UNIVERSITY OF TURKU

Enhancing Data Privacy in Artificial Intelligence

A Study on Corporate Practices and Regulatory Compliance

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Khanh Nguyen

Supervisors:

Professor Jouni Isoaho (University of Turku)

Professor Seppo Virtanen (University of Turku)

May 2024

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Khanh Nguyen
Title: Enhancing Data Privacy in Artificial Intelligence: A Study on Corporate Practices and Regulatory Compliance
Number of pages: 86 pages, 7 appendix pages
Date: May 2024

The rapid development of Artificial Intelligence (AI) has been a requirement for the creation of innovative possibilities and efficiencies in the different sectors. Meanwhile, the reliance on AI for personal data during its training process involves various issues of privacy and data security as well. This thesis aims to explore the contemporary panorama of data privacy techniques and problems in AI design, including corporate strategies and the application of regulatory rules.

The thesis involves a hybrid of quantitative and qualitative techniques, using a survey of professionals in AI and a case studies' approach for AI companies. The thesis shows a picture of a network between technical, legal, and ethical challenges during data privacy. Among the key challenges are ethics in getting people's consent, privacy in data usage, and transparency in AI decision-making. Then an analysis is carried out regarding whether the regulations including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) are sufficient in dealing with this AI privacy concern. These laws and principles lay the groundwork for the protection of data, however, they are not enough in the context of AI development.

Taking into consideration the overall findings, the thesis develops the outline of a set of guidelines and recommendations to be followed to improve data protection in AI development. Such measures can consist of adopting Privacy-by-Design (PbD) principles, carrying out Privacy Impact Assessments (PIAs) regularly, developing within the organization a culture of privacy, and establishing privacy standards on an industry-wide basis. The lessons from the thesis also help to continue the discussion on the Ethics in AI development and supply practical guidance in the data privacy areas for the companies and policymakers in the AI era.

Keywords: Artificial Intelligence, Data Privacy, AI Training, Regulatory Compliance, GDPR, CCPA, Privacy-by-Design, Responsible AI.

Table of contents

List of tables & figures

Acronyms

AI	Artificial Intelligence
CCPA	California Consumer Privacy Act
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
KMO	Kaiser-Meyer-Olkin
MPC	Multi-Party Computation
PCI DSS	Payment Card Industry Data Security Standard
PbD	Privacy-by-Design
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment

1 Introduction

Artificial Intelligence (AI) promotes or helps industries like healthcare, finance, transportation, and entertainment advance their technology. The data-intensive nature of this area can be found in looking for unusual behavior patterns and making decisions on AI-based algorithms (Chui et al., 2018). AI's development over the last few years has relied heavily on giant data sets, supercomputers, and complicated machine learning computations engaged by experts. These breakthroughs have, in turn, allowed AI systems to manage complex jobs and do many tasks, especially relying on automation and providing helpful information that would be difficult to access earlier.

Nevertheless, the issue of using and storing personal data in AI systems is accompanied by many privacy rights exemptions, is insufficiently secured, and has a huge number of ethical dilemmas (Tene & Polonetsky, 2013). The gathering, retaining, and processing of such tiny pieces of personal information, characterized by most online activities, have become an important issue as people often do not know how and for which purpose their data is being used or shared. Besides, the disclosures of data leaks and the generally unclear nature of some AI algorithms have even more restrictions on privacy based on concerns such as algorithmic bias, bias against certain individuals, and illegal profiling (Barocas & Selbst, 2016).

In the stage of arising these issues, governments and regulatory bodies have made efforts to establish data protection laws. General Data Protection Regulation (GDPR) in the European Union (EU) and California Consumer Privacy Act (CCPA) in the United States (US) answer this trend from the data privacy laws being developed (Rustad & Koenig, 2019; Hoofnagle et al., 2019). These regulations include actions that are designed first of all to protect personal data, make organizations transparent in their data processing, and hold data practice on the same responsibility level as the law itself. The GDPR which became effective in May 2018, has set a new norm of data protection across the world. It enables people to exercise the right to access, modify, and remove their personal data and urges organizations to obtain personal consent before processing data. However, the GDPR imposes a privacy-by-design principle as well and this requires AI system developers to embed data protection measures at every stage of product development. Furthermore, the CCPA which came into force in January 2020 gives residents of California the power to understand what data are being collected about them, the right to ask for deletion of data, and the right to opt-out of the sale of their personal data. The

CCPA has become the groundwork for several other states to follow suit in the US; therefore, advertisers should be prepared for similar legislation to be introduced in other states.

Concerning this trend, a low number of organizations are reconsidering their data processing practices and putting strong privacy and security regulations in place. The companies that now produce and deploy AI mechanisms have to navigate this legal and ethical maze of requirements in order to carry out their obligations and retain their trust among people. This has seen a sharp rise in investments in privacy-enhancing technologies like differential privacy and homomorphic encryption, as well as the enforcement of human ethics and the guidelines in AI.

1.1 Problem statement

In the fast-moving landscape of AI, the issue of data privacy now forms a key element of a list of growing concerns. Privacy concerns regarding AI systems mainly lie in the fact that these systems rely heavily on big data for their learning and decision-making. Thus, the threat of privacy breaches and misuse of sensitive information is very real making everyone more vulnerable. Herewith lies the most tedious task for the companies that are developing AI solutions and see them in the market because of the multi-faceted nature of the technical, legal, and ethical aspects of data privacy (Fjeld et al., 2020).

Generally, AI and data privacy research are related to theoretical models that are applied and this field of research is established. As an example, Abadi et al. (2016) proposed the idea of differential privacy that utilizes a mathematical module for processing data while ensuring that an individual's privacy is maintained. This method, which, in turn, may be realized by introducing noise into the data as well the results of analysis eventually, making it impossible to recognize a particular person among this set of data. In a similar vein, Gasser & Almeida (2017) dwelled on the concept of Privacy-by-Design (PbD) which underscores the integration of privacy thinking right from the first stage of the design of AI systems up to their deployment and maintenance.

However, the conceptual models are the foundation of the theory of privacy protection for AI. They give valuable insights and guidelines to privacy protection principles. The gap in empirical research on how these principles are applied in practice currently exists (Veale et al., 2018). Organizations that are using AI systems look at these problems such as data protection laws and data privacy when developing and implementing these systems. These

challenges may arise in the form of technical limitations, and in measures like computational overhead, to the operationalizing of legal requirements in the context of AI. A missing link in the current digital ecosystem is that empirical research on data regulation and compliance methods in the AI field is inadequate which in the long run limits the development of appropriate privacy solutions and fair governance frameworks. Without specific information on how companies manage the security of data in the AI context, it will be hard to distinguish the methods of best practices, common mistakes to be avoided, and areas of boosting efforts. This knowledge gap often results in a dissonance between theoretically sound principles of privacy-preserving AI and the practical issues that become a challenge for organizations.

To remedy this, there is an urgent need for empirical studies that analyze the purpose, track, and compliance strategies used by these companies to adhere to the ethical standards of the AI field. This thesis can be directed to provide a complete stepwise understanding of today's AI data privacy. Consider technical points in addition to legal and ethics parts and lastly, organizations' technical challenges and barriers are going to be analyzed.

One of the most important lines of empirical research may be related to case studies and face-to-face interviews with AI experts and managerial staff. Through the induction of specific case studies, researchers can draw attention to the most often problems and successes of data privacy in AI projects and can conclude about the practical implementation of privacy-preserving methods and the current strategies of compliance. Such qualitative data correlated with the numerical results of how different privacy models are used in the industry will help us evaluate the impact of such models. Another important part of empirical studies in this field is the review and examination of the legal and regulatory system with AI and data privacy. As per the opening statement, the emergence of regulations mandating privacy within the data, such as the GDPR and CCPA, has had a substantial effect on the way companies are dealing with data privacy in AI. Empirical work needs to evaluate how these rules are being enacted among individuals and organizations and the level of effectiveness these rules have achieved in ensuring people the security and privacy of their personal information.

The area to be further, which is the data privacy of AI ethically should be explored through more empirical research. Computer-based forms of AI that improve and exceed human cognitive abilities become the leading issue of public discussion regarding bias, discrimination, and violation of individual freedom. Empirical studies on the ethics of

designing AI systems and data accuracy can provide evidence that would contribute to the development of ethical standards and rules for the responsible use of AI.

1.2 Research objectives and questions

Data privacy is increasingly being held to higher standards with the development of AI, hence, this thesis focuses on reviewing the situation of data privacy practices and challenges in the development of AI systems. The thesis will, however, focus on the approaches that the corporations are using to secure personal data and adhere to the necessary law. The objective of this thesis is to explore the technical, legal, and ethical issues of data privacy in AI. The ultimate target is to guide AI technology development in a responsible and trustworthy manner that not only is compliant with individuals' privacy rights but also well-protected.

The specific objectives of this thesis are fourfold:

- To identify and analyze current data privacy practices in AI development:
  Here, data protection in the AI context will be inspected thoroughly to include the different techniques and ways that the companies are charged with the duty of safeguarding personal data from the hands of hackers. This would involve, among other things, a look at the technical efforts applied in current practices in pursuit of the empirical picture that summarizes the state of data privacy, e.g. data anonymization, encryption, and access control, on the other hand, organizational policies and procedures regarding data management and governance.
- To explore technical, legal, and ethical challenges faced by companies:
  This target aims to demonstrate various barriers and difficulties that a company undergoes in pursuing data security during the developmental phases of AI. From a technical point of view, security and privacy issues can appear when dealing with enormous amounts of data and lack of compliance to privacy-enhanced methodologies like differential privacy and federated learning, and also when laws and regulations are executed across different apps’ platforms or jurisdictions. Legal issues may involve rather uniquely the interpretation and implementation of data protection legislation, the negotiation of data sharing arrangements, and the dealing with the cross-border data transfer. Ethical concerns arise due to bias in algorithms, uneven treatment, lack of openness and clarity, and guardianship in the AI systems that are based on personal records.

- To assess the effectiveness of GDPR and CCPA in addressing AI privacy concerns:
  To address this issue, the thesis will provide a summary of the main aspects of two of the most influential data protection laws around the world, namely the GDPR that takes effect in the EU and the CCPA of the US, that deal with the impact and effectiveness of AI regulation and the reduction of privacy risks. How different regulations in AI have been used and implemented in the past shall help us understand the strengths and weaknesses while identifying potential areas of improvement in regulation.
- To provide recommendations for enhancing data privacy protection in AI:
  Upon completing the above tasks, a thesis will be suggested which will have practical recommendations and guidelines for ensuring safe and secure data usage in AI. Based on the analysis of existing practices and those of regulation and the AI industry, these recommendations will be guided by the insights gained and can be reformulated to meet the specific conditions and challenges the AI industry is facing. Recommendations could be in the form of showing areas in which the technical measures could be improved, for instance, through the use of privacy-enhancing technologies, and the design of robust data governance frameworks. They could also examine legal and ethical issues that come with the AI systems, highlighting the need for transparency and accountability in making AI decisions or bringing the idea into a wider discussion with stakeholders and communities to ensure that the systems are aligned with people's values and expectations.

To achieve these objectives, the thesis will be guided by the following research questions:

- What are the current practices and methods used by AI companies to protect personal data?
- What are the major challenges organizations face in safeguarding privacy while leveraging data for AI?
- How effective are GDPR and CCPA in governing AI practices and mitigating privacy risks?
- What strategies and best practices can help strengthen data privacy in AI while enabling responsible innovation?

These research agenda points will be the pillars of the thesis, ensuring the alignment of the research questions with the ultimate purpose and the applicability of the findings to the community of practitioners and relevant stakeholders.

The thesis research method will be qualitative and quantitative approaches for the investigation of this subject. Qualitative methods help in doing case studies and content analysis to get detailed data on present data protection methods, issues, and compliance in the AI industry. It will encompass a level of interaction with a variety of field experts, namely AI developers, privacy data experts, professionals in law, and policymakers, which will give a comprehensive view of the intricate problems involved. For the collection of data, quantitative research includes surveys and statistical analysis to measure the influence of various data privacy issues in different aspects of the AI industry. This will be achieved through collecting and significantly assessing data from a truly representative sample of AI companies, to uncover trends, patterns, and correlations associated with data privacy protection and regulatory compliance. The essays used will be summarized and then exemplified to be understood easily. Among all those, specific suggestions, and suggestions to improve AI data privacy in the developmental phase will be paid more attention. In the thesis, the topic will be additionally touched upon and the consequences for future AI and data privacy will be explored, pointing out the importance of bringing people together and building a vision to make it possible for AI to be created and used safely and ethically.

1.3 Significance of the thesis

This thesis adds to the existing knowledge base regarding AI privacy and the empirical understanding of business practices, the challenges involved, and the perceived threats to it. In addition, it underscores the imperative of intersecting multiple disciplines for the purpose of solving AI privacy issues. Moreover, it forms the foundation for comprehensive AI privacy frameworks. The outcome contributes to the provision of recommendations that companies can rely upon while designing their privacy practices and assists in the development of the policy framework and regulatory intents. On a separate note, this thesis already brings enlightenment by making people aware to make decisions that are well-informed regarding their information and advocate for stronger privacy guidelines.

1.4 Delimitations

The aim of this thesis is concerned with examining the activities related to data privacy that are a result of the emergence of AI technologies as well as the problems faced by organizations in this respect. The thesis will involve investigating AI systems from a system design point of view to discover, collect, process, and protect data during the training and deployment of AI models. This involves evaluating the technological innovations as well as organizational practices that are employed as ways of maintaining data security including data anonymization, encryption protocols, access control mechanisms, and governance frameworks.

The thesis will examine the complicated terrain of data privacy in AI from the various phases of the AI lifecycle which includes, obtaining and cleaning data, training and testing models, and deploying the models. This part will look through and examine the strategies and tactics employed by firms to maintain compliance with data protection standards and the challenges and trade-offs faced in the bid to balance the desire for data innovation with the need to safeguard the privacy of data. The thesis will not try to address the privacy issues related to AI application use of consumers. Certainly, the protection of consumers' privacy is crucial in regard to AI even though this thesis will solely focus on the practices and challenges around the AI implementation by the organizations. Therefore, this thesis will not get into issues, for example, the effect of AI on individual privacy rights, the risk of AI systems remaining loyal to arbitrary biases or discriminations, and the societal repercussions of AI adoption.

Furthermore, the thesis will primarily focus on two major data protection regulations: as examples the GDPR in the EU and the CCPA in the US. These regulations have been in position for the comprehensive nature and global reach in terms of data privacy. The GDPR, the most among others, has formulated a very high standard of data protection developed by other jurisdictions. This thesis will research organizations' practices of interpretation and implementation of requirements under GDPR and CCPA laws concerning AI development. That implies a review of the specific parts of the regulations set forth that are relevant to AI, for example, data minimization, purpose limitation, and privacy by design and default principles. Besides, the research will be on the system also tackling the issue of the challenges and opportunities presented by these regulations to AI development and the strategies that organizations are using in the process to ensure observance of the rules.

Yet because the GDPR and CCPA are the key focus of the legal review, the work can be extended to cover regional or sectoral data protection regulations that can influence the development of AI. For example, as the Health Insurance Portability and Accountability Act (HIPAA) of the US stipulates terms of personal information handling, the healthcare sector AI systems may adapt to these terms; the data security standard created by PCI Data Security Standard (PCI DSS) sets strict security requirements for organizations processing credit card information that can impact AI applications in the financial industry. Through the awareness of other laws on this theme, the research tended to provide a detailed view of the whole framework governing data privacy in AI. However, data protection mechanisms of other frameworks such as the Personal Information Protection and Electronic Documents Act (PIPEDA) will not be discussed as extensively because GDRP and CCPA are the most comprehensive frameworks with wide applications in different industries and jurisdictions.

1.5 Thesis structure

The remainder of this thesis is structured as follows:

- Chapter 2 delves into AI privacy, examining which technologies are reliable, governments' strategies, and ethics. The chapter provides a rationale for the research and the practices used in AI in the field of data privacy.
- Chapter 3 presents the problem gradually; it explores the saga and modeling approaches of data privacy against the background of AI training and development. It discusses the complications of data acquisition, informed consent, and regulatory issues, on the one hand, and the place of privacy-enhancing technologies in solving privacy matters, on the other hand.
- Chapter 4 presents the technical problem statement, clarifying the technical challenges and discussing the proposed methodology to solve data privacy-related problems of AI systems. It elaborates on various mechanisms such as differential privacy, federated learning, etc. along with the process of compliance with regulation and execution of ethical data practices in AI.
- Chapter 5 introduces solution design, suggesting ways for implementing data privacy improvements in AI with the help of reliable strategies and practices. In this chapter, the discussion elaborates on the design of complete privacy policies, expansion of privacy through privacy dashboards, conducting periodic privacy impact assessments,

creating a privacy-friendly culture within organizations, and collaborating on industry standards.

- Chapter 6 reveals testing and analysis that includes both quantitative and qualitative methods to appreciate the reality of the data privacy practices and spot the things that might be still improved. It proposes the use of descriptive statistics, cross-tabulation analysis, reliability analysis, hypothesis testing, factor analysis, regression analysis, and open-ended questions thematic analysis. As a result, the thesis portrays a case study qualitative analysis touching on regulatory compliance, ethical issues, privacy-protecting technologies, and collaborative approaches to data protection.
- Chapter 7 rounds off the thesis by recapitulating the key findings, considering the role of research and practice, dwelling on the advantages and disadvantages of the thesis, and offering recommendations to be investigated in future research. Its role is to integrate all components of the thesis and lay down the contribution of AI in data privacy as well as some paths for further investigations.

2 Literature review

The central aim of this thesis lies in a thorough and systematic examination and integration of the existing data privacy and AI research. This research, on the one hand, seeks to identify the state of the art and then analyze it to highlight the findings that have been significant, theorized, and practical issues that have shaped the interconnection of data privacy and AI. This review moves to identify the main topics in relation to which the research gap of this thesis will be examined. Also, to identify the areas where the existing research literature needs additions and contributions of the new information from this thesis.

2.1 Scope

To achieve a nuanced understanding of the multifaceted issue at hand, the literature review will traverse a broad spectrum of topics, methodically unpacking each aspect to build a comprehensive framework of understanding:

- Theoretical foundations of data privacy:
  The crucial part of the whole text will accomplish an in-depth analysis of data privacy, beginning from its initial appearance as a notional concept down to the point of it being a core element of digital morality in the time of AI.
- Data privacy and AI:
  Meanwhile, the discussion will be focused on AI and will be sliced into potions as it is scrutinized for challenges to the traditional views on privacy. On the one hand, the thesis will explore the quandary of AI techs as a privacy surveillance tool and a privacy friend on the other hand. Ethical issues within the consent framework, anonymity, and the inherent possible human bias will be considered to establish a moral framework for AI implementation.
- Previous research on data privacy in AI:
  Through this work, which summarizes the academic works and ideas on privacy and AI, the thesis demonstrates the broad context of AI and its impact on people. It will select breakthroughs, milestone studies, and classical works based on old and recent research, allowing the audience to concentrate on the methodological approach, discovery, and conclusion.
- Privacy-Enhancing Technologies in AI:
  This part will thoroughly review the technologies planned to be used in AI, ensuring privacy is inherent in such systems. Additionally, it will analyze the theoretical basics,

practical implementations, and examples of technologies such as differential privacy, homomorphic encryption, and others to predict whether they would address the problem of recognizing the benefits and preserving privacy.

- Regulatory frameworks for data privacy:
  The legislative framework that regulates AI and privacy is examined, as it is the crux of having a comprehensive discussion on data protection laws and regulations. This part will comprise also the lesser-known but essential, elegant regional and country-specific regulations to provide a complete view of the compliance fraternity worldwide.
- Compliance and Enforcement Challenges:
  This section will delve into how organizations carry out their responsibilities backed by a complex web of privacy laws while highlighting the roadblocks.

2.2 Theoretical foundations of data privacy

The digital age has brought up a new set of privacy concerns through the evolution of the opportunities of collecting, storing, and processing personalized information. Initially, privacy means the clear distinction of individual space. Now, the concept of privacy has various angles of data protection, consent, and information (Warren & Brandeis, 1890; Nowak & Phelps, 1992). Given the growing amount of data, it redefines the traditional privacy paradigms, which leads to the appearance of problems such as transparency, responsible use, and privacy of data. Zhu (2011) offers contextual integrity to explain that privacy is seemingly high in some social contexts and requires ethically justified one-way data handling. Moreover, the international nature of these networks creates additional hurdles for authorities to police their privacy guidelines as data crosses multiple national borders to have contact with different legal and cultural values (Row, 2022). This context illustrates the challenge of balancing between the various differing consent and control regulations as one may differ by a specific target jurisdiction.

2.2.1 Data privacy in AI

The data exporting process for AI training is ordinarilly done by adding massive data measurements, which can comprise critical and personal information. The approach has massive concerns about the rule of consent procedures and the reliability of the data collection process. These concerns are made worse by the invasive data collection practices that are not

fully understood and are therefore not open and transparent to the subject of the data. While the scientists claim that the requirement of transparent consent processes is urgent, it still should maintain user autonomy and ensure that individuals are knowingly informed about how their data will be used. (Kaminski & Malgieri, 2020)

In addition, data-usage opacity within the AI systems is onerous for accountability. One disadvantage of the "shadowy" nature of how data is training algorithms and making decisions can be the absence of transparency; thus, accountability can be vague, and perhaps individuals seem uninformed of what their information can do to the decision-making processes. It could result in some cases where the decisions undertaken by intelligent systems could change individuals' lives, at least without their consent. Therefore, it gives rise to the consideration of ethics and affordability of privacy. (Burrell, 2016)

Furthermore, the AI system risks magnifying even the existing biases in the training data, which can go a long way in creating discriminatory outcomes and even violate principles of privacy and fairness. The fact that historical data can perpetuate the bias already existing in the AI system leaves no choice but to enact measures to discern and correct the biases (Barocas & Selbst, 2016). Sorting out these issues necessitates carefully considering privacy challenges, which should be incorporated at the beginning of AI development and its implementation to prevent any AI technologies from infringing upon individuals` privacy rights.

2.2.2 Privacy-by-Design (PbD)

Privacy by Design (PbD)'s fundamental principle is that privacy cannot be considered a post-privacy issue. Instead, this must be a part of the system design, starting with the original concept and going through to the final product (Cavoukian, 2012).

- Proactive not Reactive; Preventative not Remedial: PbD emphasizes proactive anticipation and preventing privacy-invasive events in the first place because it is more effective than it being attempted once that has happened. This proactive approach is the key to ensuring that the protection of private data is the priority.
- Privacy as the Default Setting: This is achieved by setting up comprehensive systems with privacy as the default setting, thus ensuring the privacy of individuals' data without needing extra effort to secure their data. This principle serves as the

cornerstone of creating systems that, by default, adhere to the data privacy rules (Cavoukian, 2012).

- Embedded into Design: PbD includes the consideration of privacy during the Design and architecture of IT systems and business procedures, which is one of the basic requirements of PbD. This integration assures that privacy considerations are carried throughout the privacy development cycle to enhance the privacy integrity of the system.

2.3 Data privacy and AI

There is a gathering of all personal information to train AI using unconsented people thus causing extreme ethical and legal doubts about privacy and autonomy (Mittelstadt, 2017). Data protection in the EU under the GDPR is resolved by these standards and explicit consent is required for data collection. On the one hand, constraining improvements in AI algorithms are troublesome due to the intricacy of algorithms, which can hardly be understood and are managed by multinational tech corporations outside of the supervision of any single national jurisdiction. Another difficulty that makes its presence felt here is during data processing, whereby complicated algorithms make decisions that are not only complex but may affect an individual's life, which hinders their ability to understand and challenge those decisions (Kubler, 2016). The non-transparency and unaccountability represent the core concern that underlines the imperative of implementing intelligent AI systems that enable users to digitally analyze and challenge decisions that are made by or with AI.

