MASTER THESIS | MASTER'S THESIS

Titel | Title

The Role of Consent in Data Protection in the European Union for AI Applications: Challenges and Solutions

verfasst von | submitted by

Diba Khaeez

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt | Post-graduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht (LL.M.)
Betreut von | Supervisor:	Dr. Lukas Feiler

The Role of Consent in Data Protection in the European Union for AI Applications: Challenges and Solutions

Diba Khaeez

Supervisor: Dr. Lukas Feiler

Contents

Abstract

In the last decades, the swift development of artificial intelligence (AI) technologies has changed countless aspects of our daily lives, from personalized recommendations and virtual assistants to automated decision-making systems in various areas. These developments considerably rely on collecting and analyzing enormous quantities of personal data, which raises serious questions regarding protecting people's right to privacy. As data-based AI applications become increasingly universal, the role of consent as a legal basis for data processing has emerged as a crucial topic in data protection.

The fundamental basis for guaranteeing people's control and autonomy over their data has long been the idea of consent, as safeguarded by data protection laws and regulations across the European Union (EU).

However, due to the special characteristics of Artificial intelligence technologies, their need to progress, the complexity of data processing activities, and the possibility for unexpected

uses and reuses of data, the submission of consent in the context of AI, presents several issues.

This thesis aims to explore the different issues surrounding the role of consent in data protection for AI applications in EU regulations, examining the challenges it faces and proposing potential solutions to address them. By exploring the legal and ethical implications of consent within the context of AI, this research will contribute to the ongoing dialogue on the connection between data protection and AI governance.

Research Objectives:

a) To examine the legal and ethical implications of using consent as a basis for data processing in the context of AI applications.

b) To analyze the challenges and limitations associated with obtaining informed and meaningful consent in the context of AI.

c) To propose practical solutions and recommendations for policymakers, organizations, and individuals to address the challenges related to consent and data protection in AI applications.

Methodology:

The primary research method for this study is a literature review. In addition, a Qualitative research method, a survey, will be conducted to gather the insights and personal experiences of individuals in the case of using AI applications.

The survey aims to:

1. Assess awareness of terms and conditions when signing consent for AI applications.

2. Identify the extent of harm caused by inadequate understanding of these terms.

Target Audience: Men and women aged 20 to 40 living in the European Union, representing active AI users.

Sample Size:

In this survey the online collected samples were 50 to 100 participants.

Survey Instrument:

For collecting data a structured questionnaire by researcher was designed in 9 closed-ended questions.

Data Collection:

Online survey to ensure accessibility and voluntary participation.

Data Analysis: Quantitative data analyzed statistically.

Ethical Considerations: Informed consent was obtained, and privacy and data protection were ensured.

This research will employ a multidisciplinary approach, combining legal analysis and case studies to illustrate the challenges and potential solutions. The study will involve a detailed review and analysis of relevant legislation, regulations, and guidelines concerning data protection, consent, and AI applications.

Abstract (German)

In den letzten Jahrzehnten hat die rasante Entwicklung von Technologien der künstlichen Intelligenz (KI) unzählige Aspekte unseres täglichen Lebens verändert, von personalisierten Empfehlungen und virtuellen Assistenten bis hin zu automatisierten Entscheidungsfindungssystemen in verschiedenen Bereichen. Diese Entwicklungen basieren wesentlich auf der Erfassung und Analyse enormer Mengen persönlicher Daten, was ernsthafte Fragen hinsichtlich des Schutzes des Rechts auf Privatsphäre aufwirft. Da datenbasierte KI-Anwendungen zunehmend universell werden, ist die Rolle der Einwilligung als Rechtsgrundlage für die Datenverarbeitung zu einem zentralen Thema im Bereich des Datenschutzes geworden.

Die grundsätzliche Basis für die Gewährleistung der Kontrolle und Autonomie der Menschen über ihre persönlichen Daten wurde lange Zeit in der Idee der Einwilligung gesehen, wie sie durch Datenschutzgesetze und -vorschriften in der Europäischen Union (EU) geschützt wird.

Aufgrund der besonderen Eigenschaften von KI-Technologien, ihres Fortschrittsbedarfs, der Komplexität der Datenverarbeitungsaktivitäten und der Möglichkeit unerwarteter Nutzungen und Wiederverwendungen von Daten stellt jedoch die Einholung von Einwilligungen im Kontext der KI verschiedene Probleme dar.

Diese Arbeit zielt darauf ab, die verschiedenen Probleme im Zusammenhang mit der Rolle der Einwilligung im Datenschutz für KI-Anwendungen in EU-Vorschriften zu untersuchen, die Herausforderungen darzulegen und mögliche Lösungen zur Bewältigung dieser Herausforderungen vorzuschlagen. Durch die Untersuchung der rechtlichen und ethischen Implikationen der Einwilligung im Kontext der KI wird diese Forschung einen Beitrag zum laufenden Dialog über die Verbindung von Datenschutz und KI-Governance leisten.

Forschungsziele:

a) Untersuchung der rechtlichen und ethischen Implikationen der Nutzung von Einwilligungen als Grundlage für die Datenverarbeitung im Kontext von KI-Anwendungen.

b) Analyse der Herausforderungen und Einschränkungen im Zusammenhang mit der Einholung einer informierten und bedeutungsvollen Einwilligung im Kontext von KI.

c) Vorschlag praktischer Lösungen und Empfehlungen für politische Entscheidungsträger, Organisationen und Einzelpersonen zur Bewältigung der Herausforderungen im Zusammenhang mit Einwilligung und Datenschutz in KI-Anwendungen.

Methodologie:

Die primäre Forschungsmethode für diese Studie ist eine Literaturübersicht. Zusätzlich wird eine qualitative Forschungsmethode, eine Umfrage, durchgeführt, um die Einsichten und persönlichen Erfahrungen von Einzelpersonen im Zusammenhang mit der Nutzung von KI-Anwendungen zu sammeln.

Ziele der Umfrage:

1. Bewertung des Bewusstseins für die Allgemeinen Geschäftsbedingungen bei der Unterzeichnung von Einwilligungen für KI-Anwendungen.
2. Ermittlung des Ausmaßes der durch ein unzureichendes Verständnis dieser Bedingungen verursachten Schäden.

Zielgruppe:

Männer und Frauen im Alter von 20 bis 40 Jahren, die in der Europäischen Union leben und aktive KI-Nutzer darstellen.

Stichprobengröße:

Bei dieser Erhebung wurden online Stichproben von 50 bis 100 Teilnehmern erhoben.

Umfrageinstrument:

Für die Datenerhebung wurde vom Forscher ein strukturierter Fragebogen mit 9 geschlossenen Fragen entworfen.

Datenanalyse:

Quantitative Daten werden statistisch analysiert. Ethische Überlegungen: Einwilligung nach Aufklärung eingeholt, Privatsphäre und Datenschutz gewährleistet.

Diese Forschung wird einen multidisziplinären Ansatz verfolgen, der rechtliche Analysen und Fallstudien kombiniert, um die Herausforderungen und potenziellen Lösungen zu veranschaulichen. Die Studie wird eine detaillierte Überprüfung und Analyse relevanter Gesetze, Vorschriften und Richtlinien im Zusammenhang mit Datenschutz, Einwilligung und KI-Anwendungen umfassen.

Keywords: Artificial Intelligence, Consent, GDPR, Personal data protection,

Introduction:

The EU General Data Protection Regulation (EU-GDPR), adopted in 2016, has significantly reshaped the field of data protection[1] . Its main goal is to give individuals more control over their personal data to reduce privacy risks and give them increased protection. The GDPR includes specific restrictions on the use of data, such as Article 22, which grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, that significantly affects them. Profiling uses algorithms to find connections between different datasets, which can then be used to predict behavior or control access to services[2].

Importantly, even when processing is based on the legitimate interest of the controller under Article 6(1)(f) GDPR, if such processing involves automated decision-making as described in Article 22, the additional requirements of Article 22(2) must also be met (cf. ECJ C-634/21). This means that the controller must ensure that the processing falls within one of the exceptions outlined in Article 22(2), such as obtaining explicit consent or ensuring that the decision is necessary for a contract.

The GDPR introduces new obligations that make it distinct from previous laws. The main difference between GDPR and previous laws is the emphasis on individual protection, the rights to access and transparency, the obligations that the controller must fulfill, and data protection by design, and by default. One of the most significant obligations for collectives, institutions, and companies is the obligation to obtain the proper consent for the processing of sensitive personal data. Even receiving consent for processing personal data needs collectives to meet several examinations and conditions as they are mentioned in Chapter 2 of GDPR.

Control of accuracy over personal data directly affects well-being since highly mistaken judgments might be made about individuals. This is especially important in the frameworks

[1] Saheb, T. and Saheb, T. (2024) 'Mapping Ethical Artificial Intelligence Policy Landscape: A Mixed Method Analysis', Science and Engineering Ethics, 30(2), p.9.
[2] Regulation (EU) 2016/679 (General Data Protection Regulation) art 4(4).

of AI. It transfigures the type of factors, capacities, and decisions that people are subject to. Therefore, the European Union parliament and the council adopted Regulation (EU) 2016/679 on April 27, 2016 (GDPR), which changed the rules for the collection, distribution, sharing and use of personal data. This involves new challenges related to permission to process personal data for various AI systems, lawful decision-making, profiling, and non-automated processing, as well.

In Article 4 of GDPR a concept of profiling is defined as "means any form of automatic processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements".

The purpose of this thesis is to delve into the risks and consequences following consent for AI applications to apply and use personal data. The research also seeks to conduct a survey of data protection authorities and sensitivity levels in personal information as per the GDPR regime for analyzing how adequately is AI using personal privacy under control by the regulatory framework set forth under the GDPR. To have a comprehensive view, it is necessary to first examine the different aspects of AI, including its definition, the types of data it requires, and the relevant provisions of GDPR. As such, this study will initially explore these fundamental concepts before examining the effects of consent in the context of AI applications.

1. Introduction to Artificial Intelligence

Nowadays, the term Artificial Intelligence has multiple definitions, which vary depending on the field of discussion. These fields range from natural sciences and engineering to phi-

losophy, politics, economics, and others. Unlike in engineering, where many terms are formally defined by organizations responsible for establishing technical standards, AI is often defined through the agreement of the scientific community.[3].

This thesis presents a study on the role of giving consent to AI systems to use individual's personal data, which approaches important questions such as: what is the relation of AI with data and knowledge? Can AI work mainly without the use of data? What techniques are used in AI to process the data?

To answer the mentioned questions, it's necessary to know that the computational model of AI is based primarily on logic, more specifically on a formalization of human reasoning[4]. Data is the basis of all applications of AI techniques, unlike most software construction projects that only use the data to affect the algorithms that are executed in the application. More than a structured process, AI is a knowledge-intensive process, or as defined by engineers, it is a knowledge-based system. Although there are AI techniques that do not depend directly on data, this situation is an exception, rather than a rule[5].

1.1Definition and Scope

AI is a field that focuses on developing machines that can mirror human intelligence, primarily through computer systems. This involves the ability to learn, set rules, and then use them to infer a logical conclusion or approximate solution[6].

AI is such a vast area of technological development and application with relevance in multiple subfields and domains. Machine learning (ML) research, algorithms evolve that enable computers to learn something from data as well as make predictions or decisions, is one

[3] 'AI Guide for Government: A Living and Evolving Guide to the Application of Artificial Intelligence for the U.S. Federal Government' (AI Guide for Government) https://coe.gsa.gov/coe/ai-guide-for-government/print-all/index.html accessed 18 June 2024.
[4] Logic-Based Artificial Intelligence' (first published 27 August 2003, substantive revision 27 February 2024).
[5] I.C. Baierle, M.A. Sellitto, R. Frozza, J.L. Schaefer, and A.F. Habekost, 'An Artificial Intelligence and Knowledge-Based System to Support the Decision-Making Process in Sales' (2019) 30(2) South African Journal of Industrial Engineering 17.
[6] Teztecch, 'Artificial Intelligence is the Simulation of Human Intelligence Processes by Machines, especially' (Medium, 12 January 2020) https://medium.com/@teztecch/artificial-intelligence-is-the-simulation-of-human-intelligence-processes-by-machines-especially-5ca1b0c828ec accessed 18 June 2024.

key aspect of AI. Another equally significant area of AI is Natural Language Processing (NLP), which enables the computer to understand, interpret, and produce human language, thus used in business chatbots for customer service inquiries and translating languages[7]. Robotics stands for the design and deployment of robots involved in tasks in manufacturing, healthcare, and services. Even more specifically, the inclusion of machine learning through artificial intelligence into computer vision has enabled it to interpret visual data for applications in facial recognition, object detection, and autonomous vehicles. Furthermore, practiced systems aim to replicate the decision-making capability of human experts in areas such as medicine, finance, and engineering so that the machine bears judgment and only a small human role[8].

Artificial intelligence has a bright future because it is finding its way into many areas of relevance. AI can make a difference in health as well, such as personalized treatments and better diagnosis. Even robot-assisted surgeries are done today[9]. The finance industry is also benefiting from AI, using it for automated trading, identifying risks, and fraud detection. Education is being transformed with AI-powered adaptive learning platforms and auto-grading[10].

The entertainment industry is currently using AI in content recommendation and the creation of new games.[11]. Meanwhile, as AI grows, it's very important to give attention to ethical considerations in order to come up with rules that assure its fair and transparent use. There are several challenges to the potential promising future of AI, related to ethical and social effects, such as bias, privacy concerns, job displacement, and decision transparency.

[7] Liran Antebi, 'Fields of Artificial Intelligence' in ‘Artificial Intelligence and National Security in Israel’ (INSS 2021), 41-45.

[8] S Popenici, S Kerr, E Pantelis, A Moutsatsos, K Zourari, W Kilby, C Antypas, P Papagiannis, P Karaiskos, E Georgiou, and L Sakelliou, 'Exploring the Impact of Artificial Intelligence on Teaching and Learning in Higher Education' (2017) 37 Med Phys 2369-79.

[9] J Awwalu, A.G. Garba, A Ghazvini, and R Atuah, 'Artificial Intelligence in Personalized Medicine: Application of AI Algorithms in Solving Personalized Medicine Problems' (2015) 7(6) International Journal of Computer Theory and Engineering 439.

[10] European Central Bank, ‘Financial Stability Review, May 2024’ <https://www.ecb.europa.eu/press/financial-stability-publications/fsr/html/ecb.fsr202405~7f212449c8.en.html> accessed 11 September 2024.

