REALISING PLATFORM CONTROL IN DATA MARKETPLACES THROUGH SECURE MULTI-PARTY COMPUTATION

Master thesis – Management of Technology 2020

Riccardo Dolci

The image above was retrieved from https://martech.zone/what-is-passive-data-collection/

TU Delft

REALISING PLATFORM CONTROL IN DATA MARKETPLACES THROUGH SECURE MULTI-PARTY COMPUTATION

A qualitative study exploring the use of Secure Multi-Party Computation (MPC) as an instrument for realising platform control in data marketplaces

Master thesis submitted to Delft University of Technology in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Riccardo Dolci

Student number: 4889258

To be defended in public on August 13th, 2020

Graduation committee

Chairperson:	Dr. ir. G.A. (Mark) de Reuver, Information and Communication Technology
First Supervisor:	Dr. ir. G.A. (Mark) de Reuver, Information and Communication Technology
Second Supervisor:	Dr. M.E. (Martijn) Warnier, Multi-Actor Systems
Advisor:	Mr. W. (Wirawan) Agahari, Information and Communication Technology

Preface

This thesis project represents the conclusion of my master degree in Management of Technology at Delft University of Technology. It was a wonderful experience, characterised by many challenges both from the academic and personal side. I could not be able to reach this achievement without the help of several people. Therefore, I would like to acknowledge all the ones who supported me during this unique journey.

Firstly, I would like to thank my first supervisor Dr Mark de Reuver who offered me the opportunity to work on this project and gave me critical feedback to improve the quality of my thesis. Secondly, I would like to thank my advisor Wirawan Agahari for guiding me throughout the entire research and solving all my doubts. I would also like to thank my second supervisor Dr Martijn Warnier for the useful feedback provided.

A special thank you goes to my family who always supported and encouraged me throughout my entire academic career. For this reason, I would like to dedicate this thesis to my parents, Gianmarco and Laura, for all the sacrifices they made for me, and to my brother Federico, for being always there for me. Finally, I would like to express my gratitude to all the friends who accompanied me during this amazing and memorable experience. In particular, I would like to thank my old inseparable friends, the Street Sharks from Monza and Dibe, and the new ones made during the master, the Italian squad in Delft, the Paps roommates, David, and my classmates.

Riccardo Dolci

Biassono, July 2020

Executive summary

Practical problem: In today's digitally transformed and connected world, data has become a critical strategic corporate resource. In this context, data marketplaces are becoming more popular since they enable wider accessibility and more efficient interaction among companies. Despite this, there are several barriers in sharing data through this type of platforms, for instance, lack of trust, security, privacy and transparency. The introduction of privacy-enhancing technologies, such as secure Multi-Party Computation (MPC) could offer a significant contribution to overcoming these barriers. However, it is still unclear if secure MPC could be implemented in the data marketplace domain, especially as an instrument for controlling the platform, and what are the affordances that it could offer to data marketplace providers. For this reason, this research study aims to investigate the potential adoption of secure MPC by a data marketplace provider for realising platform control.

Methodology: the exploratory nature of this research required to conduct a qualitative study to address the problem and achieve the aforementioned target. In particular, given the specific characteristics of this research, a survey research was undertaken. Regarding the data collection method, semi-structured interviews were conducted among data marketplace providers operating in the mobility domain, data marketplace experts and MPC developers and experts.

Results: the adoption of MPC could generate three main affordances for a data marketplace provider in terms of platform control: (1) preserving the data, (2) enabling data ownership and (3) preserving the result of the computation. These affordances are generated by the relationship between the data marketplace provider's goals in terms of platform control and the features of the MPC technology. Regarding the former, the following goals were identified: (1) ensure the security and the privacy of the data; (2) guarantee that a data provider has complete control over its data; (3) ensure the correct execution of the computation. Concerning the latter, three key features offered by the MPC technology could enable platform control: (1) information-theoretic security or computational security, (2) agreement protocols before starting the computation and identification mechanisms if someone deviates from it, (3) and correct execution of the computation.

The realisation of the affordances could be influenced by three factors: (1) perception of the technology, (2) need for the technology, and (3) degree of effort required. The results showed that secure MPC could satisfy several different needs of a data marketplace provider. However, some constraints could influence the adoption of MPC among data marketplace providers. Firstly, a data marketplace provider may perceive the MPC as unsafe because of the difficulty to understand the

technology. Secondly, a data marketplace provider could consider that secure MPC does not currently present an adequate maturity level to adopt the technology in its platform. Finally, a data marketplace provider could prefer to maintain its current situation in order to avoid a radical change.

The adoption of MPC technology by a data marketplace provider could cause several impacts on its platform. If the platform has a centralised structure, the data will not be stored in the platform anymore, but they will remain with the data provider. Moreover, if a data marketplace focuses only on data exchange offerings, it would be able to offer a new type of product in its platform (e.g. insights). Finally, the adoption of the MPC in a data marketplace could cause additional overhead in the functioning of the platform.

Theoretical and practical contributions: regarding the former, this study contributes to the literature of data markets, platform control, MPC, and affordance theory. Concerning the latter, this research provides practical contributions to the business actors involved in data-sharing domains and to MPC developers.

Limitations: firstly, it was not possible to focus the research on data marketplace involved exclusively in the mobility domain and to reach theoretical saturation also for the fourth sub-research question of the study because of the difficulty of reaching informants. Secondly, two of the data marketplace providers interviewed worked for a data marketplace, which is not currently operating anymore. Moreover, in some cases, it was necessary to interview a person with a different role in the company compared to the one initially selected. Thirdly, since some of the interviewees did not have the time to study the MPC description document before the interview, it was necessary to verbally explain it, thus possibly affecting both the validation of the document and the understanding of the technology.

Future research: Firstly, by conducting more interviews, it could be possible to identify more factors. Secondly, future research could be undertaken to validate the model of this research through quantitative studies. Thirdly, further researches could be pursued to update the taxonomy of data marketplaces. Fourthly, future research could be carried out to explore the introduction of secure MPC in other settings. Finally, it could be interesting to explore the different perspectives of the actors involved in a data marketplace (e.g. data providers and buyers).

Keywords: data sharing, data marketplace, platform control, secure multi-party computation, affordance theory.

Table of contents

List of figures

List of tables

1. Introduction

1.1 Practical problem

In an ever more connected world, data is generated every day through several channels and at an incredibly high quantity and rhythm (Wiseman, 2019). Each day 2.5 quintillion of data bytes are produced, with an expected acceleration due to the rapid growth of technological innovation, for instance, the Internet of Things (IoT) (Marr, 2018). In fact, the amount of data generated just in the past two years is 90 per cent of the one currently present in the world (Marr, 2018). Data can be produced anywhere by several sources such as humans, devices, organisations or a combination of these and stored in structured or unstructured formats (Ghotkar & Rokde, 2016).

Data has become a critical strategic resource for establishing successfully a company in a market (Spiekermann, 2019). Nowadays, as The Economist (2017) claimed, data represents the world's most valuable resource. The power of data in the business world demonstrated that companies must consider data, not only as a technical matter but as a company's asset that, like any other product, has economic value (Spiekermann, 2019). However, no single actor holds all the data necessary for improving the quality of their decision making (KPMG, 2018). B2B data sharing, which is the practice of sharing data to other companies, or getting data from other organisations for different business purposes (European Commission, 2018), represents an excellent solution to overcome this issue and provide several benefits for both data suppliers and users. In fact, it can help the former to promote collaborations between firms, generate alternative sources of income, and facilitate innovation (European Commission, 2018). On the other hand, obtaining data from other firms may create the opportunity of developing new services and products, and improve the customers' satisfaction and internal efficiency (European Commission, 2018).

In order to fully exploit the potential of data, new technologies which allow more extensive accessibility and reuse of data among private and public actors are currently emerging. In this context, data marketplaces, which are digital platforms where companies can periodically buy and sell data (European Commission, 2018), are becoming increasingly popular in the business world (Ghosh, 2018). Data marketplaces allow to connect several actors from different domains and obtain a more accessible and efficient interaction thanks to standardised interfaces and services (Spiekermann, 2019). Despite the advantages mentioned above, there are still several challenges in sharing data among companies and establishing data marketplaces successfully in the market.

Firstly, the high number of platforms that have failed recently, for instance, Microsoft's Azure Data Marketplace, discourage the creation of new business in this sector (Spiekermann, 2019). Moreover, present data marketplaces do not satisfy some relevant properties such as transparency, security, privacy and adherence to regulations (Banerjee & Ruj, 2019). For these reasons, data owners may be less inclined to share their data since they believe that other parties could use it to take competitive advantages against them (Steinfield, 2014). Besides that, by exchanging strategic data, companies expose themselves to security breaches conducted by fraudsters who could steal or alter critical information (Soliman & Janz, 2004). As a result, it is challenging to provide security and trust among companies in sharing data through this type of platform (Spiekermann, 2019).

The introduction of new technologies for controlling the operation of data sharing through data marketplace could solve the issues mentioned above. One example is Secure Multi-Party Computation (MPC), which is "a class of cryptographic techniques that allow for secure computation over sensitive data sets" (Volgushev et al., 2019, p.1). In other words, secure MPC allows distrustful parties with sensitive data to perform computations on their data without disclosing them to each other (Lindel, 2019). Thus, secure MPC aims to share knowledge without sharing data (Bestavros, 2017). In fact, every actor involved in the process can obtain the final result of the computation, without providing its raw data. Thanks to this innovative solution, it will be possible to make mutually distrusting parties carry out computations, guaranteeing the protection of their data as well as the authenticity and integrity of the final output (Volgushev et al., 2019).

Despite the several globally recognised benefits introduced by MPC, deploying a performant MPC for practical use is challenging due to the domain-specific expertise required and its poor scalability and efficiency (Choi & Butler, 2019). On the other hand, in recent years, after the development of secure MPC research and the progress of Internet technology and computing capabilities, secure MPC protocols have been greatly improved, allowing to implement them in real case scenarios (Zhao et al., 2019). Although extensive research and technological progress have already supported the development of MPC, it is still unclear what is the contribution brought by its applications, especially in the data marketplace domain.

