privacy by allowing people to know how their data is processed and used. Additionally, it can aid in pinpointing and eliminating biases and discrimination that may result from the application of AI algorithms. Finally, it also improves accountability and trust in decision-making processes that entail the usage of AI algorithms.

The GDPR significantly contributes to data protection, privacy and transparency in the EU, and its provisions are also applicable to data processing in AI systems. However, the GDPR regulates data processing in a general matter, and it does not contain specific provisions for AI usage of AI technology. Although some Articles of the GDPR, specifically, Article 22, is about AI systems, it is not extensive, and their application is too narrow to cover all matters in AI. Thus, since Article 22 of the GDPR is not sufficient enough to handle AI transparency, the Commission came up with a new regulation, AI Act, to fill the gaps. The AI Act is all about AI technology usage. The AI Act and other relevant laws, especially with the GDPR, are expected to safeguard privacy and transparency in an AI-driven world.

Accordingly, similar to the GDPR, the AI Act provides accountability and transparency in data processing in AI systems and automated decision-making and seeks to control the application of AI technology in the EU. Considering the similarities of these regulations, it could be assumed that the AI Act is intended to replace the GDPR or weaken its role concerning transparency. However, the cases analysed under the thesis and the provisions of the AI Act reveal that the GDPR alone is not enough to deal with AI systems, so having the AI Act, which regulates AI systems, was needed to fill the gaps that the GDPR does not fill. Thus, the thesis

contends that even if the GDPR offers a robust legal framework for safeguarding personal data, it might not be adequate to handle the particular problems presented by AI. Therefore, new legislation was needed to address the increased threats and concerns that the advent of AI has brought to the privacy of personal data.

However, even the existence of legislation dedicated to AI does not mean the solution to all problems posed by AI systems. It is critical to understand that providing algorithmic transparency is challenging, particularly when dealing with sophisticated AI algorithms. AI systems may analyze vast volumes of personal data to assume sensitive information about people that can be exploited for discriminating, manipulative, or any other unlawful purposes, creating privacy concerns. Besides, since AI systems involve many data sets for data processing, some of which may include sensitive personal information and require robust algorithm protection. For instance, if businesses violate their need to be transparent under the AI Act or they are not able to create a safe environment to safeguard data, in such a case, privacy is seriously threatened.

Furthermore, since data can include trade secrets and other intellectual property, which are essential for businesses' activities to keep them confidential unless the 'right' degree of transparency is determined, then disclosure of such data can be harmful to some extent. Furthermore, as it is argued under the thesis, not all opacity occurs by purpose, and sometimes transparency cannot be ensured for various reasons, for example, Black Box algorithms may be used in the AI systems, which makes it complicated to explain the decision made through this AI system.

In an AI-driven society, algorithmic transparency is essential for protecting data privacy and promoting trust in AI systems. The GDPR and AI Act provides a legal framework with the intention of fostering algorithmic accountability and transparency. Collaborative work is needed to execute existing rules effectively to ensure privacy and transparency in AI systems. As a result of the rule's emphasis on individual privacy rights, principles such as the right to access and the right to an explanation are part of AI-based decision-making, which is a requirement under both the GDPR and the AI Act.

However, since ensuring transparency in the automated decision-making process, individual rights to privacy should not be ignored, and a balance must be maintained between privacy,

transparency and other fundamental values. Thus, this study has brought attention to the necessity for a thorough legal and regulatory framework to control the application of AI technology. To make sure the use of AI technology does not violate people's privacy right, the legal framework should include the concepts of transparency and accountability in a clear way and provide a comprehensible guide. However, neither the GDPR nor the AI Act provides a guide determining the level of transparency that is needed to explain the logic behind the decision made by AI systems.

While the GDPR and the AI Act are significant milestones in the right direction, more must be done to ensure that AI is created and utilized in a way that respects people's rights and advances transparency. Another difficulty for legislators is keeping up with new hazards and threats to privacy due to the fast rate of technology innovation and development. For example, ChatGPT can be an example to give a signal for future privacy problems. Thus, there is a need for more flexible laws to address potential future risks posed by AI systems. In addition, it may be required to constantly amend and update legislation to maintain its effectiveness as AI systems become more complex and revolutionary.

In conclusion, clear rules and policies with respect to privacy and transparency must be established on the use of AI systems, including limitations on the gathering and use of specific categories of data, the level of explanation of decisions made by AI considering different types of data, such as sensitive, trade secret and ones can be reidentified a person from different sources. However, despite several flaws, the AI Act is an essential step in assisting with developing norms and standards and promoting transparent AI systems. It needs to be seen if the AI Act does this adequately to promote transparency and ensure privacy.

