Balancing Privacy, Trust and Innovation in Autonomous Vehicles:
A Study in the Portuguese Context

Diana Rodrigues

Dissertation written under the supervision of professor

Rosa Fioravante

Dissertation submitted in partial fulfilment of requirements for the MSc in International Management with specialization in strategy and consulting, at the Universidade Católica Portuguesa, January 2025.

Abstract

This thesis explores the interplay between General Data Protection Regulation (GDPR) compliance, privacy concerns, and trust in the context of autonomous vehicles (AVs) in Portugal. It examines how GDPR awareness, transparency, and privacy-by-design principles influence consumer perceptions and their willingness to trade privacy for enhanced safety and functionality. Employing a quantitative research approach, the study surveyed Portuguese residents to assess GDPR awareness, privacy concerns, and trust in data handling by AV companies.

The findings reveal that while GDPR awareness fosters trust, it paradoxically heightens privacy concerns, underscoring the ambivalence of transparency. High support for privacy-by-design principles demonstrates a consumer preference for integrating proactive privacy safeguards directly into AV systems. Furthermore, regional, and demographic analyses highlight disparities in trust and GDPR awareness, pointing to the need for tailored educational campaigns and transparency mechanisms.

By addressing these dynamics, the research suggests actionable insights for AV manufacturers, policymakers, and regulators seeking to balance innovation, compliance, and consumer trust. It emphasizes the potential of strategic privacy integration to enhance consumer confidence, balancing ethical adoption of AV technologies with needs of market expansion.

Title: Balancing Privacy, Trust, and Innovation in Autonomous Vehicles: A study in the Portuguese context

Author: Diana Alexandra Valente Rodrigues

Keywords: GDPR, autonomous vehicles, data privacy, trust, transparency, privacy-by-design, Portugal, digital innovation

Resumo

Esta tese explora a interação entre a conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD), as preocupações com a privacidade e a confiança no contexto dos veículos autónomos (AVs) em Portugal. Examina a forma como a sensibilização para o RGPD, a transparência e os princípios de privacidade desde a conceção influenciam as perceções dos consumidores e a sua vontade de trocar a privacidade por maior segurança e funcionalidade. Empregando uma abordagem de investigação quantitativa, o estudo inquiriu os residentes portugueses para avaliar a sensibilização para o RGPD, as preocupações com a privacidade e a confiança no tratamento de dados pelas empresas de AV.

Os resultados revelam que, embora o conhecimento do RGPD promova a confiança, paradoxalmente aumenta as preocupações com a privacidade, sublinhando a ambivalência da transparência. O elevado apoio aos princípios de privacidade desde a conceção demonstra uma preferência dos consumidores pela integração de salvaguardas proactivas da privacidade diretamente nos sistemas AV. Além disso, as análises regionais e demográficas destacam disparidades na confiança e na sensibilização para o RGPD, apontando para a necessidade de campanhas educativas e mecanismos de transparência adaptados.

Ao abordar estas dinâmicas, a investigação sugere ideias acionáveis para os fabricantes de AV, decisores políticos e reguladores que procuram equilibrar a inovação, a conformidade e a confiança dos consumidores. Salienta o potencial da integração estratégica da privacidade para aumentar a confiança dos consumidores, equilibrando a adoção ética de tecnologias AV com as necessidades de expansão do mercado.

Título: Equilíbrio entre privacidade, confiança e inovação em veículos autónomos: Um estudo no Contexto Português

Autor: Diana Alexandra Valente Rodrigues

Palavras-chave: RGPD, veículos autónomos, privacidade de dados, confiança, transparência, privacy-by-design, Portugal, inovação digital

Acknowledgments

I want to take this opportunity to thank all the amazing people who made all this possible by supporting and encouraging me along the way.

First and for most, I would like to express my profound gratitude to my parents, grandparents and sister, whose relentless love, encouragement, and sacrifice laid the foundation for what I have achieved, and for all the effort and hard work they put into my education. Your belief in me has been my greatest source of strength and motivation.

I am grateful to my friends and colleagues for their continuous support and understanding through the ups and downs that have marked this journey. Your acts of kindness and friendship have been important in maintaining my feet on the ground and keeping me focused while still supporting me all the way.

I would also take this opportunity to thank my advisor, whose help and advice have fundamentally shaped this dissertation. My heartfelt appreciation for all the important insights and constant encouragement that have helped me in this research work indeed, not to mention all the much-needed patience and encouragement afforded me during the execution period.

Lastly, I would like to acknowledge myself. This dissertation represents countless hours of hard work, resilience, and determination. I am proud of the commitment I have put into making this project a reality. I want to thank myself for believing in me, hanging in there when it got tough, and pushing for greatness at every turn.

Table of Contents

1.Introduction

Problem Statement

The rapid evolution of autonomous vehicle (AV) technologies presents numerous challenges, particularly concerning data privacy and adherence to stringent regulatory frameworks such as the General Data Protection Regulation (GDPR) (He Li et al., 2019). These vehicles rely heavily on extensive real-time data collection, including geolocation, behavioural patterns, and environmental inputs, to ensure functionality and safety (Cichy et al., 2021). While this reliance facilitates innovative and personalized solutions, it also raises significant concerns about data misuse, trust, and transparency, as emphasized by Pierides & Zyphur (2019) and Berente et al. (2021).

Under the GDPR, companies are required to implement robust data protection measures, including consent mechanisms, data minimization, and transparency (GDPR Articles 5 and 12). This forces firms to balance innovation with compliance, particularly in the automotive sector, where trust plays a crucial role in the adoption of new technologies (Goddard, 2017; He Li et al., 2019). However, while transparency is seen by consumers as a means to build trust, it also generates anxiety about potential data misuse, complicating efforts to establish confidence in AV systems (Pierides & Zyphur, 2019). Moreover, the ethical implications of AI-driven data collection highlight the necessity for proactive frameworks such as Privacy-by-Design (PbD), which integrate privacy protections directly into system architectures (Cavoukian, 2009; Felzmann et al., 2020).

In Portugal, the adoption of AVs offers a unique opportunity to explore the interaction between regulatory compliance, consumer trust, and functional innovation within a specific sociocultural and regulatory context. Portugal's strong alignment with GDPR standards, along with its active involvement in EU digital transformation initiatives—such as leadership in Smart Cities and IoT-based mobility projects—makes it an exemplary case study for understanding how companies can navigate these challenges in the AV sector (European Commission, 2021; Martinez & Viegas, 2017).

Academic and Practical Relevance

The interplay between privacy, transparency, and trust in AVs has been explored through multiple academic perspectives:

Regulatory Compliance: Scholars like Wu & van Rooij (2021) discuss how complicated it is to navigate through different regulatory frameworks that overlap and stress that an ethical approach, beyond compliance, is what helps in building trust among consumers. Similarly, He Li et al. (2019) discuss challenges related to compliance with the GDPR and building trust.

Privacy Innovations: Privacy-by-Design (PbD) is one proactive framework that embeds privacy protection directly into technological systems. Works such as Felzmann et al. (2020) have pointed out that perceived risks compared to benefits significantly affect the adoption of technologies, especially in privacy-sensitive contexts such as AVs.

Behavioural and Ethical Perspectives: Sarathy & Robertson (2003) raise ethical concerns about data privacy issues in digital technologies and appeal for an interdisciplinary solution entailing legal, technological, and consumer-centric approaches. Besides that, Cichy et al. (2021) investigate ethical challenges related to IoT and AV systems.

However, the debate is still open on how to apply, among others, **Privacy-by-Design (PbD)** principles, which may be suitably operationalized within AV systems (Cavoukian, 2009; Bu, Wang, Jiang, & Liang, 2020). Furthermore, the function of transparency in balancing privacy concerns and trust from consumers (Felzmann et al., 2020; Pierides & Zyphur, 2019; Cichy, Salge, & Kohli, 2021) calls for further research with respect to how consumers perform trade-offs between privacy and functionality (Adjerid, Peer, & Acquisti, 2018; Sarathy & Robertson, 2003).

To contribute to the above mentioned still open debate, this thesis investigates consumers' perceptions of GDPR compliance, privacy concerns, and transparency in Avs. It does so by asking the following research question: How do Portuguese consumers perceive GDPR compliance, privacy, and transparency in autonomous vehicles? As such knowledge is critical for companies aiming to balance ethical privacy concerns and the goal of AV market expansion (Bélanger & Crossler, 2011; Cichy, Salge, & Kohli, 2021; Felzmann et al., 2020). This study aims to addressing the above mentioned RQ through a set of sub-questions:

1. **GDPR Awareness and Trust**:
    - To what extent are respondents aware of GDPR principles and does this awareness influence user trust in the data handling practices of autonomous vehicle companies?
2. **Trust in data handling by AV companies**:
    - How does awareness of GDPR guidelines and concerns about privacy risks influence Portuguese users' trust in data handling by autonomous vehicle companies?
3. **Privacy concerns**:
    - How does GDPR awareness influence users' perceptions of privacy risks associated with autonomous vehicle data practices?
4. **Trade-offs Between Privacy and Enhanced Features (such as safety and functionality)**:
    - How willing are users to exchange certain aspects of privacy for enhanced features, such as enhanced safety or better functionality?
5. **Integration of Privacy-by-Design (PbD)**:
    - How do users feel about the integration of privacy-by-design principles in autonomous vehicle technology?