The practical problem presented in the previous paragraphs can be summarised as follows: in an ever more connected world, data has become a critical strategic resource for the economic success of a company. However, no single actor has all the data necessary for improving the quality of their decisions. B2B data sharing represents an excellent solution to overcome this issue and provide

several benefits for both data suppliers and consumers. In this context, data marketplace is becoming increasingly popular in the business world since it allows more extensive accessibility and easier and more efficient interaction between the parties. Nevertheless, there are several barriers in sharing data via data marketplaces, for instance, lack of trust, security, privacy and transparency. The introduction of privacy-enhancing technologies such as secure MPC could provide a significant contribution to solving these barriers thanks to its unique characteristics. Although extensive research and technological progress have already supported the development of MPC, it is still unclear if it can be applied in the data marketplace domain, especially as an instrument for controlling the platform, and what are the benefits that it could provide for the successful development and diffusion of data marketplaces.

1.2 Literature overview

This study starts from previous researches on data-sharing systems to better understand the B2B data-sharing practice. Afterwards, since data marketplaces enable data sharing in a more open and complex ecosystem rather than between two defined actors in a determined context, it is introduced an overview of digital platforms and platform governance. Then, the MPC literature is presented, with an emphasis on its relationship with data marketplaces and control mechanisms. Afterwards, an overview of the affordance theory and its previous applications is introduced. Finally, the knowledge gap identified in the existing literature is presented.

1.2.1 B2B data sharing

The majority of the studies regarding the practice of B2B data sharing are related with the term of Inter-Organisational Information Systems (IOS). An IOS is a shared information system that enables the data-sharing among two or more companies (Gunasekaran & Sandhu, 2010). IOS can provide several benefits for the firms involved, for instance, cost reduction, higher efficiency and competitive advantage (Steinfield, 2014). Nevertheless, since IOS include two or more organisations, several factors affect the adoption and implementation of the system. Steinfield (2014) identified two types of factors influencing the use of IOS: internal and external. The former included the presence of appropriate human, financial, and technical resources, compatible legacy systems, and business processes, while the latter referred to the level of trust between the companies (Steinfield, 2014).

Soliman and Janz (2004) conducted similar research in order to determine the critical factors that influence the adoption from organisations of this type of system. In their study, the researchers identified the following critical factors: costs, complexity, scalability, support from top management, network reliability, trust between trading partners, and data security (Soliman & Janz, 2004). In this case, the first factors refer to the internal characteristics of an organisation, while the last depends on the environment's features. In particular, they defined network reliability as the capability of a firm to rely on the exchange of its sensitive data with other parties through the network (Soliman & Janz, 2004). Moreover, they noted that data security represents one of the major concerns in terms of confidentiality and fraud to organisations.

Even though it could be easier to satisfy the organisational requirements after significant investments and a radical change, it is hard to establish a strong level of trust and security. In fact, due to the confidential and critical nature of the data exchanged, companies may take advantage of this situation (Steinfield, 2014). Furthermore, by exchanging strategic data such as manufacturing schedules and financial reports, firms may suffer from security breaches conducted by fraudsters who could steal or alter critical information (Soliman & Janz, 2004). Finally, the data gathered by a partner could have been collected through a violation of end-users' information rights, raising concerns about consumer privacy (Soliman & Janz, 2004).

1.2.2 Digital platforms

Data marketplaces represent a specific type of digital platforms (Spiekermann, 2019). Compared to the present IOS systems, data marketplaces presents a more open and complex system and an enormous number and variety of participants (Spiekermann, 2019). Due to this fundamental difference, factors other than trust and security must be considered for its successful diffusion. Platform governance, which can be described as a combination of techniques by which the owner of the platform can influence its participants (Tiwana, 2013), has an essential role in creating a successful digital platform ecosystem (Schreieck et al., 2016). In fact, platform governance aims to reduce the behavioural complexity between the platform’s owner and its participants (Tiwana, 2013). Platform control, which is the main focus of the research, is a dimension of platform governance and refers to how the platform owner verify that the participants behave in conformity with its goals (Goldbach et al., 2018). In order to achieve this target, several control mechanisms such as tools and rules can be introduced by the owner of the platform (Tiwana, 2013).

The concept of platform governance has been extensively studied in digital platform literature (Goldbach et al., 2018), especially in relation with the concept of platform openness (Schreieck et al., 2016). The aim is to understand how platform governance may increase the number of participants, which would contribute to the successful establishment of the platform in the market (Mukhopadhyay & Bouwman, 2019). However, research on governance and control techniques in platform ecosystem settings such as data marketplace is relatively scarce (Goldbach et al., 2018). Indeed, previous studies conducted on control mechanisms can be grouped in the following main areas: within organisations; at the interface between organisations; or in software platform fields (Goldbach et al., 2018). Therefore, few studies apply the concept of digital platform in data marketplaces' settings.

1.2.3 Secure Multi-Party Computation (MPC)

Secure MPC is a privacy-enhancing technology that enables mutually distrusting actors to carry out computations, guaranteeing the protection of their data and the correctness of the final result (Volgushev et al., 2019). Thus, secure MPC could be seen as a possible mean to solve the challenges faced by organisations to share data through data marketplaces.

The concept of secure MPC was first introduced by Yao' s study in 1982. Afterwards, several types of research have been conducted to explore this potential solution. Nowadays, some applications of secure MPC protocols have been implemented in different domains such as the financial, healthcare and the public one (Zhao et al., 2019; Sharemind, 2020). However, the existing literature mainly focuses on how to improve the technology in terms of efficiency and scalability without investigating its possible applications (Volgushev et al., 2019). As a result, there are few implementations of the MPC concept in data marketplace settings. In fact, only two studies related to this topic have been identified: Roman and Gatti (2016) and Roman and Vu (2018). In these studies, the authors conceptualised a data marketplace enabled by smart contracts and secure MPC. Due to this lack of knowledge, it is still unclear how MPC can contribute to the development and diffusion of data marketplaces.

This research aims to describe MPC as an instrument to establish control in data marketplaces, thus creating a safe and trustworthy digital ecosystem where participants can operate without any concern. Thanks to this, it could be possible to solve the aforementioned challenges related to the data-sharing practice and establish data marketplaces successfully in the market. Therefore, there

is a need to understand how MPC could provide affordances to realise platform control within data marketplaces.

1.2.4 Affordance theory

In order to explore the potential introduction of secure MPC in a data marketplace, the concept of affordance theory was applied. In the technology domain, affordances are defined as opportunities that an organisation with a specific goal could realise with a particular technology (Pozzi et al., 2014). In other words, affordances can be described as opportunities generated by the adoption of a specific technology by an organisation. However, the realisation of these opportunities may depend on several factors, such as the perception of the technology and the willingness to change from the current situation (Pozzi et al., 2014). Moreover, the realisation of the opportunities may cause several changes within the organisation (Pozzi et al., 2014).

The affordance theory has been applied in many different settings. Coined by Gibson (1979) in the ecological psychology field to study the relationship and interactions between an actor and his environment, it has recently been applied to several different fields, for instance, the technology one (e.g. IS and ICT), which is the main focus of this research. The majority of the studies in this domain focus on investigating cases where a particular technology have been implemented in a specific organisation (Volkoff & Strong, 2013; Leonardi, 2013; Strong et al., 2014; Hausvik & Thapa, 2017). However, in these studies, they apply the affordance theory in different ways. Volkoff and Strong (2013), Leonardi (2013), and Strong et al. (2014) used the affordance theory to describe the organisational changes caused by the implementation of the technology, while Hausvik and Thapa (2017) focused on the realisation process of the affordances identified. In particular, the latter investigated the factors which could enable or hinder the realisation of the affordances. In their study, they underlined how different types of factors such as intention, motivation, social, and environmental ones could influence the relation between commodities and the freedom of choice to use them to achieve specific goals (Hausvik & Thapa, 2017).

The affordance theory has also been used to investigate the potential adoption of technology by an organisation. For example, Bobsin et al. (2019), in their study, they utilised the affordance theory as a conceptual lens to explore the opportunities created by the adoption of ICT by non-profit organisations. Besides, they identified the barriers that could limit the realisation of the potential benefits provided by the technology in that context. As it can be inferred from Table 1, despite the wide application of the affordance theory in the technology domain, few studies are applying the

affordance approach in the privacy and security domain. In particular, no studies are investigating the affordances provided by secure MPC in any setting. This situation could be explained by the only recent improvement of this technology and its application in several sectors. The research aims to investigate the opportunities in terms of control that secure MPC could offer to a data marketplace provider. Moreover, it focuses on identifying the factors that may affect the realisation of the opportunities and the impacts caused by the introduction of the MPC in a data marketplace.

Reference	Domain
Volkoff & Strong (2013)	Organizational processes
Leonardi (2013)	Organizational processes
Strong et al. (2014)	Organizational processes
Hausvik & Thapa (2017)	Organizational processes
Bobsin et al. (2019)	Organizational processes
Sarfo (2019)	Privacy and security
Santos & Faure (2018)	Privacy and security

Table 1: Affordance theory overview

1.2.5 Knowledge gap

After conducting a literature study on the main concepts of this research, several gaps have been identified in the literature. Firstly, there are few studies regarding the data-sharing practice via data marketplace. In contrast, existing research mainly focuses on data sharing between two defined partners in a determined context. This phenomenon could be explained by the novelty of the application of data sharing practice through digital platforms. Furthermore, even though the literature has widely studied the concept of platform control, research on control mechanisms in platform ecosystem settings such as data marketplace is relatively scarce. Moreover, MPC literature focuses mainly on how to improve MPC in terms of efficiency and scalability without studying its possible applications. As a result, there is a lack of knowledge regarding how MPC can contribute to the development and diffusion of data marketplaces. In fact, there are few applications of secure MPC in the data marketplace domain, and there are no studies regarding the affordances of MPC in any setting.