BIBLIOGRAPHY

Primary sources

EU Legislation

Charter of Fundamental Rights of the European Union, 2012/C 326/02

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

The European Convention on Human Rights (ECHR), 213 UNTS 221 (1950) (entered into force 3 September 1953)

The International Covenant on Civil and Political Rights (1966), 999 UNTS 171 (entered into force 23 March 1976)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810 (1948)

EU Sources/Official Papers

AEPD-EDPS joint paper on 10 misunderstandings related to anonymization, (2021), [Online]. Available: https://edps.europa.eu/

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

European Commission, Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, (2019)

European Commission, Shaping Europe's digital future, Ethics guidelines for trustworthy AI, Report, (2019), [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, accessed 24 April 2023

European Commission, 'AI Watch Historical Evolution of Artificial Intelligence, Analysis of the three main paradigm shifts in AI', Joint Research Centre, Italy, (EUR 30221, 2020), doi:10.2760/801580

European Commission, Shaping Europe's digital future, A European approach to artificial intelligence, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, (accessed 4 May 2023)

European Commission, Liability Rules for Artificial Intelligence, The European approach to artificial intelligence (AI) will help build a resilient Europe for the Digital Decade where people and businesses can enjoy the benefits of AI, [Online]. Available: https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en (accessed 4 May 2023)

Kritikos M, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence', European Parliamentary Research Service, Scientific Foresight Unit (STOA) (EPRS), (2020)

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Brussels, 2021) COM(2021) 206 final.

Proposal for a Regulation laying down harmonised rules on artificial intelligence, European Commission 2021, [Online]. Available: https://digital-

strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence accessed 22 April 2023

White Paper 'On artificial intelligence - A European approach to excellence and trust', Brussels, 19.2.2020 COM(2020) 65 final

Secondary sources

Books

Agrawal A, Gans J, Goldfarb A, 'Prediction Machines: The Simple Economics of Artificial Intelligence', Harvard Business Review Press, (2018)

Chollet F, 'Deep Learning with Python', Manning Publications Co, (the USA, 2018), ISBN 9781617294433

Döhmann I. S, 'The legal framework for access to data from a data protection viewpoint – especially under the GDPR', Nomos eLibrary, (2023), https://doi.org/10.5771/9783748924999-175, [Online]. Available: http://www.nomos-elibrary.de/agb

Gerlings J, Jensen S. M, Shollo A, 'Explainable ai, but explainable to whom? An exploratory case study of xai in healthcare', Springer, (2022)

Moor J. H, 'The Turing Test: The Elusive Standard of Artificial Intelligence', Kluwer Academic Publisher, (2003), Vol. 30, ISBN: 978-1-4020-1205-1

Negnevitsky M, 'Artificial Intelligence A Guide to Intelligent Systems', (Pearson Education, England, 2005), Second Edi, ISBN 0-321-20466-2

Osoba A. O and Welser IV W 'An intelligence in our image: The risks of bias and errors in artificial intelligence'. Rand Corporation, (2017),

Wischmeyer T, Rademacher T, 'Regulating Artificial Intelligence', Springer: Cham, Switzerland (2020), https://doi.org/10.1007/978-3-030-32361-5

Zuboff S, ‘The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power’, Public Affairs, (2019)

Journal Articles

Anagnostou M, Karvounidou O, Katritzidaki C, et al, ‘Characteristics and challenges in the industries towards responsible AI: a systematic literature review’, Ethics Inf Technol Vol 24, 37 (2022). https://doi-org.ludwig.lub.lu.se/10.1007/s10676-022-09634-1

Busuioc M, ‘Accountable Artificial Intelligence: Holding Algorithms to Account’, Public Administration Review’, (2020), https://doi.org/10.1111/puar.13293

Benjamins R, ‘A choices framework for the responsible use of AI’, AI Ethics 1, (2021), 49–53, https://doi.org/10.1007/s43681-020-00012-5

Bernd W. W, Jan C. Weyerer, Kehl I, ‘Governance of artificial intelligence: A risk and guideline-based integrative framework’, Government Information Quarterly, (2022), Vol 39, Issue 4, 101685, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2022.101685

Cavoukian A, Polonetsky J and Wolf C, ‘SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation’, Springerlink.com, (2010), IDIS 3:275–294 DOI 10.1007/s12394-010-0046-y

Dubois E, Minaeian S, Paquet-Labelle A, and Beaudry S, ‘Who to trust on social media: How opinion leaders and seekers avoid disinformation and echo chambers’, Social media+ society 6, no. 2 (2020): 2056305120913993