For the purpose of this study, the Portuguese context is chosen as a suitable empirical setting. Portugal is one of the leading countries in digital transformation and compliance with GDPR regulations, making it a perfect case to research these issues. The country has actively integrated AI, IoT, and data governance mechanisms, aligning with EU initiatives like Horizon 2020 to foster innovation while ensuring privacy (European Commission, 2021). Regional discrepancies, such as higher digital literacy in urban areas compared to rural regions, show us how cultural and socioeconomic factors influence consumer attitudes toward AV technology (Martinez & Viegas, 2017). This context provides a promising model for understanding the privacy challenges associated with AVs and demonstrates how companies can leverage GDPR compliance as a competitive advantage. While this research focuses on Portuguese respondents, the results are derived from a limited survey sample and are therefore not generalizable to the broader Portuguese population or other regions.

To answer to the RQ, a quantitative methodology is deployed in the analysis of results of a survey conducted with Portuguese potential users of AV technology. Descriptive statistics and

simple regression analyses were performed to assess the relationships between GDPR awareness, trust, and privacy concerns. These methods are informed by frameworks from Bélanger & Crossler (2011), which emphasize privacy concerns in information systems, and Pavlou (2011), which examines trust in technology adoption. The study integrates Cavoukian's (2009) PbD framework, Pierides & Zyphur's (2019) transparency-trust models, and behavioural decision-making theories by Adjerid et al. (2018) to examine the complex dynamics of privacy in AVs.

Results from this study acknowledge that Portuguese consumers generally exhibit a willingness to trade privacy protections for enhanced safety and functionality, driven by a behavioural tendency to prioritize immediate benefits over abstract risks. Urban residents strongly support Privacy-by-Design principles, emphasizing the need to embed privacy safeguards into AV systems. Regional disparities show that urban areas like Lisbon and Algarve demonstrate higher GDPR awareness and trust compared to rural areas such as Alentejo. Additionally, demographic differences reveal that younger consumers favour privacy-preserving technologies, whereas older consumers prioritize tangible benefits like improved safety.

Structure of the Thesis

The structure of this thesis is organized into six chapters to provide a comprehensive exploration of the research topic. **Chapter 1** introduces the study by outlining the problem statement, research questions, and the overall relevance of the study, setting the stage for a deeper investigation. **Chapter 2** delves into the theoretical framework, exploring key concepts such as the GDPR, Privacy-by-Design (PbD), and transparency-trust models to establish the foundation for the research. **Chapter 3** details the methodology, explaining the quantitative approach employed for data collection and analysis. **Chapter 4** presents the findings, focusing particularly on regional differences in Portugal and consumer attitudes toward PbD principles. **Chapter 5** interprets these findings considering existing literature, discussing their implications for both academic knowledge and practical applications. Finally, **Chapter 6** concludes the thesis by summarizing the key insights, discussing limitations, and offering recommendations for future research and industry practices. Together, these chapters provide a coherent and structured exploration of how companies can balance privacy, transparency, and functionality to build trust in autonomous vehicles within the Portuguese context.

2.Theoretical Background

GDPR and Business Ethical Obligations

The General Data Protection Regulation (GDPR), introduced by the European Union in 2018, is considered a landmark in data privacy regulation. It seeks to protect the personal data of EU citizens by enforcing strict obligations on how businesses collect, store, and process this information (Goddard, 2017). One of the most defining features of the General Data Protection Regulation (GDPR) is its extraterritorial application, as articulated in Article 3. This provision ensures that GDPR applies to any organization processing the personal data of EU citizens, irrespective of where the organization is based. This global reach is a key element of the GDPR's framework, which seeks to harmonize data protection standards while reinforcing the sovereignty of EU citizens over their data. The regulation mandates transparency, informed consent, data minimization, and robust data subject rights, such as the right to data portability and the right to be forgotten, as outlined in Articles 12–23. These principles, supported by European Commission guidelines, emphasize the importance of empowering individuals in the digital age while fostering accountability among organizations (European Commission, 2021). This comprehensive regulatory approach not only safeguards personal data but also serves as a benchmark for global data protection laws, aligning with the EU's ambition to set international standards for privacy and data governance.

Key principles of data management, such as data minimization—collecting only necessary data—and transparency—informing individuals about data collection and processing—are foundational to addressing privacy concerns as highlighted by Bélanger and Crossler (2011). These principles align with later regulatory frameworks like the GDPR, which formalized such practices. Another vital principle is accountability, requiring companies to demonstrate compliance with GDPR rules and maintain documentation of their data protection practices (Li, Yu & He, 2019).

For businesses, this means establishing processes that comply with the regulation's consent requirements, ensuring personal data is only processed for specified purposes, and keeping clear records of how personal data is handled. The implementation of GDPR has heightened public concerns around data privacy, which is a significant issue for firms in the autonomous vehicle industry that rely on real-time data processing. Public perceptions of privacy risks, as discussed by Kohl et al. (2018), play a crucial role in shaping acceptance of emerging technologies like self-driving cars.

Additionally, Bulgurcu, Cavusoglu, and Benbasat (2010) show that by employing the rational-choice theory leads to a better understanding of compliance behaviors in organizations. Their framework suggests that employees and organizations analyse the costs and benefits of compliance behaviors, aligning their actions with perceived advantages such as avoiding penalties or fostering trust. While their research focuses on information security policy, its principles provide a valuable perspective on how businesses approach compliance with regulatory frameworks like GDPR. This understanding recalls the idea that awareness of regulatory obligations can motivate compliance behaviors that align with ethical and legal standards.

Beyond regulatory compliance, companies face ethical obligations to address privacy concerns and ensure individual autonomy, which includes allowing individuals control over their data, as highlighted by Bélanger and Crossler (2011). Their emphasis on the importance of privacy underscores the ethical imperative of managing personal data responsibly. Trust is another essential element. Culnan (1993) emphasizes the critical role of trust in how personal data is handled, noting that consumer privacy concerns arise when secondary data use lacks transparency or control. These principles are highly relevant to data-driven industries like autonomous vehicles, where breaches or misuse of sensitive information could lead to significant reputational damage and undermine consumer trust.

Ethical considerations in data privacy also extend to the principle of non-maleficence, which requires companies to ensure that their use of personal data does not harm individuals. While Sarathy & Robertson (2003) do not explicitly reference non-maleficence, their emphasis on ethical frameworks highlights the need for businesses to avoid practices, such as unauthorized data sharing or insufficient safeguards against breaches, that could harm individuals and erode trust. Wu & van Rooij (2021) further emphasize the importance of navigating complex regulatory landscapes, highlighting how businesses adapt to overlapping legal and ethical norms. In this context, ensuring the security and responsible use of personal data becomes a core ethical responsibility for companies as they navigate compliance with privacy laws.

Son & Kim (2008) emphasize the importance of understanding individuals' privacy concerns and their responses to data management practices, highlighting how perceptions of fairness and trust influence behaviours. Building on this, businesses must not only comply with regulations like GDPR but also integrate ethical principles of autonomy, security, and fairness into their data protection strategies.

Data Privacy and Self-Driving Cars

Problems with Data Privacy in Self-Driving Cars and the Debate

Self-driving cars, or autonomous vehicles (AVs), pose unique challenges to data privacy due to the vast amounts of real-time data they collect, process, and share. AVs rely on numerous sensors, cameras, and GPS systems to navigate safely and effectively, collecting sensitive personal data such as geolocation, driving patterns, and even biometric information (Felzmann et al., 2020). This constant stream of data is vital for ensuring the safety of AV operations but presents significant privacy concerns, particularly under GDPR, which emphasizes data minimization and purpose limitation (Li, Yu & He, 2019).

Public perceptions of privacy risks are a significant concern for the adoption of autonomous vehicles (Kohl et al., 2018). The potential for granular and sensitive data collection, including real-time tracking of individuals' movements, amplifies these concerns, highlighting the need for stringent safeguards to prevent misuse and unauthorized access. While this data is crucial for the operational safety of AVs, its collection must be carefully managed to avoid infringing on privacy rights.

Another significant issue is the transparency of data processing. As AVs become integrated into broader transportation systems, the data they collect may be shared with third parties such as insurance companies, advertising platforms, or government agencies. However, the complexity of these data ecosystems makes it difficult for users to understand how their data is being used and with whom it is being shared (Cichy, Salge, & Kohli, 2021). Despite GDPR's requirements for transparency, many users remain unaware of the full extent of data sharing in autonomous vehicle systems. This reflects broader challenges in how businesses navigate and comply with multifaceted legal frameworks, as Wu & van Rooij (2021) highlight the dynamic and situational nature of compliance in responding to complex regulations.

In addition to concerns about data privacy and transparency, cybersecurity presents a critical challenge. Autonomous vehicles (AVs), as interconnected systems, rely on continuous data communication with infrastructure, other vehicles, and cloud services, exposing them to risks such as data breaches or system manipulation. Felzmann et al. (2020) emphasize the importance of proactive, transparent design frameworks in automated systems to address such vulnerabilities, fostering trust and accountability while mitigating risks associated with their operation. A successful cyberattack could result in unauthorized access to personal data or even

control over the vehicle itself, presenting significant risks to privacy and safety (Cichy, Salge, & Kohli, 2021).

Overall, the debate around data privacy in self-driving cars is far from settled. While frameworks like GDPR provide robust guidelines for protecting personal data, the operational demands of autonomous vehicles (AVs)—such as real-time data processing—often create tension with strict privacy requirements. Bu et al. (2020) emphasize the importance of "Privacy by Design" (PbD) as a framework that integrates privacy considerations throughout the lifecycle of information systems, which aligns with the development of AVs. Although not directly addressing PETs, their study underscores the role of proactive privacy strategies in mitigating privacy risks while maintaining functionality. By combining PbD with privacy-enhancing technologies (PETs) such as anonymization and encryption, the industry can address these challenges without compromising operational efficiency, advancing both compliance and innovation in autonomous driving.