[11] Z Jan, F Ahamed, W Mayer, N Patel, G Grossmann, M Stumptner, and A Kuusk, 'Artificial Intelligence for Industry 4.0: Systematic Review of Applications, Challenges, and Opportunities' (2023) 216 Expert Systems with Applications 119456.

Steps against these are relevant for the responsible development and deployment of AI technologies so that their impact brings benefits to society while minimizing potential harm.

This study focuses on machine learning models and Natural Language Processing (NLP) both running with algorithms that require data to operate and constantly hammering home the message of the importance of data availability in facilitating the continuous processing ability and associated decision-making of such models.

This analysis focused on AI applications that employ technologies such as Facial Recognition, Recommendation Systems, Chatbots, and Medical Imaging Analysis. To provide a clearer understanding, a few notable examples including ChatGPT, Siri, Alexa, and Google Assistant, which establish the practical implementations, effectiveness and indeed challenging sides of these AI technologies, will be highlighted.

1.2 Artificial intelligence and personal data

Legal, ethical, privacy, and security requirements are crucial for harmonizing sensitive data in AI applications[12].To prevent the potential conflicts in those areas, principles of data minimization, informed consent, transparency, and data security need to be supported. The attempt to create and describe metadata models[13] that harmonize datasets in a way that complies with the legal and ethical principles of the EU becomes more difficult than ever.

The focus of this thesis is to signify the most important legal systems in the EU, describing the characteristic regulation of personal data within the GDPR, as well as their model to inform and create a fundamental understanding of the AI that is applied to develop new analysis tools and services over sensitive datasets. As we have established the significance of addressing the challenges in AI research, a pressing question arises: What specific capabilities of Artificial Intelligence pose concerns about ethical and legal consequences?

[12] Haridimos Kondylakis, Rocio Catalan, Sara Martinez Alabart, Caroline Barelle, Paschalis Bizopoulos, Maciej Bobowicz, Jonathan Bona et al, 'Documenting the De-Identification Process of Clinical and Imaging Data for AI for Health Imaging Projects' (2024) 15(1) Insights into Imaging 130.
[13] ML Metadata (MLMD) is a software library designed to track and retrieve metadata related to machine learning development and data science workflows, facilitating efficient data discovery and collaboration.

The amount of personal data that AI systems can process is more efficient than any human ever could, and the volume of this information is greater than any library that ever existed. The concept of this big data is often characterized by the three Vs: volume, velocity, and variety. Volume refers to the massive scale, and velocity meaning the real-time data processing, and variety surrounding the diverse sources and formats of data[14]. Each one of these three Vs can cause potential risks.

As mentioned earlier, AI systems can analyze patterns, make predictions, and offer personalized recommendations. For instance, AI can modify marketing campaigns to individual preferences, improve healthcare outcomes through personalized treatment plans, and enhance user experiences by customizing digital content[15].

However, the most predictable point after considering the AI's abilities for the collection, storage, and use of personal data, is that with this amount of power that human gave to the AI, we should expect several complex issues.

The nature of AI systems, as defined under the AI Act is software developed with certain techniques that can produce various outputs of content, predictions, or decisions.[16], often needs a remarkable amount of data to function well and continue improving. This is just as often sensitive personal data that includes medical records, financial information, or personal communications. This kind of data is very sensitive; therefore, an AI system becomes a goldmine for cybercriminals. There are several cases that highlight how much data stored by AI is valuable for cybercriminals that they even attempt cybercrimes against companies with the highest levels of cyber security.

For instance, In July 2019, Capital One company[17] discovered that an outside individual had gained unauthorized access to the personal information of approximately 100 million

[14] Sheshadri Chatterjee and N.S. Sreenivasulu, 'Personal Data Sharing and Legal Issues of Human Rights in the Era of Artificial Intelligence: Moderating Effect of Government Regulation' (2019) 15(3) International Journal of Electronic Government Research 21-36.
[15] Penfriend, 'Targeted Advertising with AI' (Penfriend) https://penfriend.ai/blog/targeted-advertising-with ai#:~:text=The%20Role%20of%20AI%20in,data%2C%20creates%20personalized%20advertising%20messages accessed 04 June 2024.
[16] Artificial Intelligence Act (2024) Article 3 https://artificialintelligenceact.eu/article/3/ accessed 20 August 2024.
[17] MDL No. 1:19md2915 (AJT/JFA).

U.S. and 6 million Canadian credit card customers and applicants, including names, addresses, and dates of birth. The perpetrator was quickly caught by the FBI, and the stolen data was believed to be recovered without evidence of fraud or distribution[18].

The remarkable part of this cybercrime is that the hacker uses the AI-based chat box of the bank to access the personal data of the Capital One company's customers. After this incident, the company has enhanced its cybersecurity measures and is offering free credit monitoring to those affected. A U.S. federal court preliminarily approved a class action settlement regarding this breach in February 2022[19].

For such reasons, AI systems must be secured in accordance with standard security regulations. Different guidelines and privacy standards apply across various jurisdictions worldwide [20]. Since its establishment in 2004, ENISA, the European Union's agency for cybersecurity, has been dedicated to promoting a high level of cybersecurity across Europe, with the EU Cybersecurity Act further empowering its mission [21]. Failure to follow these guidelines can lead to irreparable incidents which will be discussed further.

Another potential issue that is directly related to the characterization of Artificial intelligence is AI's ability to analyze and personalize personal data. This feature can lead to misuse, particularly when data is collected or used without proper consent. This misuse can appear in several different forms, including targeted advertising, political manipulation, and discrimination[22].

For example, in the advertising and marketing industry, Artificial Intelligence systems can transform raw behavioral data into targeted marketing messages by applying machine learning algorithms to forecast user preferences and purchasing behaviors based on past activity. The application of AI-powered personalization in marketing, while offering the potential subject market to modify advertisements to individual preferences, may eventually result

[18] Capital One Data Breach' (CNN, 29 July 2019) https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html accessed 03 June 2024.
[19] Capital One, 'Capital One Cyber Incident' (2019) https://www.capitalone.com/digital/facts2019/ accessed 03 June 2024.
[20] OWASP, 'AI Security and Privacy Guide' (OWASP) https://owasp.org/www-project-ai-security-and-privacy-guide/#how-to-address-ai-security accessed 03 June 2024.
[21] Cybersecurity of AI and Standardisation' (March 2023).
[22] Barredo Arrieta A and others, "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI" (2020) 58 Information Fusion 82.

in unintended consequences, including the potential for consumers to overconsume unnecessary products and services leading to financial losses over time[23].

In the case of political manipulation, there are different opinions about whether AI is more useful or harmful in this matter. AI's capability to analyze enormous datasets would help political campaigns with deep insights into voter preferences, behaviors, and thoughts (politicians' views); by examining social media communications, browsing habits, and other online traces, AI algorithms can construct comprehensive voter profiles that accurately predict individual leanings[24].

With this information, political entities can customize their messaging to appear to distinct demographic groups, crafting personalized communications that engage voters emotionally and ideologically. Furthermore, AI-driven voter targeting develops micro-targeting techniques to interact with individuals on a personal level, allowing campaigns to adjust messages to align closely with an individual's values and interests, thus enhancing their convincing effectiveness and increasing the chances of gaining support and eventually the votes. This accuracy enables campaigns to judiciously allocate resources and focus on key voter groups essential for achieving electoral success[25].

One of the most significant cases related to political misuse of personal data is the Cambridge Analytica scandal[26]. In this lawsuit restricting from the Cambridge Analytica scandal, Facebook users accused the company of compromising their personal information by sharing it with third parties (D. Trump campaign[27]) without proper consent and failing to prevent its misuse. The users allege that Facebook shared extensive sensitive content, such

[23] Penfriend, 'Targeted Advertising with AI' (Penfriend) https://penfriend.ai/blog/targeted-advertising-with ai#:~:text=The%20Role%20of%20AI%20in,data%2C%20creates%20personalized%20advertising%20messages accessed 04 June 2024.
[24] Busola Simon-Ilogho, Tola Kehinde, Kemi Kehinde, and Segun Kehinde, *Exploring the Impact of AI on Voter Confidence and Election Information in 2024* (2024) <https://doi.org/10.32388/UT898Q> accessed 11 September 2024.
[25] S Rayhan and S Rayhan, 'The Role of AI in Democratic Systems: Implications for Privacy, Security, and Political Manipulation' (2023).
[26] FTC Matter/File Number 182 3107, Docket Number 9383
[27] Matthew Rosenberg, 'Cambridge Analytica Scandal Fallout' (The New York Times, 4 April 2018) https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html accessed 04 June 2024

as private messages, photographs, and political views, not just basic data like Names or dates of birth.

Facebook filed a motion to dismiss the case, arguing that users have no privacy rights for information shared with friends on social media and that no obvious harm resulted from the data spreading. However, the court rejected these arguments, emphasizing that sharing information with a limited audience on social media does not nullify privacy expectations, and a privacy invasion alone constitutes an injury sufficient for legal standing.

The court acknowledged that Facebook users might have consented to some data sharing in Facebook's terms and conditions but found that the complaint sufficiently contends many users did not consent to key practices. These practices include sharing data with whitelisted apps and Artificial intelligence systems and business partners and allowing misuse of the information. Therefore, most of the plaintiffs' claims were allowed to proceed, although some specific claims were dismissed. Eventually, Facebook was accused of allowing third parties to access personal data without sufficient consent, resulting in a $5 billion fine by the Federal Trade Commission (FTC)[28].

Last but not least, ethical and socio-technical[29] aspects, are the final examined issues about AI using personal data. There are many ethical concerns in this area and covering all of them could be beyond the subject of this thesis. However, one of the most troubling issues in giving consent to AI using personal data, which is directly related to the misuse of these data, is the potential for biased data within AI systems[30].

As previously mentioned, Artificial Intelligence is fundamentally dependent on data that is produced or collected by humans, such as user-generated content and information gathered through human-designed systems and algorithms. Therefore, any existing human biases can pass through these AI systems, often resulting in the increase of those biases due to the

[28] In re Facebook, Inc., 402 F. Supp. 3d 767 (N.D. Cal. 2019).
[29] E Ntoutsi et al, 'Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey' (2020) 10(3) Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery e1356.
[30] Roselli D, Matthews J and Talagala N, "Managing Bias in AI," Companion Proceedings of the 2019 World Wide Web Conference (ACM 2019) <http://dx.doi.org/10.1145/3308560.3317590> accessed September 12, 2024.

complicated nature of socio-technical systems, like the internet. As a result, algorithms can extend or worsen existing societal discriminations and forms of differences[31].

Within social frameworks, certain groups may experience disadvantages, leading to what is known as "institutional bias[32]." This refers to the partiality of various institutions to favor certain social groups while disadvantaging others, often not because of considered discrimination, but rather through adherence to existing norms. Common examples include institutional racism and sexism, which are surrounded by societal actions[33].

Furthermore, algorithms are often integrated within pre-existing biased institutions and systemic structures, which can increase or introduce further biases by prioritizing easily measurable aspects of human behavior while excluding those that are more nuanced or difficult to measure[34].

This situation is aggravated by the relative accessibility of certain datasets, which can lead to an overemphasis on platforms like Twitter when analyzing several social phenomena[35].

Once algorithms are applied, they tend to promote specific data collection methods and policies that may encourage observation and tracking, consequently modifying or enhancing power dynamics[36]. The relationship between algorithms and social structures remains complex and not completely understood. This complexity encourages researchers to advocate for “algorithmic responsibility” to gain deeper insights into the biases, power structures, and societal influences surrounding within algorithmic systems [37].

---

[31] Fariba Karimi, Mathieu Génois, Claudia Wagner, Philipp Singer, and Markus Strohmaier, 'Homophily Influences Ranking of Minorities in Social Networks' (2018) 8(1) Scientific Reports 11077.
[32] IBM, 'Shedding Light on AI Bias with Real-World Examples' (IBM Blog) https://www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples/ accessed 05 June 2024.
[33] Daniel Chandler and Rod Munday, A Dictionary of Media and Communication (Oxford University Press, USA, 2011).
[34]Eirini Ntoutsi, Pavlos Fafalios, Ujwal Gadiraju, Vasileios Iosifidis, Wolfgang Nejdl, Maria-Esther Vidal, Salvatore Ruggieri et al, 'Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey' (2020) 10(3) Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery e1356.
[35] Yunpeng Zhao et al, 'Data and Model Biases in Social Media Analyses: A Case Study of COVID-19 Tweets' (published online 21 February 2022) PMCID: PMC8861742, PMID: 35308985.
[36]Lucas Introna and David Wood, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems' (2004) 2(2/3) Surveillance & Society 177-198.
[37] Nicholas Diakopoulos, 'Algorithmic Accountability: Journalistic Investigation of Computational Power Structures' (2015) 3(3) Digital Journalism 398-415.

One of the most remarkable cases in the matter of Artificial intelligence systems being biased, is the case of COMPAS[38], an AI system used in the U.S. criminal justice system to predict recidivism rates.

Judges, probation, and parole officers nationwide are increasingly using algorithms to assess a criminal defendant's likelihood of re-offending, with several states and academics developing their own tools alongside commercial merchants. There were several investigations about COMPAS, a tool by Northpointe, Inc., to evaluate its accuracy and potential bias. After analyzing over 10,000 defendants in Broward County, Florida, researchers found that while COMPAS correctly predicted general recidivism 61% of the time, its accuracy for violent recidivism was only 20%. The tool predicted recidivism for black and white defendants at similar rates but showed significant differences in misclassification: black defendants were often incorrectly labeled as high risk, and white defendants as low risk[39].

Specifically, black defendants who did not re-offend were nearly twice as likely to be misclassified as high risk compared to white defendants (45% vs. 23%), while white re-offenders were misclassified as low risk almost twice as often as black re-offenders (48% vs. 28%). Even after controlling the variable quantities like prior crimes, age, and gender, black defendants were 45% more likely to receive higher risk scores and 77% more likely to be shown as high risk for violent recidivism. This analysis highlights significant racial biases in the COMPAS algorithm, raising concerns about its fairness which is comprehensively explained in Article 5 GDPR, and accuracy in criminal justice decisions[40].

The case of COMPAS highlights significant concerns about bias and fairness in AI algorithms, particularly in critical areas like the criminal justice system, where misclassification can have reflective implications for individuals and communities.

[38] Case C-138/11

[39] Jeff Larson, Surya Mattu, Lauren Kirchner, and Julia Angwin, 'How We Analyzed the COMPAS Recidivism Algorithm' (ProPublica, 23 May 2016) https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm accessed 06 June 2024.