Halonen K-M, ‘Disclosure rules in EU public procurement: Balancing between competition and transparency’, Journal of Public Procurement, Vol. 16 No. 4, pp. 528-553, (2016), doi: 10.1108/JOPP-16- 04-2016-B005

Haresamudram K, Larsson S and Heintz F, ‘Three Levels of AI Transparency’, Computer, (2023), Vol. 56, no. 02, pp. 93-100, doi: 10.1109/MC.2022.321318

Heald D, ‘Transparency as an instrumental value’, In C. Hood & D. Heald (Eds.), Transparency: the key to better governance? (pp. 59–73). Oxford: Oxford University Press, (2006)

Huang, MH, Rust, R.T, ‘A strategic framework for artificial intelligence in marketing’. J. of the Acad. Mark. Sci. 49, (2021), 30–50. https://doi-org.ludwig.lub.lu.se/10.1007/s11747-020-00749-9

Gregorio De G, Dunn P, ‘The European risk-based approaches: Connecting constitutional dots in the digital age’, (2022), 59, Common Market Law Review, Issue 2, pp. 473-500, [Online]. Available: https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/59.2/COLA2022032

Gruschka N, Mavroeidis V, Vishi K and Jensen M, ‘Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR’, Research Group of Information and Cyber Security, (2018), University of Oslo, Norway, arXiv:1811.08531v1 [cs.CR]

Kaissis A. G, Makowski R. M, Rückert D. et al, ’Secure, privacy-preserving and federated machine learning in medical imaging’, Nat Mach Intell 2, 305–311 (2020). https://doi.org/10.1038/s42256-020-0186-1

Kaul V, MD, FASGE, Enslin S, PA-C, Seth A. Gross, MD, FASGE, ‘History of artificial intelligence in medicine’, American Society for Gastrointestinal Endoscopy, (New York, 2020), Vol 92, No. 4 : 2020

Kazim E, Denny M. T. D, Koshiyama A, ‘AI auditing and impact assessment: according to the UK information commissioner’s office’, AI and Ethics, Vol 1, 301–310 (2021)

Kretschmer M, Pennekamp A and Wehrle K, ‘Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web’, (2021), ACM Transaction on the Web, Vol. 15, No. 4

Larsson S, Heintz F, ‘Transparency in artificial intelligence’, Internet Policy Review, Vol 9, Isssue 2 (2020), https://doi.org/10.14763/2020.2.1469

Marr B, 'Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results', 1st Edit, (Chichester, UK: Wiley, 2016)

Mitchell M, 'Why AI is harder than we think', (2021). arXiv preprint arXiv:2104.12871

Moradi M and Samwald M, 'Deep learning, natural language processing, and explainable artificial intelligence in the biomedical domain', arXiv:2202.12678

Mökander J, Axente M, Casolari F, Floridi L, 'Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation', Minds & Machines, Vol 32, 241–268 (2022). https://doi.org/10.1007/s11023-021-09577-4

Ntoutsi E, Fafalios P, Gadiraju U, Iosifidis V, Nejdl W, Vidal M-E, Ruggieri S, Turini F, Papadopoulos S, Krasanakis E, et al, 'Bias in data-driven artificial intelligence systems—An introductory survey' Wiley Interdisciplinary Reviews: Data Mining and Knowledge 2020), e1356

O'Neill O, 'A Question of Trust. The BBC Reith Lectures', Cambridge: Cambridge University Press, (2002)

Pasquale F, 'Restoring Transparency to Automated Authority', Journal on Telecommunications & High Technology Law, Vol 9, (2011)

Romanou A, 'The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise', Computer law & Security review, (2018), Vol 34, Issue 1

Selbst D. A and Powles J, 'Meaningful information and the right to explanation', International Data Privacy Law, (2017), Vol. 7, No. 4

Spyridaki K, 'Chief Privacy Strategist, SAS Europe, "GDPR and AI: Friends, foes or something in between?', sas.com, [Online]. Available: https://www.sas.com/en_us/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html#, accessed 31 January 2023

Starke, G, De Clercq, E & Elger, B.S, 'Towards a pragmatist dealing with algorithmic bias in medical machine learning', Med Health Care and Philos, (2021), Vol 24, 341–349, https://doi.org/10.1007/s11019-021-10008-5

Storm M & Alex Wolk van der A, 'Privacy and the EU's Draft AI Regulation: What's New and What's Not?' (2021) 4 The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

Temme M, 'Algorithms and Transparency in View of the New General Data Protection Regulation', 3 Eur. Data Prot. L. Rev. 473 (2017)/ European Data Protection Law Review (EDPL), Vol. 3, Issue 4 (2017)