Proposed Solutions to Data Privacy in Autonomous Vehicles

The complexity of data privacy in autonomous vehicles (AVs) has driven various scholars to propose solutions, each offering unique mechanisms to protect user data without undermining the vehicles' operational needs. Key proposals include Privacy by Design (PbD), Privacy-Enhancing Technologies (PETs), and ethical and legal frameworks, all contributing to the balancing act between AV functionality and robust data protection.

Privacy by Design (PbD)

PbD advocates integrating privacy at every stage of a system's lifecycle, ensuring that privacy protections are proactively included in the design process rather than being added as an afterthought (Bu et al., 2020). Sarathy & Robertson (2003) emphasize the importance of proactive and ethical approaches to managing data privacy, which aligns with the principles of Privacy by Design (PbD) and the GDPR's emphasis on data minimization and transparency. By embedding privacy protocols into AV architectures, firms can address real-time data flow requirements essential for AV functionality, while fostering user trust and maintaining compliance with emerging privacy regulations.

Privacy-Enhancing Technologies (PETs)

PETs represent another significant solution, focusing on tools like encryption and anonymization to safeguard data at specific stages, primarily during storage and transmission. Kohl et al. (2018) emphasizes the importance of addressing public concerns about data security and privacy in autonomous vehicle systems, suggesting that measures such as encryption could mitigate fears of unauthorized data access during transit. Similarly, anonymization is a critical technique for addressing privacy concerns in AI systems by reducing risks associated with the exposure of personal data. Felzmann et al. (2020) discuss the importance of ensuring transparency in how data is processed and highlight that effective management of data risks, including anonymization and transparency measures, is key to fostering trust and accountability in automated decision-making systems.However, PETs function primarily as isolated safeguards and lack the system-wide integration of PbD, which applies privacy controls throughout the entire AV data lifecycle, providing a holistic framework for AV manufacturers.

Ethical and Legal Frameworks

In addition to technical frameworks, ethical and legal frameworks provide foundational guidelines for data privacy in emerging technologies. As noted by Santanen (2019), ethical frameworks emphasize user trust, transparency, and accountability, urging firms to prioritize user rights beyond regulatory obligations. While Santanen focuses on technological innovation in general, these principles are highly relevant to Autonomous Vehicles (AVs), where privacy is critical to fostering consumer confidence. Key ethical principles, such as transparency and accountability, underpin the moral imperative to safeguard user data against misuse. The GDPR enforces obligations like data minimization, informed consent, and transparency, aligning legal mandates with the ethical goal of respecting individual autonomy and preventing harm (Goddard, 2017).

Why Privacy by Design Stands Out

Among these approaches, Privacy by Design emerges as the most comprehensive solution. Unlike PETs, which address specific data security phases, or ethical frameworks that rely on voluntary adherence, PbD provides an integrated approach, embedding privacy protections into every layer of the AV system. This holistic structure ensures consistent privacy safeguarding across all data processing stages, proactively managing risks while maintaining AV efficiency. Thus, while PETs and ethical frameworks contribute valuable insights, PbD remains the most

encompassing framework, positioning it as the optimal choice for AV manufacturers aiming to meet regulatory standards and foster consumer trust.

Ethical Dilemma

Sarathy & Robertson (2003) highlight the ethical conflicts businesses face, particularly when profit motives clash with obligations to protect individual privacy and societal welfare. These challenges align with broader ethical dilemmas discussed by Felzmann et al. (2020), where decision-makers in automated systems must balance competing principles, such as the demands for transparency and accountability against the need for innovation and operational efficiency. In the context of autonomous vehicles, this dilemma extends to protecting consumer privacy while fostering technological advancement.

For companies in the autonomous vehicle sector, this dilemma is particularly acute. On the one hand, AVs require vast amounts of real-time data to function safely and efficiently, while on the other hand, GDPR mandates that personal data collection be minimized and that individuals have control over how their data is used (Li, Yu & He, 2019). This creates a conflict between the need to collect data for vehicle functionality and the ethical responsibility to protect individual privacy.

Ethical dilemmas are crucial for companies because they affect both consumer trust and business reputation. Companies that fail to address ethical concerns, such as privacy violations, risk damaging their relationships with consumers and facing regulatory penalties. Culnan (1993) highlights that consumer confidence is strongly tied to the responsible handling of personal data, particularly when transparency and control are ensured. These insights underscore the importance of ethical data practices in industries like autonomous vehicles, where trust is crucial for gaining a competitive market advantage.

This research tackles the central ethical dilemma in autonomous vehicles, exploring how firms can balance GDPR compliance with the need for data to enhance vehicle functionality. Felzmann et al. (2020) and Cichy et al. (2021) emphasize that trust in AVs is contingent on responsible data handling, yet little is known about how GDPR awareness influences this trust. The research question guiding this study is: *How do Portuguese consumers perceive GDPR compliance, privacy, and transparency in autonomous vehicles, and how can companies balance these factors with functionality to build trust and gain a competitive edge?*, which aims to address these gaps by providing empirical evidence within the Portuguese context.

This question addresses the ethical tension between data use and privacy protection, aiming to offer insights that align with both regulatory obligations and consumer trust.

To go a little deeper, the current research encompasses five sub questions, each of them addressed to a particular gap that exists within literature:

Sub-Question 1: *To what extent are respondents aware of GDPR principles and does this awareness influence user trust in the data handling practices of autonomous vehicle companies?*

Indeed, a number of scholars such as Goddard (2017) and Bélanger and Crossler (2011) have studied these topics in detail and highlighted the importance of the GDPR to boost transparency and accountability. However, on the particular case of trust in firms operating AVs, there is limited empirical evidence so far. There is a lack of understanding of how the increased awareness about the GDPR would improve trust, hence remains one major gap.

Sub-Question 2: *How does awareness of GDPR guidelines and concerns about privacy risks influence Portuguese users' trust in data handling by autonomous vehicle companies?*

Pierides and Zyphur (2019) argue that while transparency—one of GDPR's central principles—can build trust, it may also paradoxically amplify privacy concerns. This anomaly has not been tested in an empirical sense in the AV industry, much less with a specific focus on Portugal, which has a jurisdiction where GDPR compliance issues form part of its regulatory focus.

Sub-Question 3: *How does GDPR awareness influence Portuguese users' perceptions of privacy risks associated with autonomous vehicle data practices?*

Privacy concerns are recognized as a significant barrier to technology adoption (Sarathy & Robertson, 2003), particularly in data-intensive systems like AVs. However, there is very limited understanding regarding the nature of these concerns when one is more informed about the General Data Protection Regulation. This study covers that gap by exploring how a better understanding of key provisions in the GDPR may make people more anxious or ease their privacy concerns.

Sub-Question 4: *How willing are users to exchange certain aspects of privacy for enhanced features, such as enhanced safety or better functionality?*

The "privacy paradox" (Adjerid, Peer, & Acquisti, 2018) describes a situation where individuals value privacy yet willingly trade it for immediate benefits like safety or convenience. Although this paradox has been studied in other contexts, there is a lack of empirical research on the privacy-safety trade-off specific to AV technologies. This survey question explores how Portuguese consumers weigh both options of privacy against enhanced functions for AVs.

Sub-Question 5: *How do users feel about the integration of privacy-by-design principles in autonomous vehicle technology?*

Cavoukian (2009) supported PbD as a proactive way of addressing privacy risks. While PbD is conceptually sound, there is scarce empirical evidence regarding user acceptance and perceived importance of PbD in AV technologies. This paper investigates whether Portuguese users consider PbD integration to be an effective solution for enhancing trust and reducing privacy concerns.

The systematic examination of the above sub-questions helps this study fulfil some of the literature gaps. The present research is not only going to develop the empirical insights on the relationship between the awareness about the GDPR, concerns about privacy, and trust but also is going to examine what kind of trade-offs the users will make and attitudes the users show toward the measure for protection of privacy, such as PbD. It leads to a better understanding of the data privacy issues related to AV systems with the under-researched perspective of a Portuguese context.

Why focusing on the Portuguese market

Portugal presents a unique context for examining the deployment of autonomous vehicles, particularly through its Smart City initiatives that integrate sustainable urban mobility solutions. As Martinez & Viegas (2017) highlighted, Lisbon's adoption of shared autonomous mobility systems demonstrates the potential for improving efficiency and reducing emissions in urban contexts. GDPR enforcement across EU member states, including by national data protection

authorities like Portugal's Comissão Nacional de Proteção de Dados (CNPD), creates a rigorous compliance landscape for industries handling sensitive data, such as autonomous vehicle manufacturers. This reflects the broader challenges outlined under GDPR's regulatory framework (Goddard, 2017).

Portuguese consumers demonstrate sensitivity to innovation adoption, influenced by broader concerns over regulatory frameworks and societal trust, which are significant barriers across Europe (European Commission, 2021). Culnan (1993) emphasizes the importance of trust, transparency, and consumer control in data usage practices. These principles are particularly relevant in the context of European concerns about data privacy, where regulations like GDPR and heightened consumer expectations challenge the adoption of emerging technologies such as autonomous vehicles.

By examining the Portuguese context, this research aims to provide insights into how companies can navigate these privacy challenges while maintaining operational efficiency.

3.Research Design

Research Approach

This study employs a **quantitative research approach** to investigate the relationships between GDPR awareness, trust in AV companies, privacy concerns and willingness to trade privacy for safety and functionality (Bélanger & Crossler, 2011; Pavlou, 2011; Sarathy & Robertson, 2003). Quantitative methods were selected because they enable the systematic measurement of variables, such as GDPR awareness and trust, and the statistical testing of hypotheses about their relationships. This approach is appropriate for addressing the central research questions, which focus on measurable phenomena and require robust, replicable findings. By relying on standardized metrics, the study contributes to theory development by providing empirical evidence on how GDPR awareness impacts trust and privacy concerns.