[40] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' (ProPublica, 23 May 2016).

Harmonizing sensitive data in AI applications requires strict observance of principles such as data minimization, informed consent, transparency, and robust data security measures[41].

In the following chapter, we will explore the processes through which these regulations are developed, highlighting the challenges and shortcomings that have led to various issues. Additionally, we will examine how the European Union has been required to harmonize these regulations in order to moderate potential problems and enhance overall compliance across member states.

2. Understanding Data Protection Regulations in the European Union

2.1 Introduction

One of the significant goals of the European Union is to create a legal framework applicable to personal data processing in this digital age[42].

To successfully protect something, it is essential to first clearly define what it is. In this context, the very first question is: What is the definition of personal data?

Based on Article 4 (1) GDPR, Personal data includes any information relating to an identified or identifiable natural person. In this article, also natural person is also defined and these comprehensive definitions role as a powerful guard for potential harm.

To recognize personal data, we can also remark on the definition of non-personal data. Non-personal data is almost the opposite of what is in Article 4 (1). It either never was personal or has been withdrawn of its ability to attribute to a single individual. Recital 26 of the GDPR says data is personal information if it "can be exploited for identification purposes," and identifies several ways this exploitation can happen, broadly stating that all available

[41] Oladoyinbo TO and others, "Exploring the Challenges of Artificial Intelligence in Data Integrity and Its Influence on Social Dynamics" (2024) 18 Asian Journal of Advanced Research and Reports 1.

[42] Heliskoski J, "Piet Eeckhout, External Relations of the European Union. Legal and Constitutional Foundations" (2005) 2 International Organizations Law Review 234

technologies could potentially identify articles with certain costs or time. If the data does not fit this criterion, it is classified as non-personal and is technically outside the scope of European data protection laws, meaning data protection principles do not apply[43].

Historically, Personal data is known as the foundation of privacy and data protection[44], which have been among the honorable values protected with several international and regional instruments.

Nowadays, the right to personal data protection is protected and guaranteed in Article 8(1) of the EU Charter of Fundamental Rights, which has legally binding force, and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). Rights established by the EU Charter of Fundamental Rights are equally valid as the Treaty[45].

The system of protection of personal data established by the EU is regulated mainly by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC GDPR[46].

GDPR establishes a general framework for the protection of natural persons regarding the processing and free movement of their personal data. It is a regulation of the EU data protection policy aimed at synchronizing the encouragement and protection of innovation and economic growth with more effective protection of privacy and individuals' rights. This new standard of data privacy in the EU puts into action rigorous measures of data protection to guarantee the protection of the personal information of individuals[47].

Meanwhile, GDPR provides for extraterritorial application of its rules with respect to companies processing personal data of data subjects in the EU. This application is irrespective of where the companies are based which can be found under Article 3 of the GDPR. In addition, Article 27 GDPR requires companies not established in the EU but covered by

[43] Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data Under the GDPR' (2020) 10(1) International Data Privacy Law 13

[44] European Commission, 'What Is Personal Data?' https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en accessed 7 June 2024.

[45] Everyone has the right to the protection of personal data concerning him or her.

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 25 July 2024.

[47] L Hemlali, 'The Competence of Non-Lead Supervisory Authority under the EU GDPR's One-Stop-Shop Mechanism: CJEU Judgment in Facebook and Others (C-645/19)' (2022) Journal of Media Law.

its provisions to choose a representative within the EU. It is one of the elements in the overall approach of the GDPR toward regulating cross-border personal data processing activities and finds special relevance in the context of AI[48].

Although the GDPR provided strong protection for personal data, regulators did not stop there. Recently, the EU Artificial Intelligence Act (AIA) has been launched and took personal data protection to a new level.

AIA categorizes AI systems into four categories regarding their risks. However, a fixed approach based on application areas might lead to overly strict regulations, particularly for versatile general-purpose AI (GPAI). Recent updates add various stages of evaluation for high-risk systems but remain inadequate. A proposed model of risk assessment inspired by climate risk frameworks provides a more precise, scenario-based method in the setting of AI risks since better regulation would not restrain innovation[49].

Despite the dynamic progress of new regulations, protection against a few high-risk AI systems remains insufficient. However, it is essential to recognize that as AI continues to advance and introduce new risks, these developments will be shaped constantly and challenge existing legal frameworks. Exactly like the way the evolution of data protection laws has progressed from its inception to the present day. In the following chapter, the long way of this process will be discussed.

2.2 History and Evolution of Data Protection Laws

To have a comprehensive understanding of personal data protection, it is essential to consider its historical context and foundational principles which we will briefly address in this section.

If we look back at time, we will find that the origins of protection of personal data laws date back to 1973 in Sweden[50]. When the practice of such laws was unknown or disapproving

[48] Dan Cooper, Lisa Peets, Mark Young, Kristof Van Quathem, Paul Maynard & Sam Jungyun Choi, 'European Commission Proposes GDPR Enforcement Procedure Regulation' (Inside Privacy, 5 July 2023).
[49] Claudio Novelli et al, 'Taking AI Risks Seriously: A New Assessment Model for the AI Act' (2023) AI & Society. P 1_5
[50] C J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

to many of the countries and territories around the world, the trend of data protection effectively started to increase to alarming coverage. In 1973, Sweden adopted the Data Act to protect individuals in the processing of personal data and each of the Nordic countries has since followed suit[51].

This principle first came into distinction as countries with developing structure strategies began to adopt relevant laws. The European Economic Community (EEC) collaborated with its member states from the Council of Europe to establish privacy protections, with a specific emphasis on the organization of personal data in Sweden. The International Protection of Personal Data Soon after, in 1981, the Convention for the Protection of Individuals. The system of allowance for these regulations was primarily implemented as a trademark to better enable these Nordic countries to compete with established economies and times, things, individuals, and entities were being targeted that belonged to the European Economic Community[52].

In the Treaty of 1981, which was amended in 1992 and again in 2001, although the Data Protection Directive was not originally intended to apply to police and other law enforcement authorities, the 1995 Treaty of Amsterdam called for this to be clarified. It was only in 1998 that the European Union adopted the Directive on the Protection of Personal Data. As a result, there is much history within the European Union, and a trend has emerged over the decades[53].

In the European Community (EC) and the EU since this beginning, the Data Protection Policy has found protection in Art. They were concerned about the protection of individuals regarding the processing of personal data and the free movement of such data, and particularly Article 286 of the ECT has been used by the European Communities as a legal basis[54].

[51] Sweden Data Protection Overview' (DataGuidance) https://www.dataguidance.com/notes/sweden-data-protection-overview accessed 25 July 2024.
[52] Convention 108: Background' (Council of Europe) https://www.coe.int/en/web/data-protection/convention108/background accessed 25 July 2024.
[53] *The Amsterdam Treaty* (Eur-lex) <https://eur-lex.europa.eu/EN/legal-content/summary/the-amsterdam-treaty.html> accessed 11 September 2024.
[54] BMKOES, 'Privacy Notice of the BMKOES according to Article 13 of the GDPR' (Data Protection Regulation) https://www.away.co.at/en/dsgvo/ accessed 28 June 2024.

2.3 Key Principles of Data Protection

Whenever the GDPR is mentioned, the importance of its principles is undeniable. GDPR regulation contains an extensive set of principles related to the processing of personal data that are mainly located in Articles 5, 6, and 9. The purpose of these principles is to protect of fundamental rights relating to the right of data protection such as informed consent, privacy, freedom, transparency, communication, and more.
These principles shall be applied to all those processing personal data such as natural or legal persons, public or private authorities, agencies or any other body[55].

The first key principles highlighting data protection within the European Union especially in Article 5 GDPR are:

'Lawfulness, fairness, and transparency'[56].

Lawfulness, the first principal, concerns conflicting or opposing values, and additional reasons to prohibit or disable AI-related applications or mechanisms, including, inter alia, not only human rights, fairness, autonomy, agency, efficiency, and the common good[57].

The second principle, Fairness, concerns risk to individual trust and well-being, justice and poverty, fairness and discrimination, democratic governance, rich nations imposing the risks generated by AI on poor nations heavily, remarkably heavy threats, distraction, responsibility, agreement, economic degradation through unemployment, opacity, exploitation, and inequality fuels abuses[58].

The last principle is about management transparency, including the human clarity of decisions, the documentation and supervision of decision-making processes by stakeholders,

[55] Laura Bradford, Mateo Aboy, and Kathleen Liddell, 'COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes' (2020) Journal of Law and the Biosciences 1, 8.
[56] Data Protection Commission, 'Principles of Data Protection' https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection accessed 28 June 2024.
[57] Brewczyńska M, "Between Legitimacy and Lawfulness: In Search of Rationality and Consistency in EU Data Protection" (2023) 9 European Data Protection Law Review 112.
[58] Malgieri G, "The Concept of Fairness in the GDPR," Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM 2020) <http://dx.doi.org/10.1145/3351095.3372868> accessed September 12, 2024.

and certifications and audit trails regarding the processes.
The principles mentioned above will be explained in more detail below[59].

Lawfulness means that handling of personal data in the EU shall be lawful when the data is processed in accordance with one or several requirements listed in GDPR.
These criteria involve obtaining the consent of the data subject, which will be thoroughly investigated in the following chapter. Additionally, there are obligations related to processing data in connection with a contract to which the data subject is a party, the need to obey to legal obligations, the requirement to safeguard the vital interests of the data subject or another individual, and the necessity of performing a task in the public interest or in the exercise of official authority[60].

For instance, Article 3 of the GDPR identifies territorial scope, meaning that the Regulation includes controllers and processors who are physically established and based in the EU or EEA, and those outside the EU/EEA who target individuals located within these countries.

This makes it applicable not only to foreign companies with target clients or customers located in Europe but generally to any entity operating within the European Union, as well as internet-based companies in so far as profiling takes place on individuals living in the EU, whatever the place of origin may be[61].

It is in this sense that data minimization forms a specific focus in the lawfulness of personal data processing. The likelihood of processing being lawful is increased to the extent that it is possible for new AI systems to be based on less, or at least less sensitive, data.

Fairness, however, is very broad in comparison with the lawfulness of the processing. Fairness means that handling personal data in the EU must be fair to the data subject. With this,

[59] Felzmann H and others, “Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns” (2019) 6 Big Data & Society 205395171986054.
[60] Christopher F Mondschein and Cosimo Monda, 'The EU’s General Data Protection Regulation (GDPR) in a Research Context' in Pieter Kubben, Michel Dumontier, and Andre Dekker (eds), Fundamentals of Clinical Data Science (Springer 2019) 55-71.
[61] M Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54(2) “Common Market Law Review”.

fairness is above all a matter of substantially addressing the rights and interests of individuals. It, therefore, gives unique protection to the data subjects on issues revolving around profiling and automated decision-making. For instance, Article 22 of the GDPR has put in place prohibitions and restrictions on profiling and automated decision-making. It has also established a requirement for human involvement in specified instances to prevent the harmful effects of an automated decision[62].

This principle also includes that the outcome of the profiling process cannot be a simple disallowance of social and legal rights or services. To ensure fairness, data controllers and processors cannot hide data practices from data subjects or use personal data in ways that would unjustifiably surprise them which guides us to the next principle, transparency[63].

Transparency introduces the idea that individuals should be provided with comprehensive information about a controller's data practices and activities. In fact, transparency is nearly always a good approach in establishing trust and satisfaction with data subjects and is strongly emphasized by the new Regulation.

The GDPR's provisions related to transparency are extensive. In summary, the controller of data, who is to determine for what purposes and by which methods personal data shall be processed, shall provide the following information:

(i) the identity and contact details of the controller of the data;
(ii) the means, and also the purpose of, processing, including the lawful grounds for the processing (as in Article 6);
(iii) the legitimate interests of the controller, if appropriate (as in Article 6(1)(f));
(iv) the recipients or categories of recipients of the personal data (as provided for in Article 13(1)(e));
(v) whether the personal data is to be transferred to a third country or to an international organization and, if so, what kind of guarantee is there (as in Article 13(1)(f)); and

[62] Andreas Häuselmann and Bart Custers, 'Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR' (2024) 52 Computer Law & Security Review 105942.
[63] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130-187.

(vi) the engagement to notify the subjects in case changes are made in the processing of personal data pertaining to them (as in Article 13(2)).
Also, the controller or collector has to inform the issues such as the right of deletion or restorations of the data regarding the data subject. For this, a cloud service provider is obliged by Art. 28.3d to ensure extensive information related to transparency in a contract.[64].

3. Specific Regulations for AI in the EU

Currently, there are various regulations within the EU that are related to the development of AI technology. In its exploration of the connection between AI and data processing, it becomes relevant to understand how these regulations interact with appearing frameworks. The interrelations of these two regulatory topics are explained on a chapter-by-chapter basis.

At the moment, the GDPR provides for the framework governing data protection and privacy within the European Union. The law is directly applicable in all EU Member States and engenders protection for individuals within the entire territory of the EU.

The fact that GDPR makes up practical legislation for data protection is undeniable; However, it does not particularly focus on AI. GDPR is directly applicable legislation to all EU Member States, with the aim of protection extending to persons living anywhere in the European Union. Although broad, this puts a basis for data protection, which is not specific to AI under the GDPR.
Several of the specific articles within GDPR hence impact AI significantly. Article 15 grants every data subject the right to access their personal data. Article 7 mentions the requirements to obtain valid consent. Article 20 provides for data portability, allowing people to obtain and reuse their personal data across different services. Article 22 restricts automated

[64] Data Protection Commission, 'Principles of Data Protection' https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection accessed 28 June 2024.

decision-making, including profiling, that significantly affects individuals Pseudonymization is the processing of personal data in such a manner that it no longer contains factors that allow for direct identification of a data subject, as defined in Article 4(5); it is used to reinforce privacy and the security of data.[65].

Article 9 prohibits the processing of sensitive data unless certain conditions are met, while Article 5 lays down principles for the lawful processing of personal data, such as requiring processing to be reasonable and limited to what is necessary. Moreover, it is mentioned under Article 37 that controllers and processors within certain organizations are to determine a data protection officer who should oversee and recheck the compliance with the provisions of the GDPR[66].

August 2024 marked the date of full entry into force for the Artificial Intelligence Act, which became a milestone for the regulatory approach towards artificial intelligence by the EU. The AI Act is a legislation that institutes an all-around legal framework which would be developed specifically to regulate AI technologies and their applications.
The new Act classifies AI systems according to the potential risk they pose to the protection of fundamental rights and safety.[67].