2.3.1 Impact of AI on privacy

While the use of AI-powered systems is becoming more prevalent both by government bodies and corporations, it is often done without appropriate consent raising many privacy concerns (Zuboff, 2019). These systems track locations and online behaviors securing the exact pattern of lifestyles, habits, and potential consumption intentions, which in turn, makes them do targeted advertising or even behavior manipulation. Furthermore, AI has the potential to make direct decisions like crime detection or score calculations which in turn influences significant life-changing decisions. Factors like algorithmic complexities and opaqueness make it impossible for individuals to receive explanations concerning decisions that adversely affect them (O'Neil, 2016). While this raises some privacy concerns, the differentially private and encrypted computation technologies show a prospect that may further support privacy

protection. These technologies enable not only capturing data in research but also safeguarding personal privacy. Thus, these technologies ensure valuable data analysis and at the same time eliminate the possibility of compromising individual privacy (Dwork & Roth, 2014).

2.3.2 Ethical considerations

The ethical basis of data usage in AI is built on the consent principle, meaning that individuals have to be cleared and know the specifics of data collection, application, and possible implications thereof (Martin, 2018). Nevertheless, as the data following AI algorithms might be employed beyond the originally agreed purposes, the current concept of informed consent can remain elusive. To come up with comprehensive solutions to the process of AI deployment and the issues it raises, such as privacy, novel, flexible, and robust approaches are necessary.

Transparency in AI systems operations is no less important, needing open explaining to all stakeholders about the intricate workings of the AI systems, what data they feed on, and the logic behind their decision-making, including the regulatory bodies and the public (Diakopoulos, 2016). Nevertheless, this transparency is crucial in order to keep public faith, assess AI systems' fairness and accuracy as well as their potential bias, and in the development of rules and remedies in the event of harm. With AI becoming the central part of our society and with all the power it gives to AI developers, it becomes paramount to have ethical awareness inculcated into AI developers' minds from the early stages of AI development. This will ensure that AI is a mechanism to improve the welfare of humanity and responsible AI functioning (Jobin et al., 2019).

2.4 Previous research on data privacy in AI

The fast-growing research discipline of AI ignited many investigations to unveil the manifold ways privacy threats this superpower brings out. This collaborative work is a combination of empirical studies that seek to evaluate the procedures of AI data privacy control and, from a wide perspective, a theoretical discussion that tries to discover the issues that will come about when combining AI with users' privacy. Despite the wealth of knowledge these studies give, discerning the gaps and areas not covered in literature still presents a challenge that readers can take up as part of a continuous effort.

2.4.1 Empirical studies

Empirical researchers such as Polonetsky et al. (2015) have successfully used comprehensive surveys to identify privacy-related issues for industries implementing AI systems. Their work highlighted the problems encountered by organizations that strive to develop AI systems respecting privacy mechanisms. The survey results revealed alarming concerns among industry experts on whether the privacy of individuals can be guaranteed with adequate privacy protections in place in the presence of the data-hungry nature of AI technologies. This research not only underlined technical difficulties in harmonizing the data requirements of AI with privacy fears but also gave insight into how companies deal with these issues by adopting the PbD principles and improving methods for data anonymization.

The other key advantage of the empirical research is data privacy in AI, which Zarsky (2016) targeted in the apps of machine learning or predictive policing and credit scoring. Zarsky's point of departure was a detailed assessment of the real-life technical limits of the feasibility of data privacy and transparency in intricate AI systems. His research highlighted the tremendous danger of bias and discrimination attributed to the black-box algorithmic decision-making processes; thus, it stressed the need for greater transparency and accountability in AI systems. Zarsky highlighted that algorithms could significantly intensify or even create additional social injustices if not adequately supervised and controlled. Therefore, Zarsky argued for more extensive ethical and regulatory frameworks and oversight.

2.4.2 Theoretical analyses

The connection between AI and privacy is particularly complex, being inherently ethical, ethical, legal, and philosophical that the norms of privacy in the digital age need to be redefined. Taddeo & Floridi (2018) in their paper talk about AI's implementation into ethical frameworks where they give a clear example of AI's requirement into ethical guidelines while at the same time they spotlight the possible threats AI poses to individual freedom and privacy. They demand the formation of ethical guidelines that should not only be adaptable but also strong enough for the AI development process, paying attention to ethics awareness. An addition to this notion is contextual integrity (Nissenbaum, 2004), a concept that redefines the purpose of privacy and challenges conventions. By acknowledging the specificities of the informational flows, she claims that the breach of normative data exchange practices may lead

to an invasion of privacy as breaking the established data exchange practices can be considered as a privacy violation, thus the way AI creativity may disrupt social norms and make everyone uncomfortable, which brings attention to privacy.

2.4.3 Gaps in literature

Even though many studies have been conducted in this field, there are significant void areas and untapped regions that still need to be dug efficiently within the literature. A non-existent gap in this line of research is the missing longitudinal studies that track changes in privacy practices and issues in AI. Also, research should be based on more comprehensive findings about the empirical characteristics of AI technology in comparison with existing theoretical modalities, such as deep learning and generative networks. On the other hand, the space for literature could be made more prominent by including end-users who may have a view different from the researcher's because their privacy is directly in question in the development of AI technologies and whose voices are underrepresented in academia. This violation of gaps among the pillars of privacy presents a chance for future researchers to have a more elaborate and complex view of privacy in the AI framework.

2.5 Privacy-Enhancing Technologies in AI

As the development of AI technologies progresses, corresponding innovations in security systems for safeguarding privacy are also seen. At this stage, it is privacy-enhancing technologies (PETs) that are taking the lead in the construction of such systems, providing creative solutions to minimize privacy risks while preserving the beneficial use of AI. The ones that are most frequently used are differential privacy, federated learning, and secure multi-party computation, which display how different methods are employed in the protection of privacy.

2.5.1 Technological solutions

Differential Privacy is a method that provides powerful privacy protection by making the difference between the data meaningless or targeting the results of data analysis using randomization. Instead of allowing researchers and data analysts to piece together sensitive information in the datasets, this approach enables them to get valuable insights from the datasets while keeping the individual data entries private. Unlike the usual privacy settings that essentially disguise personal information or remove it entirely, differential privacy

prevents the added or obliterated data item from affecting the outcome of the analysis, thus anonymizing the meaning of the individual items. (Dwork & Roth, 2014)

Federated Learning is a breakthrough in data widgets and model teaching. Unlike other solutions requiring data from diverse sources into a common framework, federated learning enables models to be imparted directly onto devices from which data is created. Following that, the generative model is updated by identifying anonymized data without one being exposed to protected data. This way of operating considerably tones down privacy concerns by storing critical data locally while still making it possible to create better AI models based on aggregated input from users. (Konečný et al., 2016)

Secure Multi-Party Computation (MPC) is a cryptographic technique that executes a mathematical function over data sets of several parties without exposing any data. Within the AI, Secure MPC could be used for training models, comprising the combined data from various sources where no one party was granted direct access to the raw data of all the others. The technique is even more notable in situations where data sharing happens only in scenarios with privacy concerns or regulatory requirements, as it removes the involvement of data disclosure. (Yao, 1986)

2.5.2 Effectiveness and limitations

Privacy-enhancing methods in AI are considerably effective, with sophisticated mechanisms used to safeguard privacy and advance the evolution and creation of machinery. Differential privacy is an example of the data industry. Google and other tech giants have applied it in several instances, including user interactions, to improve the privacy of public datasets. As mobility and edge devices are prevalent in situations where data privacy is vital, federated learning has already acquired a following. Secure MPC shares its function in financial services and healthcare, providing privacy-preserving data analysis. However, the downside of such technologies is that several limitations constrain them and represent the cornerstone of issuing the fundamental principle of harmonizing AI with privacy protection. With the tech becoming more robust and sophisticated, AI assimilation has played a significant role in ensuring AI scalability responsibly and ethically. Research and developments in these areas are crucial, as they help tackle emerging issues and exploit all the benefits of keeping privacy in AI in check.

2.6 Regulatory frameworks for data privacy

World data privacy laws are the instruments of the state to express the importance of privacy in the modern world as a human right. The EU's GDPR is synonymous with strict data privacy legislation promoting principles like data minimization and the data subjects' right to determine their own information management, setting a precedent for other regions to embrace similar robust pieces of legislation (Dwivedi et al., 2021). Whereas the EU consistently and extensively applies similar laws to all sectors, the US uses sector-specific laws with GDPR-like rights but with a narrower scope (Schwartz & Solove, 2013). These rules are in the valve as inventions, especially AI, progress transparency and explainability in AI's automated decision-making processes become significant. It guarantees that AI systems are clear and comprehensive enough for users, regulators, and other stakeholders to understand and evaluate them. Also, in Asia, countries like China, Japan, and Singapore are at the forefront of creating data protection legislation thus making the legal field involved in AI practice very complex (Greenleaf, 2017). Given these varying legal settings, AI developers must take up an adaptive and strong data protection system, while also honoring the local laws and preserving the desires of individuals' privacy globally.

2.6.1 General Data Protection Regulation (GDPR)

GDPR is placed by the EU as an essential measure for data privacy and a reference standard for data privacy worldwide. GDPR emphasizes data collection, processing, and storage, the protection of personal data, and the rights of individuals. Conspicuously, it provides the principles, for example, data minimization, where only vital data should be collected, as well as purpose limitation, where data should only be collected explicitly, for lawful purposes. Therefore, the Data Protection regulation remains crucial for AI operations inside or targeting EU residents, as these systems need to align with the principles established by this regulation. This would be done by ensuring that AI algorithms are transparent and explainable, particularly in cases where a decision someone makes changes the life of a particular individual. Furthermore, the GDPR requirement of data minimization and purpose limitation are among the most significant barriers for AI systems that rely on too bulky data, forcing developers to search for more innovative ways to make their systems function in a manner that complies with privacy regulations, while not compromising the functionality and effectiveness of AI technology.

2.6.2 California Consumer Privacy Act (CCPA)

CCPA is a historic privacy act in the US, which offers California residents similar rights to the GDPR, including the right to know their collection of personal data, the right to demand deletion of their data, and the right to opt out of sale of their data. Even though the CCPA is less comprehensive than the GDPR, it represents an important step toward stricter US data privacy regulation since it would still cover companies operating in California and collecting personal data from California residents.

2.6.3 Data Protection Act in Finland

The background of the Finnish Data Protection Act (1050/2018) is the EU's GDPR, which has been implemented in Finnish law. The Act started to operate on 1 January 2019 and as the main piece of legislation enables protect personal data and the privacy of individuals in Finland (Korpisaari, 2019). All organizations managing personal data in Finland whether any sized and what sector they are in will be subject to the Act, which stipulates the specific regulations and obligations for data controllers and processors.

The Data Protection Act in Finland is a characteristic point that there is an Office of the Data Protection Ombudsman that is law a national supervisory authority for data protection in Finland (Office of the Data Protection Ombudsman, 2021). The Data Protection Ombudsman's office is involved in data protection compliance monitoring and enforcement. It also oversees the implementation of the GDPR and the Data Protection Act. The Ombudsman provides organizations and individuals with guidance and advice on data protection issues. The Ombudsman shall have the authority to investigate complaints, do audits, and impose financial penalties on organizations that violate data protection regulations, to deal with accountability in the processing of data by such organizations.

The Finnish Personal Data Act additionally has its own specific regulations in some areas of the processing of personal data, for example, science & research, statistics & public archives. These standards of the GDPR intend to find the compromise between the goal of personal data protection and data-driven innovation and research (Korpisaari, 2019). Organizations engaging in this activity must consider complying with additional requirements while safeguarding the data subjects' rights. This involves obtaining consent, adhering to fairness, and ensuring transparency and accountability, of their data processing practices.

The Finnish Data Protection Act and the GDPR will have the same influence on a company collecting and processing personal data for AI systems as the main implications in the context of AI development. AI-based companies should be sure that they adopt a proper law of data processing bases, about data subject informed consent or legitimate interest in the data processing (Korpisaari, 2019). The latter requires upholding strong technical and organizational measures for data protection, including data pseudonymization, encryption, and access controls. Also, they may be using new technology, such as AI, that may pose high risks to individuals' freedoms and rights. Besides, the Act puts forward openness and accountability in making AI decisions and asks organizations to give important information to data subjects about the formula used in AI decision-making and the implications of such processing. Data subjects have the right to demand human intervention, freely express their views, and challenge decisions solely automatically, so the AI systems would be operated in a clear, open, and responsible way.

2.7 Compliance and enforcement challenges

A hugely significant problem that companies undertake as the implementation of AI is the rapidly changing characteristic of machine learning systems. Data-driven AI technology is designed to learn and adapt based on further data collection and different use cases. Hence, ensuring ongoing compliance with data privacy regulations based on fixed data management rules and intents is difficult. Another illustration could be GDPR's principles of data minimization and purpose limitation conflicting with the intensified data use of machine learning algorithms, which may lead to compliance issues (Kaminski & Malgieri, 2020).

Additionally, the global conduct of such market players operating on AI requires meeting several data regulations, which change a lot, across jurisdictions globally. I it requires a careful look at regional legal requirements, and thus, most companies must diversify their compliance techniques to satisfy the various requirements, such as those stipulated under the GDPR, CCPA, and other regional regulations. This process is straining resources and concerns the developers by adding complexities to using AI technologies where their requirements differ (McMahon, 2015).

2.7.1 Enforcement

The control activity of the data privacy laws also brings forth a lot of complexities, most especially at the technical level, which makes it difficult for regulators to monitor compliance

and identify offenses. This risk of rapidly evolving AI technologies makes the creation of aligned regulatory frameworks so hard that it further leads to inconsistent law enforcement while areas such as facial recognition and automated decision-making, are the biggest issues. Privacy is a critical issue due to these technologies which oftentimes are not regulated promptly, thus causing public calls for stricter mechanisms to safeguard consumer privacy (Kaye, 2019). And thus the use of self-governance by certain jurisdictions, along with the possible situations, where voluntary compliance contradicts the law, makes law enforcement more difficult. In addition to that the regulation needs to be synchronized on an international scale to meet the global operation character of AI systems and the personal data protection principle. This therefore underscores the need for international collaborations in the development of strategies for enforcement that continue to adapt to the pace of technology and ensure security for privacy on a global scale.

2.8 Summary and identification of research gaps

The literature review has explored the layered landscape of confidentiality in AI and the main features of the world's regulatory frameworks in compliance with AI institutions, the efficiency of PETs, and, finally, the general ethical consideration. The main thing here is forming global consent for the importance of personal data protection. This is the basis for stepping regulations like GDPR and CCPA, which must be very strong in handling data and people's rights. Nonetheless, the practice of delivering these principles at the legal level differs from place to place; consequently, AI development and use takes on different forms around the globe.

Empirical research has highlighted concrete difficulties in compliance with the privacy legislative framework and problems of consent, transparency, and the inevitable risk of bias. From a moral standpoint, these theoretical and ethical analyses also articulate why sensible, ethical frameworks are indispensable in directing the use of AI. Among the critical methods of protecting privacy are differential privacy, federated learning, and secure MPC. However, their inadequacies manifest in the form of accuracy-privacy trade-offs, scalability problems, and increased computational demands.

3 Problem elaboration

The literature review in chapter two gave a thorough description of the dynamic and differentiated landscape of data privacy as it relates to AI. Prominent issues were discussed, among which are ethical concerns, regulatory issues, and AI technological development. This chapter's focus builds upon the foundation as an overview of what challenges organizations face when they move to AI systems deployment, data protection included.

The early parts of the chapter will explain data privacy regulations in the AI lifecycle, from data acquisition and dealing with the issue of regulation, ethical considerations, and all others. By closely investigating the concerns via the prism of technological corporations' reality, it will be made feasible to deeply consider the manifold dimensions of the issue at hand and identify both where to look for advancements and where to focus the thesis. The later parts will explore the manifold difficulties of data privacy in the era of AI training, addressing issues like acquiring informed consent, utilizing data in certain ways, and ensuring openness. Added to that are the consideration of the complex nature of regulatory compliance in different jurisdictions as well as the many challenges and deficiencies that may arise in a practical application in the face of theoretical principles. What is more, it is also important to discuss the contribution of PETs, one of the possible methods of avoiding such situations.

This chapter will merge the views obtained from both quantitative and qualitative research together which will, in turn, provide a full spatial understanding of the data privacy area in AI development. This will again be a stepping stone to produce a set of evidence-based recommendations and practices. The bottom line is to realize the responsible and ethical adoption of AI while protecting the rights of individuals and building trust in new technologies that can mobilize quick changes.

3.1 Data privacy challenges in AI training

3.1.1 Data acquisition and usage

Data procurement for AI training is one of the essential stages in any AI system development. The data collection procedures of corporations that include AI range from single techniques, ideal for training a narrow AI, to a complex constellation of methods used for building general AI (Makarius et al., 2020). These modalities range from data scraped from public areas, buying the data from brokers, and collecting consumer-oriented content directly by

responding to their interaction with products and services. Every tool within this application puts privacy at risk. Likewise, data scraping usually walks on a thin line between public and private information. Almost purchased data still has visible clues of low provenance. Data subjects' consent must be verified to be accurately used. However, there is no simplicity here, and user-generated data, usually seen as a matter of straightforwardness, involves the complexities of people's intentions and awareness who wish to share their data.

Subject to privacy inflection points in the trajectory of AI, data gets involved. In the data collection phase, privacy concerns are the following: Are individuals informed their data is being collected, and if they are aware of it, why and how will it be used? In the process of data collection, data may get combined, changed, or manifested in forms that can ultimately derive more about an individual than what is observed in an original dataset. Along with the deployment of AI systems, there arises the danger of inadvertent leakage of individual data or learnings that may be connected to that person based on the initial data anonymity.

3.1.2 Informed consent

In the area of AI, the concept of informed consent is now more than just a box that needs to be checked as a standard procedure. Rather, it represents an interconnection among ethics, legality, and operational management (Kiseleva et al., 2022). The AI models commonly use enormous and complicated databases, and many of such data may consist of a web of individual data points, each of which seems to need traceable consent. While access to such data brings many benefits, it also causes barriers to fully informed consent due to the enormous diversity of the data. This very nature of AI is complicated by its layers of algorithms and data models, which increases the opacity of data use (Wulf & Seizov, 2022). Hence, it serves as an essential issue for explaining the present impact and future use of the data subject's data. The principle of informed consent is complexly approached in AI settings. The complex algorithms often used are so intricate that exhaustively explaining to the user's data uses that range the whole data lifecycle is virtually impossible or at least unpractical (Sarker et al., 2002), resulting in a consent process that, though compliant on the surface, may not reveal a level of understanding or agreement that the informed consent principle wants to achieve.

However, the approach involves a specific dilemma between the flexibility AI creators seek and the accuracy needed by privacy regulations like the GDPR (Hoofnagle et al., 2019). Broad consent enables the use of data regardless of the field of AI application. Therefore, it

stimulates innovation and encourages flexibility in the research and development of AI technologies. Whereas the GDPR requires that there is an explicit linkage of consent to specific purposes, the CCPA allows businesses to use customer data for multiple purposes as long as these purposes are closely related to the original purpose (Kretschmer et al., 2021). This consent model contributes to the protection of the privacy of individuals but, on the other hand, can be regarded as an obstruction of the research nature of AI, where data utility can manifest itself only through vast volumes of usable data.

While balancing these two sides - most society on the one hand and specific consumers consenting on the other - corporations face another legal and ethical challenge. Balancing these different interests is more than a regulatory barrier; it is an effort to earn trust and ensure the mature development of AI-related technologies (Reviglio & Agosti, 2020). The structural authenticity of AI is in jeopardy and the faith of individuals, whose data train the AI systems, is gone. To encounter this challenge, a great deal of effort needs to be deployed, and ethical issues associated with it involve personal privacy rights, legal validity, and social acceptance of AI systems (Rodrigues, 2020). While on the one hand, it is important to strive for an effective implementation of AI, on the other AI adoption must retain a person's rights and freedoms.

3.2 Regulatory compliance in AI training

3.2.1 Diverse regulatory environments

Nonetheless, the irregularity of data privacy laws is established, however, the stipulations of laws from one European member state, Germany with strict regulations, are completely different. GDPR of the EU is a standing, invulnerable barrier that cannot be undone with its intended purposes which are used as its tools: consent, one's right to access and the right to be forgotten (Zuboff, 2022). In connection to that, CCPA is closely connected with the GDPR in terms of rules that are different, but similar, focused on consumer’s rights in data sales and disclosure. In addition, countries such as China and Japan have habitually diffused deeper into the continent, so the complicated situation remains (He, 2013). That means the need for diffusion of a cross-nationally applicable solution for this issue and agreeing on adaptive compliance with local regulations is required for businesses.

3.2.2 Institution of Privacy-by-Design: concerns and issues

The Guiding principle for carrying out these regulations is PbD which calls for privacy consideration to be incorporated as the first step in developing any AI (Díaz-Rodríguez et al., 2023). This meant a break with the independent privacy design to a privacy-from-the-outset privacy design instead. Nevertheless, it requires a deep knowledge of the AI technology at its core as well as the intricacies of privacy law. On the one part, the firm should weigh the need for data resources for enhancing the AI model versus the privilege obligation of confidential information on the other part. Through these means, they can evolve such techniques as secure data anonymization, consent, and transparency.

3.2.3 Compliance and innovation: collocating aside

The contrary obligation to abide by the toughest rules and regulations on privacy might disturb the AI's development efficiency. AI research & development can be hampered by the implementation of such regulations as GDPR defined for data security (Martin et al., 2019). This hinders the choice of data exploration methods and model training which are crucial courses for AI development. Take for example; the data minimization requirement is faced with the AI which needs a massive amount of data for higher precision and advanced methods. Finally, the requirement of additional permission and related administrative processes could also hamper the development of the AI sector that positively contributes to society.

These voids impose a fundamental choice on companies that try to balance two aspects: that of the urgent development of AI and the data privacy standards. Despite this fact, the way to achieve compliance has a multitude of hurdles – from the interpretation of the jurisdiction of multiple legal instruments to the application of privacy principles in AI ecosystems that in most cases are very intricate (Gerke et al., 2020). The solutions should be within multi-domain/multidisciplinary frameworks consisting of legal skills, moral/ethical questions, and lately the latest technologies. As companies navigate this terrain, the goal remains clear: to use AI technologies that most efficiently protect public' privacy while responsibly growing the technology to what is ethical and sustainable (Bankins & Formosa, 2023).

3.3 Corporate practices and the gaps in privacy protection

3.3.1 Operationalizing ethical data practices

In implementing ethical data practices in corporations, numerous problems, such as AI's unforeseeable nature, usually make it challenging to find a solution or a working way (Stahl et al., 2023). Most parties accepted the concept of data minimization and transparency. However, applying all data processing principles within the AI lifecycle is complex, from data collection to model deployment. Take engineering as an example – the compulsion to cut back data collection limits what data is picked and does not align well with AI methodologies that seek accuracy and robustness from many data (Chanda & Banerjee, 2022). Paradoxes of ethics, along with choosing between model performance and privacy, remain unresolved criticisms in these forms of algorithms.

Transparency, another feature that helps maintain ethical data practices, is often put to the test, especially in AI systems (Balasubramaniam et al., 2023). The AI systems' core is the algorithms that are the engine of such systems and have a decision-making process that is not always understandable by non-experts. This multi-layered puzzle becomes even more intricate because of the protected or non-disclosed nature of many AI technologies because companies do not necessarily want to fully disclose the inside mechanisms of their algorithms for competitive reasons. Furthermore, users may not be well-informed, and having cheap access to their data utilization as the basis of transparency and trust is a concern.

3.3.2 Implementing the corporate practices aligned to newly evolving regulations

The high level of global divergence among the data privacy regulations places corporate data security strategies in a challenging situation to apply transformative strategies responsive to the frequently changing legal environment (Lonzetta & Hayajneh, 2018). Though, most of the big corporations wind up in an interested position playing "catch up", adapting and adjusting their practices to the most recent requirements. The GDPR, for example, brought many conditions that forced companies to rely on it to undergo massive operational overhauls, one of which was asking for explicit and affirmative consent for data processing use and stringent data protection impact assessments. Similarly, the CCPA has forced the organization to go through the process of re-assessing the methods of data collection and processing practices, especially around the areas of access, deletion, and the opting of selling personal data.