Sample Selection

Target Population: The target population includes Portuguese residents aged 18 and above who are potential or current users of autonomous vehicles (AVs). This population was chosen to reflect a diverse demographic in terms of age, gender, and geographic location, providing insights into variations in GDPR awareness and trust across Portugal.

Sampling Method: The sampling method employed in this study was convenience sampling, guided by an effort to include a diverse demographic of Portuguese residents. While the survey was distributed across various platforms to reach participants from different age groups, geographic regions, and urban or rural settings, no formal stratification or randomization was applied.

Sample Size: The survey had 272 responses, and the final sample consisted of 194 valid responses after data cleaning, which is sufficient for the statistical techniques employed in the study. This sample size ensures adequate power for detecting significant relationships while maintaining generalizability.

The survey collected responses from a diverse group of Portuguese residents. However, given the convenience sampling method and limited sample size, the results are not statistically generalizable to the Portuguese population as a whole.

Data Collection Methods

Data was collected through an **online survey**, distributed using GDPR-compliant platforms to ensure ethical adherence and data security. The survey included:

Demographics: Questions on age, gender, region, and level of knowledge of AV technology to analyse subgroup differences.

GDPR Awareness and Trust: Likert-like scale questions to measure respondents' awareness of GDPR principles like data minimization, consent, transparency, and their levels of trust in AV companies.

Privacy Concerns and Willingness to Trade Privacy: Likert-like scale questions assessing respondents' anxieties about specific data practices, such as geolocation tracking and behavioural data collection, and also willingness to exchange personal data for enhanced safety or functionality in AVs.

Views on privacy-by-design in AV's technology: Likert-like scale questions evaluating user perspectives on the incorporation of privacy-preserving technologies in AV development since its origin.

The survey method was chosen for its efficiency in reaching a geographically dispersed population and its alignment with the study's quantitative focus. Likert-like scale questions provided standardized responses, facilitating robust statistical analysis.

Data Analysis Techniques

The study employed a combination of descriptive and regression analysis methods to address the research questions and contribute to theory development:

1. **Descriptive Statistics (Figures 1-10 and Table 1):**

Purpose: To summarize and provide a baseline understanding of the key variables (GDPR awareness, trust levels, and privacy concerns).

Contribution: Descriptive statistics (e.g., mean, and standard deviation) lay the foundation for the analysis by identifying central tendencies and demographic patterns as seen in Table 1.

2. **Simple Linear Regression (Table 2)**

Purpose: To evaluate the direct relationship between GDPR awareness (independent variable) and trust in AV companies (dependent variable).

Justification: This model isolates the predictive power of GDPR awareness on trust while controlling for privacy risk perceptions in Model 2.

Contribution: The results demonstrate that GDPR awareness significantly predicts trust ($\beta = 0.1446$, $p < 0.05$), while privacy risk perception ($\beta = -0.202$, $p < 0.01$) has a negative effect. This paradox highlights the dual role of transparency: while greater awareness fosters trust through regulatory visibility, it also amplifies privacy-related anxieties. These findings extend Eisenhardt's (1989) transparency-trust framework, showing that GDPR awareness enhances trust but also increases concerns about data misuse. This underscores the need for complementary measures, such as robust privacy protections and user empowerment tools, to mitigate anxieties and reinforce sustainable trust. This model, with the very low R^2 value,

presents only a small part of the variability in the trust levels; therefore, other factors not measured here could actually be more important: personal experience with data breaches, perception of the reliability of AV technology, and general societal trust. It calls for further research, involving more complex models which take into consideration additional variables: prior use of AV, socio-economic status, and perceived technological literacy.

Reliability and Validity Measures

To ensure reliability and validity:

Pilot Testing: The survey was pilot tested with 30 participants to refine questions for clarity and consistency.

Validation Checks: The survey instrument was reviewed by experts in data governance and consumer behavior to confirm alignment with theoretical constructs.

These measures align with standards for empirical quality, bolstering confidence in the study's findings.

Ethical Considerations

The study adhered to strict ethical protocols, including:

Confidentiality: Data was anonymized, and no personally identifiable information was collected.

Informed Consent: Participants were fully informed about the study's purpose and their rights before participation.

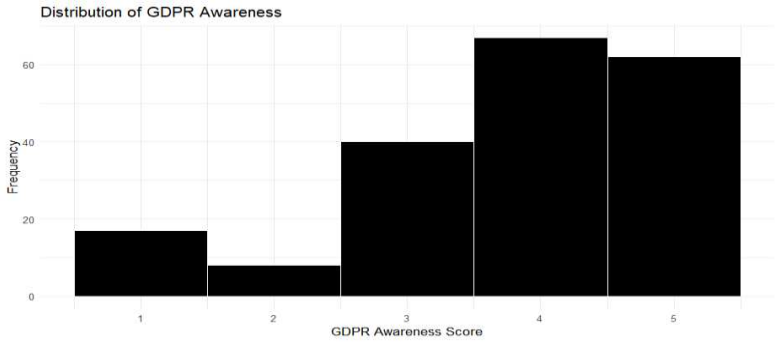
Data Security: All data was stored on GDPR-compliant platforms, ensuring compliance with data protection regulations.

These measures demonstrate a commitment to research integrity and participant protection. Reflecting Pierides and Zyphur's (2019) critique of the ethical dimensions inherent in research practices, these measures move beyond mere regulatory compliance to address potential institutional power imbalances. By embedding ethical reflexivity into research design, the study actively promotes participant empowerment and equitable engagement.

4.Results/Findings

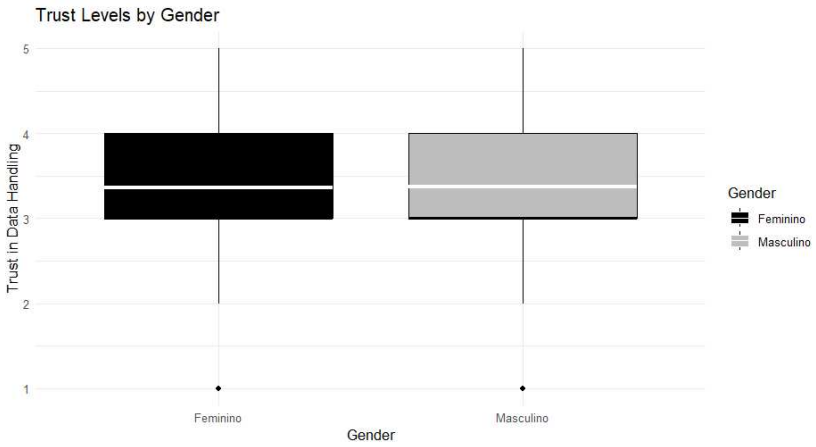
This study presents the quantitative findings derived from descriptive statistics, regression analyses, and visual data representations. These results are contextualized within the broader literature and highlight key factors influencing GDPR awareness, trust in data handling, and privacy concerns. It is important to note that while the findings highlight patterns across regions and age groups, these results are based on a limited sample and are not representative of the entire population.

Figure 1: Distribution of GDPR Awareness



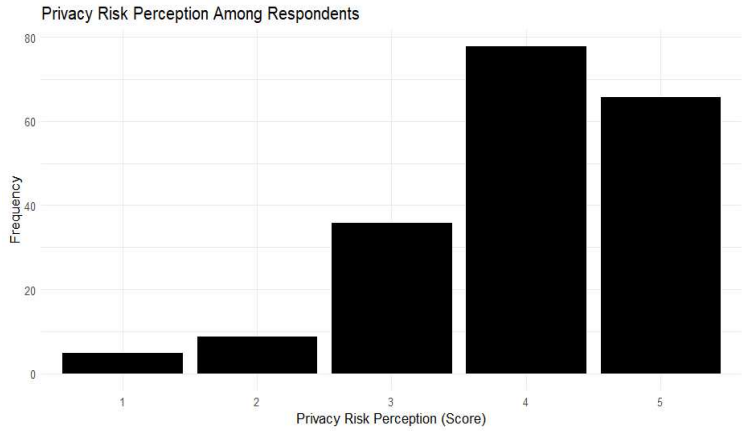
In Figure 1, the histogram shows that most respondents report moderate to high levels of GDPR awareness, with a peak around score 4 on a 5-point scale. This aligns with the expectation that GDPR's public visibility has enhanced general awareness.

Figure 2: Trust Levels by Gender



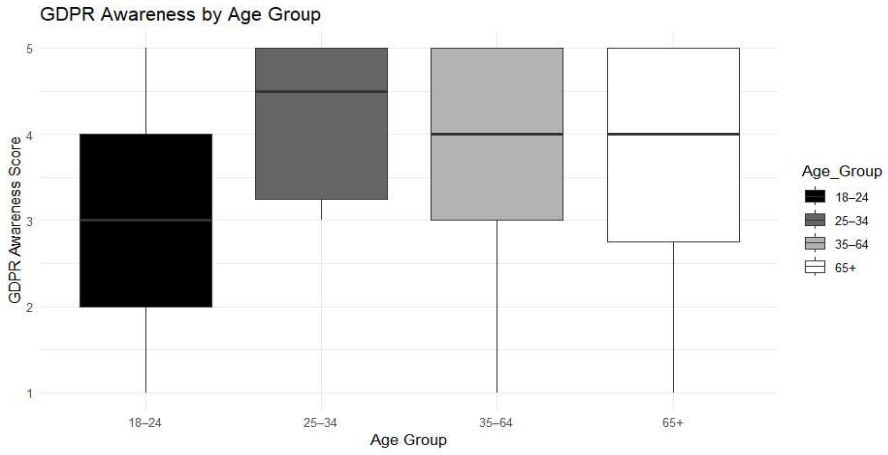
In Figure 2, the boxplot shows very few differences in the trust levels between different genders, what suggests gender-neutral perceptions of trust in AV companies. Both groups reported moderate trust levels with similar distributions.