1.3 Research objective and research questions

1.3.1 Research objective

In this research study, the author aims to investigate the potential adoption of secure MPC by a data marketplace provider for governing its platform and manage the interdependencies of its participants. Discovering how a data marketplace provider can adopt MPC as an instrument for realising platform control is expected to facilitate the diffusion and adoption of this new solution. In fact, through this research, data marketplace's providers may discover an alternative strategy in the pursuit of platform control which can contribute to achieving sustainable economic success for their platform.

1.3.2 Research questions

In order to achieve the goal of this research and address the knowledge gaps previously identified, the main research question was formulated as follows:

"How does MPC enable a data marketplace provider to realise platform control?"

Besides the main research question, it is necessary to develop a set of sub-questions to manage the study. In particular, the information gathered from the answers of each sub-question of this study were utilised to address the main research question. The main research question was divided into the following sub-questions:

1. **"What goals are perceived to be important for data marketplaces providers in terms of platform control?"**
2. **"What are the key features/aspects of MPC that could enable platform control in data marketplaces?"**

As already mentioned in section 1.2.4, an affordance is an opportunity that a company with a specific goal could realise with a particular technology (Pozzi et al., 2014). In other words, affordances can be described as benefits generated by the adoption of a particular technology by an organisation. Therefore, an affordance is generated by the relationship between the goals of the organisation and the features of technology (Pozzi et al., 2014). In this case, the first two sub-questions are instrumental in understanding and identifying the elements of an MPC and a data marketplace that could give rise to an affordance.

3. **"What are the affordances that secure MPC could offer to a data marketplace provider in order to realise platform control?"**

The third sub-question aims to describe the potential benefits in terms of platform control that a data marketplace provider could achieve with secure MPC. In other words, an affordance will be presented as an enabler by which a data marketplace provider can achieve platform control.

4. **"What are the factors that could affect the realisation of the affordances?"**

Since affordances are just potential benefits, their realisation may be influenced by several factors such as the perception that an organisation has towards the technology or the willingness to adopt the technology (Pozzi et al., 2014). The fourth sub-question will provide information regarding the factors which could facilitate or hinder the realisation of the benefits identified in the third sub-question.

5. **"What are the impacts that the realisation of the affordances could cause on the control-related business model elements of a data marketplace?"**

The realisation of an affordance could cause several changes within an organisation (Pozzi et al., 2014). Thanks to the last sub-question, it can be possible to understand the impacts that the realisation of the benefits identified in the third sub-question could have on the control-related business model elements of data marketplaces, such as its market access and its architecture.

1.4 Thesis structure

The thesis report is composed of six chapters. Chapter 1 contains the practical problem, the literature overview of the main concepts of this study and the objectives of the research. Chapter 2 describes the state of the art of the core concepts of this research, which are data marketplace and MPC. Firstly, it presents the concept of data marketplaces, including the product it trades, its definition, types and its challenges in establishing in the market. Secondly, a description of the MPC technology, how it works, its potential and its possible applications, especially in the data marketplace domain, are discussed. Chapter 3 contains the theoretical framework used in this study and its relationship with the concept of data marketplace and MPC. In particular, it explores the concept of platform control, its application in the data marketplace context and its relationship with the computer security concept. Moreover, it investigates the affordance theory and explains how it was used to link the different core concepts and generate the conceptual model of this research.

Chapter 4 describes the methodology used in this research. The chapter starts by presenting the framework of the research and the specific activities conducted during each step. Then, the collection data methodology used in the research, semi-structured interview, is presented. Finally, the data collection process is described in detail, including how the data have been collected and analysed. Chapter 5 contains the result of the qualitative study and the interviews conducted. Firstly, the affordances arisen by the potential use of MPC as a mean to achieve platform control are described. Then, the factors that could affect the realisation of these affordances are presented. Finally, the impacts that the realisation of the affordances could cause on the control-related business model characteristics of a data marketplace are illustrated. In Chapter 6, the main research question and its related sub research questions are answered by elaborating the main findings. Afterwards, a reflection on secure MPC and other security technologies is conducted. Then, the theoretical and practical contributions of this research are described, and the limitations encountered during the study are illustrated. Finally, recommendations for future research are provided.

2. State of the art

In this chapter, the state of the art of literature on data marketplace and MPC is presented. Section 2.1 explores the concept of data marketplaces, including the product it trades, its definition, types and its challenges in establishing in the market. Afterwards, a description of the MPC technology, how it works, its potential and its possible applications, especially in the data marketplace domain, are discussed.

2.1 Data marketplace

2.1.1 Data and its unique characteristics

Before introducing the data marketplace's concept, it is essential to describe the product it trades (e.g. data) and its unique characteristics. Categorising this type of good, assessing its quality and identifying its impacts is radically new in the economic field (Koutroumpis & Leiponen, 2013). Data presents many different properties compared to other tangible products, which cause several challenges for its successful commercialisation both in terms of pricing and protection mechanisms (Spiekermann, 2019). Regarding the pricing mechanisms, data, unlike other types of goods and services information, are categorised as experience goods; the buyer, indeed, has less information concerning the good compared to the seller (Koutroumpis & Leiponen, 2013). As a result, it is challenging for the latter to estimate the real value of the product, and the former could take advantage of this favourable situation (Koutroumpis & Leiponen, 2013). Moreover, data buyers sometimes cannot estimate the real value of data products because they cannot be entirely revealed before being sold (Spiekermann, 2019). This phenomenon is also called Arrow's paradox (Arrow, 1962) and negatively affects the willingness to trade data.

Concerning the protection mechanisms, data belongs to the category of non-rivalrous goods, meaning that they can be used at the same time by many different people in multiple places (Koutroumpis & Leiponen, 2013). Moreover, data are intermediate goods; in fact, they are usually combined and transformed with complementary technologies to produce other products and gain utility (Koutroumpis et al., 2017). As a result, it is challenging to enforce database rights to protect data once the resource is shared (Koutroumpis & Leiponen, 2013). Indeed, database rights can protect only the structure of the database, but not the individual data it contains (Koutroumpis et al., 2017). Therefore, when some analyses are conducted on the data exchanged, it is not clear how to apply the original rights to the final result (Koutroumpis et al., 2017).

The previous paragraphs present several characteristics of data as a product and their impacts on its trade. These are significant factors which must be considered for the realisation of systems that enable the data trade process. In fact, in order to create a successful system, establish it permanently in the market and make data a successfully tradable good, it needs to provide a stable protection regime and mechanisms which can increase the willingness to share data from the data owner.

2.1.2 Definition of a data marketplace

The data market has been characterised by private and commercial data exchanging systems (e.g. IOS) which mainly focuses on data sharing between two defined partners in a determined context (Spiekermann, 2019). This dominance is weakening due to the emergence of multilateral and open data marketplaces (Spiekermann, 2019). Data marketplace represents an alternative solution to share data and information by connecting a large number of participants through a complex ecosystem (Spiekermann, 2019). In particular, this innovative tool allows to the several parties linked via the marketplace to obtain an easier and more efficient interaction thanks to standardised interfaces and services (Spiekermann, 2019). A data marketplace is a digital platform through which data products are exchanged for business purposes (Koutroumpis et al., 2020; Becker et al., 2014). These types of digital platforms act as a neutral intermediary and allow a significant number of parties to share and sell their data as a product (Spiekermann, 2019). Nowadays, the popularity of data marketplaces is rapidly growing due to the need of business to achieve proper information and to the maturation of the data market ecosystem (Fruhwirth et al., 2020). As the number of participants within the platform increases, firms have more opportunities to use external data to improve their business, explore new revenue opportunities and achieve their goals (Muschalle et al., 2013).

Data marketplaces can offer both dynamic and static data and can be accessed by different modes, for instance, repositories, Application Programming Interfaces (APIs) and subscriptions (Fricker & Maksimov, 2017). The data access and usage is controlled by standardised licensing models and regulations established by the data marketplace (Spiekermann, 2019). The ecosystem of a data marketplace is mainly composed of data providers, data buyers, third-party service providers and the marketplace owner. A simplified representation of the ecosystem, its actors and the data flow are described in the figure below.

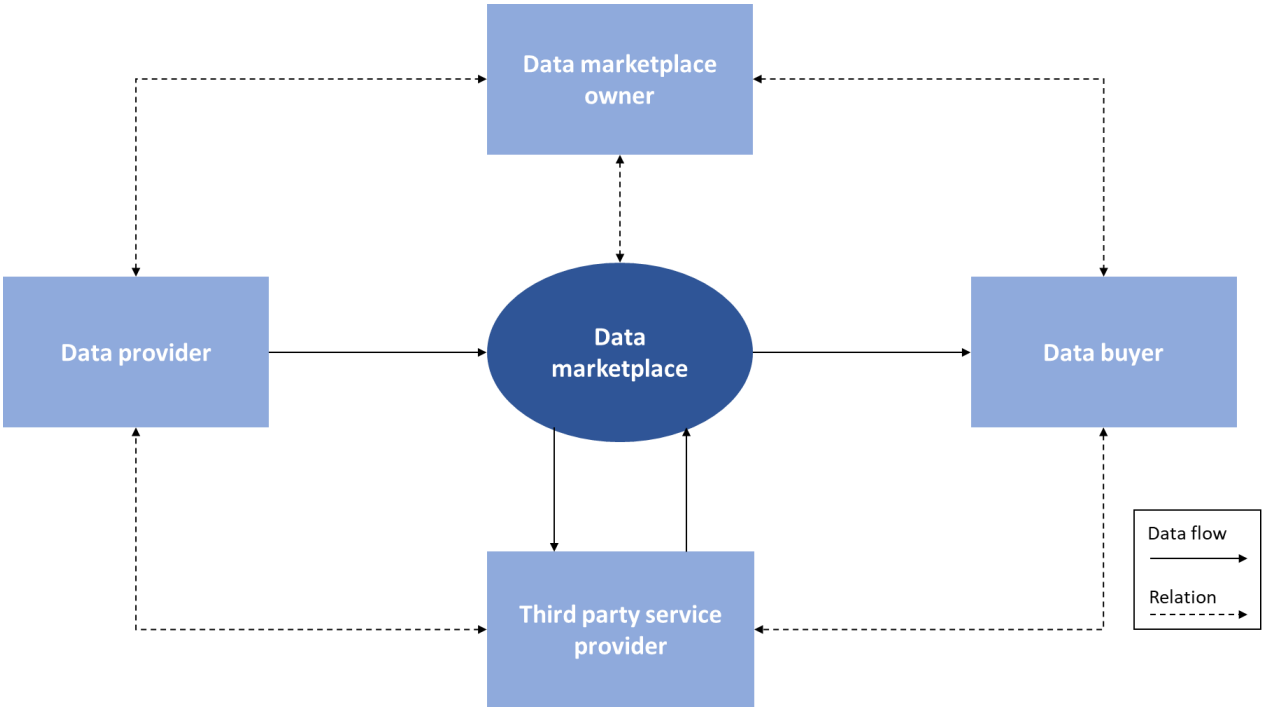

Figure 1: Data marketplace ecosystem, adapted from Spiekerman (2019)

As it can be inferred from the figure, data marketplaces aim to link data providers and data buyers that have mutually compatible interests. The former sell or share its data through the data marketplace in order to monetise them, while the latter search and buy the data present in the platform to achieve their goals. Finally, data marketplaces usually provide third party service providers which can facilitate the exchange process by leveraging data offerings and easing the access and usage of the data for the buyers (Spiekermann, 2019).