Touretzky D, Gardner-McCune C, Martin F, Seehorn D, 'Envisioning AI for K-12: What Should Every Child Know about AI?', Association for the Advancement of Artificial Intelligence (www.aaai.org), (2019), The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19)

Treleaven P, Barnett J, Knight A and Serrano W, 'Real Estate Data Marketplace', AI Ethics (2021) DOI: 10.1007/s43681-021-00053-4

Wachter S, Mittelstadt B, Floridi L, 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation', International Data Privacy Law Vol 7 (2), (2017)

Wachter S, 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', Oxford Internet Institute, University of Oxford and The Alan Turing Institute, British Library, (London, United Kingdom, 2018)

Wulf J. A and Seizov O, 'Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU', European Business Law Review, (2020)

Wulf J. A and Seizov O, 'Please understand we cannot provide further information: evaluating content and transparency of GDPR-mandated AI disclosures', AI & Soc (2022), https://doi.org/10.1007/s00146-022-01424-z

Varošanec I, ‘On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI’, International Review of Law, Computers & Technology, Vol. 36, No 2, pp. 95–117, (2022), https://doi.org/10.1080/13600869.2022. 2060471

Websites/Miscellaneous

Arrieta B. A, D´ıaz-Rodr´ıguez N, Ser D. J, Bennetot A, Tabik S, Barbado A, Garc´ıa S, Gil-Lopez S, Molina D, Benjamins R, et al., ‘Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible AI’. Information Fusion, (2020)

Artificial Intelligence, Eng. Oxford Living Dictionaries, [Online]. Available: https://perma.cc/B22X-KZAD (accessed 18 April 2023)

Centre for Information Policy Leadership (CIPL), ‘Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice’, (Second Report, 2020, Hard Issues and Practical Solutions)

Chang Y; Wong S. F, and Lee H, ‘Understanding Perceived Privacy: A Privacy Boundary Management Model’, PACIS, Proceedings. 78. (2015), [Online]. Available: http://aisel.aisnet.org/pacis2015/78

Chilton S. A & Ben-Shahar O, ‘Simplification of Privacy Disclosures: An Experimental Test’ (CoaseSandor Working Paper Series in Law and Economics No. 737, 2016)

Chollet F, Allaire J. J, ‘Deep learning with R, Shelter Island’, NY: Manning, Book review, Biometrics (2020) 76:361–2, DOI: 10.1111/biom.13224

Diakopoulos N, ‘Algorithmic Accountability Reporting: On the Investigation of Black Boxes, Columbia Journalism School: Tow Center for Digital Journalism, (2014)

Dastin J, ‘Amazon scraps secret AI recruiting tool that showed bias against women’, (2018), [Online]. Available: https://www.reuters.com/article/us-amazon-com-jobs-automation-

insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G, Accessed 10 April 2023

Data Protection Working Party, 'Guidelines on transparency under Regulation' (2016/679), 17/EN WP260

EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, (2019)

EDPB, Response to the MEP Sophie in't Veld's letter on unfair algorithms, (2020), [Online]. Available: https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf

EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (2021)

Edwards L, Veale M, 'Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You are Looking For', 16 DUKE L. TECH. REV (2017)

Euronews, 'Which countries are trying to regulate artificial intelligence?', (2023), [Online]. Available: https://www.euronews.com/next/2023/05/03/which-countries-are-trying-to-regulate-artificial-intelligence, accessed 10 May 2023

European Parliament, 'Artificial intelligence: threats and opportunities, News, [Online]. Available: www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities accessed 2 April 2023

Felzmann H, Villaronga F. E, Lutz C, Tamo`Larrieux A, 'Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns', Big Data & Society, (2019)

Gerl A and Pohl D, 'Critical Analysis of LPL according to Articles 12 - 14 of the GDPR', (ARES 2018, Hamburg, Germany), DOI: 10.1145/3230833.3233267

Graells S. A, 'The Difficult Balance between Transparency and Competition in Public Procurement: Some Recent Trends in the Case Law of the European Courts and a Look at the New Directives' (University of Leicester School of Law Research Paper No. 13-11), (2013)

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, (2017), 17/EN WP251rev.01

Harris A. L, 'Artificial Intelligence: Background, Selected Issues, and Policy Considerations', Congressional Research Service Report R46795, (2021, Washington, DC: U.S. Congress)

Hristov P, Dimitrov W, 'SIMPRO 2018: Challenges and opportunities for sustainable development through quality and innovation in engineering and research management', (2018), University of Petrosani, 8th International Multidisciplinary Symposium