Figure 3: Privacy Risk Perception Among Respondents



In Figure 3 we can observe that most respondents scored 4/5 on privacy risk perception, indicating a high level of concern about potential data misuse, such as geolocation tracking.

Figure 4: GDPR Awareness by Age Group.



Furthermore, in Figure 4, the boxplot indicates that GDPR awareness increases with age, with older respondents reporting the highest awareness levels. This trend could reflect the influence of generational differences in regulatory awareness-

Figure 5: GDPR Awareness by Region.

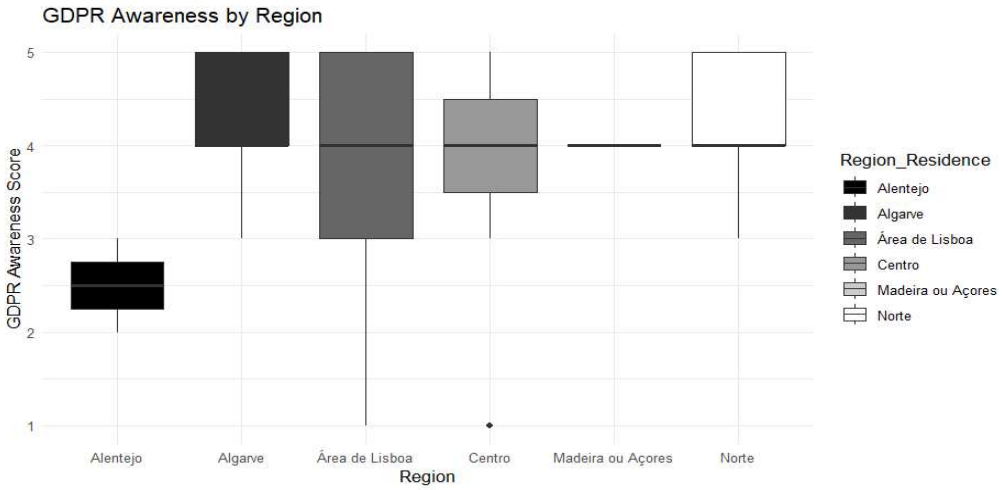
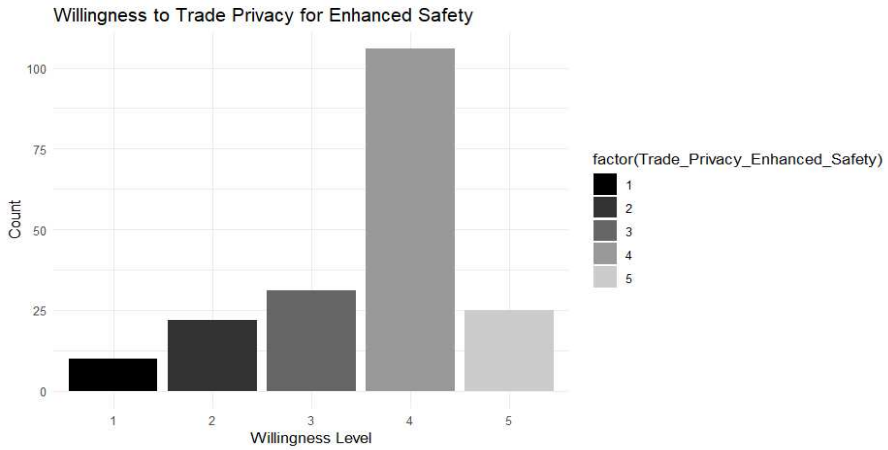


Figure 5, shows that respondents from Lisbon and Algarve reported significantly higher GDPR awareness in comparison with the ones from Alentejo, suggesting that urban areas may benefit from better information access and regulatory focus.

Figure 6: Willingness to Trade Privacy for Enhanced Safety.



In Figure 6, the bar chart shows a strong willingness for users to trade privacy for safety enhancements, with most respondents scoring 4 out of 5. This finding emphasizes consumer prioritization of safety over privacy.

Figure 7: Preference for Functionality vs Privacy.

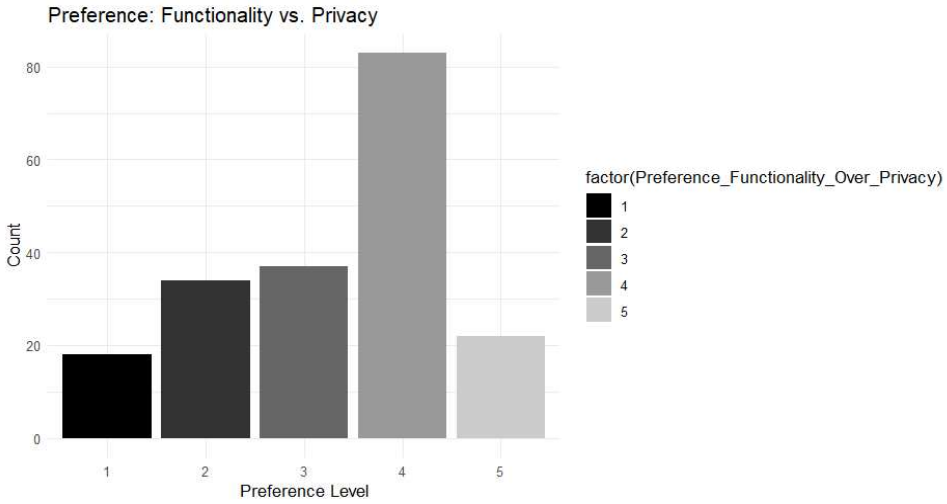


Figure 7 shows that respondents favor the most functionality over privacy, with most scoring a preference for functionality level of 4 out of 5, very similar to the results on Figure 6. This suggests a consistent valuation of tangible benefits over abstract privacy concerns.

Figure 8: Distribution of Privacy Concern Score.

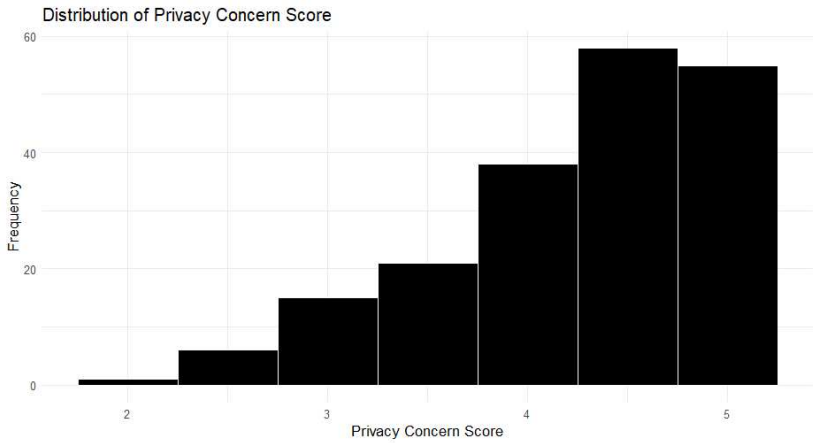
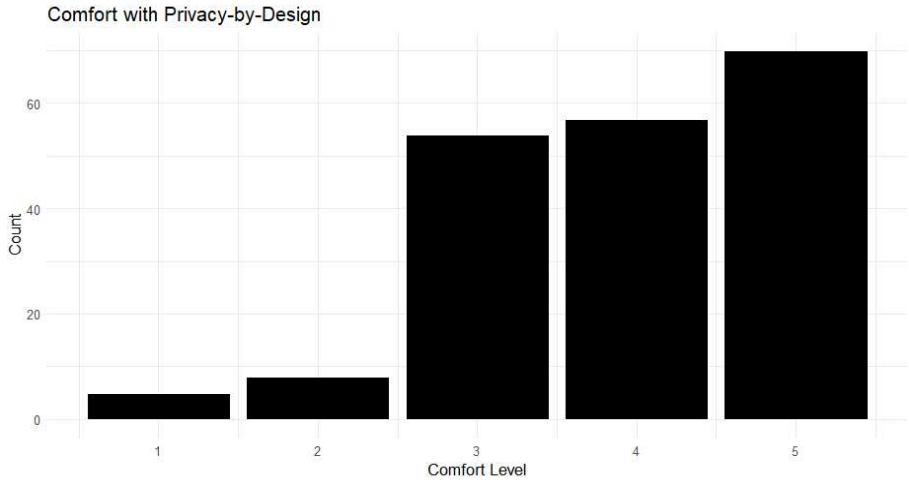


Figure 8, highlights that the distribution of privacy concern scores, which encompasses awareness of privacy risks and importance of data protection, skews high, with most respondents clustering around higher scores. This result reinforces the widespread nature of privacy anxieties.

Figure 9: Comfort with Privacy-by-design



In Figure 9, the majority of respondents expressed high comfort with integrating PbD principles into AV technology, with most giving it a level of 5 out of a 5-point scale, underscoring the importance of proactive privacy measures.