2.1.3 Types of a data marketplace

Even though several academic studies have been conducted, there are different definitions of data marketplaces (Stahl et al., 2016). Data marketplaces can differ from each other according to their functionality, type of data traded, architecture, and business model (Spiekermann, 2019). Spiekermann (2019), in his research, developed a taxonomy of data marketplace in which presents the attributes that distinguish the various types of data marketplaces and the different business models adoptable by a data marketplace. The results can be observed in the table below:

Attribute	Characteristics				
Value proposition	Data-centric			Transaction-centric	
Market positioning	Data supplier			Neutral	
Market access	Closed		Hybrid		Open
Integration	Domain-specific			Domain-unspecific	
Transformation	Raw data	Normalisation		Aggregation	Quality assurance
Architecture	Central		Hybrid		Decentral
Price model	Free	Fixed price/subscription	Package	Pay-per-use	Progressive price
Revenue model	Free	Freemium		Flat rate	Fee
	Listing fee	Transaction fee/commission		Service fee	Storage fee

Table 2: Data marketplace taxonomy, adapted from Spiekerman (2019)

According to his taxonomy, data marketplaces focusing on the analysis of the data to achieve new insights are defined as data-centred, while data marketplaces focusing on the exchanging functionality of data products by providing the necessary infrastructure and controlling the trade are referred as transaction-centred (Spiekermann, 2019). Concerning the governance, data marketplaces can be managed by the same parties involved in the trade (e.g. data providers) or by a neutral entity (Spiekermann, 2019). The market access defines the degree of openness of a platform (Spiekermann, 2019). Data marketplaces' owners can restrict access to their platform to only selected partners, or allow unknown participants to operate in the platform (Spiekermann, 2019). Hybrid platforms provide access to new participants that satisfy specific requirements (Spiekermann, 2019).

Data marketplaces can offer a wide range of data coming from different domains, or they can decide to specialise in a particular industry sector (Spiekermann, 2019). Data exchanged in the platform can be unprocessed raw data, normalised data, aggregate data and quality data (Spiekermann, 2019). Regarding the platform architecture, it is possible to distinguish two different approaches: centralised and decentralised (Spiekermann, 2019). In the former, the data are traded through a central location, while in the latter, the data are stored in different locations and kept by the data provider (Spiekermann, 2019). Finally, several pricing and revenue models can be used by a data marketplace.

As previously discussed, this research focuses on how the introduction of secure MPC could change the control-related business model elements of data marketplaces. For this reason, considering the taxonomy presented in table 1, the attributes that could be affected are the following: market access, transformation and architectural design. The implementation of secure MPC in a data marketplace setting may change its degree of openness, increasing the number of participants operating within the platform. In addition, MPC could affect the type of data traded in the platform, shifting from raw data to aggregated data or insights. Finally, MPC could also change the way data marketplaces store data, thus affecting the architectural structure.

2.1.4 Trend and challenges

As already mentioned, new multilateral data trading platforms are increasingly emerging in the data market (Fruhwirth et al., 2020). This type of platform may contribute to the development of an efficient market for data. As discussed by Roth (2008), a market needs to satisfy several requirements to be efficient. Firstly, an efficient market has to ensure thickness (liquidity) which increase the opportunities for both data providers and buyers to have a large selection of possible parties to transact with (Koutroumpis et al., 2020). In other words, a market can be defined as thick when it presents a sufficient number and variety of parties within the platform. Secondly, even though the thickness is a necessary condition, popularity may create congestion, increasing the time for a transaction and reducing the possibility of choosing alternatives. Therefore, in order to create an efficient market, it is necessary to ensure market clearing and quick transactions, but not too quick, since participants must have the opportunity to consider alternatives (Koutroumpis et al., 2017). However, in digital markets, congestion usually is a nonissue (Koutroumpis et al., 2020). Thirdly, it is necessary to create a safe market; the marketplace needs to avoid and detect behaviours that damage and influence other participants. For instance, it is necessary to protect the data, its usage, and prevent sellers from trading with parties that are outside the market (Koutroumpis et al., 2020).

Even though multilateral data marketplaces can achieve market thickness and quick transactions, they suffer from limited safety, thus making data still scarcely traded through this type of platform (Koutroumpis et al., 2020). Present data marketplaces, indeed, fail to satisfy some relevant requirements such as fairness, security, privacy and adherence to regulations (Banerjee & Ruj, 2019), which are necessary for addressing the challenges presented in sections 1.2.1 and 2.1.1, and for creating a safe, trustworthy and successful ecosystem. As a result, it is complicated to establish

data marketplaces successfully in the market (Spiekermann, 2019). This phenomenon can be reflected by the several data marketplaces that have failed recently, for instance, Microsoft's Azure Data Marketplace (Spiekermann, 2019).

2.2 Secure Multi-Party Computation (MPC)

2.2.1 Definition of secure MPC

Secure Multi-Party Computation (MPC) is "a class of cryptographic techniques that allow for secure computation over sensitive data sets" (Volgushev et al., 2019, p.1). In particular, it allows mutually distrusting parties to perform computations, guaranteeing the security and privacy of their data as well as the authenticity and integrity of the final output (Volgushev et al., 2019). The figure below provides an example of how a secure MPC process can be conducted among its participants.

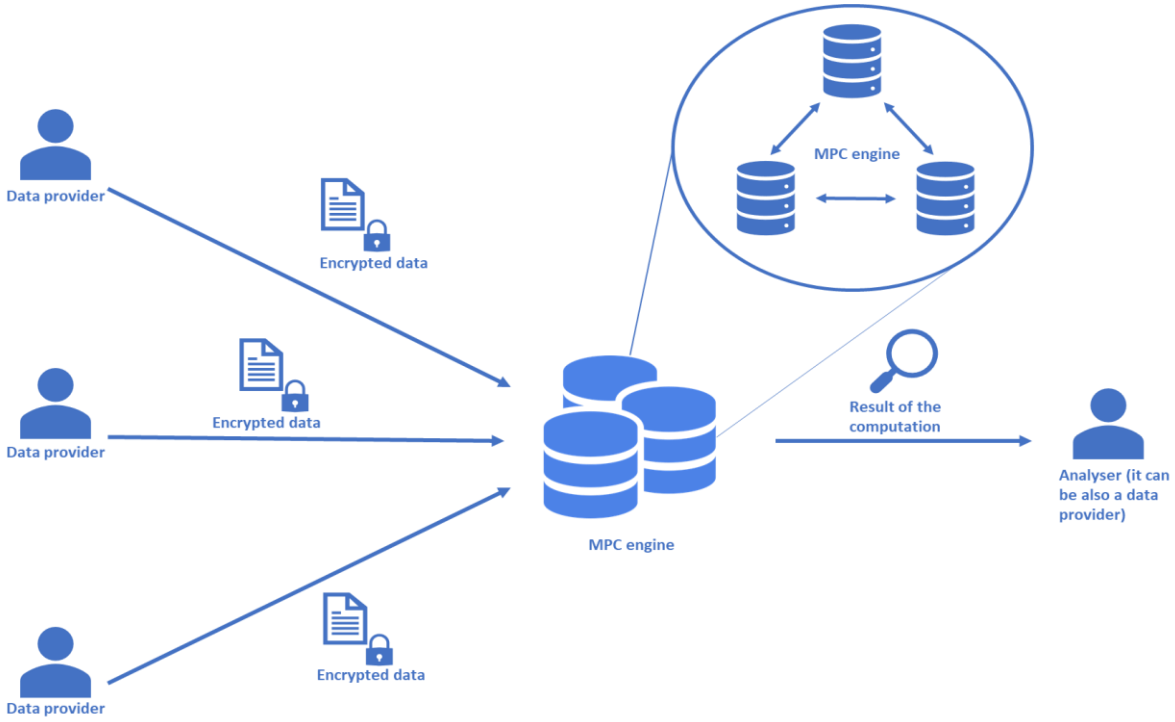

Figure 2: MPC process, adapted from Roman & Vu (2018)

The participants involved in the process can be divided into the following roles: (1) a defined number of data owners who provide the data in an encrypted format for the computation; (2) an automated MPC engine which performs operations on the encrypted data. The MPC engine is constituted by a distributed network of independent and non-colluding servers managed by different parties. No single server can decrypt the original inputs or obtain any information from them since the computation is conducted on encrypted data (Okamura & Teranshi, 2016; Chida et al., 2014); (3)

one or more analysers who receive the encrypted result of the computation (e.g. insights or aggregate data).

The computation is carried out on a pre-agreed function which, once established, cannot be changed (Archer et al., 2018; Lindel, 2019). Therefore, all actors know the use case beforehand and have to agree on starting the process. Finally, it is essential to underline that data are never exposed in a clear form during the process, meaning that only the owner of the data can access to it (Roman & Vu, 2018).