The ongoing surfing through different mechanisms is costly, cumbersome, and full of implied risks, such as non-compliance due to lack of attention or improper interpretation of the regulations. Consequently, multinational corporations are also exposed to the extra complexity of ensuring the data practices conform with all jurisdictions in which they operate, which is not easy, especially when you consider the lack of commonality of privacy laws internationally (Laboris, 2019). This is where every company's approach to compliance is inconsistent, even opposite each other, as they try to deal with confusing or counteracting regulations, thereby widening the gap between corporate conduct and regulatory standards.

3.3.3 Bridging the compliance gap in AI training data

Training AI is not smooth sailing, privacy-wise, because of the high number and type of data sets needed. It is painstaking to make sure that the training data of a wide variety (different in their sources, consent mechanisms, and legal frameworks) are fully compliant with privacy regulations, given this fact. Privacy requirements at the time of specific data collection may afterward be utilized for AI learning, which can run against the certified conditions (Khan et al., 2023). This vulnerability is heightened when third-party data, or scanning for public information, becomes involved since the approval and rights of individuals become even more unclear.

The application of synthetic data and differential privacy techniques has realized the possibilities but also complicated the process of privacy safeguarding (Khalid et al., 2023). The fact is that synthetic data can reproduce tangible assets without disclosing personal information. However, the questions around the implications of such an act and the residual risks of re-identification remain. Contrariwise, in differential privacy, ensuring information utility and anonymity requires delicateness and expertise, which might limit the practicality of AI model applications.

Therefore, companies are increasingly looking for PETs and robust data governance frameworks as a remedy, which they employ. Nevertheless, the practical occurrence of these technologies and systems is only possible through a critical shift towards a more privacy-friendly approach to AI development. The authority would ensure PbD, regular data protection impact assessment, and developing a system for ongoing programming and implementation of the evolving privacy regulations (Romanou, 2018). Furthermore, it all comes down to training the company culture of privacy awareness and responsibility for embedding the privacy surrounding AI initiatives in the company.

3.4 The role of PETs in addressing privacy concerns

3.4.1 Effectiveness of PETs

Differential privacy defines a mathematical formulation whereby the quantification of privacy impacts related to the disclosure of data can be undertaken. By adding controlled, random noise to the data or the results of its analysis, differential privacy provides a level of protection over personal data that would be exposed in large datasets (Wood et al., 2018). As a result, removing or adding an individual database item does not affect the outcome to the extent that it could reveal or conceal datasets. In some cases, AI systems implement this technique, which has helped researchers and corporations work with personal information for training and analysis without violating individuals' privacy. Its deep connection with mathematics frames the technical base for privacy guarantees; therefore, it is often recommended because it is a good option for projects that need rigorous privacy controls.

The main driver for federated learning to be fundamentally different from all the other forms of AI training is that it allows us to avoid sending all training data to one central server (Brecko et al., 2022). Whether the model is trained locally on a user's device and only communicates updates rather than raw data to a central server, doing this helps drastically reduce the need for data centralization, which would bring about the connected privacy risks. Besides that no one's data is shared, this decentralized approach enables more precise AI models where such data remains on the user's device. The fed is one of many ways to enforce privacy regarding AI innovation. It does not have to come at the cost of sacrificing individual privacy rights, but at the same time, it leverages the benefits of AI innovations.

3.4.2 The drawback of PETs in practice of corporate settings

However, they come with difficulties in implementation, such as in corporate risk management (Abbas et al., 2023). The installment of differential privacy, among the strategies for data anonymization, requires a delicate balance between the protection of private data and the usefulness of data. A problem that may arise from this process is that the quality or usefulness of the data can diminish when noise is added to the data or outputs, making the data less suitable for particular types of analysis or AI model training, which may lead to less accurate machines. Accuracy vs privacy, in this case, remains a central element for companies, particularly in cases when extremely high accuracy is required.

In addition to PETs, the practical organization's employment must be backed by high skills and resources. The mechanisms of systems based on differential privacy or federated learning imply experts in the technologies and essentials of data privacy regulations and the ethical aspects of AI production (El Mestari et al., 2024). In addition, the evolving nature of these technologies requires corporations to be highly flexible to adopt and adjust to the new AI techniques that will continue to appear.

3.5 Bridging the compliance gap in AI training data

3.5.1 Understanding the compliance gap

Due to the difference between the theories and principles that led to data regulation frameworks and the real-life challenges that businesspeople face as they strive to create effective AI systems, a compliance gap exists in data privacy regulations when applied to AI (Haidar, 2023). The principles adopted by the regulation, like GDPR and CCPA, promote data safety. For instance, GDPR and CCPA must report where the information emanates, obtain the privilege of the data owner, etc. Nonetheless, the very nature of AI that deals with data often in a data-driven manner mainly depends on training large, complex datasets; therefore, applying such principles can be complex. This gap becomes a topical issue from the compliance point of view, as well as ethical issues about the data, which drives AI development and causes data users to have no permission.

3.5.2 Strategies for crossing the divide

- Enhanced transparency and communication:
  Organizations can realize great strides toward bridging the compliance gap by extending more transparency in AI data practices (Mikalef et al., 2022). This implies not only the communication of the motives why data is collected but also how AI modes are taught, the data protection measures therein, and the rights people have over their data. Reduced opacity is an essential source of trust and can make the AI system easy for ordinary people to understand.
- Innovative consent mechanisms:
  Investigating new AI-compatible models of informed consent is one of the essential actions (Bouhouita-Guermech et al., 2023). This might mean creating consent models with a granularity that allows people to control their data more hands-on or tapping into blockchain and other securely maintained ledgers to record consent transactions.

These developments can facilitate closer relations between AI data practices and what the privacy regulations comply with.

- Organizational culture shift:

  Communication of the organizational culture where data privacy becomes a priority could help cut the gap in compliance (Sharma & Aparicio, 2022). Such a paradigm entails incorporating data protections at all levels of the AI development process – from data gathering to model deployment and further. Tracing out the principle of privacy by instilling it in the employees and using continuous training and awareness programs would invoke a high degree of compliance and ethical data use.

- Collaboration and co-regulation:

  Data privacy legislation is a complicated issue requiring cooperation between corporations, regulating bodies, and privacy advocates (Lynskey, 2023). With the joint efforts of industry standards, regulatory frameworks, and co-regulation strategies, AI data privacy can be expected to be tactful and refined. Such joint ventures can help adopt standard privacy-protecting practices and share newly created PETs across sectors.

4 Engineering problem description

The intersection of privacy bases in cyberspace and AI implementation has resulted in a turning point where theories and realities clash. The last chapters mentioned privacy difficulties, emphasizing the PETs, law-making complexities, and ethical obligations. This chapter concentrates on the engineering implementations and solutions for these multidisciplinary issues. Privacy engineering deals with differential privacy, federated learning worldwide regulations, and integrated ethics. For these to survive, an agile systems engineering approach incorporating AI privacy principles while allowing for innovations is needed.

4.1 Engineering challenges

4.1.1 The approach of differential privacy in AI systems

Differential privacy applied in AI systems projects is essential for retaining relevance and user privacy, especially where data utility is concerned (Jain et al., 2018). Differential privacy implies the addition of random components either to the data or its analysis. Hence, when large datasets are considered together, the data looks like statistical noise. This method will result in individual privacy by using data to enhance AI technology. Nonetheless, the employment of differential privacy demands a delicate balance- adding excessive noise to the data can drastically reduce the usability of the information and, thus, is no longer suitable for training AI networks or data analytics. At the same time, the amount that may not be big enough may not offer enough protection for users' privacy. Also, the computational overburden caused by the competing differential privacy algorithms can be a big problem, primarily when those algorithms must be implemented on devices with limited capabilities or in situations requiring real-time processing data (Dwork & Roth, 2014).

4.1.2 Key themes: federated learning and data heterogeneity

This is a new method for AI model training in a federated manner that distributes the training across multiple devices or servers, keeping their data where it is (Xia et al., 2021). This methodology's de-centralization nature increases privacy by reducing the need to centralize data. This is just an example of self-expression, but the possibilities are limitless. On the other hand, federated learning brings up new engineering concerns, especially about data heterogeneity and the convergence of model parameters. Data quality, quantity, and

distribution spread across multiple devices or nodes can create a disjointed and unequal distribution, which may lead to distorted or biased models that need to be more balanced (Byabazaire et al., 2020).

4.1.3 Navigating regulatory compliance in AI engineering

Implementing all the rules and regulations of the world's data privacy systems is one of the primary issues affecting AI systems builders (ElBaih, 2023). The law and regulations across the globe may have their requirements, starting from the stringent privacy protection measures under the GDPR to the consumer rights-oriented approach of CCPA and many more. The engineering AI systems have to maintain being flexible enough so that they can do well in different legal conditions. The legal compliance integration should be integrated into technical development before starting with technical development (Corrales Compagnucci et al., 2021).

4.1.4 Operationalizing ethical data practices in AI development

Establishing strict informed procedures and guaranteeing the operation of AI models is based on transparency and subjected to fairness are the key areas of ethics (Mohammad Amini et al., 2023). Creating means for getting consent that is clear and straightforward will turn out to be an additional challenge among other things in this sector. The inhabitants must comprehend the consequences of the choices they have made for their data and then do them with confidence. Such involves engineering systems that can display user preferences at multiple instances in different applications with profiles that can be tracked.

4.2 Methodology

To tackle the engineering problems mentioned above, a research process with different stages becomes necessary. This section provides a relevant approach aimed at solving the engineering problems emanating from differential privacy, federated learning, regulatory compliance, and ethical data practices in AI systems. It is planned that the deliverables will be based on data-driven insights, with the solutions being practicable and contributing to the progress of privacy-preserving AI development.

4.2.1 Research design

Getting started with the complicated work of augmenting data privacy in AI implies applying a methodology of the same type, which can work effectively and remain adaptive. Considering the complexity of these issues that fall into the technical, legal, and ethical issues categories - the thesis employs a mixed-design approach that can collect quantitative and qualitative data. This method enables the profound, holistic exploration of the inquiry, not just identifying the problems but presenting reasonable solutions.

The quantitative part of the analysis involves processing the information from the “Data Privacy in AI Training Questionnaire”, which can be found in *Appendix 1*. This survey aims to collect the opinions of the professionals involved in the AI development process ranging from data scientists, AI engineers, compliance officers, lawyers, executives, managers, and IT/cybersecurity specialists. The questionnaire has different aspects of data privacy such as AI training organizational practices, challenges, and perceptions away. The survey is split into five sub-parts covering the different aspects:

- Section 1 (Background Information) deals with the collection and provision of demographic and organizational contextual information on the respondents. Inquiries regarding the participant's role, industry, company size, and geographic location aim to identify the diversification of the sample and allow for analyses based on these characteristics. Those are details that are essential for figuring out the settings where the data privacy practices and challenges take place.
- Section 2 (Data Collection Methods) provides an in-depth analysis of the organization’s data collection practices for AI training. It provides information about matters like consent mechanisms, training data sources, and privacy policy update frequency. This way the organization's compliance with the data privacy principles and best practices could be evaluated and it could serve as a basis for measuring the current state of data privacy in AI training.
- Data Usage and Handling is the topic of content 3 (Data handling and usage) of the company's training practice on AI. Questions that point out the challenges in the process of anonymizing, different scenarios of anonymization, the transparency, and instances of data mismanagement, provide an idea of the data privacy practices of the organization and its gaps. In this section, a roadmap will be laid down that will detail key areas where proposed services can contribute to providing more data security.

- Section 4 (Compliance and Regulation) may be relevant to the entity's knowledge of, and compliance with, the applicable data privacy laws. It measures the degree of realization of the regulations, rival policies, and influence of regulations on AI. These questions enable us to recognize the problems that companies experience when they must communicate with the existing law and provide techniques by which to go about shaping a successful compliance plan.
- Section 5 (Privacy Enhancements and Recommendations) focuses on the adoption of PETs and their effectiveness in protecting data privacy. It also seeks open-ended recommendations and best practices from respondents. These questions contribute to understanding the current state of privacy-enhancing measures and gather insights for improvement, enabling the development of actionable recommendations.

The questionnaire shall be the main data-capturing method for the numbers part of the thesis, meaning that that it will give structured data via sampling from varied AI professionals in several organizations. With collected data, descriptive and inferential statistical analysis processes will be carried out to give the whole picture of data privacy in AI training as well as its challenges. Descriptive statistics deriving from the questionnaire results will present us with a picture of actual practice, difficulties, and ideas of data security now. The frequency table, average, and variability measures will be calculated to show the data and reveal the patterns. Performing a comparative analysis that is demographic and contextual will help to establish the types of practices and the problems that vary across the different industries, company sizes, and geographical locations. Furthermore, the questionnaire data will be analyzed to determine the association between variables. As an instance, the effect of PET’s adoption and privacy protection effectiveness seen by the public can be studied. The correlation and regression analyses, which reveal the associations and the predictive characteristics, point to the factors that are related to data privacy practices and results. The open-ended questions of the questionnaire will provide us with useful qualitative data pertaining to the problems organizations face and help us develop recommendations for data privacy improvement during AI training. Insights such as these are sometimes used to identify the reasons for causing the rise in issues and which areas should be worked on and incorporated into recommendations and best practices.

Altogether, this questionnaire can be described as a convenient tool for collecting quantitative statistics which are going to be used to develop insight and obtain a data-based understanding of data privacy problems in AI training. The survey data covers background information, data

collection processes, data usage and handling, compliance and regulation, and privacy enhancements. This allows the conduct of a comprehensive review and provides a basis for informed guidelines to make sure the privacy of data is safeguarded in AI developments.

For the qualitative part of the research, case studies are employed to carry out an analysis of practical contexts with privacy-preserving AI implementation and resultant outcomes. Case studies will provide in-depth analysis about organizational, cultural, and collaborative attributes that contribute to the improvement of data privacy in the development of AI. This mixed methods research approach is driven by the conviction that a thorough assessment and circumscription of the engineering vulnerabilities that may impinge on the provision of data privacy in AI can only be gathered with the conjunction of quantitative and qualitative rigor. The case studies used here will provide an excellent practical presentation of how theoretical privacy principles can transform into practical solutions. The thesis tries to blend those approaches to advance the field by offering meaningful insights and providing practical solutions, which in turn will contribute to the development of AI systems that are not only innovative but also respect private data and public values.

- Case Study 1: Federated Learning with Differential Privacy on Personal Opinions: A Privacy-Preserving Approach.

  Case study 1, which is aimed at covering the interconnected relationship between developing technologies and fast-growing privacy issues, will be discussed in detail (Ahmadzai & Nguyen, 2023). It brings use cases for applying federated learning and differential privacy techniques. Among all the cases, this one is undoubtedly the most revealing as its concrete nature epitomizes the theoretical concepts which we have in the field of literature review much easier.
- Case Study 2: Regulatory Compliance and Ethical Considerations: Compliance challenges and opportunities with the integration of Big Data and AI.

  The second case study is intended to carry out a diagnostic analysis of the problems faced by enterprises in the AI sector concerning the regulatory provisions and ethical aspects (Farombi & Klaus, 2024). It elucidates the codes and practices pertaining to the path of AI governance by the selective process of legal compliance and ethical design. The case leverages the arguments from the literature review and provides a solid canvas for the representation of the multi-dimensional issues of compliance in an AI environment.

- Case Study 3: Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare.

  The Healthcare Case Study 3 highlights the synergy nature of collaborations happening in the evolving online healthcare realm with stakeholders striving to achieve patient-oriented care (Williamson & Prybutok, 2024). It evokes how balancing both tech innovation and ethical responsibility is a critical element of this equation. Consequently, this case reflects the inescapable role of collaborative spirit and implementation of such AI-based systems throughout healthcare in line with the regulatory themes and patient-centered outcomes talked about earlier on.

4.2.2 Data collection

Data collection is crucial in the research because the empirical evidence from this set of engineering problems is tackled. This section will provide quantitative and qualitative data collection strategies for the quantitative and qualitative approaches employed.

Quantitative data would be ensured by means of the "Data Privacy in AI Training Questionnaire" execution. The questionnaire will be spread by the target group of AI professionals engaged in development in the technology, finance, health care, and retail industries. The survey will be conducted online via a secure survey platform which guarantees the respondents confidentiality and anonymity. The questionnaire consists of five sections: background information, data gathering method, data management and application, compliance and regulation, privacy improvements, and recommendations. The queries are supposed to take in both absolute and numerical statistics as well as qualitative comments.

The qualitative data will be collected from analyzing case studies, documents, and publicized data. Alongside that, relevant case studies are expected to be identified and adopted which will showcase the use of privacy-enhancing strategies in the building of AI. When picking the case studies, their connection to the research goals, the diversity of industries and organizations, and the availability of sufficient data for thorough analysis will be used.

4.2.3 Analytical method

The collected experimental data will be analyzed using statistical software to conduct:

- Descriptive Statistics:

  The Frequencies, Percentages of the answers to questions will be computed to provide

an overview, and all statistics will be measured to sum up the probability of loss or breach of privacy in the conducted survey.

- Cross-Tabulations:
  The correlations will be shown in the cross-tabulations among the analyzed variables to illustrate the ties between the enterprise size or the level of understanding of the regulatory composition and the estimated difficulty of changing the operation plan.
- Significance Tests:
  The required means of making such statistical tests, such as the chi-square ones or t-tests, will be applied to learn the probable cause of observed issues in the survey data.
- Regression Analysis:
  The relationship between using such technologies as PETs and AI model performance criterion will be explored.
- Other Statistical Tests:
  Whatever the case, verify ideas about the trade-offs in applying-at-the-same-time PETs during the AIs development.

This phase will focus on quantifying the consequences of PETs application in AI systems, revealing the best approaches to ensure the balance of privacy protection with data usefulness.

The qualitative analysis will involve the following steps:

- Familiarization:
  The case study materials will be meticulously read and investigated hoping to grasp the full picture regarding the situations, methods, and results evolution in AI related to data security.
- Coding:
  According to the case studies theme, quotes, and watching, appropriate coding will be carried out in the light of identified themes, good practices, challenges as well as lessons learned.
- Thematic Analysis:
  The qualitative data will be summed up and patterned to the similarity to identify some connections and relations, culminating with organizing the thematic outlooks supported by other case studies that also took place. The analysis will include the part

of discovery deep insights and the worth of utilized recommendations for AI technological transactions in view of data protection.

- Interpretation:

  In designing the interpretations of the in-depth research findings, the research objectives and the solution proposals in Chapter 5 will be considered. The analysis will seek "Laconic qualitative ones" that will include both quantitative and qualitative information.

The amount of qualitative data analysis is supported by using qualitative data analysis software, for example, NVivo and ATLAS.ti to assist in coding, organizing, and extracting the case study data.

5 Solution design

An effective privacy policy for AI is necessary for the design of the AI that manages the growing structural personal data. The policy will remain in compliance with global data privacy laws like the GDPR in the EU and the CCPA in the US, setting well-defined principles for the collection, usage, storage, and dispensation of personal data. In addition, it is a very important tool for maintaining an organization's good name as it spurs trust through transparency. This is particularly relevant when it comes to AI and where system opaqueness may constitute the data security issue and privacy abuse. The transparency of the sensitive information policy therefore helps to adhere to the legal requirements and convince the public of the responsible handling of their personal data.

5.1 Developing comprehensive privacy policies

5.1.1 Clarity and transparency of privacy policy

A policy concerning privacy, especially for organizations generating large bases of personal data through AI, is mandatory. It guarantees the organizations that they are on the right path with the use of GDPR in Europe and CCPA in the US, by stating how the personal information is collected, used, stored, and shared. On the other hand, as much as this policy is important for keeping and building trust, it is also evidence of the organization’s inclination to honor and keep the right to privacy (Oswald A. J. Mascarenhas, 2019). This is crucially significant, as it covers the hidden part of the AI systems which may be a cause for concern about data misuse and privacy breaches.

5.1.2 Solution overview

For any organization to draw up a new privacy policy that ensures that data privacy in AI is also protected, it needs first to consult legal specialists and data protection professionals. Utilizing the collaborative method ensures that privacy policy is in connection with the most updated legal requirements and industry best practices while at the same time, also looking at the unique issues and challenges of the AI platform development (Khalid et al., 2023).

A comprehensive privacy policy for AI development should include the following key components:

- Detailed list of the personal data types that are focused on in the AI development, including all special and sensitive categories. Complete explanations of personal data used in the AI development process which should include data acquisition, pre-processing, model training testing, and deployment (Singh, 2023).
- Data anonymization, encryption, differential privacy applications, and other well-known PETs are widely used while developing AI (Ajala et al., 2024).
- A transparent consent architecture that provides support to individuals to make intelligent decisions regarding the collection and use of their data for AI as well as enabling the choice of staying out or revoking the consent (Felzmann et al., 2020).
- Clearly defined personal rights (access, rectify, or delete) personal data their objection to some data processing activities or request for the intervention of a human being in automated decision-making processes.
- Periods of data must be retained and data disposal practices that are secure must be guaranteed as privacy by making sure that the data no longer than required for AI development is preserved.
- The regulations for third-party authorities on sharing individual data for AI, the consent of individuals for the same, and the safety measures for data transmission are also of significance (Andreotta et al., 2022).

5.1.3 Implementation strategy

A privacy policy is just one of the steps that is necessary to enforce security; its effectiveness relies on proper implementation and organization-wide commitment. To ensure that the privacy policy is understood, adopted, and adhered to by all relevant stakeholders, organizations should consider the following implementation strategies:

- Organizing workshops and training for employees engaged in AI development and the people within the roles supporting the function including data management, legal, and compliance (Broekhuizen et al., 2023). The main objective of these sessions is to emphasize the significance of data privacy, and details of the privacy policy and to provide practical guidance for policy implementation.
- Embedding the privacy policy within the organization’s central data governance framework, harmonizing it with the policies, processes, and standards pertinent to data management and security (Dennedy et al., 2014).

- Designation of clear responsibilities in terms of implementation and enforcement of the privacy policy including the appointment of a Data Protection Officer (DPO) or privacy champion within the organization to oversee the compliance effort (EUROPEAN DATA PROTECTION SUPERVISOR, 2024).
- Monitoring and auditing regular compliance to the privacy policy by metrics and Key Pperformance Indicators (KPI) to monitor the progress and to identify areas for further improvement.
- Cultivation of privacy culture in the entire organization, with a focus on data privacy as a joint liability and open communication and collaboration on privacy subjects (Cockcroft & Rekker, 2015).

5.2 Enhancing transparency with privacy dashboards

5.2.1 The importance of transparency in trust building

The concept of openness should form the basis of the development of AI systems, with businesses being required to publicly state how much personal data they collect, and how it is used and protected (Díaz-Rodríguez et al., 2023). Such transparency helps to create trust among users, which potentially follows from the fears of data misuse and adds to the acceptance of computer science technologies. Open communication leads to the issue of current privacy by organizations and helps them to build up their reputation, which is an effective way. Moreover, a lot of global information security laws, such as the GDPR, among others, require organizations to practice transparency in data processing, guaranteeing that they will only provide clear explanations concerning the way they handle the data of individuals. In-compliance can be costly as companies can be subjected to hefty fines and damage their image, especially when it comes to the issue of transparency in data management.

5.2.2 Solution overview

Organizations can improve transparency in AI development by adopting a simple privacy dashboard. The privacy dashboard is an interactive device that enables individuals to see and control their personal data, giving them a transparent overview concerning their data collection, use, and sharing in the context of AI development (Raschke et al., 2018).

Key features of a comprehensive privacy dashboard for AI development may include:

- Data inventory: A concise description of the personal data types being collected and processed for AI, including the sources, types, and retention periods of data.
- AI usage: Understanding how personal data is used in AI training, testing, and deployment, this includes the AI models and applications.
- Consent management: Intuitive controls for individuals to control their consent to activities to be opted in or out related to data processing regarding AI development (Tabassi, 2023).
- Data access and portability: Instruments for people to collect, save, or move their own data in a well-organized, standard, and machine-readable form (Bourgeois & Bourgeois, 2014).
- Data correction and deletion: Methods for people to request the rectification of wrong personal data or de-identification of their data once it is not required for AI development.
- Algorithmic transparency: Information related to the impact of AI on people, the logic that AI is involved in decision-making when it comes to people, and an explanation of how AI models make outcomes (McKendrick & Thurai, 2022).