Figure 10: Privacy-by-Design score by Region

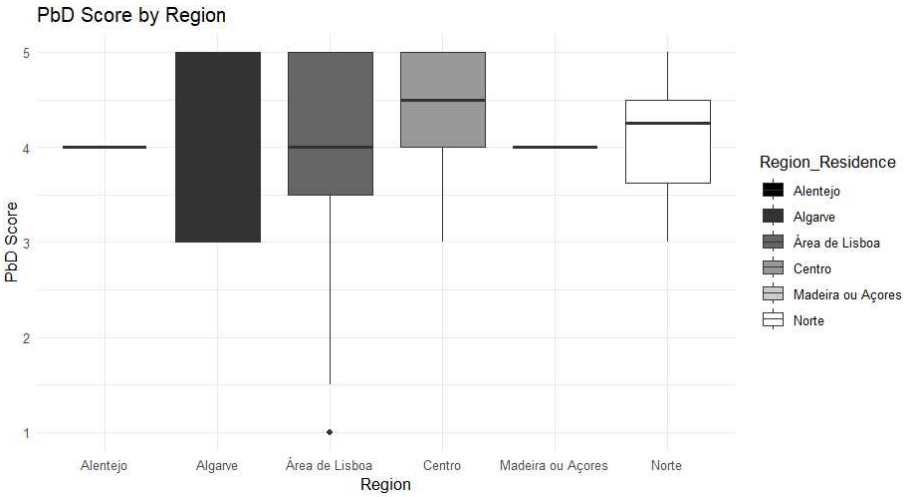


Figure 10 highlights that Norte and Algarve regions reported the highest PbD scores (which encompasses both comfort and support for the integration of PbD into AV technologies), while Alentejo lagged behind. This may reflect disparities in digital literacy and privacy education.

Table 1: descriptive analyses of some variables

Metric	GDPR_Awareness	Trust_Data_Handling	Comfort_PbD Support	Privacy_Protections
Min.	1,000000	1,000000	1,000000	1,000000
1st Qu.	3,000000	3,000000	3,000000	4,000000
Median	4,000000	3,000000	4,000000	5,000000
Mean	3,768041	3,365979	3,922680	4,293814
3rd Qu.	5,000000	4,000000	5,000000	5,000000
Max.	5,000000	5,000000	5,000000	5,000000
SD	1,197064	1,112844	1,017566	0,881855

Table 1 summarizes key variables from the study, including GDPR awareness, trust in data handling, comfort with Privacy-by-Design (PbD), and support for privacy protections. Respondents demonstrated moderate to high GDPR awareness, with an average score of 3.77 (SD = 1.20), which indicates a general awareness of the GDPR principles (Figure 1). Trust in data handling scored an average of 3.37 (SD = 1.11), reflecting moderate trust in how AV companies manage consumer data, consistent across genders (Figure 2) but influenced by other factors explored in regression analysis. Respondents showed high comfort with PbD principles (Mean = 3.92, SD = 0.92), showing a strong support for embedding privacy safeguards into AV systems. Support for embedding privacy protections into the creation of AV technologies also scored high levels (Mean = 4.12, SD = 0.88), showing the importance of proactive privacy measures in increasing trust and confidence among consumers.

Table 2: Regression Analysis: GDPR Awareness and Demographics Predicting Trust in Data Handling

Simple Regression Results		
Dependent variable:		
Dependent Variable: Trust in Data Handling		
	Model 1: GDPR Awareness Only	Model 2: + Demographics
	(1)	(2)
GDPR Awareness	0.135**	0.146**
	(0.066)	(0.069)
Gender		0.037
		(0.160)
Age Group		-0.290
		(0.497)
Privacy Risk Perception		0.158
		(0.231)
Age_Group65+		0.700
		(0.439)
Privacy_Risk_Perception		-0.202**
		(0.085)
Constant	2.855***	3.468***
	(0.262)	(0.405)
Observations	194	194
R2	0.021	0.064
Adjusted R2	0.016	0.034
Residual Std. Error	1.104 (df = 192)	1.094 (df = 187)
F Statistic	4.166** (df = 1; 192)	2.132* (df = 6; 187)
Note:		*p<0.1; **p<0.05; ***p<0.01

Table 2 presents regression models examining relationships between GDPR awareness, trust in data handling, and demographic factors. In Model 1, GDPR awareness positively predicts trust in data handling ($\beta = 0.135$, $p < 0.05$), suggesting greater awareness enhances confidence in AV companies' data practices, though the small coefficient implies that other factors, like privacy concerns and transparency, play a larger role. In Model 2, GDPR awareness remains a significant predictor of trust ($\beta = 0.146$, $p < 0.05$) even after controlling for demographics, while privacy risk perception negatively impacts trust ($\beta = -0.202$, $p < 0.05$), showing that concerns about data misuse destroy confidence. Demographics such as age and gender were not significant predictors, indicating trust in AV companies is more influenced by organizational practices and regulatory compliance than by individual characteristics.

GDPR Awareness and Trust

Key Findings: As we can observe from **Figure 1 and Table 1,** respondents' awareness of GDPR principles was **moderate to high**, with a mean score of 3.77 (SD = 1.20). Also, as demonstrated in **Figure 4**, GDPR awareness slightly increases with age, with older respondents reporting higher levels of awareness than younger ones (18–24). These disparities arise also at the regional level as it is shown in **Figure 5** with respondents in Lisbon, Algarve, Norte, Centro and Madeira/Açores reported higher GDPR awareness compared to those in Alentejo. These observations are descriptive, as no statistical tests were conducted to confirm significance. Furthermore, it was conducted a regression analysis (**Table 2**) which confirms that GDPR awareness significantly predicts trust in data handling (**$\beta = 0.135$, $p < 0.05$** in Model 1, and **$\beta = 0.146$, $p < 0.05$** in Model 2), even when demographic variables such as age group and gender are included into the model. The variable 'Age Group' captures the broader age categories, while 'Age Group 65+' isolates respondents aged 65 and older to examine whether they exhibit distinct patterns in trust compared to other age groups.

Interpretation: These results suggest that the respondents exhibit high levels of GPR awareness with urban areas and older populations exhibiting greater levels of it, these trends may reflect better access to information or a heightened focus on regulatory compliance in more developed regions. To further answer sub-question 1, we can observe that GDPR awareness positively influences trust, although the modest effect size indicates that additional factors may moderate this relationship. Furthermore, the positive correlation supports the hypothesis that GDPR awareness fosters trust by enhancing transparency. However, the modest effect size suggests that other factors, such as privacy concerns and organizational practices, likely influence trust more substantially, these results reinforce the need for regulatory frameworks like GDPR to emphasize transparency as a foundation for trust, while acknowledging that additional measures are necessary to build robust consumer confidence in data handling.

Trust in Data Handling

Key Findings: As shown in **Table 1**, respondents reported **moderate** levels of trust in data handling by AV companies, with a mean score of 3.37 (SD = 1.11). Furthermore, in **Figure 2** we can observe that trust levels were similar across genders. On the other hand, GDPR awareness significantly predicted trust in data handling in the regression analysis. Specifically, GDPR guidelines awareness was positively associated with trust (**$\beta = 0.135$, $p < 0.05$** in **Table**

2). Besides that, we can see in **Table 2, Model 2** that privacy concerns significantly and negatively predict trust in AV companies' data handling practices (**$\beta = -0.202$, $p < 0.05$**). This means that respondents' concerns about privacy risks (such as location tracking and data misuse) increase, as their trust in AV companies decreases. Although GDPR aims to foster trust through transparency, these results highlight that privacy anxieties can undermine trust, supporting prior findings that extensive data collection can create apprehension among consumers.

Interpretation: The positive relationship between GDPR guidelines awareness and user's trust in data handling by AV companies show the important role of transparency in enhancing consumer confidence. However, the modest effect size suggests that GDPR awareness alone is insufficient to build robust trust in data handling practices. Also, privacy risk concern undermines trust, reflecting the dual effect of transparency: while it fosters trust, it can also amplify anxieties about data misuse which allows us to get insights into sub-question 2. The lack of significant demographic predictors suggests that trust in data handling may be more influenced by organizational practices and transparency efforts than by individual characteristics.

Privacy Concerns

Key Findings: In order to address sub-question 3 we can observe that over **70% of respondents** demonstrated high concern about privacy risks, focusing on geolocation tracking and behavioral data collection (**Figure 3**). These privacy concern scores show a skewed distribution, with most respondents scoring 4/5 on a 5-point scale (**Figure 8**). Furthermore, the regression analysis in **Table 2** reveals that GDPR awareness significantly increases privacy concerns (**$\beta = 0.368$, $p < 0.01$**). This suggests that greater familiarity with GDPR principles, such as transparency and data rights, leads to heightened sensitivity to data privacy risks. While GDPR provides a framework to ensure compliance, its emphasis on transparency can paradoxically amplify concerns, as respondents become more aware of the complexities of data handling practices.

Interpretation: These results suggest that GDPR awareness increases consumer awareness of data vulnerabilities, leading to heightened anxieties about privacy risks. And to better answer sub-question 3, we also observe that privacy concerns are widespread and not limited to specific demographic groups, underscoring the universal importance of addressing data protection

issues. Figures 3 shows the distribution of Privacy Risk Perception scores of respondents and Figure 8 the distribution of privacy concern scores, these present the results of univariate analyses for each separate variable and are constructed to give an overall view of the distribution of every variable.

Willingness to Trade Privacy for Enhanced Safety or Functionality

Key Findings: As illustrated in **Figure 6** respondents score high levels of willingness to trade privacy for enhanced safety, with most scores clustering at level 4 out of 5. Besides that, **Figure 7** shows that most respondents favoured functionality over privacy, with the highest frequency at level 4 out of 5.

Interpretation: To help on answering sub-question 4, the descriptive results suggest that many respondents perceive safety as a higher priority than privacy in certain contexts and that, across the sample, considerations of functionality consistently outweigh privacy concerns, as shown by the high agreement scores on individual survey items.

Privacy-by-Design Support

Key Findings: Comfortability due to the integration of Privacy-by-Design into AV's received a strong support, with most of the respondents assigning the highest score of 5 (Figure 9). Besides that, it was performed a regional analysis (Figure 10) which highlights that respondents from Norte and Algarve regions exhibit higher median PbD scores (which encompasses not only comfortability but also importance of PbD integration into AV technology), compared to Alentejo and Madeira/Açores. Outliers in Lisbon underscore the variability in urban responses, reflecting a diverse perception of privacy protections within metropolitan areas.