Secure MPC can be applied to several real-world settings. One example could be the supply chain collaboration (SCC), which is defined as a collaboration among two or more organisations to manage and coordinate supply chain activities (Cao & Zhang, 2011). Firms produce goods and services which require supplies from other companies. Usually, a firm decides how much it wants to produce, then it verifies its inventory and makes the orders to its suppliers (The MPC Lounge, 2013). This process is repeated until the top of the supply chain where raw materials are sourced (The MPC Lounge, 2013). It is recognised that this way of operation does not optimise the resources' use (The MPC Lounge, 2013). Each company, indeed, optimises its capacity and stock locally, but the combination of local optimal plans is seldom an optimal plan globally (The MPC Lounge, 2013). In the entire supply chain, several resources are wasted, which cause additional costs for customers and companies (The MPC Lounge, 2013). In order to set an optimal global supply chain plan, companies would have to exchange data among them (The MPC Lounge, 2013). However, parties are not willing to exchange the necessary strategic data such as costs and capacities, because of security and competitive reasons. Secure MPC would significantly contribute to achieving an optimal global supply chain plan by sharing sensitive data without disclosing any relevant information.

2.2.2 The secret sharing technique

Nowadays, the most popular real-world MPC implementations make use of the secret-sharing technique due to its efficiency and its ability to allow more actors to participate in the computation (Pedersen et al., 2007). The idea is that each party split its data into multiple encoded parts known as secret shares. These shares are used for a specific computation and then recombined to get the final output. As a result, thanks to this technique, it is possible to operate the data without revealing any information about it (DeCoste, 2018).

Since the understanding of how the secret-sharing technique works in secure MPC can be complicated, an illustrative example is provided. Three employees want to calculate their average salary without disclosing their salary to each other. Thus, they decide to use secure MPC to achieve their target. Suppose that the three employees earn the following salary: employee1 ($50k), employee2 ($40k), employee3 ($30k). Following the secret sharing process, each employee randomly divides its salary into three secret shares, where the total sum of the shares represents the original salary. The table below describes how the secret shares are generated.

Employee	Secret share 1	Secret share 2	Secret share 3	Salary
Employee 1	15	25	10	50k
Employee 2	-30	50	20	40k
Employee 3	-10	0	40	30k

Table 3: Secret shares

Afterwards, each secret share is sent to a different independent server for the computation phase. The table below shows the result of the secret-sharing process.

Server 1	Server 2	Server 3
15	25	10
-30	50	20
-10	0	40

Table 4: Secret sharing process

It is essential to underline that it is not possible to learn anything from a single secret share since it is just a part of the initial salary. However, these secret shares offer meaningful information when computed. In fact, as it can be seen from the table below, if each secret share is added up, it is possible to obtain three different results.

Server 1	Server 2	Server 3
15	25	10
-30	50	20
-10	0	40
TOT = -25	**TOT = 75**	**TOT = 70**

Table 5: Results of the secret-sharing process

Finally, if these results are summed and divided by three as in the formula below, it is possible to calculate the average salary of the three employees.

$$Average\ salary = \frac{-25 + 75 + 70}{3} = \$40k$$

Thanks to this method, it is possible to know the average salary of the three employees without learning any single input.

2.2.3 MPC robustness towards adversaries

The security and correctness of the MPC protocol depend on the type of protocol and the number of corrupted parties (Eldefrawy et al., 2018). If the number of honest parties is higher than the one of adversaries (honest majority), it is possible to ensure correctness and information-theoretic security, which ensures complete security against computationally unbounded adversaries (Evans et al., 2018; Eldefrawy et al., 2018). If the number of honest parties is lower than the number of adversaries (dishonest majority), the output may not be delivered (e.g. protocol abortion) and it is possible to ensure only computational security, where it is assumed that the participants have limited computing power and that some mathematical problems are unsolvable with that level of power (Halevi et al., 2018; Eldefrawy et al., 2018). In some cases, as demonstrated by Damgard et al., (2011), it is possible to create a fully secure MPC protocol as long as one party remain honest. Therefore, in order to implement an unconditionally secure MPC protocol which delivers a correct output, it is necessary to assume at least one honest party.

Adversaries can be categorised depending on how they are deviating from the protocol. In particular, two kinds of adversaries exist, and each of them defines a different kind of security: semi-honest security and malicious security (Evans et al., 2018). In semi-honest security, the corrupt parties execute the protocol honestly, but at the same time, they could try to gather some information during the communication among the parties (Evans et al., 2018). Semi-honest adversaries can also be considered passive since they try to learn information by observing the protocol execution. For this reason, semi-honest adversaries are usually named as honest-but-curious (Evans et al., 2018). This is a quite weak adversary model, which presents a low level of security in real-world scenarios. However, these types of protocol are relatively efficient and are typically an essential first step for obtaining more secure protocols (Hazay & Lindell, 2010). In malicious security, the corrupt party may voluntarily deviate from the prescribed protocol in order to cheat (Evans et al., 2018). Protocols that ensure security in this model offer a very high-security level as honest parties are protected regardless of the adversarial behaviour of the corrupt parties (Aumann & Lindell, 2007).

Security against malicious active adversaries usually causes a decrease of the efficiency level that brings to covert security, an alternative kind of active security (Aumann & Lindell, 2007). Covert security can be achieved in real-world settings, where active adversaries will not deviate from the protocol because they can be caught (Aumann & Lindell, 2007). This scenario could be the case in many businesses and financial scenarios, where it is difficult to ensure honest behaviour, but where the firms participating in the process cannot sustain the damage to the reputation, negative publicity, and financial penalties related with getting caught cheating (Aumann & Lindell, 2007). Covert adversaries could be described as active adversaries that behave passively because of business concerns (Aumann & Lindell, 2007). Thanks to this solution, it is possible to create safety protocols which are more efficient in practice (Aumann & Lindell, 2007).

2.2.4 Trend and challenges

The secure MPC concept was first introduced by Yao' s study in 1982. Afterwards, several types of research have been conducted to explore the potential of this innovative solution. However, as Choi and Butler (2019) noted, at the current stage it is challenging to deploy a performant MPC for practical use because of the domain-specific expertise required, its poor scalability, its low efficiency and high computational overhead. On the other hand, the increasing development and spread of new technologies, for instance, cloud computing and IoT had increased the popularity of secure MPC (Zhao et al., 2019). At the same time, many applications of secure MPC protocols have recently been implemented in different domains such as the financial, healthcare and the public one (Zhao et al., 2019; Sharemind, 2020) . Therefore, this phenomenon will push more companies and researchers to find new methods to improve this technology and diffuse its adoption. For this reason, it is reasonable to assume that the barriers mentioned above will be overcome in the future.

2.2.5 MPC and data marketplace

In the context of data marketplaces, secure MPC would enable to perform meaningful computations on the data provided by the data owners and sell the result to an interested party, while maintaining the security and privacy of the data. The figure below provides a simplified overview of how the data exchanged a data marketplace would execute the process with the MPC technology and the role of each actor.

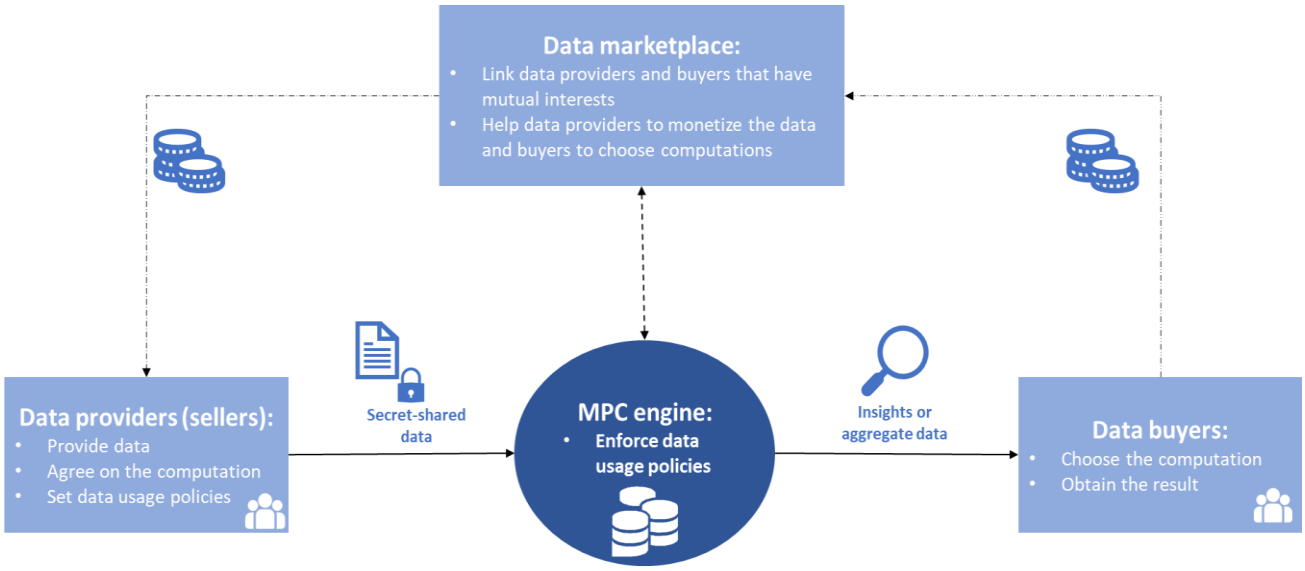

Figure 3: MPC and data marketplace

In this case, data markets would play a role as a broker, matching data demand and data supply. In particular, the data exchange process would present the following steps: (1) the data providers encrypt their data and, after establishing the function of the computation in accordance with the other parties, send the data to the MPC engine; (2) the MPC engine executes the defined computation on the encrypted data; (3) the buyer receives the result of the computation. In conclusion, MPC could be seen as a new solution to increase the level of safety, thus satisfying all the requirements necessary for the creation of an efficient market. This solution would revolutionise how data are exchanged and processed within a data marketplace, possibly pushing more data providers to trade their data through data marketplaces.