5.2.3 Implementation strategy

To successfully implement a privacy dashboard for AI development, organizations can consider the following strategies:

- Partnering with specialized software providers: Partnership with other vendors that provide privacy management solutions enables organizations to rapidly implement a privacy dashboard with no need for huge in-house development (Fountaine et al., 2019). Most of these providers come with pre-built templates and configurable options that are often adjusted according to the requirements of the AI development.
- Ensuring intuitive design and accessibility: The privacy dashboard should be made user-friendly with an attractive design and accessibility to users with varying needs and technical capabilities. This could include user testing and using the feedback to fine-tune the design and functionality of the dashboard.
- Integrating with existing systems: Data management and data consistency should be guaranteed by embedding the privacy dashboard is to the organization’s formal data governance structures which cover data catalogs, metadata repositories, and access control systems (Tableau, n.d.).

- Providing clear guidance and support: Organizations should make sure that users understand the privacy dashboard and contain a library of resources that users can turn to when they're confused and need more information. Among by-products may be a user manual, video clips, and a help desk, which will handle all questions and complaints.
- Regularly updating and auditing: Because AI development methodology and data privacy laws are always on the verge of being updated and improved, the privacy dashboards should be updated periodically to cover the most recent amendments and regulations in these fields (Nguyet, 2024). This activity could facilitate the realization of these gaps and keep to the regulatory requirements.

5.3 Conducting regular Privacy Impact Assessments (PIAs)

5.3.1 Proactive identification and mitigation of privacy risks

As AI applications grow and are used in the current fast-paced landscape, organizations must actively work on identifying and engaging the impending privacy issues in this context. Ensuring that consequent Privacy Impact Assessments (PIAs) are done intermittently, such that at various stages of the AI project lifecycle is one of the effective ways.

PIA is a structured methodology through which the privacy implications and possible outcomes of a system that uses AI as a basis or the one that is currently in use are assessed (Clarke, 2009). This could be done by considering elements like the kind of data that is being processed, the purpose and rationale of such processing, the nature of technology, and how it has an impact on individual rights and freedoms. Organizations always run PIAs at different stages of AI development. This makes it possible for organizations to discover and fix privacy risks initially such that the later stages will be easy to remediate, and this will be easy because of long and expensive remediation efforts.

Regular PIAs offer several key benefits for AI development:

- Early risk identification: PIA facilities detect potential privacy risks and exposures at a very early stage of AI projects enabling the organizations to design any technologies required to be installed from the very start (Office of the Privacy Commissioner of Canada, 2011).

- Informed decision-making: Structured as a framework for evaluating privacy effects, PIAs allow organizations to make evidence-based decisions when designing, developing, and implementing AI systems, considering risks and benefits (Villegas-Ch & García-Ortiz, 2023).
- Compliance and accountability: Regular PIAs serve as a reflection of a company's adherence to privacy and help in ensuring compliance with specific legislations such as the GDPR requirement for Data Protection Impact Assessment (DPIA) in some high-risk processing cases.
- Stakeholder engagement: PIAs offer a chance to interact with relevant stakeholders, such as data subjects, regulators, and internal teams that promote teamwork and lay trust in the development of AI (Hoffman et al., 2023).

5.3.2 Solution overview

To implement a robust PIA process for AI development, organizations should consider the following key steps:

- Establish a clear trigger and scope: Specify when a PIA should be performed, including the case when developing a new AI system, making substantial modifications to an existing system, or handling sensitive or high-risk data (ScienceDirect, n.d.). Define the boundaries of the PIA, to wit, the AI use case, data flows, and who is affected.
- Assemble a cross-functional team: Assemble a varied group of experts, which will include data scientists, privacy experts, legal advisors, and business stakeholders, ensuring a thorough evaluation of privacy impacts (Perifanis & Kitsios, 2023).
- Conduct a data mapping exercise: Find and list personal data types processed, purposes of processing, data sources, and data flows within the AI system.
- Assess risks and impacts: Assess the estimated privacy problems and implications that are related to the AI system, including data sensitivity, the level and area of processing, the probability and opposition of damage to the individuals, and the efficiency of existing safety measures, among others (Khan et al., 2023).
- Develop mitigation measures: Create measures in line with the identified risks and impacts to minimize or eliminate privacy risks, which may include data minimization, pseudonymization, encryption, or access controls.

- Document and review: Comprehensively record the PIA process, the identified risks, the proposed mitigation measures, and any residual risks (Vemou & Karyda, 2020). Periodically, re-visit and modify the PIA as the AI system changes or new threats appear.

5.3.3 Implementation strategy

To effectively integrate PIAs into the AI development lifecycle, organizations can consider the following implementation strategies:

- Creating standardized templates and checklists: Create a PIA template and checklist which will be used as standard and also will contain all the key privacy issues to be considered in AI development inclusive of data quality, transparency, individual rights, algorithmic fairness (Mantelero, 2022). This makes for uniformity and thoroughness in the evaluation process.
- Providing training for project managers and teams: Train and coach project managers and development teams on how to perform PIAs efficiently, such as identifying and assessing privacy risks, choosing suitable mitigation measures, and documenting the process.
- Integrating PIAs into project management frameworks: Integrate PIAs with the organization's already implemented project management methodologies like agile or waterfall to ensure that privacy aspects are accounted for throughout the AI development process (Notario et al., 2015).
- Establishing governance and oversight mechanisms: Specify distinct roles and duties in carrying out and reviewing PIAs and appoint a privacy champion or steering committee to lead and guide.
- Continuous monitoring and updating: Continuously evaluate the efficiency of the PIA procedure and adjust it as necessary to incorporate changes in the AI development environment, new privacy threats, or updated regulatory compliance (Regona et al., 2022).

5.4 Responsible AI governance

5.4.1 The importance of organizational culture in sustainable data protection

Responsible AI governance provides a framework for the encouragement of a privacy-focused culture as well as for the creation and implementation of industry standards. These are brought together into a comprehensive strategy. This approach, therefore, aims at building a holistic privacy culture through building proactive and consistent internal measures along with active participation in other sector's initiatives to ensure that data privacy standards are advanced.

5.4.2 Solution overview

To embed data privacy and ethics into the culture and practices of AI organizations, the establishment of comprehensive responsible AI governance frameworks includes:

- Well-defined principles, policies, and procedures on data security, data privacy, and ethics. There should be a consistent alignment of these principles, policies, and procedures with regulations and industry best practices. They should be regularly reviewed and updated to keep them up to date with an always-changing techno-sphere as well as society's evolving norms (Chua et al., 2017).
- Stipulated positions and positions of responsibility like the privacy officer, the ethics board, or an AI governance committee. These positions play an active role in AI development through their ability to provide strategic guidance, resources, and oversight to monitor its development (Eccles, 2022).
- Ongoing training and briefings for staff and contractors on compliant data usage, ethics in AI-building, and apposite law and regulatory requirements. The programs that are creative, applicable, and custom-made to each team’s roles and responsibilities are the best (Rhem, 2023).
- Incentives and performance metrics among others ably match innovation and responsibility while taking privacy and ethics into consideration on the same footing alongside business and technical objectives (Li et al., 2023). This would mean that the privacy and ethics clauses should be added to the performance evaluation of workers, project approvals, and funding authorizations.
- Monitoring, control, auditing, and improvement activities should be made accountable. The risk assessment, impact reviews, and active feedback systems from

stakeholders should be continually conducted. Ethical processes for detecting and resolving potential pitfalls involving privacy and ethics should equally be put in place.

- Proper involvement in the network of industry collaborations, standardization development, and information-sharing activities such as prudent AI governance. It allows organizations to follow new trends, give a push to the development of AI science, and become pioneers in implementing an ethical AI approach (de Laat, 2021).

5.4.3 Implementation strategy

To effectively implement responsible AI governance and cultivate a lasting culture of privacy, organizations can consider the following strategies:

- Secure cross-functional support and role-modeling from senior executives to demonstrate leadership commitment to privacy and ethics (Kaneberg, 2020).
- Provide regular and comprehensive training on data protection regulations, PIAs, and PETs, tailored to different roles and teams.
- Integrate privacy metrics into performance evaluation and reward systems to incentivize responsible practices.
- Foster cross-functional collaboration among data science, engineering, legal, and compliance teams to ensure a holistic approach to privacy (Igbinenikaro et al., 2024).
- Conduct periodic assessments and audits of privacy initiatives to identify gaps, monitor progress, and drive continuous improvement.
- Engage proactively in industry forums and standards development to share best practices, learn from peers, and contribute to the advancement of privacy-protective AI (Zamiri & Esmaeili, 2024).

Through the utilization of an inclusive and sustainable AI governance management strategy, companies can ensure the existence of trust, while minimizing the risks, and, ultimately, pursuing the benefits of AI as a society while respecting individual autonomy as well as the fundamental values of society.

6 Testing and analysis of results

This chapter conveys the testing and analysis from the aforementioned quantitative and qualitative research done for this thesis.

6.1 Quantitative component analysis

6.1.1 Descriptive statistics

The research targeted different AI software developers with respect to their positions and sectors in the same manner to accommodate different perspectives. The roles of Data Scientists and AI Engineers seemed the most popular at 23.3%, followed by the roles of Executives and Managers, which was at 21.1% each, after that were the roles of IT and Cybersecurity specialists at 12.2% each, with Compliance Officers and Legal Counsel at 12.2%. The industries most concerned were Healthcare (32.2%) and Finance (25.6%), the ones where AI is highly developed, and, therefore, appropriate data regulation is vital. The survey participants ranged from micro businesses to enterprises with a geographical distribution of 25.6% from North America, 22.2% from Europe, and 22.2% from Asia. The variety of sizes and nationalities in the sample meant that we could accurately determine what practices were being adopted in data privacy worldwide.

Respondent Profile Category	Options	Frequency	Percent	Valid Percent
Role within the organization	Compliance Officer / Legal Counsel	11	12.2%	12.2%
	Data Scientist / AI Engineer	21	23.3%	23.3%
	Executive / Manager	19	21.1%	21.1%
	IT / Cybersecurity Specialist	19	21.1%	21.1%
	Other	20	22.2%	22.2%
Industry	Finance	23	25.6%	25.6%
	Healthcare	29	32.2%	32.2%
	Other	19	21.1%	21.1%
	Retail	9	10.0%	10.0%
	Technology	10	11.1%	11.1%
Company Size	Large (250+ employees)	23	25.6%	25.6%
	Medium (51-249 employees)	24	26.7%	26.7%
	Micro (0-9 employees)	27	30.0%	30.0%
	Small (1-50 employees)	16	17.8%	17.8%
Geographic Location	Asia	20	22.2%	22.2%
	Europe	20	22.2%	22.2%
	North America	23	25.6%	25.6%
	Other	27	30.0%	30.0%

Table 1. Respondent profiles

The research shows different standards in the protection of AI data across the thesis scope. Accounting for 27.8% on the list are the opt-out approach while 20.0% are the opt-in approach, although the others, such as those stating their policies clearly (18.9%) and not requiring any consent (14.4%), are not uniform. For training Machine Learning technologies, organizations use different types of data sources including public ones (27.8%) and content created by users (24.4%), with third-party providers contributing to 22.2% of the organizations suggesting that these companies largely use external data sources. Privacy agreements expand their territories every time they are updated, but it was found that 32.2% of organizations never do this, which is a cause for suspicion since they can`t be able to become innovative while dealing with the changing data trends. Encryption (23.3%) and pseudonymization (22.2%) are the contemporary anonymization techniques that enterprises widely apply, however, 20.0% of companies lack deanonymization protection techniques which may lead to potential management risks. Other methods like differential privacy and data masking are applied, placing more emphasis on information privacy in general.

Data Privacy Aspect	Categories	Frequency	Percent	Mean	Standard Deviation
Consent Mechanism	Opt-out	25	27.8%	-	-
	Opt-in	18	20.0%	-	-
	Implicit consent	17	18.9%	-	-
	Not sure / Not applicable	17	18.9%	-	-
	No consent required	13	14.4%	-	-
Primary Source of Training Data	Public datasets	25	27.8%	-	-
	User-generated content	22	24.4%	-	-
	Third-party data providers	20	22.2%	-	-
	Other	23	25.6%	-	-
Privacy Policy Update Frequency	Never	29	32.2%	-	-
	Annually	18	20.0%	-	-
	After any significant data practice change	17	18.9%	-	-
	Bi-annually	14	15.6%	-	-
	Not sure	12	13.3%	-	-
Anonymizing Methods	Encryption	21	23.3%	-	-
	Pseudonymization	20	22.2%	-	-
	Not applicable / No anonymization	18	20.0%	-	-
	Differential privacy	18	20.0%	-	-
	Data masking	13	14.4%	-	-
Data Usage Transparency Rating	-	-	-	2.81	1.332
Compliance Difficulty Rating	-	-	-	2.70	1.203

Table 2. Descriptive statistics

The data usage transparency rating is significantly assessed from 1 to 5, which reveals the level of transparency of these organizations in AI data systems. The Average rating of 2.81 (SD=1.323) aimed at moderate transparency has room for improvement. Responses were generally evenly distributed with 24.4% of rates given as a rating of 3, 22.2% as a rating of 1, and 21.1% as a rating of 4. Such a trend vividly demonstrates the issues with a transparent perception that to some extent depends on communications and the establishment of standard transparency rules in companies.

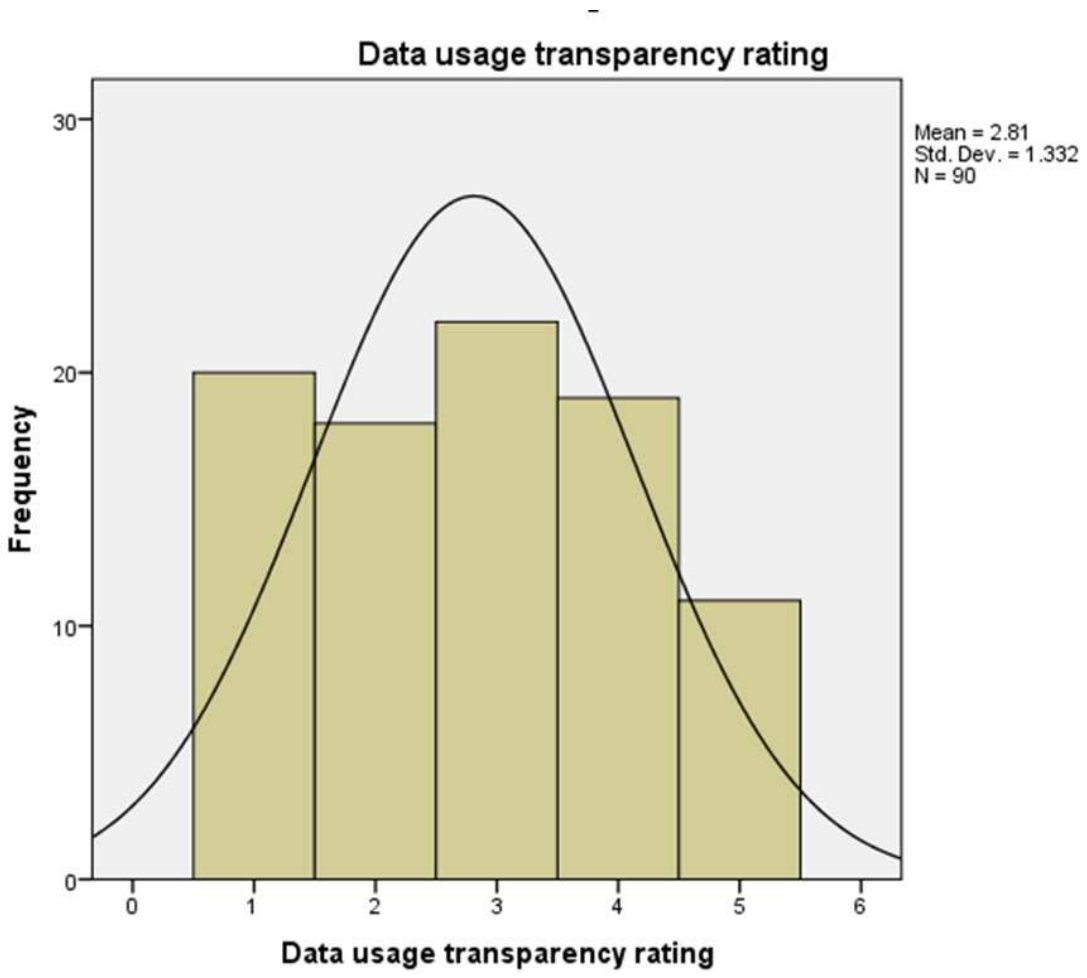


Figure 1. Histogram for transparency rating

Lastly, the ease of compliance rating, which also ranged from 1 to 5, served as an indicator of the level of hardships organizations went through as they made efforts to comply with the privacy regulations. The median rating of 2.70 (SD = 1.203) appears to indicate that this question falls under the moderately difficult category, with 37.8 respondents rating it as 3. Nevertheless, it is of significance for us to mention that almost 20% of respondents ranked the compliance hardness level at 3 and 4 respectively, which shows that some industries had less of a challenge. Such rating variation could stem from disparate strengths of a company in terms of financial, technical, and regulatory capabilities it has at hand.

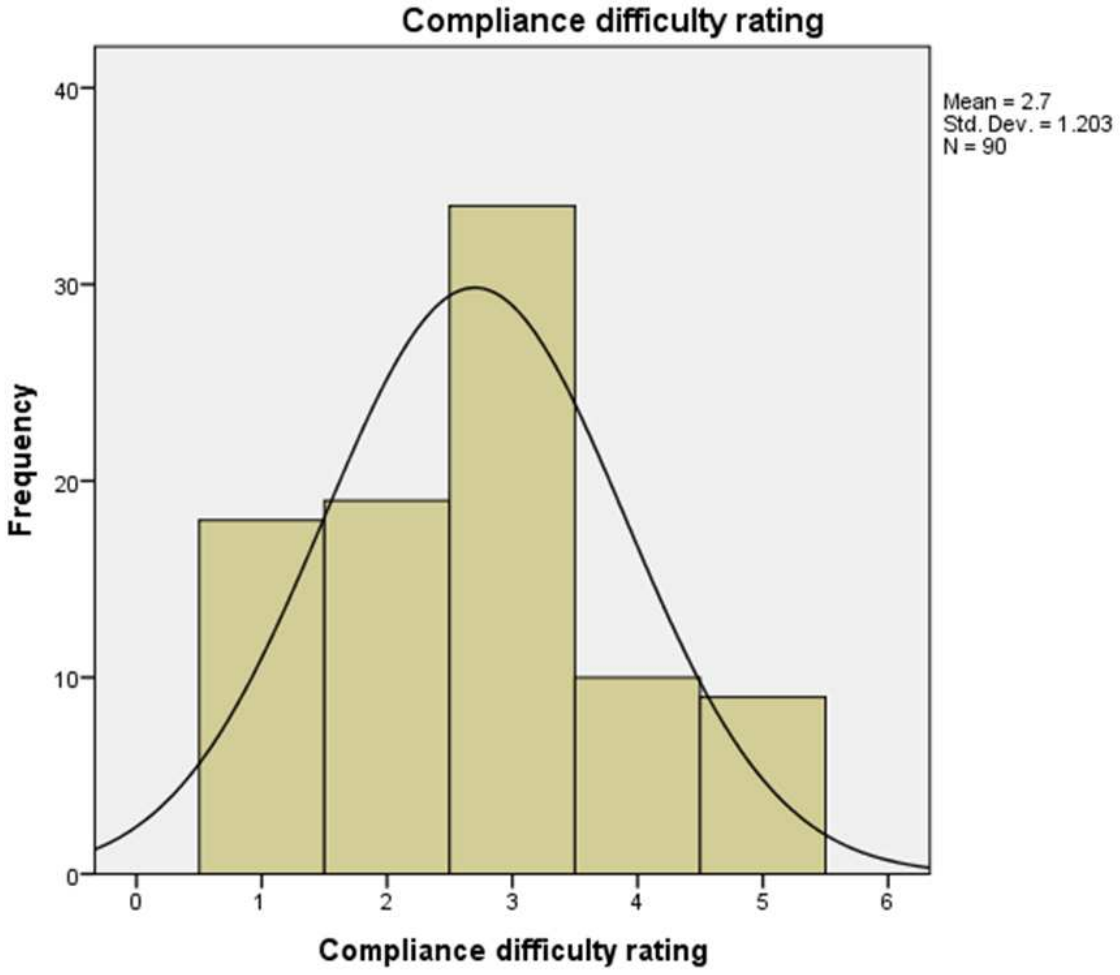


Figure 2. Histogram of difficulty rating

6.1.2 Cross tabulation

To study the existing relationship between the key variables and get a view of the data privacy world in AI development, a cross-tabulation analysis was carried out. This part deals with the results of the cross-tabulation and discusses its relevance for a better comprehension of the links between organizational traits, data security measures, and regulatory standards.

Initially, company size and the frequency of privacy policy updates were assessed. The cross-tabulation showed a high frequency of policy updates by big companies (250+ employees) - 7 of 23 big companies did it once a year while 6 of them waited for a significant change of data practice. In differentiation, micro-sized companies (0-9 employees) have the highest number of those never implementing or updating their privacy policies (11 out of 27). We can infer that company size can shape the frequency and proactivity with which privacy policies are updated, as larger organizations usually show more commitment to current policies.

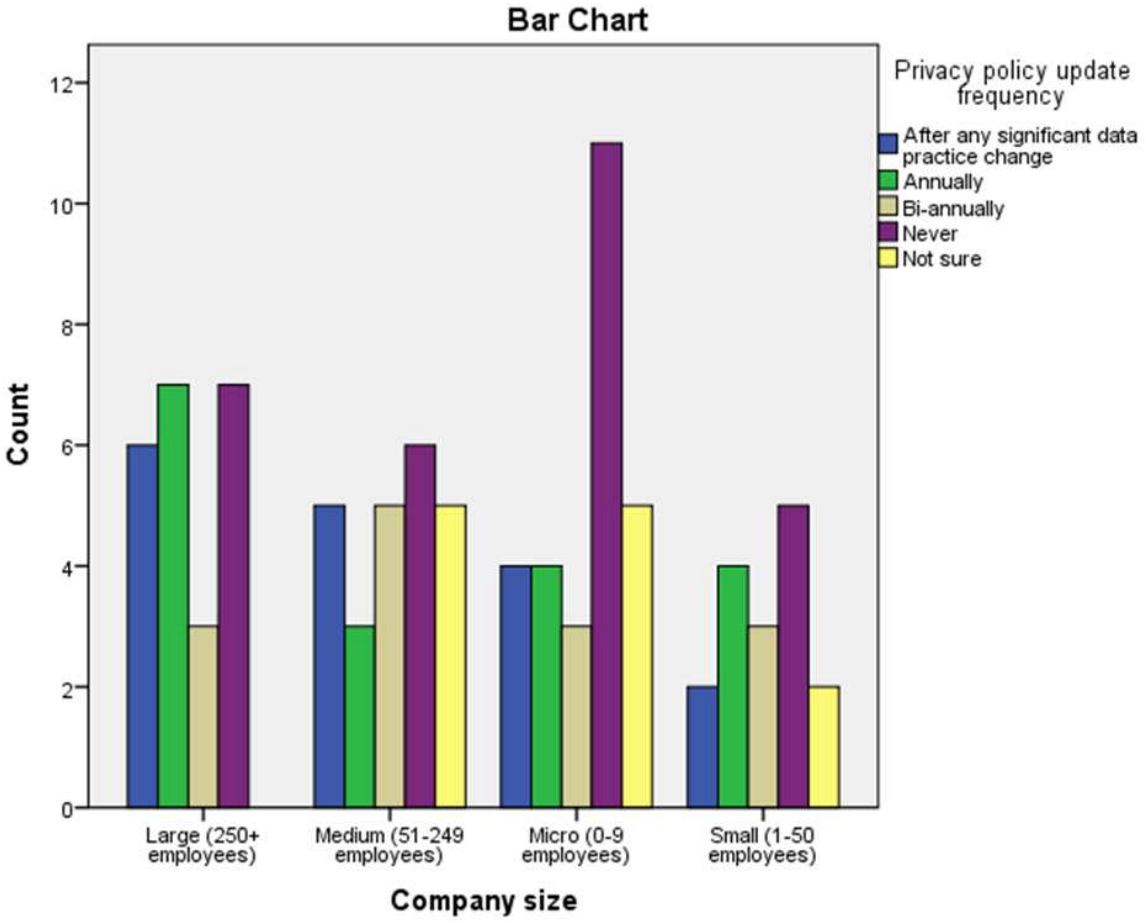


Figure 3. Company size and the frequency of privacy policy updates

Next, the ground between industry and the use of PETs was examined. The cross-tabulation indicated that the technology industry had the highest percentage of PETs utilization among the sampled companies (5 out of 10), followed by the financial industry with PETs utilization among 8 companies out of 23. However, the healthcare sector, with the largest number of companies engaging PETs (8 out of 29) may be attributed to the sensitive nature of health data and strict regulations applied to it. These findings suggest that industrial-specific elements can determine the uptake and preference toward PETs in AI development.