Interpretation: The high levels of comfort with Privacy-by-Design principles suggest a strong consumer preference for integrating privacy safeguards directly into autonomous vehicle systems. However, and to better answer to research sub-question 5, regional disparities, such as lower PbD scores in Alentejo, indicate the need for geographically tailored privacy campaigns to address localized concerns and improve overall acceptance.

5.Discussion

This research aimed to examine the extent to which the perceptions of compliance with the GDPR, privacy concerns, and transparency occur by Portuguese consumers regarding AVs. Some evidence of the above dynamics is provided, especially within the regulatory environment configured by the GDPR. Next, I will discuss the findings that provide the answer to the research questions by comparing them with the literature available at the moment and indicate the novel contributions.

GDPR Awareness and Trust in Data Handling

The study highlights that awareness of GDPR plays a role in building trust in how AV companies handle data. The respondents reported an average awareness of the principles of GDPR that is medium to high, with a mean score of 3.77. This is higher in the case of older people, or residents in urban areas, particularly Lisbon and Algarve. This might reflect easier access to information or greater emphasis on regulatory compliance in these areas. Mendonça & Andrade (2018) indicate that technological awareness increases in regions that show a rapid digital transformation and may extend into the regulatory compliance area. Their findings regarding access to technology and information show that this type of regions have a higher ability to adapt, which aligns with the trends observed in Lisbon and Algarve. Besides that, the regression analysis also showed that there is a small but significant relationship between GDPR awareness and trust, $\beta = 0.135$, $p < 0.05$, which might be considered as support for the arguments of Adjerid, Peer, & Acquisti (2018), and Eisenhardt (1989) that transparency could enhance consumer confidence. That means GDPR awareness has a significant impact on trust presumably due to reducing perceived risks and privacy concerns. But this modest effect size again suggested that awareness alone was not enough to strongly install trust, rather trust would emanate more powerfully from how the implementation of privacy protection was set up and communicated by the company, as these cited studies have noted. Awareness under GDPR is a basis on which robust organizational practices need to be implemented to further assure the consumer about confidentiality and continued transparency. These insights also helped on answering sub-question 1 and 2, showing that awareness of GDPR builds trust but at the same time underlines practical measures to enhance the trust outcome.

These findings are also in line with the rational-choice model by Bulgurcu, Cavusoglu, and Benbasat (2010), which assumes that internal compliance behaviors result from the evaluation

of costs, benefits, and awareness. In such context and in regard to GDPR, the greater the awareness, the greater the trust because it conveys commitment on the part of an organization to data protection. However, according to Bulgurcu et al., this increased awareness also introduces perceived burdens, such as operational challenges or increased scrutiny, adding to anxieties over data practices. The dual effect dual effect— trust-building through transparency and increased anxiety due to awareness— is also in agreement with the paradoxical relationship established in this study between awareness of the GDPR, trust, and privacy concerns. This shows that anxieties of this kind are mitigated by strategies involving clearer communication and consumer education.

Privacy Concerns and Their Impact on Trust

Privacy concerns were a central theme, with over 70% of respondents expressing high levels of worry about risks like geolocation tracking and behavioural data collection. These concerns were consistent across demographics, highlighting the universal nature of anxieties about data misuse (Cichy, Salge, & Kohli, 2021).

Also, privacy concerns were inversely related to trust in the companies developing the AVs: increased concerns with respect to privacy negatively predicted trust regarding data handling, $\beta = -0.202$, $p < 0.05$. Which is consistent with Sarathy and Robertson's (2003) observation that extensive data collection raises ethical and operational challenges. While their work primarily focuses on balancing societal and commercial interests, the operational implications of privacy breaches align with the idea that real-time data collection can exacerbate distrust.

GDPR awareness in itself was significantly related to an increase in concern about privacy ($\beta = 0.368$, $p < 0.01$). This lends empirical credence to Pierides and Zyphur's (2019) argument that transparency fosters trust through enlightenment but can paradoxically magnify anxieties through the ethical complexity embedded in practices around data. They highlight that data-handling methods often obscure their value-laden nature—thus, transparency could inevitably raise concerns when these hidden dimensions are disclosed. However, this study extends their work by showing that this effect is pronounced in the AV context, where real-time data collection exacerbates privacy concerns. This aligns with Sarathy and Robertson's (2003) findings on the barriers posed by privacy anxieties in data-driven technologies.

These implications meet sub-questions 2 and 3 in that concerns about privacy may injure the trust of a company's customers in the AV companies. That is because companies should not

only be ensuring compliance of privacy frameworks such as GDPR but also in alienating fears that these kinds of frameworks might heighten through the clear communication and transparency of how they handle the user's personal data. With such concerns managed, firms are able to foster a more balanced approach to privacy, trust, and utility of data.

The Privacy-Safety/Functionality Trade-off

Most participants scored high in their willingness to trade privacy for enhanced levels of safety and functionality—a trend similar across demographic groups. This behaviour follows a pattern of the privacy paradox as described by Adjerid, Peer, & Acquisti (2018), where immediate or tangible benefits, such as safety, stand out against abstract or long-term privacy concerns. These results show the nature of privacy decision-making, where we must take into consideration both the framing and context of the trade-offs, along with participants' perceptions of the immediate value of safety relative to privacy.

However, companies cannot ignore privacy concerns entirely. Felzmann et al. (2020) highlight the risks of neglecting privacy protections in favour of functionality, noting that it could decrease consumer trust and lead to regret. Their findings indicate that while users may accept certain compromises, they still demand transparency and strong safeguards to ensure accountability and trustworthiness in automated decision-making systems. These findings address sub-question 4, showing that while people are willing to compromise on privacy for safety, they still expect companies to implement strong safeguards.

Support for Privacy-by-Design (PbD)

User's comfort with the integration of Privacy-by-Design (PbD) principles reported scored high levels showing a strong support from respondents, with a mean comfort level of 3.92 out of 5. This aligns with Cavoukian's (2009) advocacy for embedding privacy directly into system architecture as a proactive measure. However, we also observed regional disparities, with Norte and Algarve residents showing stronger support for PbD compared to rural areas like Alentejo. Besides that, variability within Lisbon also showed the diverse perspectives within urban regions.

These findings highlight that privacy education campaigns should be adapted to regional contexts, aligning with Mendonça and Andrade's (2018) emphasis on adaptability in using

digital technologies within specific organizational and geographic contexts, and that firms can meet consumer expectations and build trust by embedding privacy into the AV systems right from their design. The findings address sub-question 5, showing that proactive privacy measures strongly resonate with consumers and boost their confidence and trust on AV companies.

Contributions

Theoretical Contributions:

This study contributes to the growing literature on the GDPR, privacy concerns (e.g., Bélanger & Crossler, 2011; Pavlou, 2011; Sarathy & Robertson, 2003), and trust in many ways. First of all, the study empirically validates the argument of Pierides and Zyphur (2019) by showing that awareness of GDPR amplifies privacy concerns in a data-intensive industry like autonomous vehicles. Second, this extends the work of Sarathy and Robertson (2003) by demonstrating how the nature of privacy concerns influences trust in the data handling practices of AV companies. Third, it extends the 'privacy paradox' framework of Adjerid, Peer, & Acquisti (2018) into the AV context and therefore provides new insights into the privacy-safety trade-off. Finally, this study provides new evidence regarding the role of Privacy-by-Design, as proposed by Cavoukian (2009), in improving consumer comfort and trust.

Practical Contributions:

From a managerial perspective, the study offers actionable strategies for AV companies such as the fact that it highlights the importance of tailoring privacy and trust-building measures to regional differences in GDPR awareness and digital literacy, supporting localized educational campaigns to bridge awareness gaps.

First, Managers should consider how lower GDPR awareness in regions, like it emerges in the case of Alentejo, is associated with greater consumer mistrust and limited engagement with data privacy practices. Educational campaigns should be tailored to such regions to address awareness gaps. Espeland and Stevens (2008) stress that regulatory visibility is crucial for equitable participation. Similarly, the lower regional innovation scores reported in the European Innovation Scoreboard (2021) highlight the need for localized initiatives to improve baseline digital literacy and trust.

AV companies could also partner with local councils and NGOs to design workshops and outreach campaigns using trusted communication channels such as regional radio and social media. These efforts should be customized to align with the community's cultural preferences and values.

Second, younger consumers demonstrate a preference for privacy-preserving technologies but are sceptical about data governance. Conversely, older consumers prioritize the tangible benefits of data sharing over abstract notions of privacy. Younger consumers align with behavioural perspectives discussed by Adjerid et al. (2018), where perceived control and engaging tools help simplify complex regulations and improve decision-making through engaging features like gamification. It appeals to all the principles of behavioural approaches by responding to cognitive biases and enhancing relatability. However, transparency and clear benefits are some attributes desired predominantly in a service by older consumers in most contexts. In fact, this coincides with Eisenhardt's transparency-trust framework showing clearly that clear communication is key in building trust. Even though there might be some theoretical models aligned, which again point toward the trends, variation across age groups and overlapping requires a nuanced understanding.

Based on results of this study managers could design demographic-specific messaging strategies, such as gamified tools for younger consumers and transparent communication of safety benefits for older users, aligning with behavioral theories and trust-building frameworks (Eisenhardt, 1989; Adjerid et al., 2018).

Besides that, the findings show the necessity for implementing real-time anonymization and producing transparency reports, aligning with Transparency by Design principles, to alleviate anxieties about data breaches and build consumer trust (Felzmann et al., 2020; Pavlou, 2011).

Third, high consumer anxiety over data breaches correlates with low trust in organizations' ability to manage data ethically. Real-time anonymization and transparency reports address these anxieties by providing concrete evidence of compliance. Felzmann et al. (2020) and Pavlou (2011) highlight how transparency mechanisms can reinforce trust.