3. Theoretical framework

This chapter presents the theoretical framework which was applied to answer the sub research questions and the main one. Section 3.1 explores the concept of platform control, its application in the data marketplace context and its relationship with the computer security concept. The last section investigates the affordance theory, which was used to link the different core concepts and build the conceptual model of this research.

3.1 Platform control

As a digital platform, data marketplace's governance has a crucial role in establishing its success (Mukhopadhyay & Bouwman, 2019). Platform governance, indeed, can reduce behavioural complexity by introducing the mechanisms and procedures that the different participants of the platform's ecosystem have to follow in order to operate in the platform (Tiwana, 2013). Schreieck et al. (2016) in their literature review regarding platform ecosystems identified eight concepts of governance that determine the success of a digital platform: "roles, pricing and revenue sharing, boundary resources, openness, control, technical design, competitive strategy and trust" (p.10).

3.1.1 Control mechanisms

Platform control, which is the main focus of the research, is a dimension of platform governance and refers to how the platform owner verify that the participants behave accordingly to the interests of the platform (Tiwana, 2013). Control is exercised by the platform owner using several techniques such as rules, procedures and incentives that align the behaviour of the participants with the goals of the owner in order to facilitate the coordination among the participants of the platform and improve the overall operation of the platform (Goldbach et al., 2018; Tiwana, 2013). The most commonly used control mechanisms can be subdivided into the following two categories: formal and informal (Goldbach & Kemper, 2014). Formal control can be ulteriorly subdivided into input, process or behaviour and outcome control (Mukhopadhyay & Bouwman, 2019). In input control, several selection criteria, for instance, specific skills, experience and resources are used to establish who is allowed to enter the ecosystem (Mukhopadhyay et al., 2016). In process or behaviour control, the owner sets the appropriate behaviour (e.g. procedures and methodologies) that the participants have to follow (Goldbach et al., 2018). Thus, every participant is monitored and evaluated by the owner according to its behaviour (Mukhopadhyay et al., 2016). In output control,

the owner defines the targets regarding the output requirements and the performance as an objective, which have to be achieved by the participant (Mukhopadhyay et al., 2016).

Informal control can be subdivided in self-control and clan control (Goldbach et al., 2018). In the former, the owner of the platform encourages the participants to establish their targets and self-regulate their tasks in meeting them (Goldbach et al., 2018). In this case, the owner of the platform provides to the participants the necessary information, training, and instruments for self-regulating and self-organising themselves and ensure an adequate level of freedom for making independent decisions (Kirsch, 1996). In the latter, each member of the group behaves similarly and generates comparable outcomes in accordance with the goals and rules that they shared (Goldbach et al., 2018). All the mechanisms mentioned above can be used together, and their combination represents the control portfolio used by a platform owner (Tiwana, 2013). The different control mechanisms, the way they achieve control and their category are summarised in the table below.

Control mechanism	Instrument to achieve control	Category
Input control	Entry selection criteria	Formal control
Process control	Procedures and methodologies	
Outcome control	Performance targets and objectives	
Self-control	Self-regulating activities and targets	Informal control
Clan control	Sharing values and norms	

Table 6: Control mechanisms

Platform control is usually studied with other governance mechanisms. Schreieck et al. (2018) in their study investigated the implications of adopting platform mechanisms differently, and the trade-offs that could emerge. The results showed several trade-offs: for example, they noted that control measures improve trust and perceived risk, but decrease the degree of openness, thus, reducing the number of products and services offered. Choosing the optimal degree between openness and control is critical for the creation and maintenance of a platform (Parker & Van Alstyne, 2017). Opening a system to many participants and reducing platform control may increase the level of diversity and the overall performance of the platform, facilitating innovation (Boudreau, 2010). However, open platforms with a low level of control may increase the risk of introducing low quality and harmful participants (Boudreau, 2010).

3.1.2 Control in data marketplaces

In this research, platform control is described as the whole mechanisms and procedures adopted by a platform owner to create a thriving, safe and trustworthy digital ecosystem in which its participants can conduct their operations, communicate among them and achieve their goals without any risk of being harmed or negatively affected. In particular, in the data marketplaces' context, platform control is instrumental in achieving this goal. Control mechanisms, in fact, have an essential role in protecting the data of the participants and verifying its quality. In other words, platform control in a data marketplace is about managing access to the data among its participants. Koutroumpis et al. (2017) in their study, defined three requirements for the control mechanisms of a data marketplace and its success: boundaries, rules and monitoring.

Firstly, data marketplaces need clearly defined boundaries that allow only to authorised actors to participate in trades over the platform (Koutroumpis et al., 2017). Marketplace boundaries usually define the thickness, also known as liquidity, of the platform; if there are strict boundary conditions, there will be few participants within the platform (Koutroumpis et al., 2017). Controlling the access to a marketplace assure participants about the origins of the data and the reputation of sellers and buyers (Koutroumpis et al., 2017). However, in practice, it may be challenging to achieve this result; in fact, actors may instead trade privately or with unauthorised parties outside of the marketplace (Koutroumpis et al., 2017).

Secondly, data marketplaces require rules that define how data should be used and the consequences of not doing so (Koutroumpis et al., 2017). Rules are essential to guarantee privacy since the diffusion of data has to conform to the current norms present in a determined context (Koutroumpis et al., 2017). These rules provide benefits for both the sellers and the platform. The establishment of the rules can also be done through collective-choice arrangements, where the parties can express their preferences (Koutroumpis et al., 2017). However, these rules do not have to cause congestion within the platform, decreasing the efficiency of the marketplace (Koutroumpis et al., 2017).

Finally, data marketplaces need effective mechanisms that monitor all the operations, including the quality of the data and detect any mistrustful activity (Koutroumpis et al., 2017). These mechanisms should be capable of interrupting the transaction by possible violators and establishing penalties that decrease the damage and discourage future misbehaving (Koutroumpis et al., 2017). Misbehaviour, indeed, may negatively affect the trust on the platform and trades (Koutroumpis et

al., 2017). It is essential to underline that monitoring has to ensure the safe operation of the platform, but without causing congestion and reducing the efficiency of the market (Koutroumpis et al., 2017).

This research aims to describe MPC as an instrument to establish control, in particular process control, in the data marketplace. Thanks to the implementation of this technology, several procedures and techniques that ensure safe transactions and processing of the data would be introduced in a data marketplace. As a result, MPC could improve the level of control of the platform, which could push more data providers to participate and share their data through data marketplaces.

3.1.3 Computer security

Computer security can be defined as "the protection of computer systems and information from harm, theft, and unauthorised use"(Encyclopaedia Britannica, Inc, 2019, p.1). In other words, it is the process of preventing and detecting any unauthorised usage of the computer system (Gollmann, 2010). In the technology context, computer security focuses on implementing the proper mechanisms for enforcing the policies that govern access to sensitive information and their usage (Gollmann, 2010). Computer security is based on the following four pillars: controlling the access to a system, regulating the access to the data present in the system, preserving the data exchanged among different systems, and securing the system against adversaries (Gollmann, 2010).

Computer security is also based on three main properties: confidentiality, integrity and availability (Landwehr, 2001). The first one ensures that information is not revealed without any proper authorisation (Landwehr, 2001). The second one assures that information is not altered without any proper authorisation (Landwehr, 2001). Finally, the third one, guarantees that information is accessible to legitimate users when requested (Landwehr, 2001). Recently, two new properties have been added to the previous one: authentication and non-repudiation (Landwehr, 2001). The former ensures that each actor is who he claimed to be, while the latter assures the demonstration that a specific event or transaction was executed successfully (Landwehr, 2001).

In the computer security context, control is described as a mean to achieve security (Fink, 1994). In particular, the execution of control aims to achieve the objectives presented in the table below.

Objective	Description
Accuracy	Ensuring that data entered and processed in the system remain in exact conformity with the original data
Completeness	Ensuring that all the data remain intact during further processing
Integrity	Maintaining the values of data
Validity	Ensuring the uniqueness of the data
Authority	Allowing only authorised parties to access or change data
Privacy	Ensuring the protection of the data
Audit trail	Tracing the data through the steps of a process to verify the validity and accuracy of the process

Table 7: Control objectives in terms of security, adapted from Fink (1994)

Access control is instrumental in ensuring the aforementioned properties and achieve the objectives in the table (Gollmann, 2010). Organisations present different access control techniques according to the fulfilment of their different needs and the performance level of security they want to ensure. The most common categories of access control are "mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), rule-based access control (RBAC) and attribute-based access control (ABAC)" (Rouse, 2014, p.1). In MAC, access to the information is regulated in accordance with the specific level of security that the information has (Gollmann, 2010; Rouse, 2014). These security level are "unclassified, confidential, secret, and top-secret" (Gollmann, 2010, p. 545). In this case, a subject can access to a specific resource only at its own or at a lower secret level (Gollmann, 2010). In DAC, the owner of the system or the data regulates the access to its data by defining the policies regarding who can access the data and with what purpose he wants to use it (Gollmann, 2010). RBAC is a widely used mechanism where access rights are assigned to individuals depending on their role in the process of a particular business function (Gollmann, 2010). In RBAC, the system's owner sets the rules that regulate access to the data and its usage. Usually, these rules depend on several different factors, for instance, the location and the time (Rouse, 2014). Finally, ABAC is a mechanism that governs the access to the data by establishing a set of rules, policies and relationships (Rouse, 2014). These access rights strictly depend on the characteristics of the user and the data, and environmental factors (Rouse, 2014; Hu et al., 2013). The table below summarises the different types of access control and how the control is executed.

Type of access control	Control mechanism
Mandatory access control (MAC)	Access rights depending on the level of security of the information
Discretionary access control (DAC)	Policies that regulate the access and use of the resources
Role-based access control (RBAC)	Access rights depending on the actor's role in the process in a business function
Rule-based access control (RBAC)	Rules depending on several factors, such as the location or the time of the day
Attribute-based access control (ABAC)	Set of policies based on the characteristics of the user and the information, and environmental factors

Table 8: Types of access control retrieved from Gollman (2010) and Rouse (2014)

Due to the dynamic and distributed environment of current computer systems, traditional access control mechanisms present several limitations in preserving the integrity of the data and ensuring the deletion of the data after that the access period is ended (Lazouski et al., 2010). In this context, the concept of usage control could represent an alternative solution to address these challenges for preserving digital resources. Usage control is considered the next generation of access control and is utilised to enforce rules regarding the usage of digital resources (Park & Sandhu, 2004). Therefore, it is related to data processing instead of data access. It is essential to underline that usage control is not a substitute of access control (Park & Sandhu, 2004); in contrast, they could be seen as two complementary aspects that could be used to achieve complete computer security.