It clarifies the requirements for transparency, accountability, and adequate human oversight in the use of high-risk AI applications. The objective of this Act is to ensure that only safe, ethical AI systems, or those that respect the fundamental rights of the person, are used in the EU[68].

The proposal by the European Commission on the AI Act of April 2021 indicated the path toward such a framework. It is designed to enhance innovation in AI, while maintaining public trust and ensuring conformity of AI technologies with EU values and regulations. As a result, it counts as a complement to the previously existing data protection regulations in

[65] Cloudflare, 'What is Pseudonymization?' https://www.cloudflare.com/learning/privacy/what-is-pseudonymization/ accessed 29 July 2024.
[66] Inga Ulnicane, 'Artificial Intelligence in the European Union: Policy, Ethics and Regulation' in Thomas Hoerber and Gabriel Weber (eds), The Routledge Handbook of European Integrations (Taylor & Francis 2022).
[67] European Commission, Regulatory Framework for AI https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 20 August 2024.
[68] Holland & Knight, The European Union's AI Act: What You Need to Know (March 2024) https://www.hklaw.com/en/insights/publications/2024/03/the-european-unions-ai-act-what-you-need-to-know accessed 20 August 2024.

order to deal with specific challenges and risks associated with AI[69].
Moreover, in 2021, the AI report drafted by the Internal Market and Consumer Protection Committee (IMCO) passed at the European Parliament. Therefore, it has, from now on, called for a robust legal framework to guide as far as possible such AI products and services towards better consumer protection and quality of goods and services within the EU[70].

The AI Act categorizing is based on the degree of risk. Unacceptable risk and High-risk are the main categories. Unacceptable risk AI systems include those that will be prohibited because they are against the basic rights or EU regulations like abusing vulnerabilities, doing social scoring, using techniques that involve subliminal messages, or conducting biometric categorization to infer sensitive personal information. The high-risk AI systems are those that could significantly impact safety or fundamental rights. Such as, AI used for health, employment, finance, or law enforcement. These systems fall under the Act; it has provided for periodic review to keep pace with evolving AI use cases, and more guidance will follow before the rules go into effect in February 2025[71].

Another remarkable topic in AI act is that it has a few new definitions for AI systems providers. For instance, the definition by the EU AI Act as transparency is understood to mean that "the AI system should be developed and used in such a way as to enable traceability and explainability when a human is interacting with an AI." This includes information to the users and the people concerned about the capacities and limits of the system and the rights at issue. This focus on transparency will be the trusted frame through which to understand AI technologies and develop responsibility in the development and use of AI with strengthened accountability of market actors regarding their AI operations[72].

[69] J Laux, S Wachter, and B Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) 18(1) 'Regulation & Governance' p3.
[70] European Parliament, 'Regulation on Artificial Intelligence' https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence accessed 9June 2024.
[71] European Commission, 'Questions and Answers: What Will the EU Digital COVID Certificate Look Like and How Will It Work?' (Press Release, 17 March 2021). https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683 accessed August 25 2024.
[72] AI Act, 'Key Issue 5' (AI Act, 2023) https://www.euaiact.com/key-issue/5 accessed August 25 2024.

In conclusion, while the GDPR provides a foundation for data protection that applies to AI, the Act itself introduces special regulations regarding the challenges of AI technology providers. The two frameworks thus add up to contribute a holistic approach to handling AI's impact on data privacy and protection within the EU.

3.1 GDPR Compliance for AI Systems

Regardless of the significant day-to-day advances in AI technologies, the increasing deployment of AI systems worldwide has raised awareness of the insufficiency of existing personal data protection frameworks in addressing and taking under control AI-related concerns. In the European Union, which has recently put into force a new and strengthened regime known as GDPR, companies organizing AI are required to ensure that AI systems comply with the GDPR, especially if these systems process personal data. This section examines the compliance requirements of AI systems under the GDPR. To this end, we will introduce GDPR articles that are most relevant to AI, such as the right to explanation and strength, safety, and data accuracy requirements.

Article 22 GDPR specifically deals with automated decision-making, including profiling, with significant effects on individuals. This article is divided into two basic parts. Article 22(1) prohibits decisions based solely on automated processing in cases where they produce legal effects concerning the individual or similarly significantly affect them. That means that such important impact-making automatic decisions are limited under this provision.

Furthermore, Article 22(2) provides the data subject with the right to obtain human involvement on the part of the controller in the decision-making process, to express their point of view, and to contest the decision. From this perspective, procedures could not be deprived of persons in case their interests are affected by an automated decision falling within the significant effects or legal impact criteria.

Besides the rights previously mentioned in Article 22(1) and (3) GDPR, Article 5(1)(a) GDPR, under "Principles relating to processing of personal data," introduces further requirements with which AI systems have to comply in terms of the processing of data. In this regard, AI compliance refers to certain basic requirements that were discussed above,

such as transparency, lawfulness, and fairness. In view of that, compliance in accordance with Article 5 of the principles on data protection entails adherence to principles such as data integrity, purpose limitation, and storage limitation.

Article 5(1) then goes on to specify that the data has to be accurate and up-to-date, guaranteeing the integrity of data; it is supposed to be collected for specified purposes, not to be further processed in any way that happens to be incompatible with those purposes, and it cannot be stored for an unduly long period of time (storage limitation): kept in a form that permits identification of data subjects for no longer than necessary. Further, Article 5(2) establishes the accountability principle, requiring controllers to be able to demonstrate compliance with these principles[73].

Guaranteeing the reliability of AI systems is challenged by the characteristics of AIs such as dealing with constant data inputs. As mentioned above, due to the characteristics of neural networks[74], attackers can manipulate the model by directly changing model parameters. AIs have blurred the classic distinction and classification between training and application phases as their learning is continuous[75].

Model generalization is a key feature of AIs. For example, when an AI learns via training data to label some person as a doctor, the model will likely generalize and also learn things about that person, such as what he wears around his neck. The model might not have a medical response to the stethoscope but only learned that the doctor is shown with the stethoscope in its training data[76].

[73] J Alhadeff, B Van Alsenoy, and J Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in 'Managing Privacy through Accountability' (Palgrave Macmillan UK 2012) p49.
[74] A neural network is an approach in artificial intelligence that enables computers to analyze data by mimicking the way the human brain operates.
[75] Ying Yang and others, 'Harnessing the Power of Machine Learning for AIS Data-Driven Maritime Research: A Comprehensive Review.
[76] Haridimos Kondylakis, Rocio Catalan, Sara Martinez Alabart, Caroline Barelle, Paschalis Bizopoulos, Maciej Bobowicz, Jonathan Bona et al, 'Documenting the De-Identification Process of Clinical and Imaging Data for AI for Health Imaging Projects' (2024) 15(1) Insights into Imaging 130.

4. Challenges in GDPR

These developments in the field of artificial intelligence systems, raise important and increasingly urgent questions about how to ensure that modern governance frameworks can achieve the right balance between, encouraging much-needed invention and even revolution in the AI industry and placement of those progresses in areas like health and public safety, where the systems can provide significant benefits, and, also protecting the fundamental rights, including privacy, data protection, and non-discrimination.

At the policy and regulatory level, this requires addressing challenges that are both practical and ethical. Practical challenges arise from the natural characteristics of AI systems which cause complexity, uncertainty, and vulnerability of especially machine learning systems and other forms of AI with self-adaptive capacities[77].

Ethical challenges include, most importantly, the wider social problems that are raised when human evaluators and decision-makers are replaced by automated systems using a complex, high-dimensional analysis of input data. However, Ethical challenges are not simply about this replacement and will cause a wider range of dilemmas which we will check discuss further.

This thesis discusses four types of policy and regulatory options in this regard, all having their own dimensions of trade-offs between them. However, none are ethical or technical, as well as legally regulative-pointed pure solutions.

Policymakers are aiming to create and enact a suitable path or a guide when handling the challenges of AI-based systems, which could be operationalized and feasible through data, need decisions on several fronts. Questions around the balance an individual's privacy rights against public interest or the conflict between Individuals and the Collective are ethical paradoxes that cannot be solved gracefully in policy terms but will have a foundation-built mixtures of science and human values[78].

[77] Ying Yang and others, 'Harnessing the Power of Machine Learning for AIS Data-Driven Maritime Research: A Comprehensive Review.
[78] Chris Chiancone, 'Government AI Campus: Preparing Policymakers to Lead in the Age of AI' (7 October 2023).

For instance, are mobile phone-based AI applications that identify COVID-19 infection in individuals are considered as an incursion of privacy; A public health measure commensurate with the risk posed by the global pandemic underway or both - and how should we actually regulate these types?

To address such concerns, policymakers are urged to engage in a broad-based inquiry that embraces the unique questions spawned by AI and data protection regulations. Protecting individual privacy in a data-driven world and progressing the public's interest in an ethical manner will require policymakers to internalize the potential for hidden bias and privacy intrusions inherent in new machine systems, and account for them in public governance policy[79].

Ashley Lannquist, Project Lead for AI & Ethics at the World Economic Forum explains that "Some countries have already passed laws which command that AI systems must be ethical and follow the legal norms of responsibility or respect human rights; Some also require risk-mitigation. However, a challenge and tension that emerges when we attempt to regulate something as AI with laws or even legally binding policy is the many technical terms that can be unclear. One's idea of fair and unbiased differs so there is no rational definition to that yet. What this type of regulatory environment ends up looking like will be heavily determined by societal values and their expression in the legal system[80].

4.1 Balancing the Competition and Privacy

Artificial intelligence is widely identified as a general-purpose technology expected to lead and empower the next wave of economic growth. Early indications are that AI research, development, and employment will be heavily influenced by the competitive operation of the technology, so a lack of privacy protection for individuals could slow these developments in new technologies. Drawing the line between the protection of personal data and

[79] E Ntoutsi and others, 'Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey' (2020) Reviews: Data Science https://onlinelibrary.wiley.com/doi/abs/10.1002/da.1376 accessed 9 June 2024.
[80] Bias in data-driven AI systems: An introductory survey' (YouTube, 25 August 2020) https://www.youtube.com/watch?v=7AS0S51nlOY accessed 29 July 2024.

the progress in research and innovation in AI is a great and at the same time frightening task.

It is important to recognize that the preferences of various nations regarding trade and antitrust regulations can often come together in specific sectors, despite current policy discussions that may not reflect this alignment. It is also proposed to explore the idea of a plurilateral agreement focused on competition in the technology sector, which would encompass antitrust measures and protective regulations[81].

In the realm of telecommunications, the Economic and Financial Affairs Council (ECOFIN) made a significant ruling in 1988, stating that services utilizing "calling line identification" do not require user consent before implementation This ruling highlights the complexities of privacy and consent in different market structures. In a pre-regulated environment, companies are permitted to process personal data without obtaining consent from users. In the opposite situation, due to being in a competitive market, firms may choose to avoid such processing to ease the administrative obligation associated with obtaining consent from individuals[82].

This issue raises important questions about the extent to which privacy rights are maintained in various regulatory frameworks. In pre-regulated contexts, individuals may have reduced or weakened control over their personal information, leading to potential privacy infringements. The fundamental assumption of privacy infringement is closely tied to the conception of personal autonomy over another one's data, which is usually discussed in situations where consent is not obtained or valued[83].

However, it is necessary to consider the evolving global landscape of privacy regulations, such as GDPR in the European Union. As mentioned, these regulations emphasize the importance of user consent and data protection limits, prompting a second look at how companies handle personal data across different jurisdictions. As nations across their trade and antitrust strategies, aligning these policies with several strong privacy protections will be

[81] C van Ooijen, B Ubaldi and B Welby, *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance* (2019).
[82] European Council, 'Conclusions of the Presidency' (Strasbourg, 8-9 December 1989).
[83] Aline Blankertz, 'How Competition Impacts Data Privacy and Why Competition Authorities Should Care' (September 2020).

crucial in encouraging trust and ensuring user rights are respected across the digital economy.

5. Penalties

As previously discussed, it is necessary for companies and data collectors to stick to the range of regulations governing data protection and privacy. These laws have been established to safeguard individuals' rights and ensure responsible handling of personal information.

Therefore, non-compliance with these regulations can result in significant penalties, which are used both as a limitation and a means of enforcing responsibility.

The penalties for companies that fail to comply with data protection regulations can vary widely, depending on the jurisdiction and the seriousness of that infringement. In many jurisdictions, including the European Union under the General Data Protection Regulation, organizations may face significant fines that can reach millions of euros or a percentage of their global turnover which will be discussed comprehensively further. These financial consequences are designed not only to punish the non-compliance behaviors but also to encourage companies to prioritize data protection as part of their operational framework[84].

It is remarkable to mention that when GDPR became law, organizations significantly started to fulfill the new rulings as they intended to prevent the penalties. As a result, many companies began offering guidance, checklists, and consultancy services to assist businesses in complying with the new regulatory circumstances. During this period, artificial intelligence started to provide personalized advice, establish relevant questions and carry out assessments for them[85]. This approach, in the future, made the researchers aware of the potential of legal knowledge-based systems, which examining such AI systems is not relevant to this paper.

[84] F Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) 74 'Maine Law Review' p15
[85] Francesca Lorè, Pierpaolo Basile, Annalisa Appice and others, 'An AI Framework to Support Decisions on GDPR Compliance' (2023) 61 Journal of Intelligent Information Systems 541 https://doi.org/10.1007/s10844-023-00782-4 accessed 29 July 2024.

The consequences of non-compliance extend beyond financial fines. Companies can suffer reputational damage, which may lead to a loss of customer trust and potentially reduce their market position. In the age where public awareness of data privacy potential issues and rights is growing, customers are more likely to support organizations that demonstrate a commitment to protecting personal information. Thus, failure to comply with data protection laws can have long-lasting effects on a company's brand image and customer loyalty.

Apart from these fines and reputation risks, organizations may also be exposed to legal actions by the affected person or regulatory organizations, which further adds to operational troubles and financial liabilities. As businesses turn more and more to data for decision-making, marketing, and improvements, the need to understand and comply with data protection regulations is no longer a legal duty but a strategic imperative[86].

GDPR imposes administrative penalties for violations. Article 83 is the main provision dealing with these administrative fines. According to Article 83, fines can be as high as EUR 10 million or 2% of the total worldwide annual turnover in the preceding financial year, whichever is higher, for certain violations. These include breaches of obligations related to the principles of processing, data subject rights, and obligations of data controllers and processors[87].