It follows that managers could establish quarterly transparency reports showing anonymization statistics and compliance metrics. This aligns with the "Transparency by Design" model and demonstrates proactive steps to mitigate anxieties.

Forth, the study suggests a specific managerial focus on Privacy-by-design. Indeed, as emerged from the analysis, high comfort levels with Privacy-by-Design (mean = 3.92) indicate consumer readiness for integrated privacy safeguards. As Cavoukian (2009) and Felzmann et al. (2020) emphasize, embedding privacy into system design ensures regulatory compliance and enhances consumer trust. Companies should therefore mandate PbD principles in AV systems by designing them with pre-emptive data security features. Focus on real-time anonymization, secure data storage, and GDPR compliance as core design components.

Limitations and Future Research

This study is subjected to several limitations.

First, generalizability of this study is very limited. Considering, among others, its limitation to Portugal, further paths of research can consider cross-national comparisons to explore cultural and regulatory differences in GDPR implementation. As Pierides and Zyphur (2019) emphasize, the contextual dimensions of research practices are critical, underscoring the importance of understanding how local and regional factors shape the implementation and perception of regulatory frameworks like GDPR. This would also be in line with Espeland and Stevens (2008), who argue that regulatory frameworks must adapt to local contexts.

Second, self-reported survey data introduces biases such as social desirability. This limitation, which affects the accuracy of capturing behavioral nuances, has been discussed in privacy research (Son and Kim, 2008). Future studies could employ observational methods, as suggested by the study previously mentioned, to validate findings and uncover deeper insights.

Third, the findings are based on survey responses from a convenience sample which lacks due rigor to be generalized to the broader Portuguese population or other geographic contexts. Future research should employ larger, stratified random samples to improve the robustness and generalizability of the results.

Forth, while this cross-sectional study captures attitudes at a single point in time. Future longitudinal studies could complement this quantitative analysis by tracking changes in trust and privacy concerns over time, thereby enriching the insights provided by single-time-point observations.

Future studies could incorporate additional variables, such as socioeconomic status or prior AV experience, to provide a more comprehensive understanding of consumer attitudes. This aligns

with the broader principles of Eisenhardt's (1989) agency theory, which highlights the importance of reducing asymmetry and incorporating contextual factors to foster alignment and trust. Pavlou (2011) also highlights the importance of exploring multidimensional influences.

6.Conclusion

Research Objective and Questions

This thesis focused on the relations between compliance with GDPR, consumer privacy concerns, and transparency within the context of AVs. Therefore, the central question in this research was:

How do Portuguese consumers perceive GDPR compliance, privacy, and transparency in autonomous vehicles? Seeking to formulating several managerial suggestions and implications based on results from the study.

The findings indicate that the two-side effect of GDPR awareness on consumer attitudes is positive in relation to trust in AV firms but simultaneously increases concerns about data misuse, mainly related to geolocation and behavioural tracking. The results also point to some relevant regional differences: urban areas, such as Lisbon, present higher levels of awareness of GDPR and trust, while rural regions, such as Alentejo, present lower levels of awareness and more scepticism.

The respondents were in absolute agreement with the Privacy-by-Design principles set out by Cavoukian (2009), as they placed great importance on the need for embedded privacy safeguards within the AV systems. When consumers perceived privacy protections as robust and effective, they prioritized safety and functionality over privacy. This observation supports and refines the work of Adjerid et al. (2018) on the behavioural factors affecting privacy trade-offs and extends the conceptual model of Felzmann et al. (2020) on the interplay of functionality and privacy concerns in automated systems.

Transparency thus came out as both a trust enabler and an anxiety amplifier, reinforcing Pierides and Zyphur's 2019 contention on its ambivalence. This research finds transparency as essential to bridge consumer understanding but also highlights the highly complex disclosures that overwhelm the users.

Building on such results, this study makes a significant contribution to the growing academic discussion on the interplay between privacy, trust, and technology adoption, particularly within transparency-trust frameworks. It expands the knowledge of Pierides and Zyphur (2020) by offering empirical evidence of transparency's ambivalent role in both building trust and exacerbating privacy concerns. As it is demonstrated in the research, in the GDPR-regulated context of AVs, transparency fosters trust through disclosures but also overwhelms users with excessive information, ultimately heightening anxieties.

The findings also provide critical insights into the privacy paradox explored by Adjerid et al. (2018), showing how consumers in the AV domain balance privacy trade-offs with tangible benefits, such as safety and convenience. By examining Portuguese consumers, the study highlights how regional and cultural contexts shape privacy-related decision-making, offering a more nuanced understanding of the factors mediating this trade-off. Furthermore, this research validates the Privacy-by-Design (PbD) principles proposed by Cavoukian (2009), demonstrating that they are able to alleviate consumer concerns and increase trust. The study emphasizes the practical importance of PbD principles as a cornerstone of GDPR compliance in AV systems, underscoring their relevance in addressing user apprehensions.

Lastly, the study contributes to the literature on GDPR compliance by showing the variance in consumer responses across various regions within a uniform regulatory framework. Specifically, it highlights lower awareness and trust regarding GDPR in rural areas such as Alentejo, emphasizing the need to address regional disparities to promote the equitable and widespread adoption of AV technologies.

Practical Contributions

This study also provides actionable recommendations for AV companies as they intend to effectively gain consumer trust and meet their privacy concerns. Since in rural regions such as Alentejo, awareness of the GDPR is particularly low and scepticism particularly high, targeted campaigns of education are necessary. For that reason, companies should work with local councils and NGOs to devise culturally appropriate workshops and outreach programs. Using trusted channels, such as regional radio and social media, may bridge some of the awareness gaps, as noted by Espeland and Stevens (2008) and the European Innovation Scoreboard (2021).

While younger consumers prefer using privacy-enhancing tools, these tools need to be enjoyable and not overly complicated. Gamified applications that handle privacy offer an effective alternative to promote active participation, drawing on behavioral insights provided by Adjerid et al. (2018). On the other hand, when communicating with older users, they should highlight transparency regarding the benefits, such as added safety and functionality, using a language that respects the transparency-trust framework introduced by Eisenhardt (1989).

Proactive strategies for building trust may include implementing real-time anonymization or issuing quarterly transparency reports by AV companies to showcase anonymization metrics and compliance with the GDPR. These measurements are aligned with frameworks for building user trust mentioned by Felzmann et al. (2020) and Pavlou (2011), which highlight the fact that proactive transparency increases consumer confidence.

Finally, the users show a broad consensus on Privacy by Design (PbD) principles which shows the need for AV companies to embed privacy safeguards into system design. Features such as secure data storage, real-time anonymization, and compliance-driven architecture are critical for addressing privacy concerns and fostering trust, as advocated by Cavoukian (2009).

Closing Statement

This study performed a deeper examination of the interplay between compliance with GDPR, consumer trust, and privacy concerns regarding privacy linked to autonomous vehicles. Highlighted Privacy-by-Design and strategic transparency as necessary insights into aligning regulatory adherence with consumer expectations. These findings underline the importance of balancing innovation with ethical data governance, hence contributing to the knowledge of how potential AV users in Portugal view certain important aspects of the introduction of this technology and how might AV companies better engage with this market.

References

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox. *MIS Quarterly*, 42(2), 465-488.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 1017-1041.

Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing artificial intelligence. *MIS Quarterly*, 45(3).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Bu, F., Wang, N., Jiang, B., & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management*, 53, 102124.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*, 5, 12.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MIS Quarterly*, 45(4).

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 17(3), 341–363. https://doi.org/10.2307/249775

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, 14(1), 57-74.

Espeland, W. N., & Stevens, M. L. (2008). A sociology of quantification. *European Journal of Sociology/Archives européennes de sociologie*, 49(3), 401-436.

European Commission: Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, European Innovation Scoreboard 2021, Publications Office of the European Union, 2021, https://data.europa.eu/doi/10.2873/725879.

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.

General Data Protection Regulation (GDPR) – Legal Text (gdpr-info.eu)

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.

Islam, G. (2022). Business ethics and quantification: Towards an ethics of numbers. *Journal of Business Ethics*, 176(2), 195-211.

Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, 24(4), 602-611.

Kohl, C., Knigge, M., Baader, G., Böhm, M., & Krcmar, H. (2018). Anticipating acceptance of emerging technologies using Twitter: the case of self-driving cars. *Journal of Business Economics*, 88, 617-642.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1), 1-6.

Martinez, L. M., & Viegas, J. M. (2017). Assessing the impacts of deploying a shared self-driving urban mobility system: An agent-based model applied to the city of Lisbon, Portugal. *International Journal of Transportation Science and Technology*, 6(1), 13-27.

Mendonça, C. M. C. D., & Andrade, A. M. V. D. (2018). Dynamic capabilities and their relations with elements of digital transformation in Portugal. *Journal of Information Systems Engineering & Management*, 3(3).

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977-988.

Santanen, E. (2019). The value of protecting privacy. *Business Horizons*, 62(1), 5-14.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, 46, 111-126.

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(3), 503–529.

Teodorescu, M. H., Morse, L., Awwad, Y., & Kane, G. C. (2021). Failures of Fairness in Automation Require a Deeper Understanding of Human-ML Augmentation. *MIS Quarterly*, 45(3).

Wu, Y., & van Rooij, B. (2021). Compliance dynamism: Capturing the polynormative and situational nature of business responses to law. *Journal of Business Ethics*, 168(3), 579-591.

Zyphur, M. J., & Pierides, D. C. (2020). Statistics and probability have always been value-laden: An historical ontology of quantitative research methods. *Journal of Business Ethics*, 167(1), 1-18.