The computer security field offers an alternative perspective compared to the platform one on which analyse the potential introduction of secure MPC within a data marketplace. As previously discussed, the management of the access to the resources of a data marketplace and their usage is instrumental in creating a safe and trustworthy digital ecosystem in which its participants can operate without any concern. In this case, MPC could be used by a data marketplace provider as an enforcer of the policies established by the data's owner, which would regulate the access and usage of the data among the participants of the platform. As a result, data marketplaces would achieve a level of attribute-based access control and usage control by which they will be able to improve the security of their system, thus giving to data owners a more sense of control over their data during the processing and transaction of the data.

3.1.4 Conclusion

Both the theory regarding platform control and computer security offer a way to study the potential implementation of MPC in data marketplaces and the benefits it could provide to the ecosystem. The former focuses on establishing the procedures and methodologies that align the behaviour of the participants with the platform owner's goals. In contrast, the latter focuses on regulating the access and use of the data present in the system. As it can be noticed from the figure below, secure MPC could be seen as an enforcer for both these mechanisms, contributing to the increase of the level of security and trust of the data marketplace and possibly pushing more data providers to participate in the ecosystem.

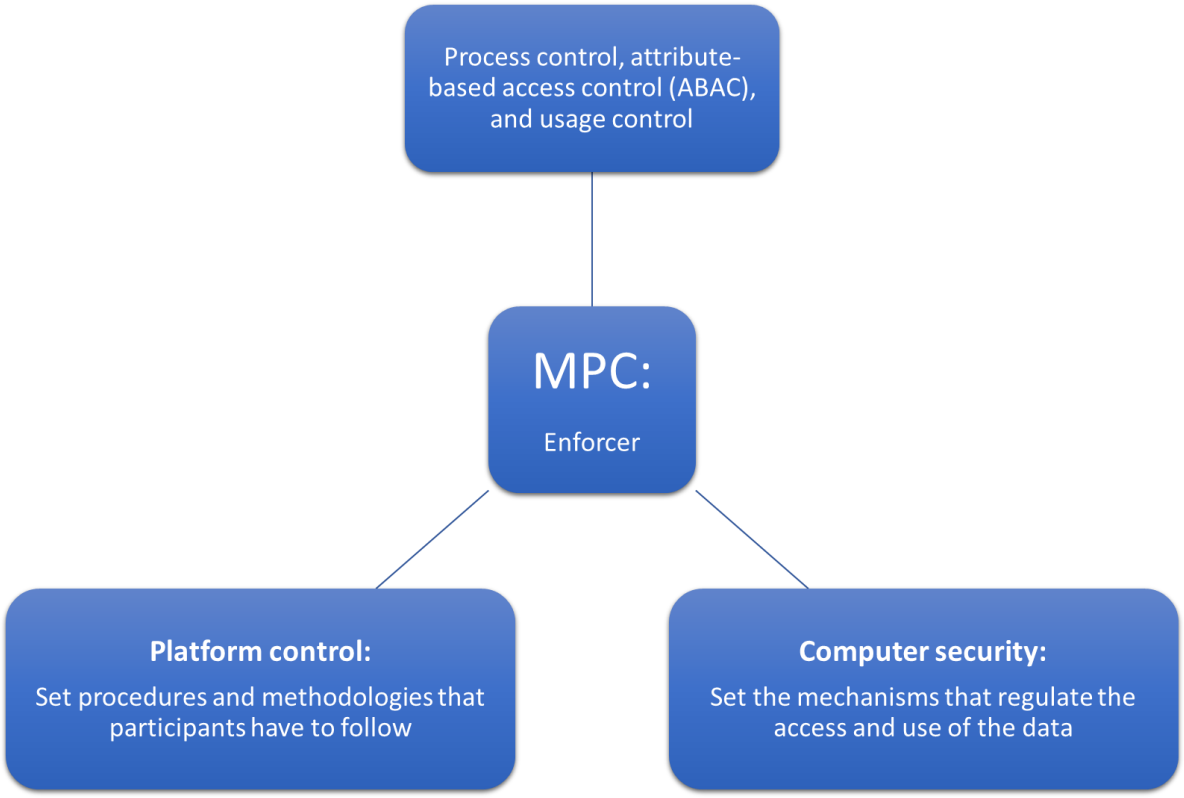

Figure 4: MPC relationship with platform control and computer security

3.2 Affordance theory

The first study that introduced the concept of affordance was originated by Gibson (1979). In particular, he described an affordance as a potential action that an actor can perform in a particular environment (Gibson, 1979). Afterwards, Hutchby (2001) introduced the affordance concept in the technological domain, which is the main focus of this research, exploring how this theory could be used to analyse the relationship between actors and technologies. The application of the affordance

theory in the technology context generates two implications. Firstly, studies do not consider only individuals as actors involved in the relationships, but also organisations (Pozzi et al., 2014). Secondly, affordances are called technology affordances and are defined as opportunities that an organisation with a specific goal could realise with a particular technology (Pozzi et al., 2014).

Pozzi et al. (2014) presented a theoretical framework based on the affordance theory in the technology context, describing it as a time dependent process characterised by different phases. This framework includes actors, which are the organisation and the IT artefact, constructs that define the different phases of the process, and temporal-causal relationships between them (Pozzi et al., 2014). As it can be noticed in the figure below, the process can be divided into the following phases: "affordance existence, affordance perception, affordance actualisation, affordance effects" (Pozzi et al., 2014, p.6).

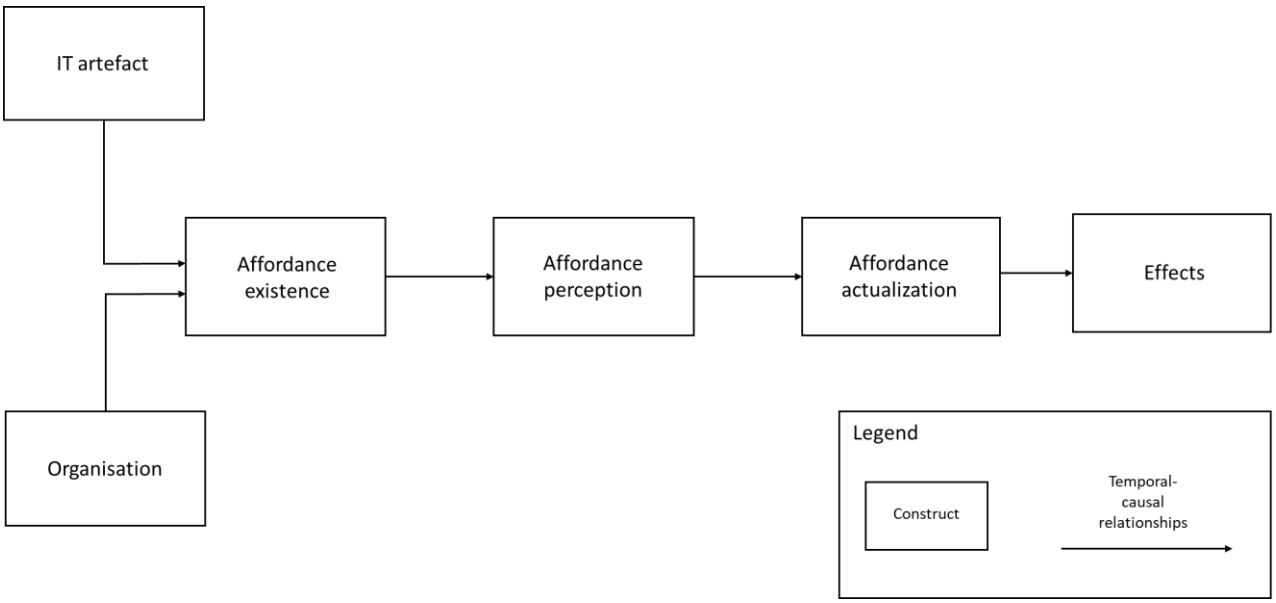

Figure 5: Affordance theoretical framework adapted from Pozzi et al. (2014)

3.2.1 Affordance existence

As it can be inferred from figure 5, affordances are created from the unique relationship between the technology and the organisation. In fact, an affordance can be described as the amount of possibilities generated by a technolgy (Markus & Silver, 2008). Thus, affordances are specific to a particular company and technology (Zammuto et al., 2007). It is essential to underline that affordances exist despite the recognition, perception, and information of the actor toward the technology (Pozzi et al., 2014). For example, a camera affords an actor to record something.

3.2.2 Affordance perception

In order to exploit the potential of affordances, they must be perceived by the actor (Pozzi et al., 2014). The affordance perception step can be described as a recognition phase during which information for identifying objects and events are collected by an actor (Greeno, 1994). This phase could be influenced by the following factors: objects' features, actor characteristics, actor's goal, and external information (Pozzi et al., 2014). In fact, an actor perceives the affordance as an opportunity to improve the performance of an action and achieve his goal only depending on his unique characteristics (Pozzi et al., 2014). As a result, the total amount of existing affordances provided by a techology is never entirely and instantly perceivable by an actor (Hutchby, 2001). Given the aforementioned example, the actor may not recognise that the camera enables him to record something because of his characteristics.