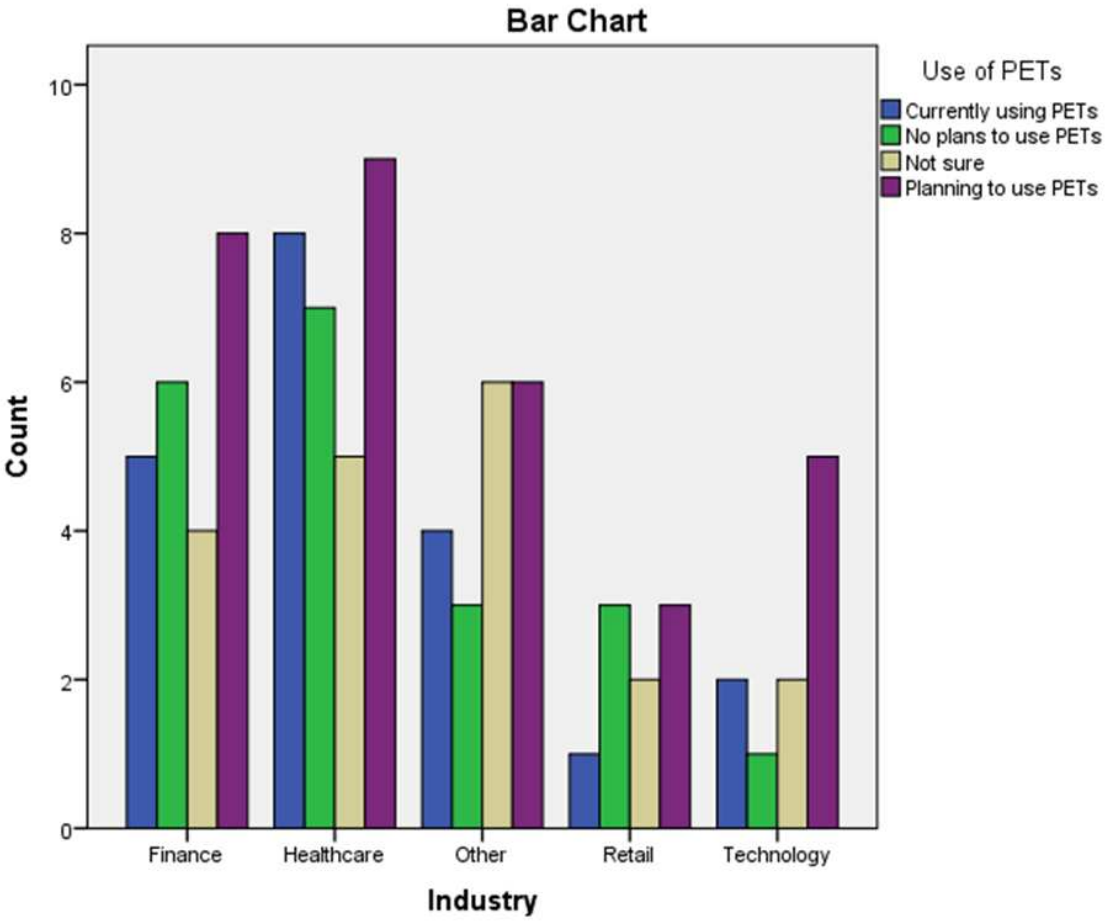


Figure 4. PETs use among industries

The investigation of geographical location and data privacy legislation understanding was the second issue examined. This performed the division of the EU companies into equal parts, where most of the companies displayed moderate understanding, with 5 out of 20 companies being very knowledgeable and 6 being slightly knowledgeable. However, among the companies from North America, there was a higher portion of unfamiliar (8 out of 23) and somewhat familiar (8 out of 23) with the product. This could imply that stricter data privacy laws in Europe as GDPR may result in companies developing a comprehensive knowledge of the regulatory environment.

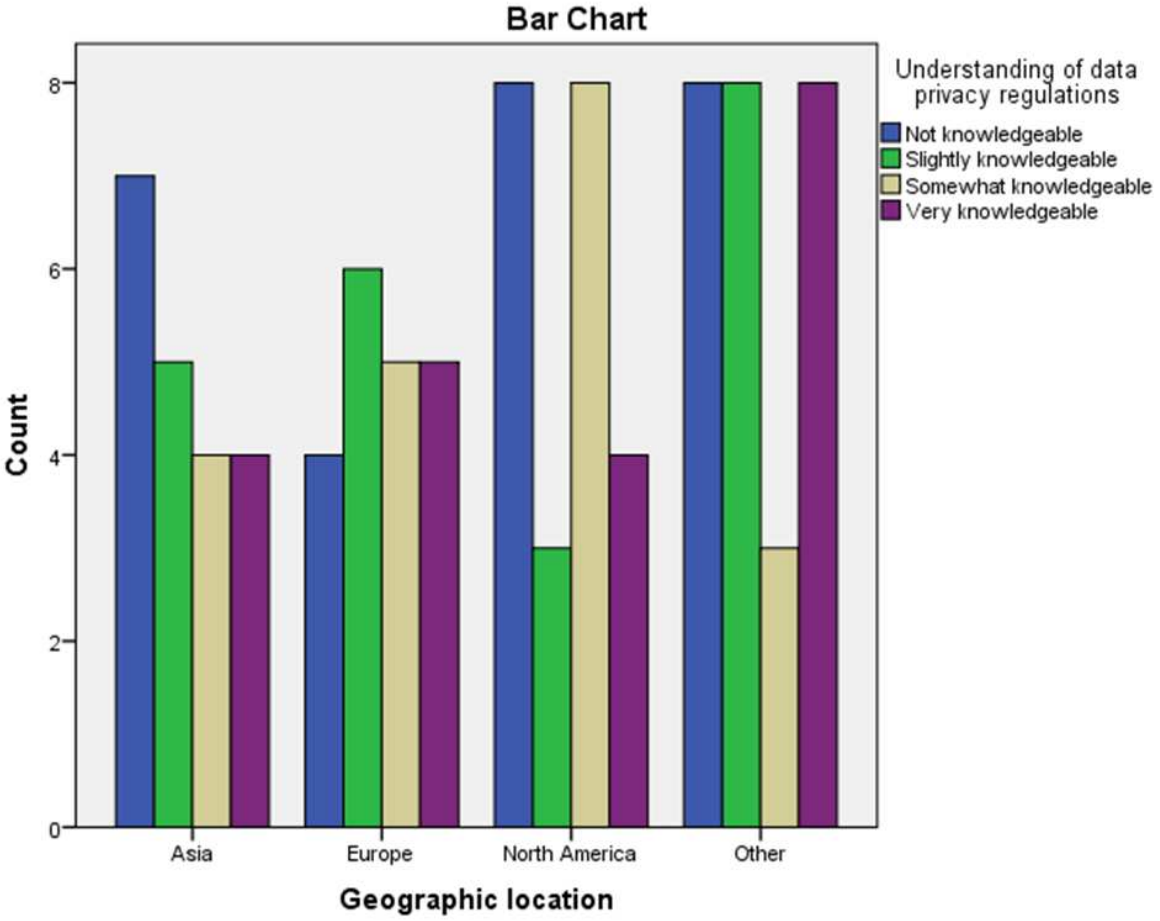


Figure 5. Geographical location and understanding of privacy legislation

Through the crosstabs of consent mechanisms and data usage transparency ratings, even more insights emerged regarding the association between data-gathering techniques and perceived transparency. It was the opt-in consents that had a greater portion of low transparency ratings (6 out of 18 obtaining a 1) and the opt-out consents that had more balance on the entire transparency rating scale. This is however an indication that whether opt-in or opt-out consent is chosen, it might also influence subjects' perception of data usage transparency, with opt-in consent potentially raising more worries about data practices.

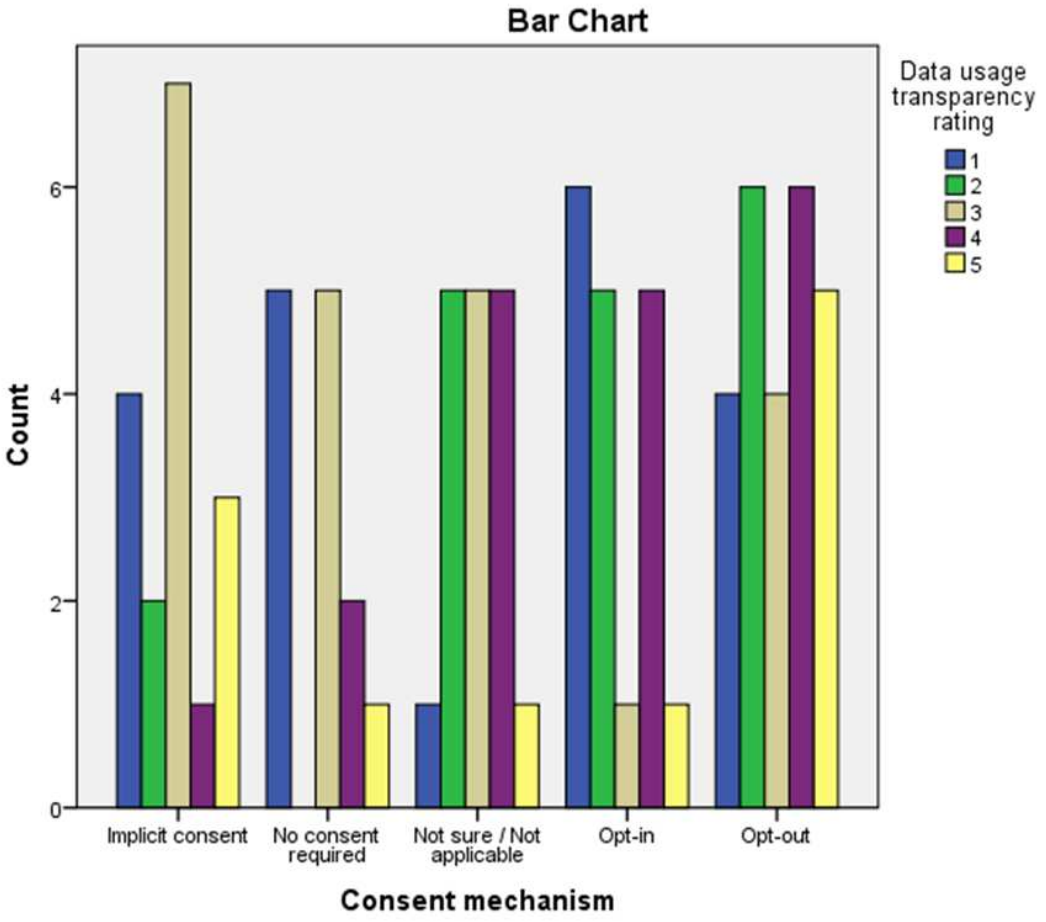


Figure 6. Consent mechanisms and data usage transparency ratings

Finally, the presentation between the industry and the cases of the inaccurate use of data was considered. The chart was cross-tabulated, and it revealed that the healthcare sector has the highest number of data misuse incidents — 16 in total — followed by the finance industry which has 11 out of 23 altogether. This observation demonstrates the greater risks and challenges that such industries face due to sensitive data and reaffirms how a Data Protection System or Incident Response Plan is necessary.

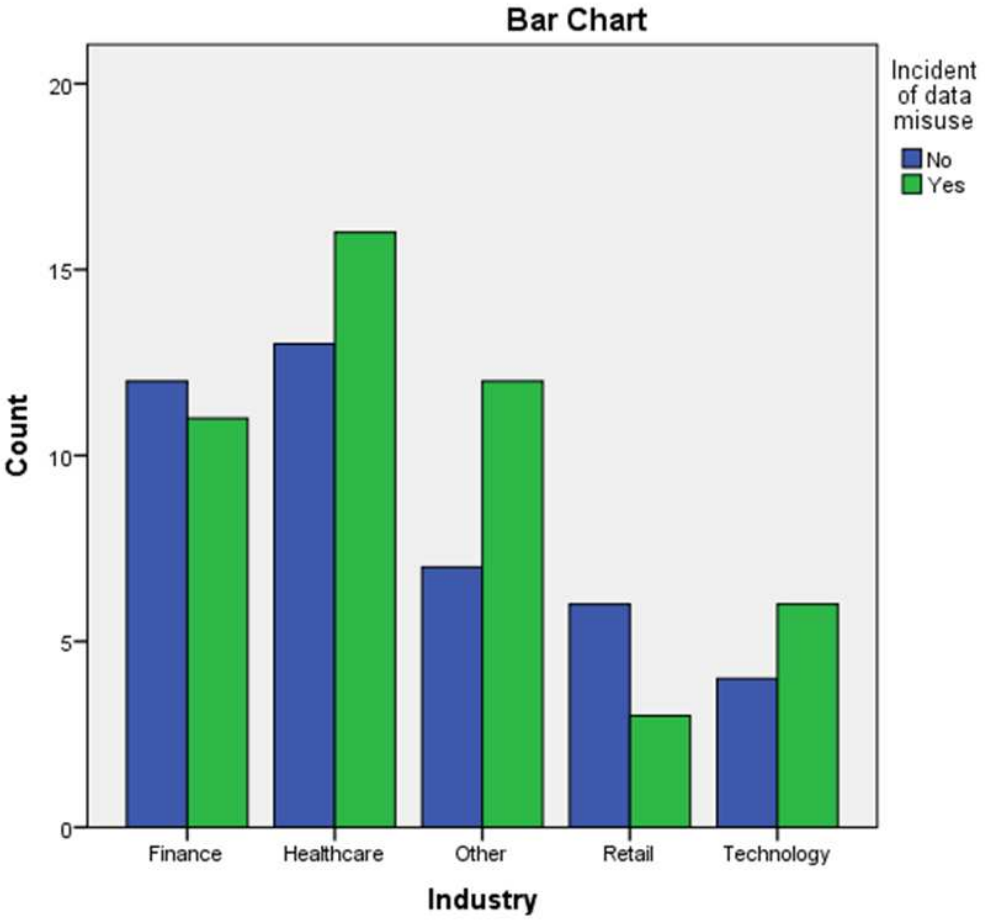


Figure 7. Case of data misuse among industries

6.1.3 Reliability analysis

Reliability analysis was conducted to assess the internal consistency of two sets of variables: assessment of AI abilities in the form of their individual creativity, intelligence, and data security compliance determines AI usefulness (recoded) and AI avoidance due to data privacy law confusion.

For the variables (effectiveness of PETs and use of PETs), Cronbach's alpha coefficient which was 0.132 meant a great number of something. It shows by presenting the Item-Total statistics table that in the case of either item deletion the reliability will not be improved as there is no Cronbach's alpha if the item deleted is provided to be used with the variable of PETs (recode). The fact that there is such low reliability raises the chance that these variables are not measuring the same underlying measurement, and therefore, should be looked at as separate assumptions.

Cronbach's Alpha	**N of Items**
.132	2

Item-Total Statistics

Variable	**Scale Mean if Item Deleted**	**Scale Variance if Item Deleted**	**Corrected Item-Total Correlation**	**Cronbach's Alpha if Item Deleted**
Effectiveness of PETs Recoded	2.42	1.123	.074	-
Use of PETs Recoded	2.87	2.072	.074	-

Table 3. Reliability analysis (effectiveness and use of PETs)

The second set of variables (awareness level of data privacy regulations and compliance difficulty rating) was on the contrary related to the negative Cronbach's alpha coefficient (-0.548). In some rare cases, Cronbach's alpha may be negative; these are cases where there is a negative average covariance of the items among themselves which in turn breaches the reliability model assumptions. This makes this a case of two variables that are not necessarily positively correlated and measure constructs in opposite directions. This is the case where the item-total statistics table displays a negative item-total correlation for both variables. The result shows a significant positive correlation between the variables. Here, we must let go of the idea that the reliability of such parameters can be more than one measure.

It points out the necessity of proper decisions about the choice of variables by which the one that has a common concept and is presumed to measure a single construct is selected. Given these coefficients, low and negativity, the chosen measurements are not amenable at all for making a diagram and these variables are best analyzed separately and along with other relative variables.

Cronbach's Alpha	**N of Items**
-.548	2

Item-Total Statistics

Variable	**Scale Mean if Item Deleted**	**Scale Variance if Item Deleted**	**Corrected Item-Total Correlation**	**Cronbach's Alpha if Item Deleted**
Understanding of Data Privacy Regulations Recoded	2.70	1.448	-.215	-
Compliance Difficulty Rating	2.61	1.319	-.215	-

Table 4. Reliability analysis (understanding of data privacy regulations and compliance difficulty rating)

6.1.4 Hypothesis testing

To investigate the components that form data protection practices and the possible problems with AI advancement, some hypotheses were formed and verified by the data collected from the questionnaire. This part is the hypothesis testing outcome thinking and analysis about the relations and significance of the key variables.

Hypothesis	**Description**	**Test Used**	**Test Statistic**	**df**	**p-value**	**Result**
1	Larger companies are more likely to use PETs.	Chi-square	32.385	9	< 0.001	Reject H0
2	Companies in the technology sector update their privacy policy more frequently than companies in other sectors.	Chi-square	31.238	16	0.013	Reject H0
3	Organizations with operations in Europe rate the difficulty of achieving compliance with data privacy regulations higher than organizations operating in other regions.	ANOVA	15.101	3	< 0.001	Reject H0
4	The transparency of an organization's data usage in AI systems is positively correlated with the organization's size.	Pearson Correlation	0.598	-	< 0.001	Reject H0

Table 5. Hypothesis testing

Hypothesis 1: Company size and PETs adoption

Larger organizations would most certainly introduce and adopt PETs during AI development. This result is in fact a substantial Chi-square test ($\chi^2 = 32.385$, $df = 9$, $p < 0.001$) that shows the existence of a significant influence of company size on PET adoption, where the larger the organization, the higher its investment in security technologies, consequently to its financial resources and security needs.

Hypothesis 2: Companies in the technology sector update their privacy policy more frequently than companies in other sectors.

Technology sector companies are issuing new privacy policies more frequently than companies in the other fields of industry. The chi-square test ($\chi^2 = 31.238$, $df = 16$, $p = 0.013$) proves this supposition correct, which correlates with higher policy changes in the tech sector compared to other industries, because of more rapid technological advancements and increasing strict regulations around data privacy. Yet, the robustness of the findings might be compromised by a heavy percentage of expected counts under five, thus it might be necessary to conduct another research with a bigger or more evenly distributed sample.

Hypothesis 3: Organizations with operations in Europe rate the difficulty of achieving.

Privacy authorities in Europe impose more binding regulations on organizations based in Europe than in the case of other regions. A one-way ANOVA ($F(3,86) = 15.101$ $p<0.001$) and subsequent Tukey HSD tests made it feasible to define that European businesses ($M = 3.95$) encounter more difficulties in terms of compliance than others in Asia, North America, and other regions probably because of the toughened requirements of GDPR.

Hypothesis 4: The transparency of an organization's data usage in AI systems is positively correlated with the organization's size.

Company size and data transparency in AI systems most often demonstrate positive interconnection. Pearson's (0.598, $p < 0.001$) and Spearman's (0.593, $p < 0.001$) correlations suggest that the bigger the organization, the greater the data compliance is. Maybe the very reason for this result is that their governance is better organized, and they know what is expected from them by their public and regulators.

6.1.5 Factor analysis

The factor analysis was performed with the purpose of evaluating the interrelations among the constructs associated with data privacy practices and challenges during AI development, such as data usage transparency, compliance difficulty, the performance of PETs, awareness, and knowledge about data privacy regulations and actual use of PETs. Another indicator was seen in the KMO test that provided a low value of 0.495, suggesting inadequate sampling for reliable factor analysis and Bartlett's test for sphericity was insignificant ($\chi^2 = 16.702$, df = 10, p = 0.081) which may suggest that the data is not suitable for factor analysis. However, these deficiencies were overcome, and three components with eigenvalues larger than one were extracted which together accounted for 72.125% of the explained variance, with commonalities varying from 0.632 to 0.833, presenting substantial portions of explained variance by extracted factors.

Component	**Initial Eigenvalues**	**Extraction Sums of Squared Loadings**	**Rotation Sums of Squared Loadings**
	Total	% of Variance	Cumulative %
1	1.407	28.145	28.145
2	1.138	22.765	50.910
3	1.060	21.205	72.115

Table 6. Factor analysis summary

Using the factor analysis, it is found that three basic dimensions were responsible for the data privacy practices prior to and following the varimax rotation technique. The first factor, characterized by strong correlations with data usage transparency (0.758) and the adoption of PETs (rearranged a negative one, -0.798), describes a set of transparency and PET features. The second factor correlates with two main components compliance difficulty (0.760) and understanding of privacy regulation (reverse 0.779) implying a dimension of regulatory compliance and understanding. Among factors that influence the efficacy of PRs (0.911), the PET dimension of efficiency is eluded. Although the Kaiser-Meyer-Olkin (KMO) value and the insignificance of Bartlett's test indicate sampling deficiencies, this part of the thesis may be taken as it points to a pre-structured understanding of the basic factors underlying the issue of AI data privacy. Such substantiation necessitates the need for further research with a larger or more representative sample to allow for a more confident conclusion.

Variable	**Component 1**	**Component 2**	**Component 3**
Data Usage Transparency Rating	.758	.182	.156
Compliance Difficulty Rating	.238	.760	.271
Effectiveness of PETs Recoded	-.056	-.027	.911
Understanding of Data Privacy Regulations Recoded	.131	-.779	.346
Use of PETs Recoded	-.798	.091	.209

Table 7. Rotated component matrix

6.1.6 Regression analysis

A multiple regression analysis was used to check whether the transparency of data usage existed under the influence of industry, company size, and region where the company was located. This model explained 36.5% of the total spectrum of data usage score ($R^2 = 0.365$) and was statistically significant ($F(3,86) = 16.479$, $p < 0.001$) where at least one of the independent variables had an impact on transparency scores. While company size was only the significant predictor ($B=0.683$, $t=6.898$, $p<0.001$), revealing that larger companies are naturally more transparent. Although recording has increased the level of transparency, neither the industry classification nor the economic situation of the nation had an excessive influence on the rating. The 95% interval for company size, ranged from 0.486 to 0.88 (one straight line), confirming the presence of a positive significant effect on transparency.

Multiple Linear Regression: Predicting Data Usage Transparency Ratings

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.604	.365	.343	1.079

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
1					
	Regression	57.596	3	19.199	16.479
	Residual	100.193	86	1.165	
	Total	157.789	89		

Coefficients

	B	Std. Error	Beta	t	Sig.	95% Confidence Interval
(Constant)	.757	.480		1.578	.118	-.197 to 1.710
Industry Recoded	.048	.090	.046	.532	.596	-.131 to .227
Company Size Recoded	.683	.099	.602	6.898	.000	.486 to .880
Geographic Location Recoded	.084	.098	.074	.863	.391	-.110 to .279

Table 8. Linear regression analysis

A logistic regression analysis was performed to constitute the possibilities of misconduct over aspects that include factors like the use of PETs, company size, the degree of compliance difficulty, and the frequency of privacy policy updates, which used the data from the 90 cases without missing values. The basement model was good at predicting "Yes" cases for misusing the data with 53.3% accuracy. In the logistic model, the prediction of data misuse did not significantly increase from the baseline model level which was found when dealing with an omnibus test result ($\chi^2 = 8.917$, df = 7, p = 0.259). Also, the proportion of explained variance was only small (Cox & Snell $R^2 = 0.094$, Nagelkerke R The Hosmer and Lemeshow test revealed the suitability of the model ($\chi^2 = 8.003$, df = 8, p = 0.433), and the accuracy rate was predicted to be 64.4%. Consequently, the independent variables (PETs use, company size, compliance difficulty, privacy policy update frequency) were insignificant and had a p-value > 0.05 when predicting data misuse, this is even more reason to delve into other influential factors.