Controllers and processors, Data protection by design and default, Records of processing activities, Cooperation with the supervisory authority, Security of processing, Notification of a personal data breach to the supervisory authority, Communication of a personal data breach to the data subjects, and Data protection impact assessment.

Penalties for violations of other obligations reach up to EUR 20 million or 4% of total worldwide annual turnover in the preceding financial year, again whichever is higher. These other obligations include:

Basic principles for processing, including conditions for consent, Rights of the data subjects, Transfers of personal data to third countries or international organizations, Infringements of the GDPR by a public authority, Non-compliance with an order by the supervisory

[86] F Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) 74 'Maine Law Review' p15

[87] GDPR.eu, 'GDPR Fines and Penalties' https://gdpr.eu/fines/ accessed 09 July 2024.

authority, Information for the national legislators, and Obligations of a supervisory authority[88].

The fines that are as a resolution of the non-compliance behaviors of collectors may be charged by the regulatory authorities like the Directorate-General for Competition (DG COMP), which is in charge for the application of Articles 101 and 102 TFEU and at the same time the punishment of the Commission Decision 2011/695/EU on the facilitation of inspections.

This chapter is filled with details on general compliance and fines; again, however, one needs to take these mechanisms in the context of the broader setting of regulatory enforcement, most notably, how they might interact with data protection and AI regulation. In this respect, charge imposition that derives from various authorities is relative to the importance of compliance, both regarding DP laws like the GDPR and regarding other regulatory frameworks in a way that would make an organization adhere to the law's demanding requirements within each area of its operation[89].

5.1 Case Studies

There are many active court cases related to breaches of the GDPR, some of which could be an introduction to the use of AI in non-compliance with GDPR[90].

In addition to exploring strategies for contesting algorithms that are in violation of the GDPR, it is equally important to investigate how the GDPR itself can be held responsible and apply sanctions on the use of artificial intelligence. In this context, court cases that have identified violations of GDPR regulations, specifically related to AI language models, can be the initiation signs for potential future complaints and legal challenges. Such cases not

[88] GDPRhub, 'Article 83 GDPR#https://gdprhub.eu/Article_83_GDPR#:~:text=If%20a%20controller%20or%20processor,specified%20for%20the%20gravest%20infringement accessed 09 July 2024.
[89] Directorate for Financial and Enterprise Affairs Competition Committee Working Party No. 3 on Co-operation and Enforcement, 'Access to the Case File and Protection of Confidential Information – Note by the European Union' (3 December 2019).
[90] M Van Bekkum and F Z Borgesius, 'Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?' (2023) 48 Computer Law & Security Review 105770.

only highlight existing violations but also set a precedent for addressing similar issues that may arise as AI technology continues to progress.

A very famous case in this context is the case of Spanish DPA vs Google. On May 18, 2022[91], the Spanish Data Protection Authority (AEPD) fined Google LLC €10 million for violating the GDPR. The violations affected Article 6 (lawfulness of processing) and Article 17 (right to be forgotten). The AEPD found that Google was sharing user data with the Lumen Project without a proper legal basis, and in a result blocking individuals' rights to erase their personal data.

Google offers a process for removing search results from Google Search and Google Maps, requiring users to provide personal information and reasons for removal. This information was then included in the publicly accessible Lumen Project database, which collects and discloses legal complaints and removal requests. The AEPD determined this practice as an infringement to the right of be forgotten (Data deletion).

The AEPD criticized Google for not providing an opt-out option for users and for failing to mention the data transfer to Lumen in its privacy policy. Additionally, the submission process led users through multiple pages, potentially causing them to select options unintentionally that might result in different regulatory treatments.

In response, Google stated it is reviewing the decision and working with privacy regulators to review its data-sharing practices. Google committed to changing its practices to comply with the GDPR and ensuring that personal data requested for removal is deleted from the Lumen Project[92].

In another recent case On August 10, 2023, the Portuguese Data Protection Authority (CNPD)[93] launched an investigation into the Worldcoin Foundation for its large-scale processing of biometric data, including irises, eyes, and faces, used to create digital identity profiles (World IDs). The CNPD found several GDPR violations after the foundation collected biometric data from over 300,000 people in Portugal, including minors, and made it

[91] E-10529-2021.
[92] AEPD (Spain) - E/10529/2021 https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_E/10529/2021 accessed 09 July 2024.
[93] Deliberação 2024/279.

impossible to exercise the right to remove or revoke consent. Additionally, they provided insufficient information to data subjects.

Worldcoin used a phone app and several in-person sites to gather data. Data subjects had to use a device called an 'Orb' to capture high-resolution images of their irises and faces for identity verification. However, the CNPD noted the absence of measures to verify ages, issues with consent forms being in English, and the impossibility of removal of the consent.

The CNPD concluded that Worldcoin violated Articles 5(1)(a), 7(3), 9(1), 13(2)(c), and 17(1) GDPR, emphasizing the infringement of consent and transparency, especially for minors. They imposed a three-month temporary processing ban due to the high risk to data protection rights and the irreversibility of violations. Similar actions were taken by the Spanish DPA and warnings were issued by the Italian DPA in early 2024[94].

6. The Role of Consent in Data Protection in AI

6.1 Introduction

In the prior chapters, we have thoroughly examined the critical challenges around data privacy within artificial intelligence systems and their applications. This chapter will focus on the essential role of consent in the functioning of these systems, exploring how it is obtained, managed, and its consequences for user autonomy and data protection.

We will analyze the legal and ethical frameworks that emphasize the concept of consent, considering the potential challenges that arise when people have interaction with AI technologies. These challenges may include issues related to informed consent, the complexity of AI systems, and the difficulties in guaranteeing users fully understand how their data will be employed and used.

[94] CNPD (Portugal) - Deliberação 2024/137 https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_Delibera%C3%A7ao_2024/137 accessed 09 July 2024.

Another purpose of highlighting this chapter is that to emphasize not only the importance of consent as a fundamental principle for data privacy in AI systems but also the complexities and responsibilities that accompanies should consider when collecting the data and want to achieve the consent of individuals.

AI systems are unstoppably affecting almost every aspect of our life. Algorithms are now being considered for complex tasks such as matchmaking people for romantic relationships, recruitment for employment opportunities, academic grading, advancing about different decisions, regulating social media, and many others. The main concern is the fact that many AI systems operate using sensitive data about humans such as health records, biometrics, browsing history, social behavior and such information which in real life people usually prevent to give them directly to the unknown collectors.

The protection and management of such sensitive data is a fundamental principle for a responsible and ethical use of AI. Unfortunately, the data protection communications which currently are adopted, is ineffective. It is being realized that a purely technical approach to data protection cannot work and that the responsibility of people is crucial in the collecting, management, and protection of socio-technical data[95].

To study about this aspect and being able to have a deeper understanding of the effects of each principle and its real-life consequences, I established a researcher-constructed questionnaire that was completed by 79 participants. The full survey along with the participants' responses will be included at the end of this thesis. In this chapter, we will also highlight selected questions which are related to each part and responses to enhance our understanding of the topic.

6.2 Definition of Consent in the Context of AI

The first question that might come to our mind is what does consent mean in general.

Consent is generally defined as the provision of permission, acceptance, or agreement.

[95] Control Over Personal Data: True Remedy or Fairy Tale?' (SCRIPTed, 2024) https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/ accessed 09 July 2024.

However, the concept of consent while mentioning collecting personal data, is a complex and multi aspect thought that represents one of the most important principles in Western ethics and law. This concept will be more complex when it is recognized that a commonly agreed definition of consent is missing among scholars and legal drafters[96].

While there are a few articles analyzing what consent means in other areas, e.g., bioethics, human rights, social sciences, sexual ethics, privacy, entertainment, and robotics, there is no comprehensive study about this concept around AI systems[97].
However, one will have to explain in respect of Under Article 4(11) of the GDPR, which defines "consent" of the data subject, whether freely given, specific, informed, and unambiguous means that the data subject has to give consent. Only the expressed intentions of the data subject should be considered, which would cover even the approach proposed above in this respect. This definition is very exact on what can be taken as valid consent and puts much weight on the need for it to be an active and conscious choice by an individual.

Article 7 of the GDPR further elaborates on what is meant by securing and demonstrating consent: Freely given: Consent already given must not be a subject of force, threat, fear, deception, duress, fraud, etc.; the person in question must be able to enjoy real freedom of preference. An officially declared form of force applied, instances of coercion, power imbalances, and grave negative consequences in cases of non-consent render consent not free (Article 7(4) GDPR).
Specific and Informed: In the same Article, it determines that processing activities should be specific in seeking consent, whereas the data subject must be informed on what he/she is consenting to. This includes clearly informing him/her of the purpose of the data processing, the identity of the controller, and the rights of the data subject.

Clear Affirmative Action: As it is mentioned in Recital 32 GDPR, Consent must be manifested by clear affirmative action from the data subject to indicate agreement, such as ticking a box on a website, signing a form, or any other statement or conduct which clearly

[96] Chunlin Leonhard, 'The Inconsistencies of Consent' (2022) 71(4) Catholic University Law Review 7.
[97] N Naik and others, 'Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?' (2022) Frontiers in ... https://www.frontiersin.org/articles/10.3389/f... accessed 09 July 2024.

indicates in specific manner his or her consent. Silence, pre-ticked boxes, or inactivity is not to be considered consent.

Right to Withdraw Consent: Article 7(3) does, indeed, emphasize that the data subject has the right to withdraw consent at any time, and it must be at least as easy to withdraw consent as it is to give it. Processing of the data has to come to an end when consent is withdrawn, unless there are other lawful bases for processing.

Burden of Proof: And eventually as mentioned in Recital 42 GDPR, a Data Controller should be able to demonstrate that there is consent and keep a record of when and how consent was obtained, in addition to what was said to the data subject when they provided the information.

Through the examining the different definitions of consent, it is visible that there are the some main themes present in all the definitions of consent in the context of AI systems that include making AI systems understandable, providing transparent information regarding the functionalities of AI systems along with the implications of such functionalities, and offering individuals and groups the option to determine whether the usage of AI systems aligns with their preferences, beliefs, and expectations.

6.3 Legal Frameworks and Regulations

The overuse of AI systems in recent years has raised questions about whether the application and use of such systems should be conditioned on the consent of affected people. These questions arise mostly with respect to AI systems that interfere with the privacy and civil freedom of individuals. For instance, algorithms that query and analyze biometric databases, algorithms that track and profile people in public spaces, algorithms that process sensitive information about people from social media and other systems like credit scoring that make determinations that may significantly affect people's lives[98].

Additional questions come up regarding the consent of third parties concerning AI systems, especially because private companies play a major role in their development and use. For better understanding, we can assume a new AI-based credit-scoring system that may depend

[98] Rowena Rodrigues, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities' (2020) 4 ‘Journal of Responsible Technology’ 100005.

on banks and insurance companies sharing financial data about individual clients. With these questions, you may not come up with straight answers but the point that is clear is that these systems should be restricted and strongly be controlled by a legal framework.

As discussed, the General Data Protection Regulation is a comprehensive legal framework that seeks to protect individuals' privacy. It obligates data collectors to have specific consent that must be obtained from individuals before processing their personal data. The GDPR applies to both personal data and sensitive personal data and permits general and explicit consent options.

Under GDPR consent and legitimate interest are two different legal bases for data processing. The controller shall have a legitimate interest in cases when personal data processing is necessary for the purposes of the legitimate interest pursued by the controller or a third party, except where such interests are overridden by the interests, fundamental rights, and freedoms of the data subject.

Consent, however, must be given freely, specifically, informed, and clear. Where consent is expressly foreseen, for example, Article 9(2)(a) GDPR, specifically in the processing of special categories of personal data, it must be in writing, clearly distinguishable from other matters presented to the data subject, and explicit. Explicit consent is called for in a number of situations—for example, in the processing of sensitive personal data or when an automated decision-making activity involves a legal or similarly important effect[99].

Deep learning-based AI systems often serve as Privacy-Enabled Services (PES) capable of creating shared learning models without revealing users' sensitive personal data[100]. However, by advantaging data sharing, these services benefit from users' involvement and interest in terms of access validation.

Various methodologies in the literature on AI-driven smart systems, privacy-preserving techniques, AI safety etc., deal with different aspects of this engagement when it comes to the question of how transparent a data usage should be, and its associations also lead to

[99] Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (17 April 2024).
[100] Norwegian Data Protection Authority, 'Artificial Intelligence and Privacy'https://www.datatil-synet.no/globalassets/global/english/ai-and-privacy.pdf accessed 29 July 2024.

compromised privacy. Very little, however, has been said about services using formal checkable technical processes that deliver consent states given and removed within the context of legal frameworks like GDPR[101].

According to the GDPR, individuals have the right to give and take back their consent for the processing of their personal data. However, users don't always actively express these decisions, which creates a need for systems that can clearly track and confirm users' consent in a secure and private manner[102]. Since consent is a crucial issue concerning personal data privacy and business considerations, it is important to manage it with reliability and strong privacy protections.

6.4Ethical challenges in AI Consent

The ethical consideration of AI systems focuses on how fundamental the concept of consent is to the ethical behavior of AI systems. Ethical AI systems are responsible, fair, and accountable. To enable AI systems to be ethical, they need to exhibit certain ethical considerations. Ethical considerations in the context of AI systems are transparent and explainable.

Transparency in AI systems refer to how clearly the systems reveal information about the input data, the algorithms they use, and the reasons behind their outputs. Explainability, in the other hand, is about making the reasoning processes of these systems understandable to people, helping them extent how the input data leads to specific outputs.[103].

As AI systems are increasingly integrated into various aspects of our daily lives, the idea of consent in relation to these technologies is being examined through an ethical lens. There are four main types of consent that highlight different perspectives on how consent should

[101] M Robol, TD Breaux, E Paja and P Giorgini, 'Consent Verification Monitoring' (2023) 32(1) ACM Transactions on Software Engineering and Methodology 1-33.
[102] Matthew Humerick, 'Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2017) 34 Santa Clara High Technology Law Journal 393.
[103] Renata Guizzardi and others, 'Ethical Requirements for AI Systems' in *Advances in Artificial Intelligence: 33rd Canadian Conference on Artificial Intelligence, Canadian AI 2020, Ottawa, ON, Canada, May 13–15, 2020, Proceedings* (Springer International Publishing 2020) 33.

be understood in the context of AI[104]. Additionally, the challenges related to consent and AI systems are discussed, along with the potential shifts in the roles of individuals involved in these technologies. To assist with these issues, 10 best practices are presented that shall enable consent in the context of AI systems while taking ethical considerations into account[105].