Kizilcec F. R, 'How much information?: Effects of transparency on trust in an algorithmic interface', In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, (2016), ACM, 2390–2395

Kim T. P and Bodie T. M, 'Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy', Journal of Labor and Employment Law Vol 35, 2 (2021), Saint Louis U. Legal Studies Research Paper No. 2021-26

Kostadinova R. Z, 'Purpose limitation under the GDPR: can Article 6(4) be automated?' (master's thesis, Tilburg University, the Netherlands)

Layton R and Celant S, 'How the GDPR compare to best practices for privacy, accountability and trust', (2017), 2017/TPRC45

Lee S. A. M, Jennifer Cobbe, Janssen H, & Singh J, 'Chapter 16: Defining the scope of AI ADM system risk assessment', In Research Handbook on EU Data Protection Law. Cheltenham, UK: Edward Elgar Publishing (2022), https://doi-org.ludwig.lub.lu.se/10.4337/9781800371682.00025

Madiega T, 'EU Legislation in Progress: Artificial Intelligence Act', EPRS, PE 698.792 (2022), EPRS, Briefing

Matulionyte R, Hanif A, 'A call for more explainable AI in law enforcement', IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), pp. 75–80. IEEE (2021)

Naudé W, 'The Race against the Robots and the Fallacy of the Giant Cheesecake: Immediate and Imagined Impacts of Artificial Intelligence', IZA Discussion Papers, (2019), No. 12218, Institute of Labor Economics (IZA), Bonn

OECD, 'Recommendation of the Council on Artificial Intelligence', (2022), OECD/LEGAL/0449

Politico, 'ChatGPT is entering a world of regulatory pain in Europe', (2023), [Online]. Available: https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/, accessed 10 May 2023

'Privacy expert argues "algorithmic transparency" is crucial for online freedoms', https://www.unesco.org/, News, (2015), [Online]. Available: https://www.unesco.org/en/articles/privacy-expert-argues-algorithmic-transparency-crucial-online-freedoms-unesco-knowledge-cafe, Accessed 10 April 2023

Sayghe A, Zhao J, Konstantinou C, 'Evasion attacks with adversarial deep learning against power system state Virtual Conference'. IEEE Power & Energy Society General Meeting (PESGM), (2020)

Technopedia, 2020 'Definition of AI', [Online]. Available: https://www.techopedia.com/definition/190/artificial-intelligence-ai. accessed 10 April 2023

What is GDPR, the EU's new data protection law?, [Online]. Available: https://gdpr.eu/what-is-gdpr/ (accessed 6 May 2023)

Wright J, Leslie D, Raab C, Kitagawa F, Ostmann F, Briggs M, ‘Privacy, agency and trust in human-AI ecosystems: Interim report (short version)’. The Alan Turing Institute, (2021)

Vale B. S and Zanfir-Fortuna G, ‘Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities’, the Future of Privacy Forum, (2022)

Vempati S. S, ‘India and the Artificial Intelligence Revolution’, Carnegie Endowment for International Peace, (2016, Washington)

TABLE OF CASES

CJEU

Advocate General's Opinion in Case C-634/21 (*SCHUFA Holding and Others)*, Press Release No 49/23, (2023)

Cosepuri Soc. Coop. pA v European Food Safety Authority (EFSA), Judgment of 29 January 2013 in Joined Cases T-339/10 and T-532/10 [2013]

Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (C-311/18) [2020] ECLI:EU:C:2020:559

Maximilian Schrems v Facebook Ireland Limited (Case C-498/16), Judgment of the Court (Third Chamber) [2018] ECLI:EU:C:2018:37

SCHUFA Holding and Others, Case C-634/21

Judgments from other Courts/Jurisdictions

SCHUFA Holding and Others, Judgment of the German Federal Court, BGH, Bundesgerichtsh of 28 January 2014 – VI ZR 156/13

Uber drivers v. Uber B.V. C/13/687315 / HA RK 20–207, District Court, Amsterdam (2021)

Uber drivers v. Uber B.V. C/13/692003 / HA RK 20–302, District Court, Amsterdam (2021)

Ola drivers v. Ola Netherlands B.V. C/13/689705 / HA RK 20–258, District Court, Amsterdam (2021)

Ústavného súdu Slovenskej republiky, Case 492/2021 Z. z., (2021), [Online]. Available: https://www.slovlex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217

Garante, Ordinanza ingiunzione nei confronti di *Deliveroo Italy* s.r.l., (2021) [9685994]

Garante, Ordinanza ingiunzione nei confronti di *Foodinho* s.r.l., (2021) [9675440]