Logistic Regression: Predicting Data Misuse Incidents

Block 0: Beginning Block

Observed	**Predicted No Incident**	**Predicted Yes Incident**	**Percentage Correct**
No Incident	0	42	0%
Yes Incident	0	48	100%
Overall Percentage			53.3%

Block 1: Method = Enter

Observed	**Predicted No Incident**	**Predicted Yes Incident**	**Percentage Correct**
No Incident	20	22	47.6%
Yes Incident	10	38	79.2%
Overall Percentage			64.4%

Table 9. Logistic regression

6.1.7 Thematic analysis (Open-ended questions)

Thematic analysis of the data yielded five kinds of data misuse cases that are likely to occur in organizations. The most prominent leaks of user data were reported because of configuration errors 19 times, and this emphasizes once more the demand for more advanced configuration management. And then unauthorized data access by the staff, which was 14 times, showed that organizations should put stricter access controls as well as employee training into consideration. Furthermore, other indicators of data loss were recorded due to misplaced devices (9 devices). This illustrates the relevance of encryption and remote wipe capabilities, and excessive data sharing with partners (6 cases) shows the need for strong data sharing agreements. However, surprisingly, a total of 42 respondents did not experience any fraud or case of data misuse, therefore, implying adherence to data protection practices in some companies.

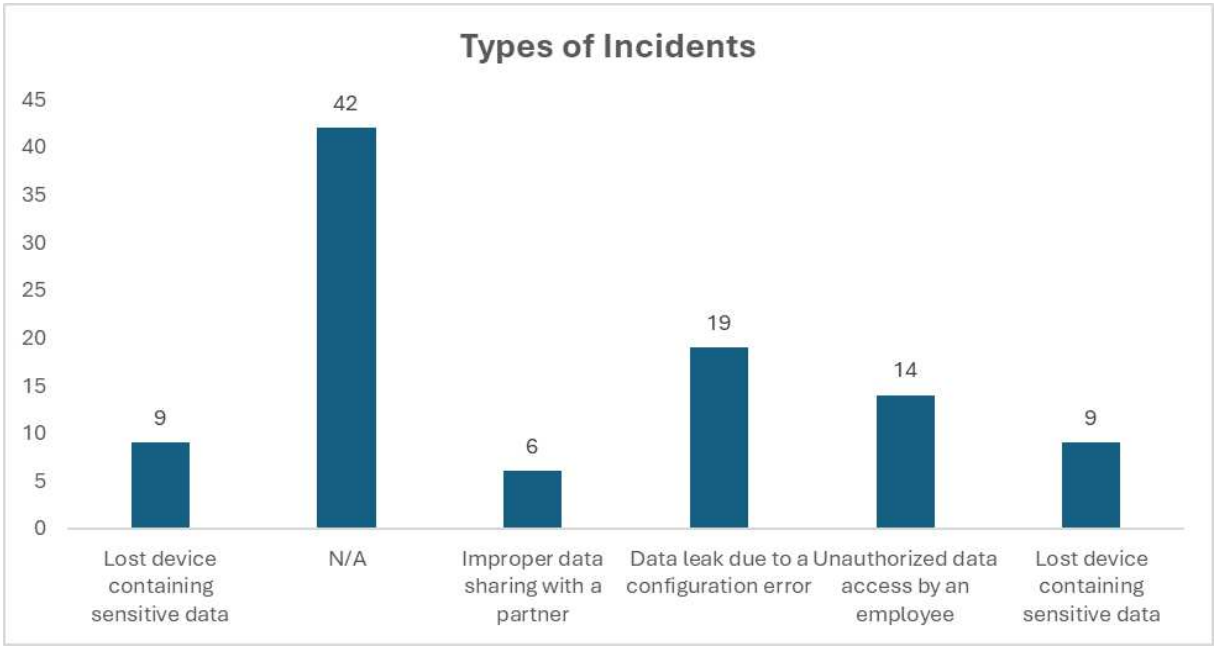


Figure 8. Types of incidents

In the content analysis, it was seen that privacy regulations of data mainly extend AI development due to the need for impact analysis and privacy design. However, a large part of the respondents think (22) that regulations strictly restrict the use of data which might in the end affect the efficiency of AI. The high level of compliance costs caused a shift to specialized staff and compliance instruments. On the other hand, 16 respondents acknowledged that the regulations facilitated building more advanced data security systems, while 12 participants noted that AI regulations were not particularly restrictive and they either were not involved in this area or were adhering to the existing compliance.

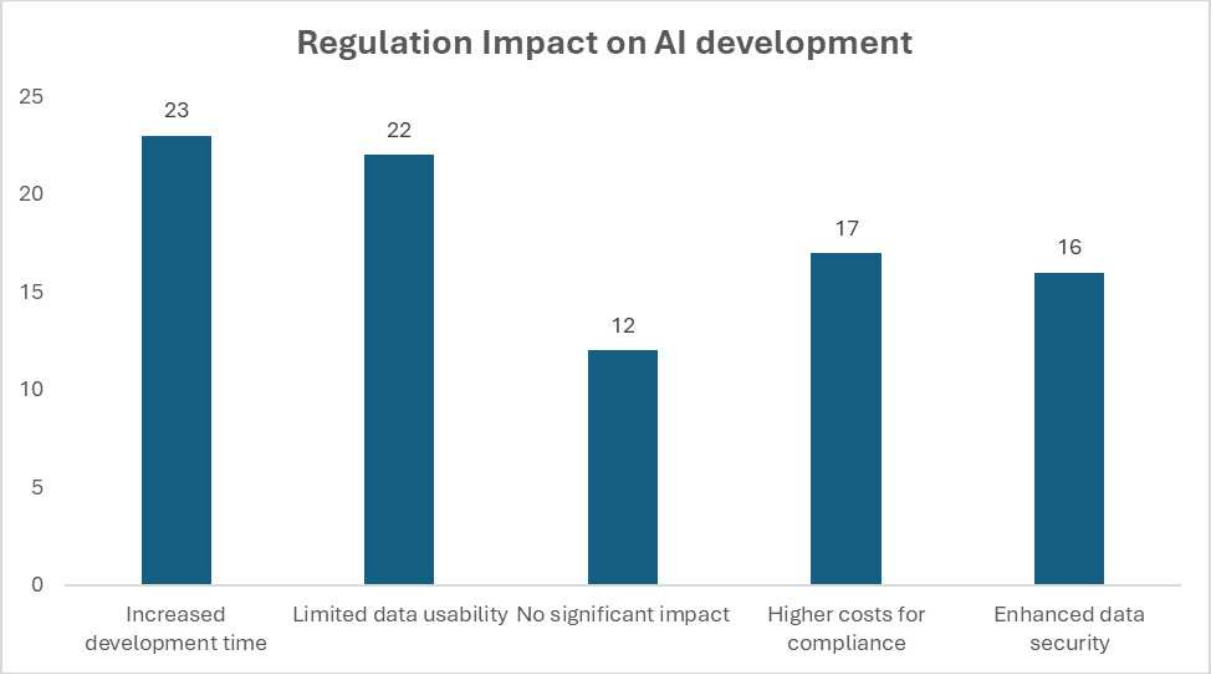


Figure 9. Regulation impact on AI development

The thematic analysis related to data privacy for AI training has highlighted 5 main recommendations. In order to decrease the risk of data breaches data minimization was most advised (24 statistical indications). Encryption of confidential data, either when stored or while in transit, may be cited 18 times to strengthen data confidentiality. Educating the employees on what is data protection was considered by us as a means of ensuring that people make fewer mistakes and ultimately build a privacy-conscious culture among all. Audits should be done on a regular basis to fulfill the purpose of validating and enhancing the controls on data protection. Finally, the implementation of privacy-enhancing techniques such as differential privacy and fedlearn technologies to protect the privacy of individual data by training AI interactively was also proposed.

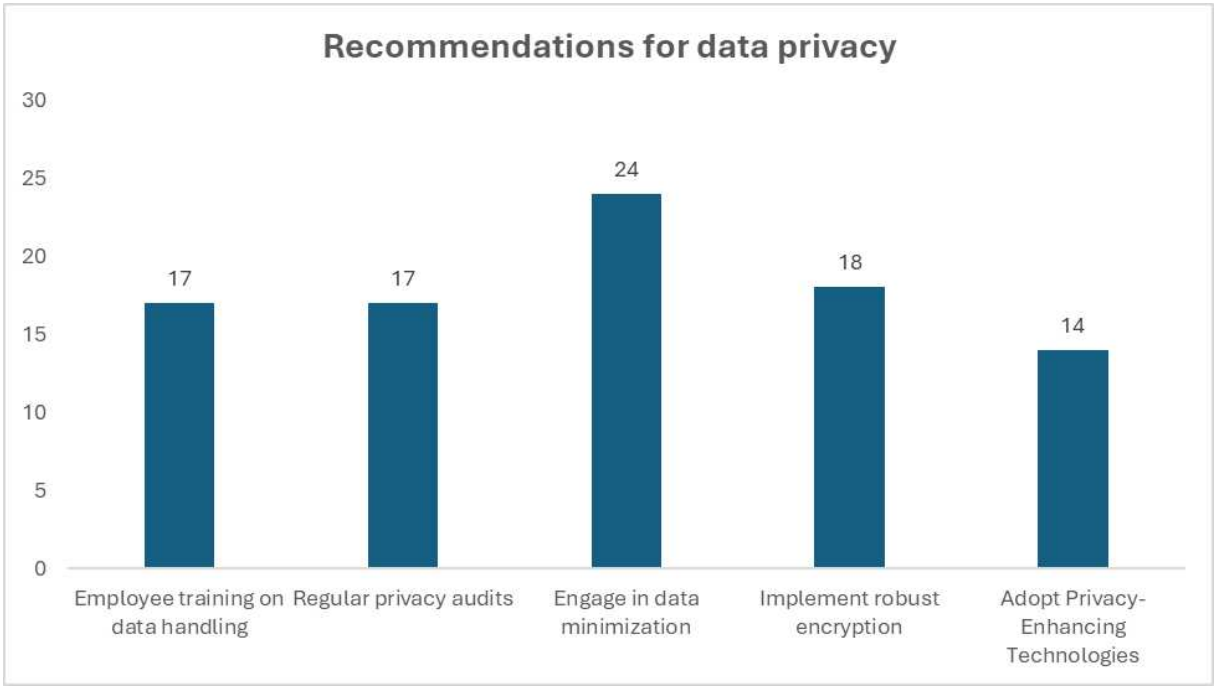


Figure 10. Recommendations for data privacy

6.2 Qualitative component analysis

The integration of both qualitative and quantitative methods is used extensively during this research to carry out a detailed thesis concerning data privacy within the AI system. Although qualitative chapters are what give readers an in-depth understanding of the statistical nature of data privacy, qualitative analysis is what offers a shift from a quantitative viewpoint. This method gives special attention to the underlying organization of the practices and policy interpretations, this expands our knowledge of private data beyond figures. The current situation of AI as a domain that is ever-shifting and volatile demands such an approach. This mix of the qualitative (information that opens decisions and implications behind the statistics) and the quantitative (there is a clear level of data) is very useful. This process is intended as a means of comprehension not only of "what" is happening in the field of privacy and AI but also of "how" and "why" these issues occur, as it offers a complete picture of the issues from within.

6.2.1 Regulatory compliance and ethical considerations

The NVivo research on AI and data security has revealed a continuum of issues and chances that companies are to face during the implementation of AI and data security technologies. The research focused on the technical challenges that firms faced, especially under GDPR, with respect to case 2, highlighting how regulatory articles and the right to explanation affected the companies, with 79 mentioned times that affirm the deep integration of AI into business operations and demand for transparency. Conversely, only one article considers just Case 1 without any mention of concern in the article, maybe this is a less involved problem or impact, Case 3 with 13 mentions shows the integrated nature of governance, regulatory compliance, and patient-centered approaches for healthcare AI.

Case Studies	**Compliance Challenges and Opportunities**	**Number of References**
Case 1	GDPR Operational Impacts	0
Case 2	GDPR Articles & Right to Explanation	79
Case 3	Collaborative Governance & Patient Privacy	13

Table 10. Thematic summaries of compliance challenges and opportunities

Concerning the ethical design of AI, the report emphasized that every healthcare organization should incorporate equity, bias acknowledgment, and patient-centered thinking. Case 2 deals with fairness bias questions with 40 references/citations and emphasis on the application of fairness-oriented machine learning methods. Case 1 explained the significance of transparency and accountability in human-made decisions, relying on 13 references, whereas Case 3, emphasizing 25 of them, illustrated the ethical concerns in healthcare through AI, describing patient autonomy as the key point. These cases as a whole illustrate that the ethical landscape of AI technology is a complicated one that contains many issues including socially responsible and ethically guided AI systems in multiple fields.

Case Studies	**Ethical AI Design Principles**	**Number of References**
Case 1	Transparency & Accountability	13
Case 2	Fairness & Bias Mitigation	40
Case 3	Patient-Centric Ethical Design	25

Table 11. Thematic summaries of ethical AI design principles

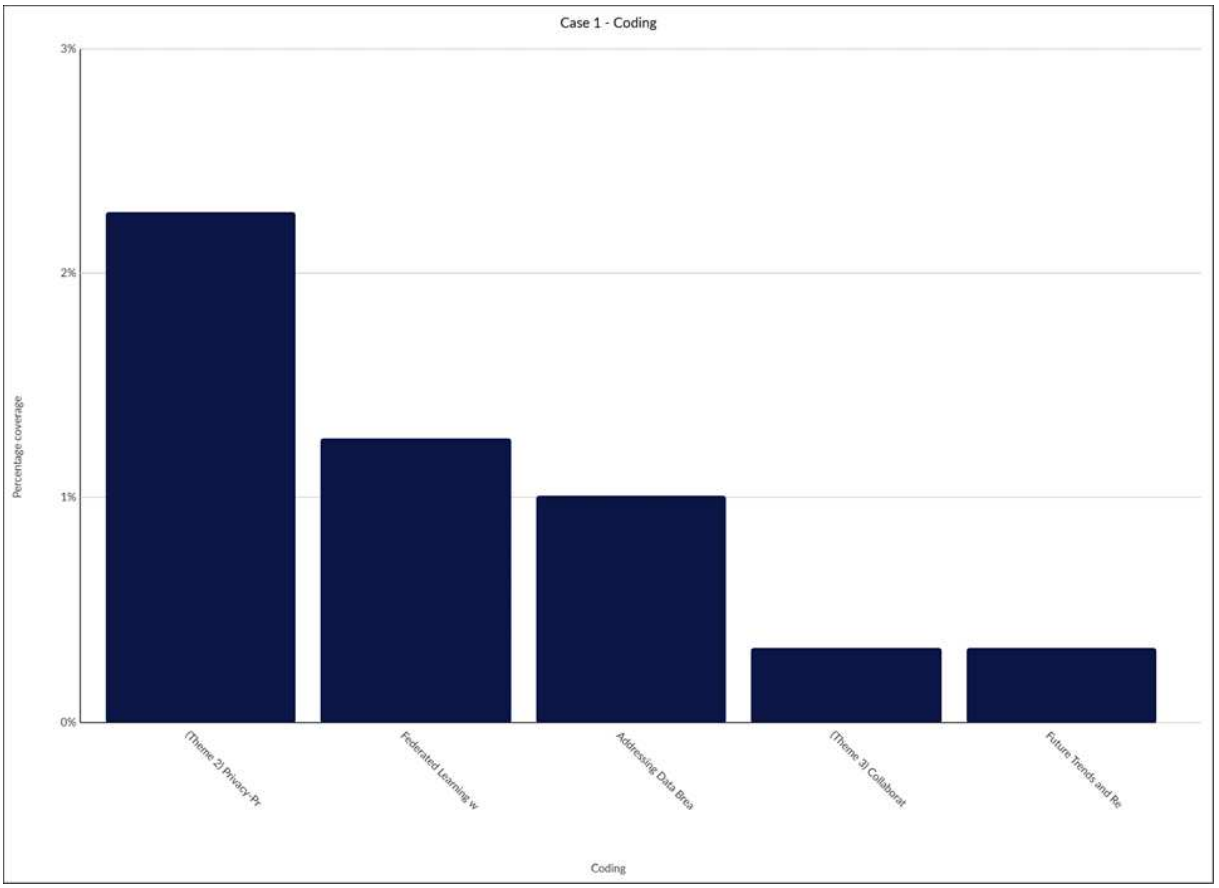


Figure 11. Covering themes of case 1

6.2.2 Privacy-Enhancing Technologies

NVivo analysis results revealed major concerns and possible solutions to the data breaches and insider threats in an oversized variety of situations that point out the PETs' necessity. Case 1, with 35 references, focuses on the organizational tactics involved in risk prevention. It involves utilizing cutting-edge cryptographic technology, strict access controls, and wide-scaled monitoring. In case 2 it is embodied that legal and compliance issues with data breaches exist, and it is important to adhere to strict privacy standards such as GDPR and HIPAA with 20 sources. Case 3, referenced at 15, promotes data protection in AI healthcare domains, arguing in favor of ethical considerations by providing personal data protection through specific methods like differential privacy.

Case Studies	Data Breaches and Insider Threats	Number of References
Case 1	Strategies and Mitigation	35
Case 2	Legal and Compliance Aspects	20
Case 3	Patient Data Security	15

Table 12. Thematic summaries of data breaches and insider threats

The research uses thematic analysis to investigate the various settings in which federated learning and differential privacy are used, as is the case of Case 1 which with 45 references leads to the use of federated learning in organizational contexts as a way to balance data protection with utility. Case 2 with 25 references looks at what the ethical issues of this technology are stressing on fairness in algorithms and that data misuse is prevented. At the same time, Case 3 presents 30 references and discusses the use of big data analytics in healthcare, including the balance between the exploitation of big databases for healthcare improvement and information healthcare protection. This shows a critical approach to the secure management of sensitive data.

Case Studies	Federated Learning and Differential Privacy	Number of References
Case 1	Application in Organizational Settings	45
Case 2	Compliance with Ethical Standards	25
Case 3	Use in Healthcare Data Analysis	30

Table 13. Thematic summaries of federated learning and differential privacy

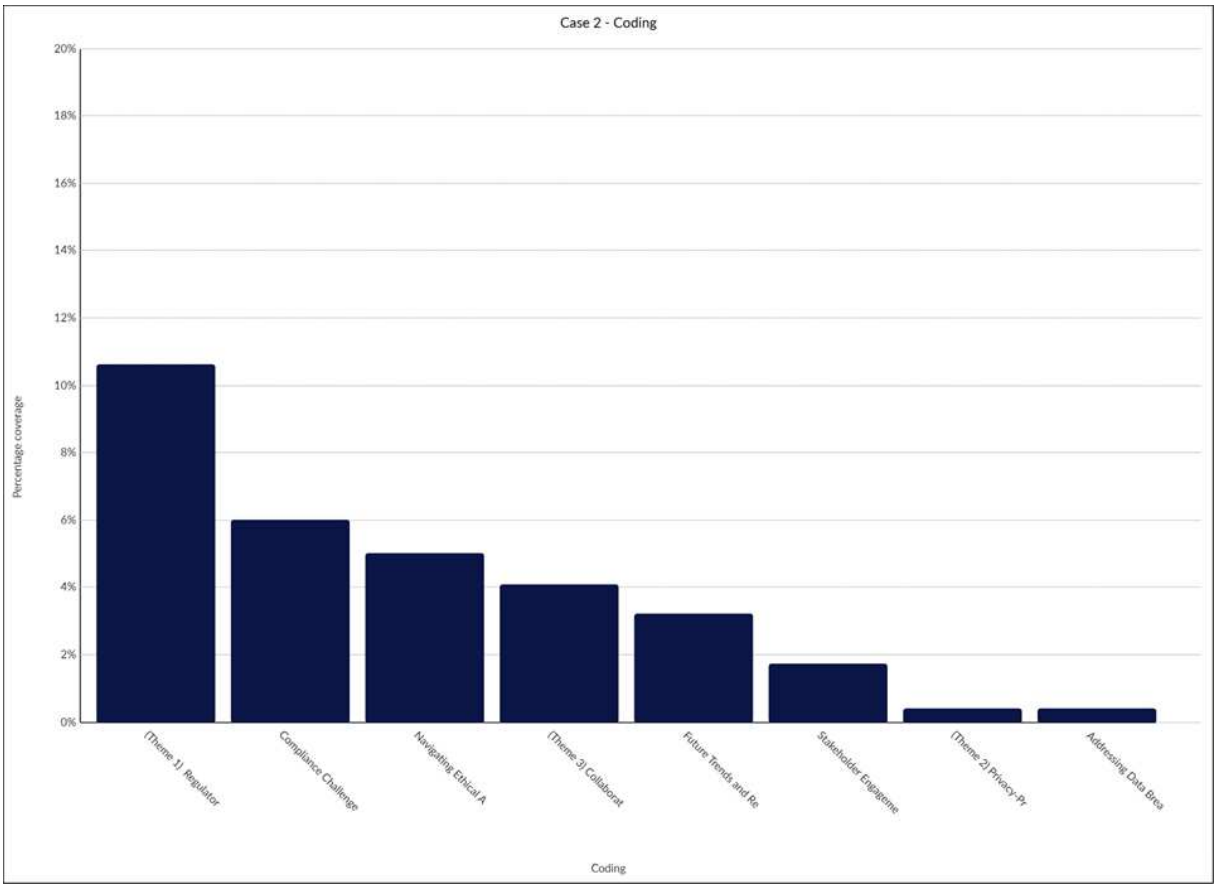


Figure 12. Covering themes of case 2

6.2.3 Collaborative approaches to data privacy

From NVivo analysis, it is revealed that stakeholder engagement and governance are the two main components in solving the challenges in AI data privacy complexity with their narration of the cases. Case number one is all about the technical collaboration of tech companies and cybersecurity-based organizations with an emphasis on information sharing which helps in effective controlling over privacy issues. Case 2 corresponds to 35 references, where it is established that this requires partnership and coordination with the regulators and the stakeholders for the creation of an ethical AI atmosphere that is ably upheld by compliance and best practices. Case 3, 25 references were done to stress the role of patient advocacy groups and ethical oversight in healthcare. Integration of patients' experiences with ethically developed AI products is endeavored to achieve info-privacy solutions.

Case Studies	Stakeholder Engagement and Governance	Number of References
Case 1	Technical Collaboration	10
Case 2	Regulatory and Industry Alliances	35
Case 3	Patient Advocacy and Ethical Oversight	25

Table 14. Thematic summaries of stakeholder engagement and governance

According to the thematic analysis of collaborative efforts, case 1 lists technical partnerships between the different sectors that will facilitate the technology transfer for privacy protection. Case 2 identifies the need to build a multi-directional and inclusive regulatory framework that allows all industry perspectives to be incorporated. The regulations must be practical and align with industry practices. Case number 3, with the most references (30), puts patient involvement and consent at the top. This illustrates how a community or a group involved in the discussions on machine-learning applications in healthcare may act to ensure both high-quality and privacy-saving policies.