Furthermore, technological solutions are introduced that can assist with the better handling of consent considerations with AI systems. Some relevant case studies and observations are also introduced to illustrate how these challenges regarding consent with AI systems have been addressed.

6.5Transparency and Explainability

Transparency refers to the accessibility of data users have on AI systems. It significantly varies based on how the data is made accessible and comprehensible to the users. Transparency communications must meet certain reasonable expectations from the perspective of the various stakeholders involved[106].

A relational character must also be respected by AI system developers. The development and handling of an AI system creates a complicated web of relations between different parties. It is important to be aware that other stakeholders must also be considered. These stakeholders may include distinct categories of system users, regulators, watchdogs, or the public, depending on the nature and function of the system in question.

In the survey referenced, question three addresses transparency in AI systems with the query: “How informed do you feel about your data being used by AI applications?” Approximately 60% of respondents selected either "very informed" or "somewhat informed."

[104] Usercentrics, 'Guide to the EU AI Act' (18 July 2023) https://usercentrics.com/knowledge-hub/eu-ai-regulation-ai-act/#:~:text=Consent%20provisions%20in%20the%20AI%20Act,-User%20consent%20and&text=Transparency%20%E2%80%93%20AI%20providers%20must%20provide,potential%20impacts%20on%20their%20rights accessed 09 July 2024.
[105] Cognilytica, 'Top 10 Ethical Considerations for AI Projects' https://www.cognilytica.com/top-10-ethical-considerations-for-ai-projects/ accessed 09 July 2024.
[106] Md Tanzıb Hosain and others, 'Path to Gain Functional Transparency in Artificial Intelligence with Meaningful Explainability' (2023) 3(2) Journal of Metaverse 166-180.

This notable percentage shows a growing awareness among individuals regarding the use of their data in AI applications.

The results indicate that as Artificial Intelligence becomes increasingly included into various aspects of daily life, there is a corresponding rise in public understanding about data usage. This reinforced awareness reflects the efforts of data collectors and AI developers to enhance transparency and communicate more effectively about data practices.

Despite this progress, it remains crucial for data collectors to continue prioritizing transparency and ensuring that consent processes are clear and comprehensive. The survey results demonstrate that while improvements have been made, ongoing observation and commitment to best practices are essential to maintain and build upon this positive trend.

However, studies shows that while transparency and control are basic elements of privacy management, which may reduce emotional violation and suspicion of consumers, they do not engender sufficient protection of privacy[107].

Sometimes, transparency and control can be used as pushing mean to obtain more data disclosure from the consumers. Economic factors such as network effects and lock-in may worsen these problems since some firms are granted more data with increased powers to influence consumer behavior. Therefore, there are some studies that even criticizes the "responsibilization" approach[108] to privacy-reliance on consumer choice under a notice and consent regime for being ineffective, since it has failed to make it easy and affordable for them to achieve the levels of privacy, they want[109].

The next concept is ‘Explainability’; This definition is a critical aspect of AI systems, referring to how understandable and interpretable the decisions and actions taken by these systems are. It plays a critical role in obtaining trust between users and AI technologies, ensuring that individuals can comprehend, challenge, and trust the outcomes produced by these systems.

[107] Gone in 15 Seconds: The Limits of Privacy Transparency and Control (2013) 11 IEEE Security & Privacy 72 https://doi.org/10.1109/MSP.2013.86 accessed August 25 2024.
[108] Giesler M and Veresiu E, ‘Creating the Responsible Consumer: Moralistic Governance Regimes and Consumer Subjectivity’ (2014) 41 Journal of Consumer Research 840.
[109] Doe J and Smith J, ‘Secrets and Likes’ (2023) https://repository.arizona.edu/bitstream/handle/10150/649175/SecretsLikesR1_Submitted.pdf?sequence=1 accessed August 18 2024.

The European Commission has recognized the ethical implications of AI and has proposed guidelines that outline requirements for the development and deployment of responsible AI systems. Among these seven key requirements that have been identified, the fifth requirement emphasizes the need for systems to be designed and to be compatible with a high level of human oversight to minimize risk and harm[110].

This principle emphasizes the need for human involvement in data processing stages due to the significant risks posed by unjustified discrimination or the social sorting of specific groups, which could reduce certain individuals at risk. Integrating human oversight is crucial not only to safeguard equity but also to enhance accountability in AI operations. This necessity lays the foundation for obligations affecting to explainability, ensuring that the reasoning behind AI decisions is transparent and comprehensible[111].

In this context, the sixth requirement further underscores the importance of designing AI systems in a manner that allows for effective oversight of their outcomes by knowledgeable individuals, appropriate organizations, or regulatory authorities. This oversight mechanism should incorporate comprehensive procedures for verification, validation, and performance assessment. By establishing strong evaluation processes, we can ensure that AI systems remain in line with the ethical standards, maintain fairness, and operate effectively in real-world scenarios.

Moreover, the involvement of competent stakeholders in these oversight processes fosters a culture of continuous improvement, where insights gained from monitoring can be used to refine algorithms and enhance their outcomes. This collaborative approach not only strengthens public trust in AI technologies but also helps prevent potential harms associated with bias and discrimination, ultimately promoting a more just and equitable society.

6.6 Types of Consent in AI Systems

An AI system is a digital computation or data manipulation machine that can learn from experience and adapt to new environments. The parameters govern these adaptations. There

[110] Heike Felzmann and others, 'Towards Transparency by Design for Artificial Intelligence' (2020) 26(6) Science and Engineering Ethics 3333-3361.
[111] Alejandro Barredo Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI' (2020) 58 Information Fusion 82-115.

is a report of an event in an environment E perceived by an entity M and transmitted to an entity C. The act of transmission is performed with intention I by the perceiving entity M and is possible due to the existence of an object O in the environment.

The transmission is perceived by C as a change with right I2 in the state of E. Assume there is an AI entity within this architecture, learnt to consistently anticipate a state change in C's perception[112]. So, the AI can decide to act by initiating the transmission, learning and adapting due to experience detected there. This type of consent involves a mode of interaction where there is prior knowledge or information and readiness for that specific type of action or decision[113].

In the context of AI systems, it takes on distinct types of engagement with the process, which can be categorically classified as explicit or implicit consent [114].

Explicit consent means that the user has been made fully aware prior to the action or decision, negating any implicit assumption of acceptance. This includes formalized acceptance opt-in or opt-out clauses, terms and conditions contracts, privacy and usage policies, etc., wherein the user accepts the terms contained therein and the institutions have a record to prove the user's acceptance.

Implicit consent arises when there is no conscious awareness or agreement beforehand. Such consent can be assumed due to factors such as the extent of use, non-response to usage, ongoing partnerships, discussion, negotiation, or trust built-up in previous experiences[115].

Informed consent is viewed as a dialectic process of mutual accommodation between the researcher, on one side, and the participant(s), on the other side. It consists of three phases: pre-consent, consent, and post-consent[116]. Most issues related to informed consent, such as unclarity about how data will be used or inaccessibility of consent forms, arise in the pre-

[112] Michael Sipser, *Introduction to the Theory of Computation* (3rd edn, Cengage Learning 2013).
[113] Adam J Andreotta, Nin Kirkham and Marco Rizzi, 'AI, Big Data, and the Future of Consent' (2022) 37(4) AI & Society 1715-1728.
[114] Munindar P Singh, 'Consent as a Foundation for Responsible Autonomy' (2022) 36(11) Proceedings of the AAAI Conference on Artificial Intelligence.
[115] Luke Hutton and Tristan Henderson, 'Beyond the EULA: Improving Consent for Data Mining' in *Transparent Data Mining for Big and Small Data* (Springer 2017) 147-167.
[116] Ziang Xiao and others, 'Inform the Uninformed: Improving Online Informed Consent Reading with an AI-Powered Chatbot' in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023).

consent phase. Gaining consent, in comparison, is much clearer: it involves having either explicit consent or implicit consent.

Explicit consent refers to a declared set of affirmative actions, such as signing a contract or clicking an opt-in button. In the context of online research, the default is no participation, and consent must be requested from participants. Implicit consent, in contrast, refers to an inferred set of actions. Automatic enrollment in a study upon meeting a set of behavioral criteria is a common implicit consent practice.

There are several fundamental differences between explicit consent and implicit consent.

First, the burden of active engagement rests on the participant with explicit consent, but it is on the researcher with implicit consent. Second, explicit consent is usually more transparent than implicit consent. Though ideal circumstances may arise where implicit consent is transparent, this is rarely the case. Explicit consent reflects a more egalitarian power relation, making it easier for participants to reject participation. In comparison, implicit consent is embedded in an uneven or hierarchical power relation[117].

Potential participants may not even be aware that they are being studied. Understanding these basic differences between explicit consent and implicit consent is essential for addressing the major challenges posed by AI to informed consent, implementing best practices in the researcher-participant relationship, exploring technology-based solutions to safeguard participant interests, examining important case studies, and looking at future trends regarding the use of explicit consent vs. implicit consent[118].

In the survey, question number 9 asked participants, "How do you typically give consent for the use of your personal data by AI applications?" Approximately 75% of respondents indicated that they provide consent by clicking a checkbox or agreeing to terms of service. However, despite this high percentage suggesting a preference for explicit consent, it is important to note that in practice, many individuals do not thoroughly read or consider these

[117] Securiti.ai, 'Types of Consent' https://securiti.ai/blog/types-of-consent/#:~:text=The%20type%20of%20consent%20required,or%20inaction%20of%20the%20individual accessed 29 July 2024.
[118] Arndt Bialobrzeski, Jens Ried and Peter Dabrock, 'Differentiating and Evaluating Common Good and Public Good: Making Implicit Assumptions Explicit in the Contexts of Consent and Duty to Participate' (2012) 15(5) Public Health Genomics 285-292.

terms and conditions before giving their consent. This oversight can lead to a superficial understanding of the data collection and usage policies, which is concerning.

In contrast, question number 7 of the survey inquired, "Have you ever experienced any negative consequences as a result of sharing personal data with an AI application?" Here, about 81% of respondents reported that they had not experienced any negative consequences. This response suggests that, despite the lack of thorough engagement with the terms and conditions, these documents are generally designed in a way that minimizes harm to individuals from the use of their personal or sensitive data.

6.7 Challenges and Limitations

It is clear that a number of the challenges and limitations in the management of consent emerge partly or fully from the nature of AI systems: their complex systems nature, the use of algorithms that can be impervious to even the designers and developers and subject to continuous change, the limits of observability and explainability for the controllers, the potential for partial control and unintended consequences, and the grade of dependance on automation. Further, these challenges and limitations are combined in the case of AI systems used in sensitive contexts (to inform decisions that have data protection, privacy, financial, health or social consequence)[119] .

However, at the same time, there are many existing approaches within complex systems and many design principles from Human-computer interaction (HCI) with partially – but not fully – covering the relevance. This suggests ‘best practices’, examples of both problematic and well-implemented consent processes and environments, and potential technological solutions that are either emerging or could be designed[120].

As consent in AI systems is a recent development, there are few, if any, published case studies of consent processes, mechanisms or policies that deal with a broad and deep range of challenges, nor clear lessons learned[121].

[119] Luke Hutton and Tristan Henderson, 'Beyond the EULA: Improving Consent for Data Mining' in *Transparent Data Mining for Big and Small Data* (Springer 2017) 147-167.
[120] Interaction Design Foundation, 'Human-Computer Interaction' https://www.interaction-design.org/literature/topics/human-computer-interaction accessed 10 July 2024.
[121] Munindar P Singh, 'Consent as a Foundation for Responsible Autonomy' (2022) 36(11) Proceedings of the AAAI Conference on Artificial Intelligence.

The examination of several initial issues, concerns, and well-intentioned preventive / remedial designs is expected to produce a richer understanding of the future of consent in AI systems. There are well-established fields investigating the challenges of technological interventions on social life and the social impact of social technologies. While in general these perspectives have looked at unintended consequences, they have been extended to consider impacts from inception onwards, meaning the design process is as much a matter of justification as it is to create new social practices and meanings.

As AI technologies are deployed in ever more fields of decision-making, new and unexpected ethical questions arise and are accommodated or not by design and social norms and expectations evolve to settle into practice in unfair ways.

6.8 Informed Consent in Complex AI Systems

A high level of complexity is an important factor for data-processing systems to be classified as AI systems [122]. We should pay attention to AI systems that go beyond a certain level of complexity. This can include aspects like the number of factors or variables they consider and how complicated the relationships between those variables can be in the data-processing process.

It is remarkable to mention that there therein exists a challenging issue pertaining to the possibility of fully informed consent being attained within complex AI systems, or at least within certain classes of them. As will be shown, such a possibility is far from insignificant. Addressing the present question and prohibiting the possibility of fully informed consent greatly broadens the scope of ethical concerns regarding AI systems as decision-making agents[123] which already discussed in prior chapters.

It is important to note that while there are standards for what it means for a person to give fully informed consent, there is still a chance that someone might give consent without

[122] Lark Suite, 'Most Important Factors to Consider When Building AI Analytics System' https://www.larksuite.com/en_us/topics/ai-glossary/most-important-factors-to-consider-when-building-ai-analytics-system accessed 10 July 2024.
[123] Ziang Xiao and others, 'Inform the Uninformed: Improving Online Informed Consent Reading with an AI-Powered Chatbot' in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023).

really understanding what they are agreeing to. Not only because people are unable to read the whole terms and condition due to several reasons (Long text, time limitations and such), but they are unable to understand the concept of those terms in the field of their meanings.

This issue isn't just about ethics in AI; it also involves how we think and understand things. The way AI systems work is very different from how humans operate, so this intellectual aspect needs to be addressed separately.

Artificial intelligence systems process their input data, make decisions, and release output data in an entirely different way compared to human beings. Note that AI complexity and further non-linearity levels are by no means restricted to artificial neural networks (ANNs)[124].

There are many other types of AI systems, or more generally data-processing systems, that while being considered as mathematical or algorithmic constructs have by now become computationally unmanageable or too complicated to be detained in any rational way, including expert systems and genetic algorithms.

Understanding consent and what it means, especially in relation to informed consent phase, is very important when it comes to AI systems. This knowledge is essential for figuring out the best practices, technology solutions, real-life examples, and future directions in how we handle consent in today's AI.