Case Studies	Collaborative Efforts Synthesis	Number of References
Case 1	Cross-Sector Technical Partnerships	15
Case 2	Regulatory Framework Development	20
Case 3	Community Engagement and Patient Consent	30

Table 15. Thematic summaries of collaborative efforts synthesis

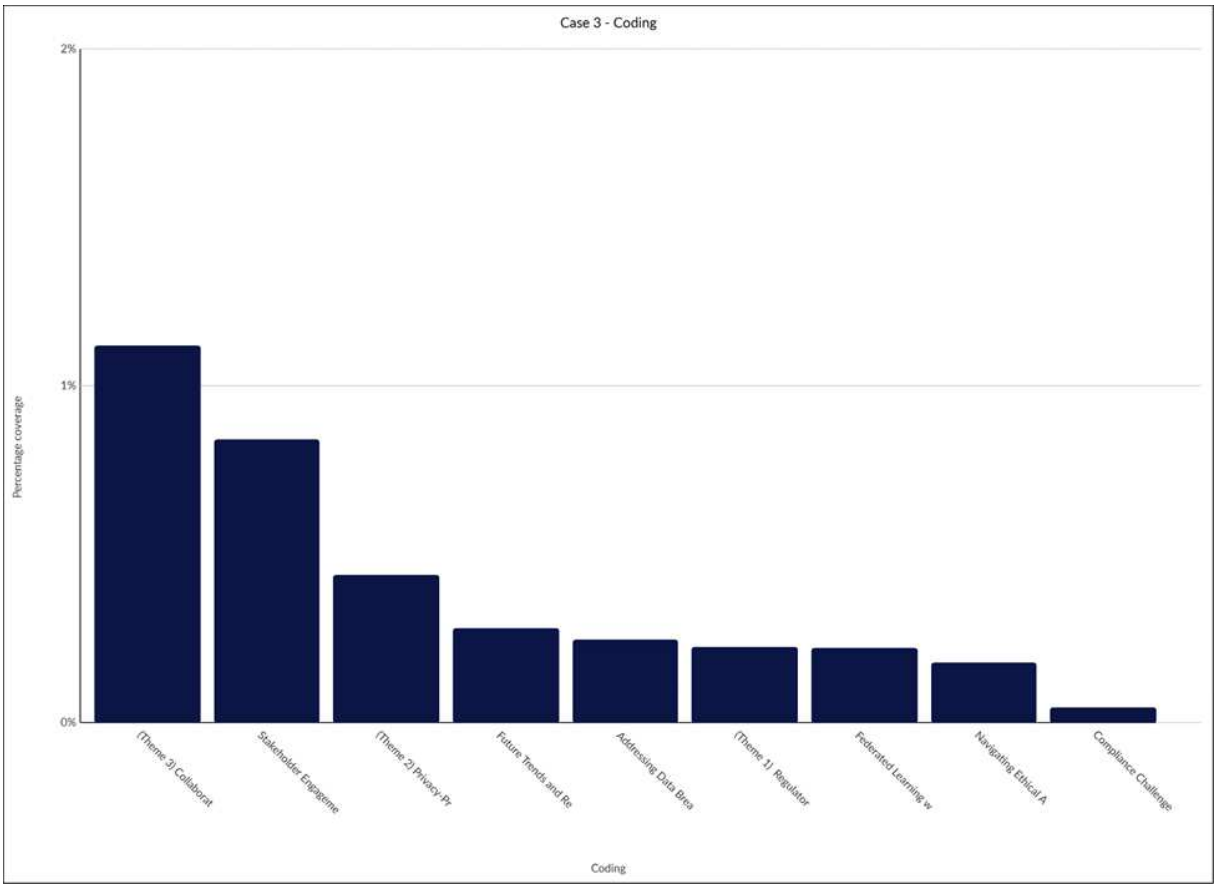


Figure 13. Covering themes of case 3

6.3 Integrated analysis and discussion

In this section, the thesis will interweave the qualitative wallets of the NVivo analysis with the quantitative findings, synthesizing the results around regulatory compliance, ethical AI design, safeguarding individuals' data privacy and PETs, and going forward by collaborative approaches to data privacy. This synthesis not only contributes to the understanding of the AI's private data space because it also breaks the difficult barrier between trends pictograph and depth.

The inclusion of qualitative data with the benefits of the quantitative model imparts difficulties and complexity to organizations in the process of getting much deeper into AI and data privacy. The integration of thematic analysis into the visual data illustrates the patterns that are repeated in case studies which are likely to develop common issues and solutions that are beyond the industry boundaries.

6.3.1 Key observations

Regulatory compliance and ethical considerations

Any of the solutions proposed to resolve the regulatory compliance and ethical issues raise the question of whether there's any need for a brain-like AI because it would agree with the legal and ethical principles designed for such purposes. The tables reveal that the treatment given to the qualitative analysis experienced an increase in the frequency of ethical as well as regulatory wrestling during the qualitative research, with a broad discussion that also has more citations. The fact that the number of companies complying with the rules and ethical standards increases shows that organizations are becoming more sensitive to the matter of adhering to regulations when dealing with AI systems development and deployment.

According to qualitative data, it can be seen that companies adopt a proactive approach to comply with the already implemented rules like GDPR in the EU and the CCPA in the US. Besides, ethics of AI design is becoming a widely taken reality that entails both the impact of AI systems on individuals and communities as well as the human values that are protected and used to build AI systems that are fair, transparent, and accountable.

PETs

The influential role of privacy-protection languages, as shown in case 1 for example, is a sign of a new era where the prevalent trend is towards more secure and private AI systems. The quantitative data, as it currently stands, further corroborates this frame that there is a nationwide will to promote the use of systems like federated learning and differential privacy, which is an industry attempt to secure data.

Federated learning is a kind of distributed learning technique, a distributed machine learning approach, or distribution machine learning, in which separate parties collaborate to train a common model using individual data that is not shared online directly. With this method, organizations can carry out AI operations with the crucial security of sensitive data. Subjective anonymization, on the other hand, has a mathematic framework that ensures a powerful privacy guarantee by adding noise from data and the model’s output; a process that makes it difficult to identify individual datasets.

These PETs are not as adopted, but we have observed a growing focus among organizations on the commitment to ensure data privacy while keeping the power of AI. The most significant aspect of the qualitative analysis includes why businesses cannot perform in the contemporary world without these tools that build trust between customers and stakeholders as well as help businesses fulfill data protection regulations.

Collaborative approaches to data privacy

The application of themes, particularly in cases 3 and those that are related to AI implementation in healthcare systems as well as the incorporation of cooperative approaches suggest that collaborative methods would be the most viable ones. As can clearly be seen in the multi-stakeholder engagement figures, this aspect of AI governance is highly collaborative in nature and encourages a democratic model of AI solutions, adding even more ideas that push for collaboration and inclusivity.

On the togetherness approach of data privacy, the different participants; that is, the industry players, academics, policymakers as well as civil society organizations, participate in developing common principles, guidelines, and best practices for the design and development of responsible AI technology. These approaches acknowledge that combating AI and data privacy issues is not just a unilateral effort but involves varied stakeholders and different views.

Given the influential and delicate nature of the health sector, collaborative approaches are more critical than others, considering the privacy of health data and the consequences for patient health by AI. The qualitative analysis demonstrates the significant role that healthcare professionals, patient advocates as well as ethics committees ought to play in the making and functioning of AI systems to ensure that these mirror the ethical and socio-economic goals of the healthcare community.

6.3.2 Patterns and Outliers

Patterns

Compliance is a key rule that all hold as an accountability feature and be audited qualitatively and quantitatively too by organizations in most of the AI applications. This is also borne out by the fact that the AI ethics cases arise from the shared responsibility that is mandated to AI application providers that are interested in this ethical AI design.

The thesis provides a clear image of the community made of organizations that have already gained the understanding that regulations compliance and business ethics are keywords for the successful implementation and deployment of AI systems. There seems to be not only increased attention to compliance and ethics across this set of case study contexts but also a

growing awareness by organizations to integrate these values into all aspects of AI decision-making, whatever the industry or application context.

Outliers

Hence, whereas maintaining privacy is the fundamental characteristic in both situations 1 and 2, case 1 with its federated learning and differential privacy technologies presents an isolated case as perhaps it is the result of a different organization approach or other advancements in the privacy issues.

This exception means that while we see the trend of choosing PETs, the specific methods, and the implementations of them are different for each organization due to diversity in their contexts, resources, and the level of possibility to solve privacy-related problems. Case 1's focus on federated learning and differential privacy may be evidence that the organization has an askew understanding of those technologies and has made a big deal of investment regarding their implementation.

An outlier is a phenomenon that draws our attention to the truth that there is no common approach to data privacy when applied to AI. Organizations should therefore consider their detailed requirements, limitations, and requirements when choosing the most suitable PETs and approaches that match their context exactly.

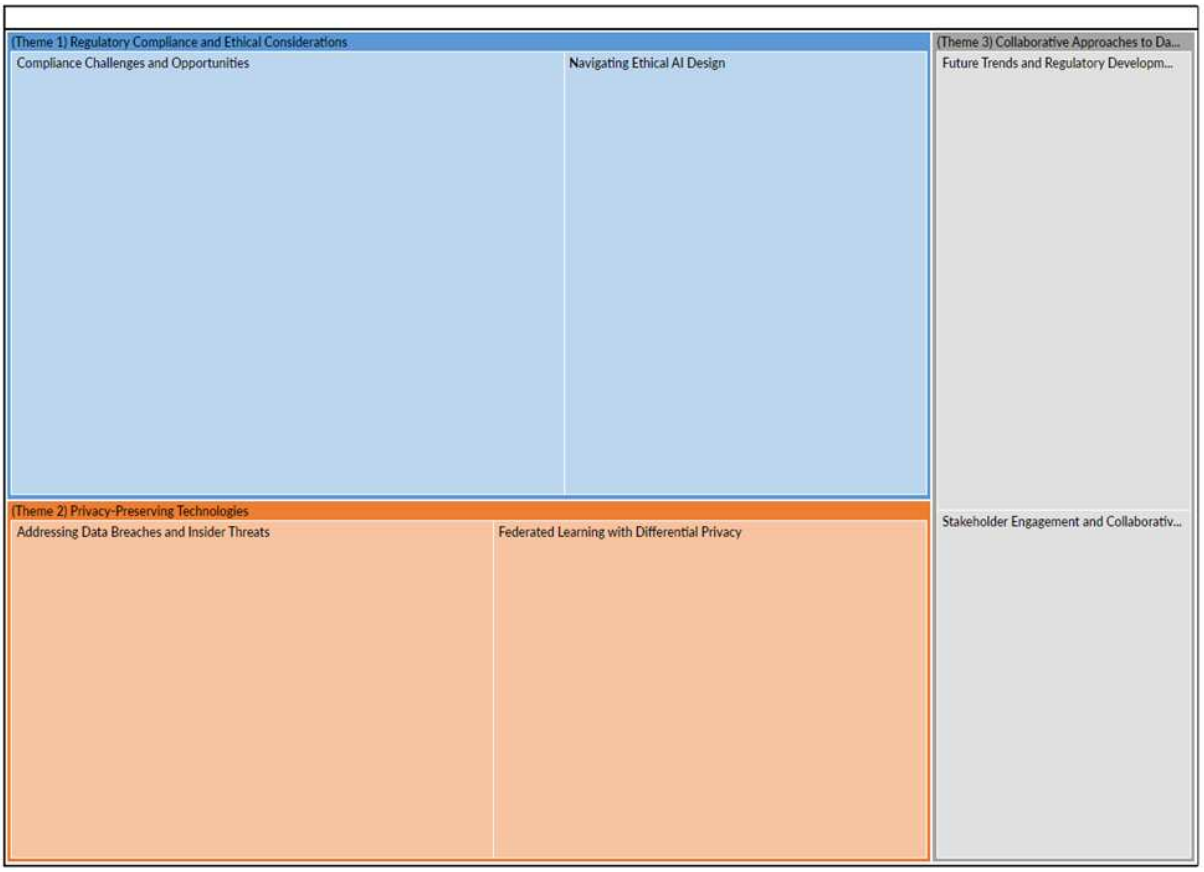


Figure 14. Qualitative data summary

7 Conclusion

This thesis aims to explore the intricate arena of data privacy for the effective implementation and conformance of AI systems in corporations, with attention paid to business practices and regulatory compliance. An upper objective was to segregate challenges, best practices, and chances for the appreciation of privacy protection in AI.

Specifically, the research objectives were threefold:

- Assess current data privacy practices adopted by companies in collecting, using, and securing data for AI training, and identify gaps in privacy protection.
- Explore the inherent challenges and risks in ensuring data privacy in AI, including technological, ethical, and legal aspects.
- Evaluate the effectiveness of existing data protection laws and regulations (e.g., GDPR, CCPA) in addressing privacy concerns in AI.

To achieve these objectives, the thesis sought to answer the following key questions:

- What are the current practices and methods employed by corporations to collect, process, and protect personal data used in AI development?
- What are the major challenges and risks that organizations face in safeguarding individual privacy while leveraging data for AI innovation?
- To what extent do existing data protection regulations effectively govern AI practices and mitigate privacy risks? What are the gaps and limitations?
- What strategies, best practices, and recommendations can help companies and policymakers strengthen data privacy in AI while enabling responsible innovation?

7.1 Summary of key findings

The empirical part of this thesis generated some significant results which are not only revealing for the present situation but also give insight into the challenges of data privacy when developing AI. It emerged during the analysis that lots of organizations make use of PETs such as encryption and pseudonymization but still, there is a wide variability when it comes to the consent mechanisms, data minimization, and transparency. Also worth noting are the large companies and those in heavily regulated areas like healthcare and finance, where privacy programs are generally more mature than in other sectors. This implies that resources and regulatory pressures push organizations to invest in privacy.

The qualitative analysis largely revealed the organizational, technical, and human factors that influence data privacy in AI. A recurring theme here is the fact that a ton of data is needed to train such AI models which however creates a tension with the need to protect privacy rights. The organizations got involved with challenges like obtaining true consent, accuracy of data, and managing the risks of re-identification and misuse. The scenario addressed the key issue of building a culture of privacy, the involvement of the community, and the integration of privacy aspects throughout the AI design and development phase.

7.2 Interpretation and implications of findings

The pilot of this research stressed a holistic perspective on data policy relevant to AI. From a quantitative point of view, it becomes evident that although the situation for PETs has been improving, there is still a lot that needs to be done in transparency, the user, and data minimization. Such an alignment supports the findings of previous studies that have revealed privacy issues in AI systems to be more difficult than it seems (Bellovin et al., 2019; Jain et al., 2018). The fluctuation in companies along the industries indicates clearly that what works for all companies does not always work similarly and there is a need for sector-specific guidelines and best practices as noted by policy experts (Calo, 2017; Kaminski, 2019).

Based on the case study results, we can conclude that AI privacy is not an issue that can be solved by just technical solutions. It rather needs the agreement from relevant parties, to-be-changed organizational commitment to privacy, and mindset changes. This echoes the notion that such ethical factors have to be considered alongside the development processes (Floridi et al., 2018; Morley et al., 2020). The obstacles revealed, for example, collecting patients' informed consent and checking data fairness, carry forward the research that will be made in such areas as building up the mechanism to utilize user consent and detecting and diminishing bias (Mostert et al., 2018; Mehrabi et al., 2021). The thesis further pinpoints the need for such interdisciplinary collaboration through which not only the technical aspects but also ethical, legal, and social aspects pertaining to these challenges need to be dealt with (Wirtz et al., 2019).

Comparing this result with the earlier findings, the research confirms many of the privacy risks identified in past works like conflicting information utility and privacy, problems of traditional consent (Solove, 2013), and the need for transparent and accountable AI systems (Wachter et al., 2017). However, the results also extend the existing knowledge base by

offering a detailed view of the activities in different sectors, showing the differences within sectors, and identifying specific steps toward privacy protection in personal data processing.

The significance of these outcomes as both theoretical and practical novelties is instantly obvious. This research, from a theoretical point of view, adds to the expanding realm of AI ethics and governance literature (Floridi & Cowls, 2019; Jobin et al., 2019). Aside from that, it further emphasizes the necessity for a system that can successfully manage the priorities presented by innovation alongside the imperatives of privacy protection. From a more down-to-earth perspective, the outcome can be used to draft suitable recommendations for AI privacy-based technology companies and policymakers who are interested in coming up with well-developed regulations for AI privacy protection (Goldfarb & Tucker, 2012; Tene & Polonetsky, 2013). The data has the essence of public management of privacy, the involvement of the stakeholders, and the development of standardized privacy-management techniques or tools (Rubinstein & Good, 2013).

7.3 Strengths, limitations and future research

To provide a well-rounded analysis, this thesis used a mixed-methods approach which combines the use of surveys for numerical analysis with the application of case studies qualitatively, to give an accommodative comprehension of data privacy challenges and AI development approaches. As the involvement in an assortment of AI specialists from various industries and countries increases, this strengthens internal validity (Creswell, 2017). The thorough case studies presented me with in-depth scenarios and high-context lessons about actual privacy challenges and ways to deal with them. This helped me apply these research findings (Yin, 2017).

Notwithstanding the fact that this thesis also has several limitations. On the one hand, the survey relied on the data which was a result of self-reporting, which, in fact, can be biased. However, on the other hand, no one can change the objective reality. In addition to this, these case studies gave qualitative perspectives. However, these case studies assign a few organizations for illustrative purposes only and might not cover each AI company and the context. Moreover, it is worth mentioning as well that the high speed of technical development means that positive results represent short-term findings, and it is important to note that this will require further research to figure out evolving threats to privacy and ways to fight them.

As such, the outcomes from this research signify various promising directions to be explored further. First and foremost, there is a need for investigations in privacy studies within application domains of AI such as healthcare, banking, and social services. Moreover, future research may delve into not only whether different techniques work to protect privacy, but also which types of technologies and organizational approaches are the most effective such as federated learning (Yang et al., 2019), differential privacy (Abadi et al., 2016), and privacy-by-design frameworks (Cavoukian, 2012). Fourth, it is the time for research that combines views of many disciplines (social, ethical, legal, etc.) and considers their connections to technical issues (Tene & Polonetsky, 2013). However, future research should focus on the creation of approaches to back public trust and engagement with AI privacy questions and techniques such as participatory design methods and educational campaigns (Seeber et al., 2020).

7.4 Concluding remarks

This thesis aims to comprehensively map the complicated picture of data privacy in AI development and determine the corresponding challenges, best practices, and opportunities for protecting essential privacy rights. By means of a thorough literary review, empirical analysis, and deep case studies, the thesis has revealed the view of the present day's corporate privacy practices and the performance of the ruling frameworks and techno-social factors that affect the results of privacy in AI.

The research findings illustrate their call for multidimensional solutions which incorporate technical measures, organizational strategies, legal questions, and normative ethics. Although there have been significant advances in data privacy-enhancing technologies and processing standards, several issues, including consent, transparency, fairness, and accountability, remain a concern. Overcoming these obstacles will need to be achieved through the continued partnership between AI developers, legislators, government officials, civil society actors, and stakeholders as well as the public.

The works of this thesis add to the intellection of AI governance and ethics, and they also give pragmatic guidance to corporations and decision-makers on how to operationalize privacy-centered AI systems. Through underlining the role of the proactive management of privacy which is the stakeholders' engagement and interdisciplinary collaboration the findings of the research open a direction to the future in which we can fully realize the benefits of AI technology in a way that respects fundamental human rights and values.

With AI technologies becoming more sophisticated and have begun to dominate all parts of life, the need for powerful privacy regulation can only widen. The essence lies in the ongoing monitoring of privacy risks by the research, practitioners, and policymakers and working up in conjunction with the scenario-specific solutions. Through these practices, we can ensure that the AI's inventive power is unlocked to contribute to the common good, avoiding violating the sacredness and integrity of individuals.

References

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*. Association for Computing Machinery, New York, NY, USA, 308-318. https://doi.org/10.1145/2976749.2978318

Abbas, Z., Sunila Fatima Ahmad, Madiha Haider Syed, Anjum, A., & Rehman, S. (2023). Exploring Deep Federated Learning for the Internet of Things: A GDPR-Compliant Architecture. *IEEE Access*, vol. 12, pp. 10548-10574. https://doi.org/10.1109/access.2023.3344029

Ahmadzai, M., & Nguyen, G. (2023). Federated Learning with Differential Privacy on Personal Opinions: A Privacy-Preserving Approach. *Procedia Computer Science, 225*, 543–552. https://doi.org/10.1016/j.procs.2023.10.039

Ajala, A., Arinze, A., None Onyeka Chrisanctus Ofodile, Okoye, C., & Daraojimba, D. (2024). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. *World Journal of Advanced Engineering Technology and Sciences, 11*(1), 294–300. https://doi.org/10.30574/wjaets.2024.11.1.0060

Mantelero, A. (2022). Beyond Data. In *Beyond Data. Information Technology & Law Series*, *36*, 1–43. T.M.C. ASSER PRESS, The Hague, The Netherlands. https://doi.org/10.1007/978-94-6265-531-7_1

Andreotta, A. J., Kirkham, N., & Rizzi, M. (2022). AI, big data, and the future of consent. *Ai & Society, 37*(4), 1715-1728. https://doi.org/10.1007/s00146-021-01262-5

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements. *Information and Software Technology, 159*, Article 107197. https://doi.org/10.1016/j.infsof.2023.107197

Bankins, S., & Formosa, P. (2023). The Ethical Implications of Artificial Intelligence (AI) For Meaningful Work. *Journal of Business Ethics, 185*(4), 725–740. https://link.springer.com/article/10.1007/s10551-023-05339-7

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *Calif. L. Rev., 104*, 671. https://heinonline.org/HOL/Page?handle=hein.journals/calr104&div=25&g_sent=1&casa_token=&collection=journals

Bellovin, S. M., Dutta, P. K., & Reitinger, N. (2019). Privacy and Synthetic Datasets. *SSRN Electronic Journal*. 671-732. https://doi.org/10.2139/ssrn.3255766

Bouhouita-Guermech, S., Gogognon, P., & Jean-Christophe Bélisle-Pipon. (2023). Specific challenges posed by artificial intelligence in research ethics. *Front Artif Intell, 6*. Article 1149082. https://doi.org/10.3389/frai.2023.1149082

Bourgeois, D., & Bourgeois, D. T. (2014). Data and Databases. In *INFORMATION SYSTEMS FOR BUSINESS AND BEYOND*. Open Textbook Challenge, Saylor Academy, Washington, DC, United States. https://pressbooks.pub/bus206/chapter/chapter-4-data-and-databases/

Brecko, A., Kajati, E., Koziorek, J., & Zolotova, I. (2022). Federated Learning for Edge Computing: A Survey. *Applied Sciences, 12*(18), Article 9124. https://doi.org/10.3390/app12189124

Broekhuizen, T., Dekker, H., de Faria, P., Firk, S., Nguyen, D. K., & Sofka, W. (2023). AI for managing open innovation: Opportunities, challenges, and a research agenda. *Journal of Business Research, 167*, Article 114196. https://doi.org/10.1016/j.jbusres.2023.114196

Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1-12. https://doi.org/10.1177/2053951715622512

Byabazaire, J., O’Hare, G., & Delaney, D. (2020). Data Quality and Trust: Review of Challenges and Opportunities for Data Sharing in IoT. *Electronics, 9*(12),

Article 2083. MDPI. https://doi.org/10.3390/electronics9122083

California Privacy Protection Agency. (2018). *CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Contents*. https://cppa.ca.gov/regulations/pdf/cppa_act.pdf

Calo, R. (2017). Artificial intelligence policy: primer and roadmap. *U.C. Davis Law Review, 51*(2), 399-436. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/davlr51&section=18

Cavoukian, A. (2012). Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*. IGI Global, Hershey PA, United States. (pp. 170–208). https://doi.org/10.4018/978-1-61350-501-4.ch007

Chanda, S. S., & Banerjee, D. N. (2022). Omission and Commission Errors Underlying AI Failures. *AI & SOCIETY*. https://doi.org/10.1007/s00146-022-01585-x

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics, 34*(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Chui, M., Francisco, S., Manyika, J., San, Mehdi, F., Chicago, M., Henke, N., & London. (2018). *NOTES FROM THE AI FRONTIER INSIGHTS FROM HUNDREDS OF USE CASES*. McKinsey Global Institute (MGI). https://www.mckinsey.com/west-coast/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20AI%20frontier%20Applications%20and%20value%20of%20deep%20learning/Notes-from-the-AI-frontier-Insights-from-hundreds-of-use-cases-Discussion-paper.pdf

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review, 25*(2), 123–135. https://doi.org/10.1016/j.clsr.2009.02.002

Cockcroft, S., & Rekker, S. (2015). The relationship between culture and information privacy policy. *Electronic Markets, 26*(1), 55–72. https://doi.org/10.1007/s12525-015-0195-9

Corrales Compagnucci, M., Fenwick, M., Haapio, H., & Vermeulen, E. P. M. (2021). Integrating Law, Technology and Design: Teaching Data Protection & Privacy Law in a Digital Age. *SSRN Electronic Journal, 12*(3). https://doi.org/10.2139/ssrn.3876281

Creswell, J. W. (2017). Mixed Methods Procedures. In *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications Ltd, London, United Kingdom. http://www.ceil-conicet.gov.ar/wp-content/uploads/2015/10/Creswell-Cap-10.pdf

de Laat, P. B. (2021). Companies Committed to Responsible AI: From Principles towards Implementation and Regulation? *Philosophy & Technology, 34*. 1557-1576. https://doi.org/10.1007/s13347-021-00474-3

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM, 59(2), 56–62.* https://doi.org/10.1145/2844110

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion, 99*, Article 101896. https://doi.org/10.1016/j.inffus.2023.101896

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J. S., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary

perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57,* Article 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science, 9*(3–4), 211–407. https://doi.org/10.1561/0400000042

Eccles, R. (2022). *Board Responsibility for Artificial Intelligence Oversight*. The Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2022/01/05/board-responsibility-for-artificial-intelligence-oversight/

El Mestari, S. Z., Lenzini, G., & Demirci, H. (2024). Preserving data privacy in machine learning systems. *Computers & Security, 137*, Article 103605. https://doi.org/10.1016/j.cose.2023.103605

ElBaih, M. (2023). The Role of Privacy Regulations in AI Development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI). *Social Science Research Network.* Article 4589207. https://doi.org/10.2139/ssrn.4589207

EUROPEAN DATA PROTECTION SUPERVISOR. (2024). *Data Protection Officer (DPO) | European Data Protection Supervisor*. Www.edps.europa.eu. https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Farombi, O. & Klaus, H. (2024). Regulatory Compliance and Ethical Considerations: Compliance challenges and opportunities with the integration of Big Data and AI. 1(2), 123-145. https://www.researchgate.net/publication/377330616_Regulatory_Compliance_and_Ethical_Considerations_Compliance_challenges_and_opportunities_with_the_integration_of_Big_Data_and_AI

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards Transparency by Design for Artificial Intelligence. *Science and Engineering*

Ethics, 26(6), 3333–3361. https://doi.org/10.1007/s11948-020-00276-4

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. Article 3518482. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3518482

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *SSRN Electronic Journal, 1*(1). https://doi.org/10.2139/ssrn.3831321

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fountaine, T., McCarthy, B., & Saleh, T. (2019). *Building the AI-Powered Organization*. Harvard Business Review. https://hbr.org/2019/07/building-the-ai-powered-organization

Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. *IEEE Internet Computing, 21*(6), 58–62. https://doi.org/10.1109/mic.2017.4180835

GDPR. (2018). *General data protection regulation (GDPR)*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Gerke, S., Minssen, T., & Cohen, I. G. (2020). Ethical and Legal Challenges of Artificial Intelligence-Driven Health Care. *SSRN Electronic Journal*, Article 3570129, 295–336. https://doi.org/10.2139/ssrn.3570129

Goldfarb, A., & Tucker, C. (2012). Privacy and Innovation. *Innovation Policy and the Economy*, 12, 65–90. https://doi.org/10.1086/663156

Greenleaf, G. (2017). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, including Indonesia and Turkey. *Social Science Research Network, 145,* 10-13. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3000244_code722134.pdf?abstractid=2993035&mirid=1&type=2

Haidar, A. (2023). An Integrative Theoretical Framework for Responsible Artificial *Intelligence. International Journal of Digital Strategy, Governance, and Business Transformation, 13*(1), 1–23. https://doi.org/10.4018/ijdsgbt.334844

He, Y. (2013). Forty Years in Paradox: Post-normalisation Sino-Japanese relations. *China Perspectives, 2013*(4), 7–16. https://doi.org/10.4000/chinaperspectives.6314

Hoffman, R. R., Mueller, S. T., Klein, G., Mohammadreza Jalaeian, & Tate, C. (2023). Explainable AI: roles and stakeholders, desirements and challenges. *Frontiers in Computer Science*, 5. Article 1117848. https://doi.org/10.3389/fcomp.2023.1117848

Hoofnagle, C. J., Sloot, B. V. D., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. tandfonline. https://doi.org/10.1080/13600834.2019.1573501

Igbinenikaro, P., Oladipo, N., & Augustine, E. (2024). FOSTERING CROSS-DISCIPLINARY COLLABORATION IN OFFSHORE PROJECTS: STRATEGIES AND BEST PRACTICES. *International Journal of Management & Entrepreneurship Research, 6*(4), 1176–1189. https://doi.org/10.51594/ijmer.v6i4.1006

Jain, P., Gyanchandani, M., & Khare, N. (2018). Differential privacy: its technological prescriptive using big data. *Journal of Big Data, 5*(1). https://doi.org/10.1186/s40537-018-0124-9

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kaminski, M. E. (2019). The Right to Explanation, Explained. *SSRN Electronic Journal*. U of Colorado Law Legal Studies Research Paper No. 18-24. Berkeley Technology Law Journal, Vol. 34, No. 1. https://doi.org/10.2139/ssrn.3196985

Kaminski, M. E., & Malgieri, G. (2020). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. *International Data Privacy Law, 11*(2), 125–144. https://doi.org/10.1093/idpl/ipaa020

Kaneberg, E. (2020). *Management of cross-functional teams: The impact of motivation and Human Resources on efficiency in Swedish organizations.* Jönköping University. (Dissertation) https://www.diva-portal.org/smash/get/diva2:1434311/FULLTEXT01.pdf

Kaye, D. B. V. (2019). *Speech police.* Columbia Global Reports, New York, United States. https://doi.org/10.2307/j.ctv1fx4h8v

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine, 158*, Article 106848. https://doi.org/10.1016/j.compbiomed.2023.106848

Khan, B., Fatima, H., Qureshi, A., Kumar, S., Hanan, A., Hussain, J., & Abdullah, S. (2023). Drawbacks of Artificial Intelligence and Their Potential Solutions in the Healthcare Sector. *Biomedical Materials & Devices, 1*, 731–738. https://doi.org/10.1007/s44174-023-00063-2

Kiseleva, A., Kotzinos, D., & De Hert, P. (2022). Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations. *Frontiers in Artificial Intelligence, 5.* Article 879603. https://doi.org/10.3389/frai.2022.879603

Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*. https://arxiv.org/pdf/1610.05492

Korpisaari, P. (2019). Finland: A Brief Overview of the GDPR Implementation. *European Data Protection Law Review (EDPL)*, 5, Article 232. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl5&div=38&id=&page=

Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web, 15*(4), 1–42. https://doi.org/10.1145/3466722

Kubler, K. (2016). The Black Box Society: the secret algorithms that control money and information. *Information, Communication & Society, 19*(12), 1727–1728. https://doi.org/10.1080/1369118x.2016.1160142

Laboris, I. (2019). *The impact of the GDPR outside the EU | Lexology*. Www.lexology.com. https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f

Li, W., Yigitcanlar, T., Nili, A., & Browne, W. (2023). Tech Giants' Responsible Innovation and Technology Strategy: An International Policy Review. *Smart Cities, 6*(6), 3454–3492. https://doi.org/10.3390/smartcities6060153

Lonzetta, A., & Hayajneh, T. (2018). Challenges of Complying with Data Protection and Privacy Regulations. *ICST Transactions on Scalable Information Systems*, Article 166352. https://doi.org/10.4108/eai.26-5-2020.166352

Lynskey, O. (2023). Complete and Effective Data Protection. *Current Legal Problems, 76*(1), 297–344. https://doi.org/10.1093/clp/cuad009

Makarius, E. E., Mukherjee, D., Fox, J. D., & Fox, A. K. (2020). Rising with the machines: A sociotechnical framework for bringing artificial intelligence into the organization. *Journal of Business Research, 120*, 262–273. https://doi.org/10.1016/j.jbusres.2020.07.045

Martin, K. (2018). Ethical implications and accountability of algorithms. *Journal of Business Ethics, 160*(4), 835–850. https://doi.org/10.1007/s10551-018-3921-3

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers, 21*(6), 1307–1324. Springer. https://doi.org/10.1007/s10796-019-09974-2

McKendrick, J., & Thurai, A. (2022). *AI Isn't Ready to Make Unsupervised Decisions*. Harvard Business Review. https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions

McMahon, R. B. (2015). Surveillance and Privacy in the Digital Age: A Primer for Public Relations. *Arcadia University. Graduate Theses & Dissertations*. 4. https://scholarworks.arcadia.edu/cgi/viewcontent.cgi?article=1003&context=grad_etd

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM computing surveys (CSUR), 54*(6), 1-35. https://dl.acm.org/doi/pdf/10.1145/3457607

Dennedy, M.F., Fox, J., & Finneran, T. R. (2014). Data and Privacy Governance Concepts. In: The Privacy Engineer's Manifesto. *Apress EBooks*, Berkeley, CA, United States. 51–72. https://doi.org/10.1007/978-1-4302-6356-2_3

Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking responsibly about responsible AI and "the dark side" of AI. *European Journal of Information Systems, 31*(3), 257–268. https://doi.org/10.1080/0960085x.2022.2026621

Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology, 19*(3), 157–175. https://doi.org/10.1007/s10676-017-9426-4

Mohammad Amini, M., Jesus, M., Fanaei Sheikholeslami, D., Alves, P., Hassanzadeh Benam, A., & Hariri, F. (2023). Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the

European GDPR Mandate. *Machine Learning and Knowledge Extraction, 5*(3), 1023–1035. https://doi.org/10.3390/make5030053

Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices. *Science and Engineering Ethics, 26*(4). 2141-2168. https://doi.org/10.1007/s11948-019-00165-5

Mostert, M., Bredenoord, A. L., van der Slootb, B., & van Delden, J. J. M. (2018). From Privacy to Data Protection in the eu: Implications for Big Data Health Research. *European Journal of Health Law, 25*(1), 43–55. https://doi.org/10.1163/15718093-12460346

Nguyet, N. T. N. (2024). *AI and the Laws: Navigating Content & IP Challenges - KPMG Vietnam*. KPMG. https://kpmg.com/vn/en/home/insights/2024/03/ai-and-the-laws.html

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Notario, N., Crespo, A., Martin, Y.-S., Del Alamo, J. M., Metayer, D. L., Antignac, T., Kung, A., Kroener, I., & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. *2015 IEEE Security and Privacy Workshops*. USA. 151-158. https://doi.org/10.1109/spw.2015.22

Nowak, G., & Phelps, J. E. (1992). Understanding privacy concerns. *Journal of Direct Marketing, 6*(4), 28–39. https://doi.org/10.1002/dir.4000060407

O'Neil, C. (2016). *Weapons of Math Destruction: How big data increases inequality and threatens democracy.* Crown Publishers, New York, United States. https://ci.nii.ac.jp/ncid/BB22310261

Office of the Data Protection Ombudsman. (2021). *Data protection*. Tietosuojavaltuutetun Toimisto. https://tietosuoja.fi/en/data-protection

Office of the Privacy Commissioner of Canada. (2011). *Expectations: OPC's Guide to the Privacy Impact Assessment Process*. Www.priv.gc.ca. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

Oswald A. J. Mascarenhas. (2019). *Corporate Ethics for Turbulent Markets*. Emerald Publishing Limited. Howard House, Wagon Lane, Bingley BD16 1WA, UK https://www.emerald.com/insight/publication/doi/10.1108/9781787561915

Perifanis, N.-A., & Kitsios, F. (2023). Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review. *Information, 14*(2). Article 85. MDPI. https://doi.org/10.3390/info14020085

Polonetsky, J., Tene, O., & Jerome, J. W. (2015). Beyond the common rule: ethical structures for data research in Non-Academic settings. *Social Science Research Network, 13.* Article 2621559. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2621559_code1513383.pdf?abstractid=2621559&mirid=2

Raschke, P., Küpper, A., Drozd, O., & Kirrane, S. (2018). Designing a GDPR-Compliant and Usable Privacy Dashboard. *IFIP Advances in Information and Communication Technology(), 526*, 221–236. https://doi.org/10.1007/978-3-319-92925-5_14

Regona, M., Yigitcanlar, T., Xia, B., & Li, R. Y. M. (2022). Opportunities and Adoption Challenges of AI in the Construction Industry: A PRISMA Review. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(1), Article 45. MPDI. https://doi.org/10.3390/joitmc8010045

Reviglio, U., & Agosti, C. (2020). Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media. *Social Media + Society, 6*(2),

Article 205630512091561. https://doi.org/10.1177/2056305120915613

Rhem, A. J. (2023). Ethical use of data in AI Applications. *In S. Ahmed, A. Al Omari, & M. S. Jamil (Eds.), AI Adoption in developed and developing countries* (pp. 55-72). IntechOpen EBooks. https://doi.org/10.5772/intechopen.1001594

Rodrigues, R. (2020). Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities. *Journal of Responsible Technology, 4*, Article 100005. ScienceDirect. https://doi.org/10.1016/j.jrt.2020.100005

Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review, 34*(1), 99–110. https://doi.org/10.1016/j.clsr.2017.05.021

Row, H. (2022). Book Review: Four internets: Data, geopolitics, and the governance of cyberspace. *New Media & Society, 24*(8), 1957–1960. https://doi.org/10.1177/14614448221084061

Rubinstein, I., & Good, N. (2013). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *SSRN Electronic Journal*. Article 2128146. https://doi.org/10.2139/ssrn.2128146

Rustad, M., & Koenig, T. (2019). Article 3, Towards a Global Data Privacy Standard, 71 Fla. *Florida Law Review Florida Law Review, 71*. 365-453. https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1446&context=flr

Sarker, R., Abbass, H., & Newton, C. (2002). Introducing Data Mining and Knowledge Discovery. In *Heuristic and Optimization for Knowledge Discovery* (pp. 1-12). IGI Global. https://doi.org/10.4018/978-1-60566-138-7.ch002

Schwartz, P. M., & Solove, D. J. (2013). Reconciling personal information in the United States and European Union. *Social Science Research Network.* Article 2271442. https://doi.org/10.2139/ssrn.2271442

ScienceDirect. (n.d.). *Privacy Impact Assessment - an overview | ScienceDirect Topics*. Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/privacy-impact-assessment

Seeber, I., Bittner, E., Briggs, R. O., de Vreede, T., de Vreede, G.-J., Elkins, A., Maier, R., Merz, A. B., Oeste-Reiß, S., Randrup, N., Schwabe, G., & Söllner, M. (2020). Machines as teammates: A research agenda on AI in team collaboration. *Information & Management, 57*(2), Article 103174. https://doi.org/10.1016/j.im.2019.103174

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security, 120*, Article 102774. https://doi.org/10.1016/j.cose.2022.102774

Singh, P. (2023). Systematic review of data-centric approaches in artificial intelligence and machine learning. *Data Science and Management, 6*(3), 144-157. https://doi.org/10.1016/j.dsm.2023.06.001

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903. https://www.jstor.org/stable/23415060

Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). Ethics of Artificial Intelligence. In *Ethics of Artificial Intelligence in Research and Innovation* (pp. 1-24). Springer International Publishing. https://doi.org/10.1007/978-3-031-17040-9_1

Tabassi, E. (2023). AI Risk Management Framework. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. https://doi.org/10.6028/nist.ai.100-1

Tableau. (n.d.). *Data Management vs. Data Governance: The Difference Explained*. Tableau. https://www.tableau.com/learn/articles/data-management-vs-data-governance

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature, 556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), Article 239. https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), Article 20180083. https://doi.org/10.1098/rsta.2018.0083

Vemou, K., & Karyda, M. (2020). Evaluating privacy impact assessment methods: guidelines and best practice. *Information & Computer Security, 28*(1), pp. 35-53. https://doi.org/10.1108/ics-04-2019-0047

Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics, 12*(18), Article 3786. https://doi.org/10.3390/electronics12183786

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160

Williamson, S. M., & Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven *Healthcare. Applied Sciences, 14*(2), Article 675. https://doi.org/10.3390/app14020675

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial Intelligence and the Public Sector—Applications and Challenges. *International Journal of Public Administration, 42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103

Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., Honaker, J., Nissim, K., O'Brien, D., Steinke, T., & Vadhan, S. (2018). Differential Privacy: A Primer for a Non-Technical Audience. *SSRN Electronic Journal.* 21(1), 209-276. https://doi.org/10.2139/ssrn.3338027

Wulf, A. J., & Seizov, O. (2022). "Please understand we cannot provide further information": evaluating content and transparency of GDPR-mandated AI disclosures. *AI & SOCIETY, 39*(1), 235–256. https://doi.org/10.1007/s00146-022-01424-z

Xia, Q., Ye, W., Tao, Z., Wu, J., & Li, Q. (2021). A Survey of Federated Learning for Edge Computing: Research Problems and Solutions. *High-Confidence Computing*, Article 100008. https://doi.org/10.1016/j.hcc.2021.100008

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated Machine Learning. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19. https://doi.org/10.1145/3298981

Yao, A. C. (1986). How to generate and exchange secrets. *Proceedings of the 27th Annual Symposium on Foundations of Computer Science, (sfcs 1986).* Toronto, ON, Canada, 1986, pp. 162-167. https://doi.org/10.1109/sfcs.1986.25

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications. CA. https://www.perlego.com/book/3842459/case-study-research-and-applications-design-and-methods-pdf

Zamiri, M., & Esmaeili, A. (2024). Methods and Technologies for Supporting Knowledge Sharing within Learning Communities: A Systematic Literature Review.

Administrative Sciences, 14(1), Article 17. https://www.mdpi.com/2076-3387/14/1/17

Zarsky, T. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Science, Technology, & Human Values, 41*(1), 118–132. https://doi.org/10.1177/0162243915605575

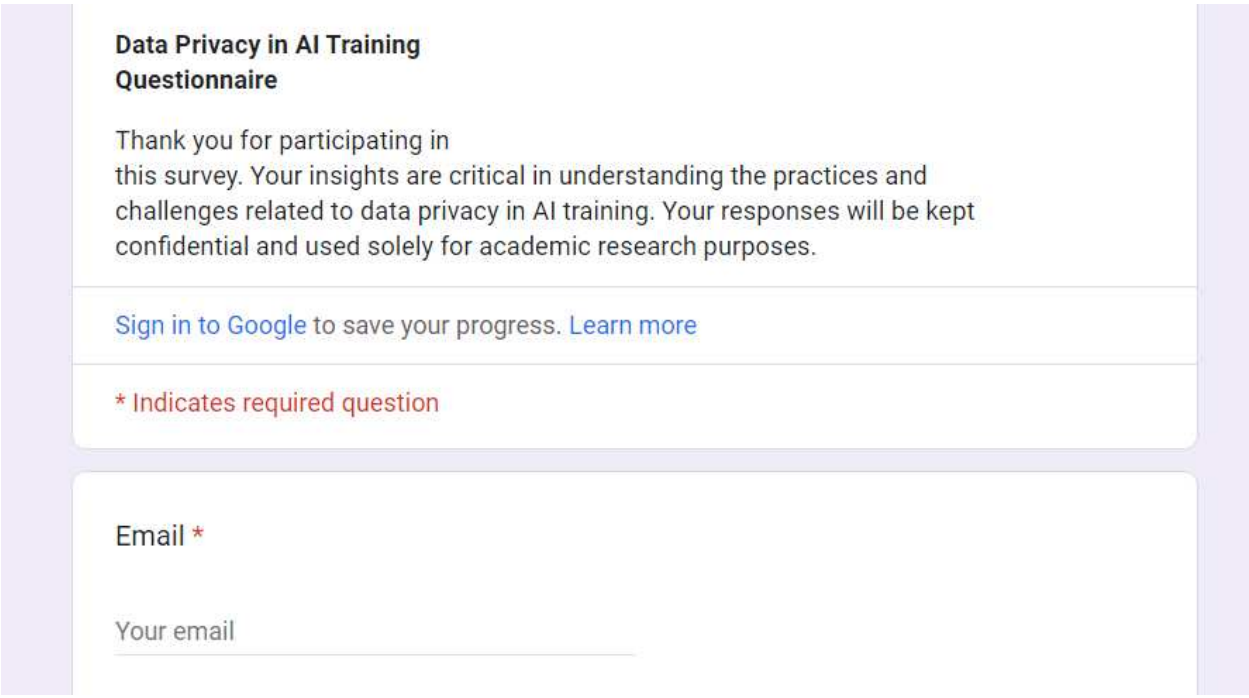
Zhu, L. (2011). Privacy in context: technology, policy, and the integrity of social life. *Journal of Information Privacy and Security, 7*(3), 67–71. https://doi.org/10.1080/15536548.2011.10855919

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power.* PublicAffairs, New York, United States. https://cds.cern.ch/record/2655106

Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory, 3*(4), 1-21. https://doi.org/10.1177/26317877221129290

Appendices

Appendix 1. Data Privacy in AI Training Questionnaire



Data Privacy in AI Training Questionnaire

Thank you for participating in this survey. Your insights are critical in understanding the practices and challenges related to data privacy in AI training. Your responses will be kept confidential and used solely for academic research purposes.

Sign in to Google to save your progress. Learn more

* Indicates required question

Email *

Your email

Section 1: Background Information

What is your role within the organization?

- ◯ • Data Scientist / AI Engineer
- ◯ • Compliance Officer / Legal Counsel
- ◯ • Executive / Manager
- ◯ • IT / Cybersecurity Specialist
- ◯ • Other (Please specify): _____

Which industry does your organization operate in?

- ◯ • Technology
- ◯ • Finance
- ◯ • Healthcare
- ◯ • Retail
- ◯ • Other (Please specify): _____

What is the size of your company?

- ◯ • Micro (0-9 employees)
- ◯ • Small (10-50 employees)
- ◯ • Medium (51-200 employees)
- ◯ • Large (201+ employees)

Where are your company's operations located geographically?

- ◯ • North America
- ◯ • Europe
- ◯ • Asia
- ◯ • Other (Please specify): _____

Section 2: Data Collection Practices

What consent mechanism does your organization use for data collection in AI training?

- ◯ • Opt-in
- ◯ • Opt-out
- ◯ • Implicit consent
- ◯ • No consent required
- ◯ • Not sure / Not applicable

What is the primary source of the training data your organization uses?

- ◯ • User-generated content
- ◯ • Third-party data providers
- ◯ • Public datasets
- ◯ • Other (Please specify): _____

How often is your organization's privacy policy updated?

- ◯ • Annually
- ◯ • Bi-annually
- ◯ • After any significant data practice change
- ◯ • Never
- ◯ • Not sure

Section 3: Data Handling and Usage

Which methods of anonymizing data does your organization employ? (Select all that apply)

- [ ] • Data masking
- [ ] • Pseudonymization
- [ ] • Encryption
- [ ] • Differential privacy
- [ ] • Not applicable / No anonymization

Could you describe the main challenges your organization faces in anonymizing data for AI training?

Your answer

On a scale from 1 (Not transparent) to 5 (Highly transparent), how would you rate the transparency of your organization's data usage in AI systems?

1	2	3	4	5
○	○	○	○	○

Has there been any incident of data misuse within your organization?

- ○ • Yes
- ○ • No
- ○ • If Yes, please provide a brief description of the incident(s):

Section 4: Compliance and Regulation

How would you describe your organization's understanding of data privacy regulations relevant to AI?

- ○ • Very knowledgeable
- ○ • Somewhat knowledgeable
- ○ • Slightly knowledgeable
- ○ • Not knowledgeable

On a scale from 1 (Not difficult) to 5 (Very difficult), rate the difficulty your organization faces in achieving compliance with data privacy regulations.

1	2	3	4	5
○	○	○	○	○

How have data privacy regulations impacted AI development within your organization?

Your answer

Section 5: Privacy Enhancements and Recommendations

Does your organization use Privacy-Enhancing Technologies (PETs) in AI training?

- ◯ • Currently using PETs
- ◯ • Planning to use PETs
- ◯ • No plans to use PETs
- ◯ • Not sure

If you are using PETs, how effective have they been in protecting data privacy?

- ◯ • Very effective
- ◯ • Somewhat effective
- ◯ • Not very effective
- ◯ • Not effective at all
- ◯ • Not sure / Not applicable

Please share any recommendations or best practices for enhancing data privacy in AI training.

Your answer

Submit

Clear form