6.9 Best Practices for Implementing Consent in AI

Commonly referenced as the "consent paradigm;" Afri-Fi, a project by Mozilla for providing free internet in south Africa, examines how AI-specific user controls and consent signifying a human-agent commitment to certain action characteristics can be designed for inclusivity among other things[125]. Additionally, spatial AI agents mapping environments

[124] Raphael Kaubruegger, Lorenzo Pastori and Jan Carl Budich, 'Chiral Topological Phases from Artificial Neural Networks' (arXiv, submitted 12 October 2017, last revised 19 May 2018) https://arxiv.org/abs/1710.04713 accessed 11 July 2024.
[125] Tom Kwanya and others, 'Responsible AI in Africa' (2023) https://doi.org/10.1007/978-3-031-08215-3 accessed 11 July 2024.

with no explicit action is also covered while pointing out the need for a balance of power between participants immersed in the spatial data meeting[126].

A best practice framework for managing consent in AI systems is created drawing from socio-technical systems literature, international best practices of design for transparency, data privacy by design frameworks, the CCARE (Context, Consent, Access, Retention, Ethics) framework, and individual industry codes of ethics [127].

These resources are widely referenced but not used holistically with consideration of AI system characteristics which brings unique design challenges.

It is also important to highlight that some tech companies are involved in data practices that don't align with best practices, often lacking defined mechanisms or incentives to protect users. The issues affecting participant well-being are made worse by the technologies and consent mechanisms currently in use. The discussion includes examining user-centric (will be discussed in next section) best practices, recognizing that the AI industry consists of global players with differing levels of regulation and attention to participant welfare[128].

Technologies for company regulation and remedies that are participant-centric are proposed and examples given. Industry standards for best practices and their effectiveness in protecting participants is discussed, along with issues regarding AI specificities and consent providers being simultaneously participants of the AI systems their members develop. A meta-analysis of best practices in consent contexts is conducted and solutions outlined for their implementation[129].

For each practice, general and AI specific challenges are outlined and examples from various industries are given that address issues encountered.

---

[126] The Alan Turing Institute, 'The Rapid Rise of Generative AI' https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai accessed 29 July 2024.
[127] Munindar P Singh, 'Consent as a Foundation for Responsible Autonomy' (2022) 36(11) Proceedings of the AAAI Conference on Artificial Intelligence.
[128] Youngsun Kwon and others, 'Harnessing Artificial Intelligence (AI) to Increase Wellbeing for All: The Case for a New Technology Diplomacy' (2020) 44(6) Telecommunications Policy.
[129] Anelia Kurteva, Tek Raj Chhetri, Harshvardhan Pandit and Anna Fensel, 'Consent Through the Lens of Semantics: State of the Art Survey and Best Practices' (2021) 15 Semantic Web https://doi.org/10.3233/SW-210438 accessed 11 July 202.

6.10 User-Centric Design Principles

This subsection emphasizes user-centric design principles, detailing how to implement consent effectively within AI systems. Grasping these principles is essential for understanding the technological solutions, case studies, and future trends associated with user-centric design in the realm of AI consent. By adopting a user-focused approach, developers can create systems that prioritize the needs and rights of users, enhancing their overall engagement and trust in AI technologies[130].

User-Centric Design Principles enshrined in an AI Consent Framework. The design principles in the framework aim to create a consent dialogue that empowers users to retain control over their data, while being provided with the necessary information and support. The principles were formulated from an exploration of the body of work conducted to date, including socio-technical studies on user understanding of Terms and Conditions, design work with individuals from different user groups, and a published set of ten AI Design Principles[131].

The user-centric design principles focus on the data subject as an individual with rights, considerations, and vulnerabilities to be considered[132]

Specifically, the principles are: Proactive: The system should not only passively present consent-related information but actively provide it. This is especially relevant for groups who may find it difficult to understand privacy notices and consent dialogues.

Meaningful: Information should be presented in a way that is relevant and personally meaningful to the user. Technical jargon and vague terms should be avoided, while information loaded with emotion-inducing content should be filtered out. Relevant: Information should

[130] Luca Longo and others, 'Explainable Artificial Intelligence (XAI) 2.0: A Manifesto of Open Challenges and Interdisciplinary Research Directions' (2023) 106 Information Fusion.
[131] B Nissen and others, 'Should I Agree?: Delegating Consent Decisions Beyond the Individual' (2019).
[132] Onqlave, 'What is Privacy by Design?' (Medium, 5 March 2021) https://medium.com/@onqlave/what-is-privacy-by-design-df953d73a676 accessed 29 July 2024.

be presented in a manner where users can focus on the specific system, they are interacting with[133].

Content unrelated to the system interaction should be avoided, as disruption may lead to unintentional consent. Understandable: Information should be presented in a language and format that is easy to process and comprehend for the intended user group. This is particularly relevant for groups with cognitive disabilities, low literacy levels, or a lack of experience with the specific technology.

7. Technological Solutions for Consent Management

Technological solutions have been developed to facilitate and manage consent. These solutions include Consent Management Platforms (CMPs), which provide a framework for the storage and management of consent. CMPs are components of larger compliance ecosystems, often provided by specialized companies with longstanding experience in data privacy[134].

Such provisions are widely implemented in the internet ecosystem with comprehensive coverage of web- and app-based digital marketing and tracking activities. CMPs are expected to play an equally essential role in the AI context, providing means to seek, record, display, and revoke consent[135].

However, most current CMPs do not provide a standardized framework for consent, resulting in a plethora of diverging solutions that complicate interoperability and the compliance assessments of AI applications. The storage of consent in closed, proprietary environments, which typically contain large amounts of sensitive data, raises privacy concerns and might breach GDPR principles, such as data minimization and purpose limitation[136].

---

[133] CENIE, 'Application of the Principle of Proactive Responsibility in Processing Personal Data within the Scope of the GDPR' https://cenie.eu/en/blogs/securhome/application-principle-proactive-responsibility-processing-personal-data-within-scope accessed 12 July 2024.
[134] Martech, 'How Consent Management Platforms Support Data Privacy Compliance' https://martech.org/how-consent-management-platforms-support-data-privacy-compliance/ accessed 29 July 2024.
[135] Marco Robol and others, 'Consent Verification Monitoring' (2023) 32(1) ACM Transactions on Software Engineering and Methodology 1-33.
[136] Santos C and others, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?," Lecture Notes in Computer Science (Springer International Publishing 2021) <http://dx.doi.org/10.1007/978-3-030-76663-4_3> accessed September 12, 2024.

To guide future research and application development, CMPs are classified according to different dimensions, such as form, functionality, and technological solutions. The main functionality offered by CMPs is a means to seek consent, a consent storage facility, and tools that allow for transparency regarding the recorded consent[137].

While many of the functionalities required for consent management are already covered by existing technologies, there is a lack of technologies specifically addressing consent. A first step towards bridging this gap is the adoption of a common understanding of consent and a clear set of requirements. Such provisions are essential for the design of compliant AI systems. Given the centrality of consent in legal terms, paths for compliance auditing and the corresponding array of technological solutions will also be discussed. Finally, case studies of practical implementations and future trends in the technological management of consent in AI are presented.

7.1 Consent Management Platforms (CMPs)

Consent Management Platforms (CMPs) are specific technological solutions for overseeing consent within AI systems. Box explains their functionalities: A consent management platform (CMP) is a technology solution for obtaining consent from users. It famously integrates with the web user's browser using code inserted into a website. This code shows popups, often with the "accept all" button that solves the consent by browsing the website and discounts websites' default practices leading to fines in the EU. Common solutions include cookie consent banners on websites and app permissions on mobile apps. CMPs are emerging as significant actors within the ecosystem of consent on the web, figuring in 56% of all recorded consent transparency provisions. Understanding CMPs is necessary to understand the case studies and future trends about technological solutions to consent in AI systems[138].

---

[137] Cookiebot, 'Best Consent Management Platforms' https://www.cookiebot.com/en/best-consent-management-platforms/#:~:text=A%20consent%20management%20platform%20(CMP)%20is%20a%20software%20solution%20that,privacy%20regulations%20like%20the%20GDPR accessed 12 July 2024.

[138] Santos C and others, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?," Lecture Notes in Computer Science (Springer International Publishing 2021) <http://dx.doi.org/10.1007/978-3-030-76663-4_3> accessed September 12, 2024.

The need for consent in the collection, use, and dissemination of personal data should be managed by a consent management system (CMS). As a standard component of privacy-protecting applications, a CMS addresses this need through the definition, acquisition, and enforcement of privacy policies regarding personal data[139]. It may be a centralized and closed entity preserving privacy policies but only for the participants of a closed network, such as a consortium of organizations establishing an opaque authority. Alternatively, a decentralized and open entity may transparently establish trust over social networks fostered by privacy policies, as well as allowing non-disclosure to policy owners while still verifying compliance. Such an entity may rely on permissioned blockchains or smart contracts[140].

8. Conclusion

It was argued in this thesis that informed consent of the subject of data is needed with respect to AI systems, since they are a continuing learning and evolutionary process. The core question is whether the current regulations set in place by GDPR protect, within the legal context, individual consent within the wider framing of the implications of that data used for AI applications. Furthermore, the transparency in the consent process and the understanding that the parties involved have in regard to the kind of data being shared with the AI systems are analyzed.

The argument is that in many conditions, the consent of the individual alone seems to offer little assurance that data will be anonymized in ways consistent with the preferences of the individual, and it certainly does not assure the individual that data will be processed or used in ways that the individual best understands and fully approves of. This brings into question

[139] TrustCassie, 'What Is a Consent Management System?' https://trustcassie.com/resources/blog/what-is-a-consent-management-system/ accessed 29 July 2024.
[140] Harshvardhan Pandit, Christophe Debruyne, Declan O'Sullivan and David Lewis, 'GConsent - A Consent Ontology Based on the GDPR' in *Advances in Information Security: Proceedings of the 2019 International Conference on Privacy and Security* (Springer 2020) https://doi.org/10.1007/978-3-030-21348-0_18 accessed 29 July 2024.

the transparency and validity of the data collection practices, which might not be as strong as is currently considered to be the position. It is important to underline, therefore, that this thesis shifts the emphasis to the defense of participation rights owed to all data subjects; the consent provisions are central, as claimed in the title and throughout, but their implications must be realized and addressed more fully.

Regarding these concerns, the survey results also reveal that the majority of individuals express a significant level of concern regarding the security and potential threats associated with their own personal data. However, despite these concerns, a remarkable number of 80% of respondents have demonstrated that they never had problems with providing consent to artificial intelligence applications.

The consent process should be organized based on users' needs and followed by clear educational resources. If these resources are designed well, they will help reduce the amount of dependence on individual consent.

As the General Data Protection Regulation provisions make clear, the alternatives to consent are not being designed and operated at present in a sufficiently difficult or predictable fashion. This is entirely appropriate, and the use of unanimous data or a discriminatory bias minimizing approach could be prioritized. However, we go further: we argue that the growth of AI systems is likely to have extreme implications for the rights of individuals with regard to data.

The defense mechanisms associated with explicit consent are consistently reactive and discriminatory in nature. Therefore, it is crucial to develop comprehensive and proactive strategies that address the evolving challenges posed by AI systems.

These strategies need to be much more empowering for the individual and with a respect for privacy and personal data protection, protecting individual interests without closing the potential for innovation and development in AI.

The essential question of this thesis was if the current method of obtaining consent effectively guarantees individual privacy in relation to the use of personal data by AI applications. In the previous chapters it was fully discussed that individuals are often not fully

informed about the terms and conditions they agree to, due to reasons such as the complexity of specialized language and the length of the documents explaining these terms. However, the more critical concern here is whether existing regulations, designed to protect data privacy, truly ensure individuals' privacy in practice.

The survey conducted as part of this thesis shows that while most participants expressed concern about the potential misuse of their data by AI systems, 80% of them had not personally encountered issues when giving consent to the AI applications. This suggests that despite the general concerns regarding the privacy risks after giving the consent, most people have not experienced direct problems with this process.

Throughout the thesis, it was argued that regulations like the GDPR have established a forceful and strong framework for data protection, and the introduction of the AI Act has strengthened these protections even further. The survey aimed to test the effectiveness of these regulations in real-world scenarios. While the results indicate that the current regulations are generally functioning well, there is still room for improvement, particularly in simplifying the consent process to enhance user understanding and trust in how their personal data is being used.

Moreover, according to the results of the survey, it has become quite clear that the AI applications have become a fundamental and essential part of most people's daily lives. This substantial level of AI integration highlights the pressing necessity to comprehensively understand the complex implications that arise from granting consent within the realm of AI systems. It is clearly commanding to develop proactive strategies that effectively tackle the ever-evolving challenges while all together emphasizing the utmost importance of privacy preservation and the safeguarding of individual data. In order to fully achieve this comprehensive perspective, a principal prioritization of transparency, accountability, and proactive measures to protect and uphold individuals' data rights is explicitly and necessarily crucial.

In conclusion, while informed consent remains important, a more holistic and forward-thinking approach is needed to address the complex ethical, legal, and societal issues arising from AI systems. This approach should prioritize transparency, accountability, and proactive protection of individuals' data rights, ultimately leading to a more responsible and sustainable deployment of AI technologies.

9. References

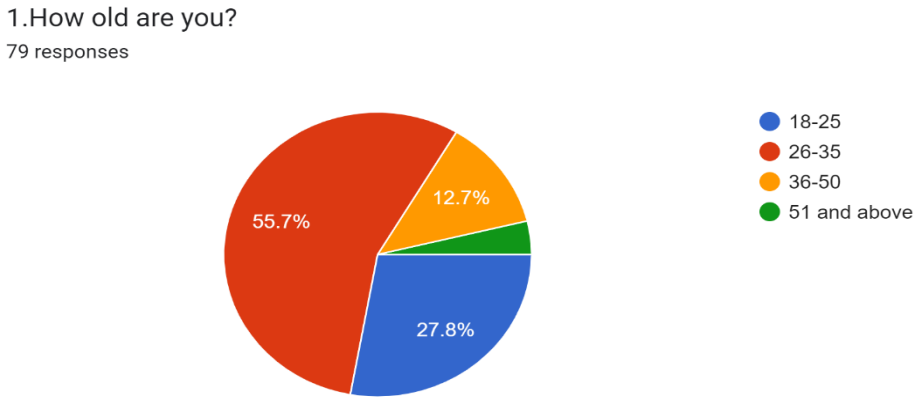
1. Adam J Andreotta, Nin Kirkham and Marco Rizzi, 'AI, Big Data, and the Future of Consent' (2022) 37(4) AI & Society 1715-1728.
2. Alejandro Barredo Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI' (2020) 58 Information Fusion 82-115.
3. Anelia Kurteva and others, 'Consent Through the Lens of Semantics: State of the Art Survey and Best Practices' (2021) 15 Semantic Web https://doi.org/10.3233/SW-210438 accessed 29 July 2024.
4. Anelia Kurteva, Tek Raj Chhetri, Harshvardhan Pandit and Anna Fensel, 'Consent Through the Lens of Semantics: State of the Art Survey and Best Practices' (2021) 15 Semantic Web https://doi.org/10.3233/SW-210438 accessed 11 July 202.
5. Anelia Kurteva, Tek Raj Chhetri, Harshvardhan Pandit and Anna Fensel, 'Consent Through the Lens of Semantics: State of the Art Survey and Best Practices' (2021) 15 Semantic Web https://doi.org/10.3233/SW-210438 accessed 29 July 2024.
6. B Nissen and others, 'Should I Agree?: Delegating Consent Decisions Beyond the Individual' (2019).
7. B Nissen and others, 'Should I Agree?: Delegating Consent Decisions Beyond the Individual' (2019).

8. CENIE, 'Application of the Principle of Proactive Responsibility in Processing Personal Data within the Scope of the GDPR' https://cenie.eu/en/blogs/securhome/application-principle-proactive-responsibility-processing-personal-data-within-scope accessed 29 July 2024.
9. Cloudflare, 'What is Pseudonymization?' https://www.cloudflare.com/learning/privacy/what-is-pseudonymization/ accessed 29 July 2024.
10. Cognilytica, 'Top 10 Ethical Considerations for AI Projects' https://www.cognilytica.com/top-10-ethical-considerations-for-ai-projects/ accessed 29 July 2024.
11. Data Protection Commission, 'Principles of Data Protection' https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection accessed 28 June 2024.
12. European Parliament, 'Regulation on Artificial Intelligence' https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence accessed 9June 2024.
13. Fatemeh Nargesian and others, 'Data Lake Management: Challenges and Opportunities' (arXiv, 13 October 2017) https://arxiv.org/abs/1710.04713 accessed 29 July 2024.
14. Francesca Lorè, Pierpaolo Basile, Annalisa Appice and others, 'An AI Framework to Support Decisions on GDPR Compliance' (2023) 61 Journal of Intelligent Information Systems 541 https://doi.org/10.1007/s10844-023-00782-4 accessed 29 July 2024.
15. GDPR.eu, 'GDPR Fines and Penalties' https://gdpr.eu/fines/ accessed 09 July 2024.
16. Harshvardhan Pandit, Christophe Debruyne, Declan O'Sullivan and David Lewis, 'GConsent - A Consent Ontology Based on the GDPR' in *Advances in Information Security: Proceedings of the 2019 International Conference on Privacy and Security* (Springer 2020) https://doi.org/10.1007/978-3-030-21348-0_18 accessed 29 July 2024.
17. Heike Felzmann and others, 'Towards Transparency by Design for Artificial Intelligence' (2020) 26(6) Science and Engineering Ethics 3333-3361.
18. Inga Ulnicane, 'Artificial Intelligence in the European Union: Policy, Ethics and Regulation' in Thomas Hoerber and Gabriel Weber (eds), The Routledge Handbook of European Integrations (Taylor & Francis 2022).
19. Interaction Design Foundation, 'Human-Computer Interaction' https://www.interaction-design.org/literature/topics/human-computer-interaction accessed 29 July 2024.

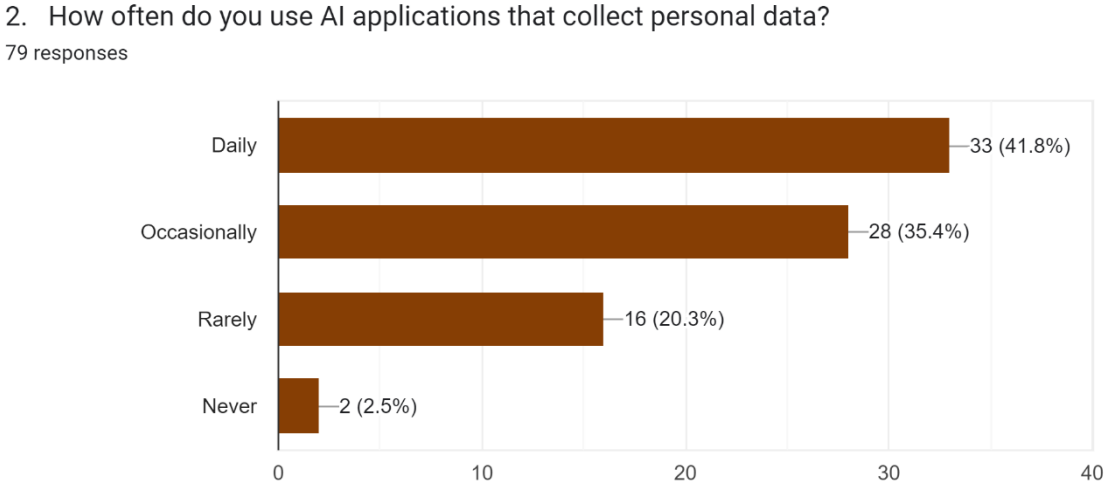
20. Lark Suite, 'Most Important Factors to Consider When Building AI Analytics System' https://www.larksuite.com/en_us/topics/ai-glossary/most-important-factors-to-consider-when-building-ai-analytics-system accessed 29 July 2024.
21. Luca Longo and others, 'Explainable Artificial Intelligence (XAI) 2.0: A Manifesto of Open Challenges and Interdisciplinary Research Directions' (2023) 106 Information Fusion.
22. Luca Longo and others, 'Explainable Artificial Intelligence (XAI) 2.0: A Manifesto of Open Challenges and Interdisciplinary Research Directions' (2023) 106 Information Fusion.
23. Marco Robol and others, 'Consent Verification Monitoring' (2023) 32(1) ACM Transactions on Software Engineering and Methodology 1-33.
24. Martech, 'How Consent Management Platforms Support Data Privacy Compliance' https://martech.org/how-consent-management-platforms-support-data-privacy-compliance/ accessed 29 July 2024.
25. Michael Sipser, *Introduction to the Theory of Computation* (3rd edn, Cengage Learning 2013).
26. Nissen B and others, 'Should I Agree?: Delegating Consent Decisions Beyond the Individual' (2019).
27. Norwegian Data Protection Authority, 'Artificial Intelligence and Privacy' https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf accessed 29 July 2024.
28. Onqlave, 'What is Privacy by Design?' (Medium, 5 March 2021) https://medium.com/@onqlave/what-is-privacy-by-design-df953d73a676 accessed 29 July 2024.
29. Onqlave, 'What is Privacy by Design?' (Medium, 5 March 2021) https://medium.com/@onqlave/what-is-privacy-by-design-df953d73a676 accessed 29 July 2024.
30. Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (17 April 2024).
31. Saheb, T. and Saheb, T. (2024) 'Mapping Ethical Artificial Intelligence Policy Landscape: A Mixed Method Analysis', Science and Engineering Ethics, 30(2), p.9.
32. Securiti.ai, 'Types of Consent' https://securiti.ai/blog/types-of-consent/#:~:text=The%20type%20of%20consent%20required,or%20inaction%20of%20the%20individual accessed 29 July 2024.

33. The Alan Turing Institute, 'The Rapid Rise of Generative AI' https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai accessed 29 July 2024.
34. Tom Kwanya and others, 'Responsible AI in Africa' (2023) https://doi.org/10.1007/978-3-031-08215-3 accessed 29 July 2024.
35. TrustCassie, 'What Is a Consent Management System?' https://trustcassie.com/resources/blog/what-is-a-consent-management-system/ accessed 29 July 2024.
36. Youngsun Kwon and others, 'Harnessing Artificial Intelligence (AI) to Increase Well-being for All: The Case for a New Technology Diplomacy' (2020) 44(6) Telecommunications Policy.
37. Ziang Xiao and others, 'Inform the Uninformed: Improving Online Informed Consent Reading with an AI-Powered Chatbot' in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023).

10. Apondix1: Survey and the results



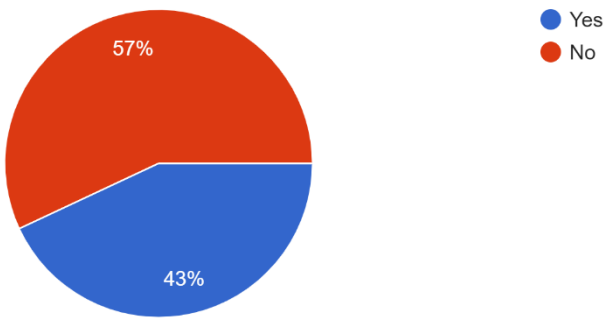
In this servay the majority of participants were in the age group of 26-35 years old and minority were 51 years old and above.



According to the results, most of the participants use AI applications daily and occasionally (77.2%), and only 2.5% never use AI applications.

4.Do you feel that your consent is adequately obtained and respected by AI applications?

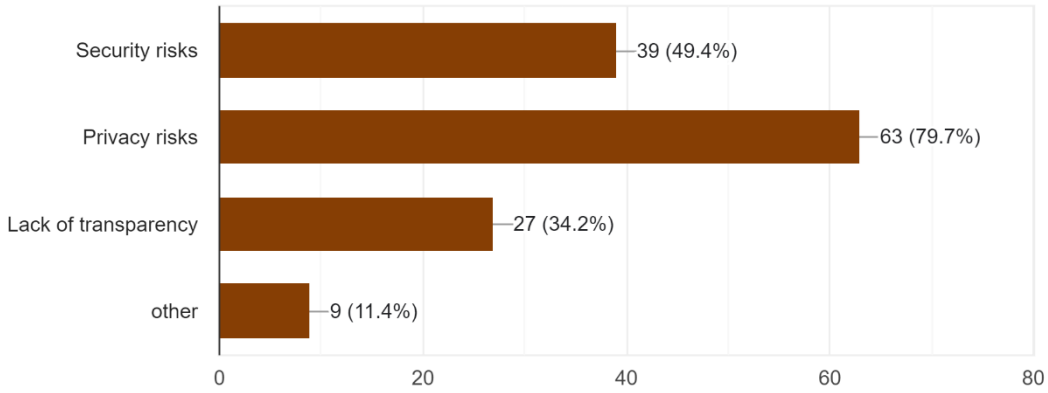
79 responses



Data was showed that the majority of participants (48.1%) felt somewhat informed about their data being used by AI applications**.**

5. What concerns do you have about sharing personal data with AI applications? (Select all if that apply)

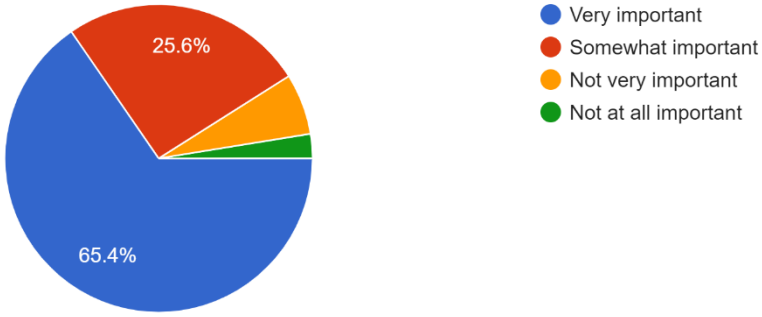
79 responses



According to this survey, most concerns about sharing personal data with AI applications for participations was privacy risks.

6. How important is it to you that AI applications provide clear information about data use?

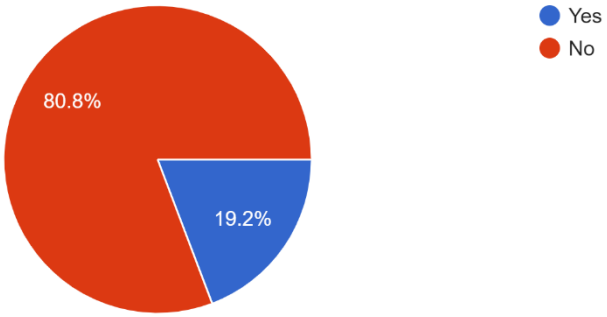
78 responses



As expected, the data showed it is very important for participants that AI applications provide clear information about data use.

7. Have you ever experienced any negative consequences as a result of sharing personal data with an AI application?

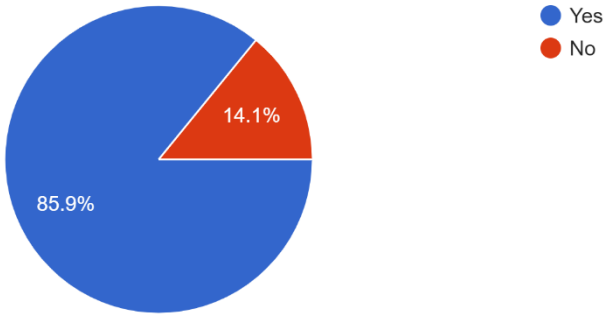
78 responses



Fortunately, the majority of participants of this survey never had any negative consequences as a result of sharing personal data with an AI applications.

8. Do you think there should be stricter regulations on the use of personal data by AI applications?

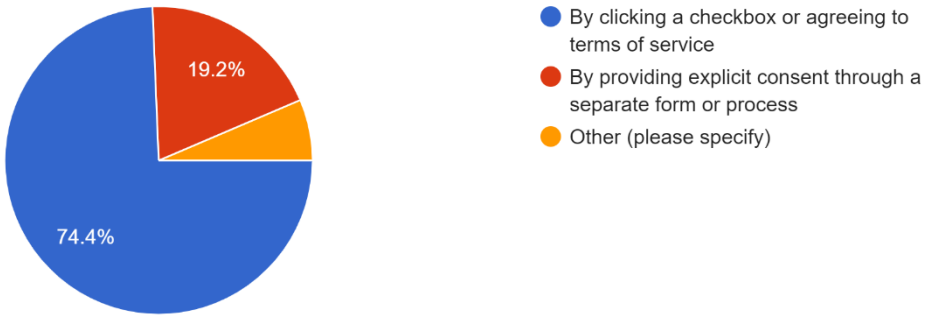
78 responses



Recording to the response of the majority of these surveys' participations (85.9%), they think should be stricter regulations on the use of personal data AI applications.

9. How do you typically give consent for the use of your personal data by AI applications? (Select one)

78 responses



The majority of responders in this survey giving consent typically for use of the personal data by clicking a checkbox or agreeing to terms of service by AI applications.