3.2.3 Affordance actualisation

The actualisation phase starts when an actor undertakes the possible action to realise the perceived affordance and achieve his target (Strong et al., 2014; Volkoff & Strong, 2013). Put differently, the actualisation can be described as the realisation of the opportunity arisen by the relation between an actor and the object. Also in this case, the actualisation phase strictly depends on the specific goals and characteristics of each actor (Strong et al., 2014). Therefore, some of the affordances perceived by the actor may not be realised. The actualisation process can be influenced by the presence of several factors which can facilitate or hinder the realisation of the potential action (Pozzi et al., 2014). Pozzi et al. (2014), identified the following factors: (1) the technology's features, (2) the realisation of past affordances, (3) the capability of the company to understand the technology, (4) the level of knowledge regarding the technology, (5) the company's capability to recognise an affordance, (6) the difficulty of the realisation, also known as the degree of effort required (Bernhard et al., 2013), (7) the organisations' ultimate goals, (8) the structure of the company and the environmental demands, and (9) the willingness to change.

3.2.4 Effects

The actualisation of the affordance can cause several changes within the organisation in both the short and long term (Pozzi et al., 2014). The realisation of the potential actions may cause the following consequences: (1) facilitating the generation of further affordances, (2) developing further IS features, and (3) causing organisational changes (Pozzi et al., 2014). It is essential to underline

that the actualisation and its related impacts on the organisation are specific to the technology and the company involved in the process (Zammuto et al., 2007; Strong et al., 2014).

3.2.5 Conclusion

The affordance theory represents a useful model for understanding the potential adoption of MPC as a mean for realising platform control in data marketplaces. In fact, it is more suitable for exploring the potential integration of technology in a corporate context compared to other frameworks such as the Technology Acceptance Model (TAM) and the Capability Approach, which focus on the individual acceptance of the technology. Firstly, it can contribute to identifying all the possible affordances that the different features of the MPC technology could offer to a data marketplace provider in terms of platform control. For example, since an MPC allows an actor to insert his data only in an encrypted form and a data marketplace provider has the goal of ensuring data protection and data privacy, then the data marketplace provider will have the possibility to preserve the data inserted by an actor.

Secondly, the affordance theory can contribute to understanding the main factors that can affect the achievement of the expected benefits offered by the adoption and use of the MPC from a data marketplace provider in order to control its platform. In fact, since affordances are only potential actions, they need to be actualised in order to obtain the technology affordances. The actualisation of an affordance, which is the realisation of the potential action, depends on several factors that could facilitate or hinder it. In this context, it is possible to predict some of the factors that could affect the realisation of the aforementioned potential actions. For example, a data marketplace provider could perceive the technology as an opportunity to improve its platform and achieve its ultimate goals. This result could push a data marketplace to adopt the MPC, and therefore to realise the actions. On the other hand, adopting an MPC could be expensive and time-consuming, which negatively affect the decision to adopt an MPC by the data marketplace provider.

Finally, the affordance theory can contribute to understanding the impacts that use of the MPC technology as a mean for platform control could cause on the control-related business model elements of data marketplaces. Considering the taxonomy of a data marketplace offered by Spiekermann (2019) in table 1, the main control-related attributes that could be affected are the following: market access, transformation and architectural design. Firstly, since MPC allows to ensure the security of the data, data marketplaces would probably change their degree of openness (e.g. market access) and allow a large number of unknown participants to operate in their platform.

Secondly, since MPC allows the data consumer to receive only the final result of the computation, MPC could also change the type of data that is traded in the platform, thus shifting from unprocessed raw data to insight or aggregate data. Finally, MPC could also change how data marketplaces store the data, switching from a centralised architecture to a decentralised one.

3.3 Conceptual model

As a result of the literature study conducted regarding the core concepts of this research, a conceptual model has been developed, following the one offered by Pozzi et al. (2014) (see figure 5). In this case, the affordance approach is instrumental in investigating the potential adoption of secure MPC by a data marketplace provider for realising platform control. The model is presented as a time dependent process characterised by different phases. This process includes the actors which are the data marketplace provider and the MPC, constructs that define the different phases of the process, and temporal-causal relationships between them. The relations between the concepts contained in the conceptual model and the aforementioned sub-research questions are described in the figure below.

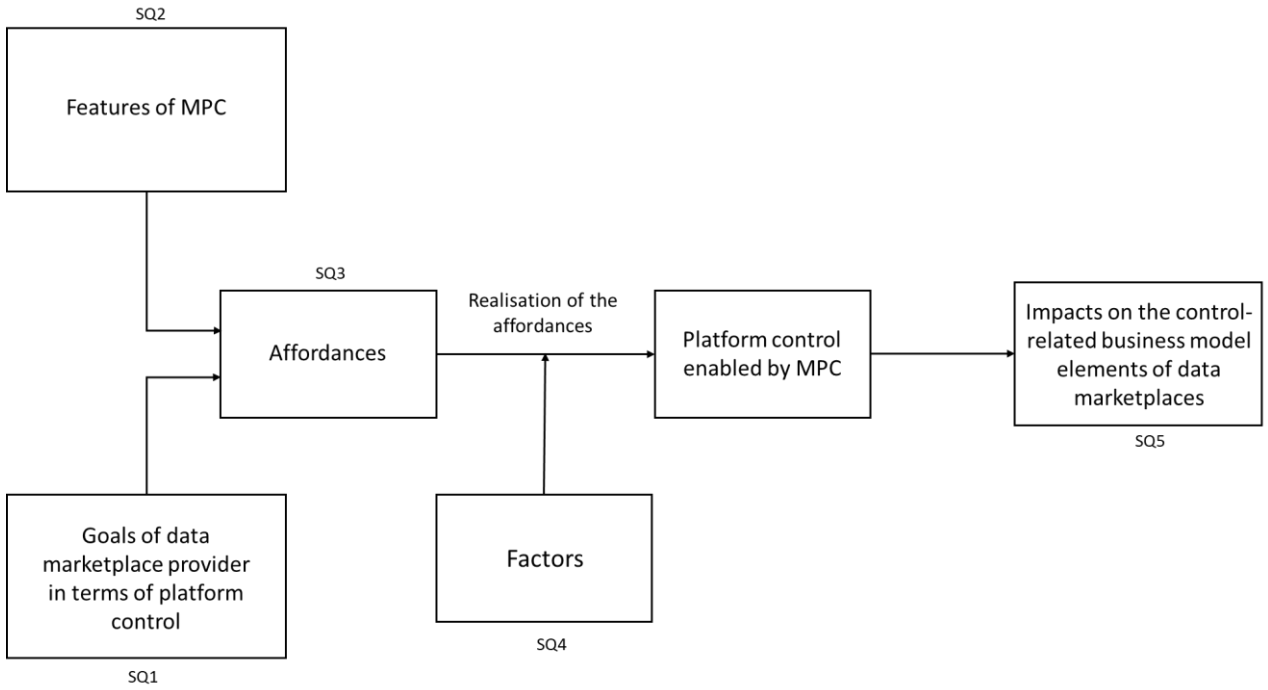

Figure 6: Conceptual model and sub research questions

As it can be inferred from figure 6, the affordances are generated by the relation between the features of the MPC and the data marketplace provider's goals in terms of platform control. Since

affordances are only opportunities that an organisation with a specific goal can realise with a particular technology (Pozzi et al., 2014), their actualisation process, which is the realisation of the potential actions, strictly depends on several factors, as explained in section 3.2. By applying the affordance theory in this context, it is possible to predict several factors that may facilitate or hinder the actualisation process of the affordances arisen such as the perception that a data marketplace provider has towards the MPC. Finally, it is expected that the realisation of the potential actions could cause several impacts on the control-related business model elements of a data marketplace, for instance, its market access and its architecture.

4. Methodology

The chapter starts by presenting the context and the domain of this study. Afterwards, the framework of the research, its strategy and the specific activities in each step are described. In particular, the collection data methodology used in the research, semi-structured interview, is presented explaining the method, why it is suitable for this research, and what are the advantages and disadvantages from using it. Finally, the data collection process is illustrated in detail, including how the data were collected and analysed.

4.1 Context of the research

4.1.1 The project

This study belongs to an EU-project project called Safe-DEED (Safe Data-Enabled Economic Development), which has been funded by the European Union's Horizon 2020 research and innovation programme (Safe-DEED, 2019). This project combines several parties from different fields across Europe, such as data science, business innovation, and cryptography, to improve security technologies, trust and the diffusion of privacy-enhancing technologies (Safe-DEED, 2019). The research aims to generate trust and security in data markets through the development of secure MPC technology, thus encouraging data owners to share their data and generates benefits for themselves and their customers (Safe-DEED, 2019). The Safe-DEED project contributed to reaching the final goal of this research through the exploitation of its network during the data collection phase.

4.1.2 The domain

The research focuses on data marketplace operating in the mobility domain. The choice of the mobility domain is twofold: the presence of sensitive data and the wide range of opportunities provided by the data exchange practice. In today digitally connected world, several different types of data are produced every day by all the devices present in a vehicle. By moving in its surroundings, indeed, vehicles through their sensors gather a considerable number and variety of data regarding the environment, mobility, driver and passengers and vehicle's condition (AutoMat Project, 2018a). As the number of sensors present in the car grows, the amount of useful data usable in the future will increase, following the same path (AutoMat Project, 2018a). The large amount of data collected continuously can offer several opportunities for different sectors such as automotive, transport and the public one (AutoMat Project, 2018b).

Firstly, the combination of different commercial data collected from the web and the on-board computers enables the distributors to create unique tailored offers for their customers (AutoMat Project, 2018b). Secondly, the data related to the condition of the vehicle gathered from the sensors present in the car allow constructors to provide a more efficient and reliable car, thus improving the level of customer satisfaction among their clients (AutoMat Project, 2018b). Finally, the data collected could be used by municipalities to obtain several benefits, for instance, improved traffic flow, higher traffic efficiency, less noise and emissions, more traffic safety (Manzi, 2017).

Data marketplaces can facilitate the realisation of the benefits mentioned above by linking data providers and data buyers that have mutual interests. However, despite the several potential advantages provided by the data-sharing practice in the mobility domain, especially in the data marketplace context, there are several challenges regarding its realisation because of privacy and security concerns. Secure MPC could significantly contribute to solving these issues by sharing sensitive data without disclosing any relevant information.

4.2 Research framework

The research framework explains how the research was conducted in steps. An overview of the research flow is provided in the figure below.

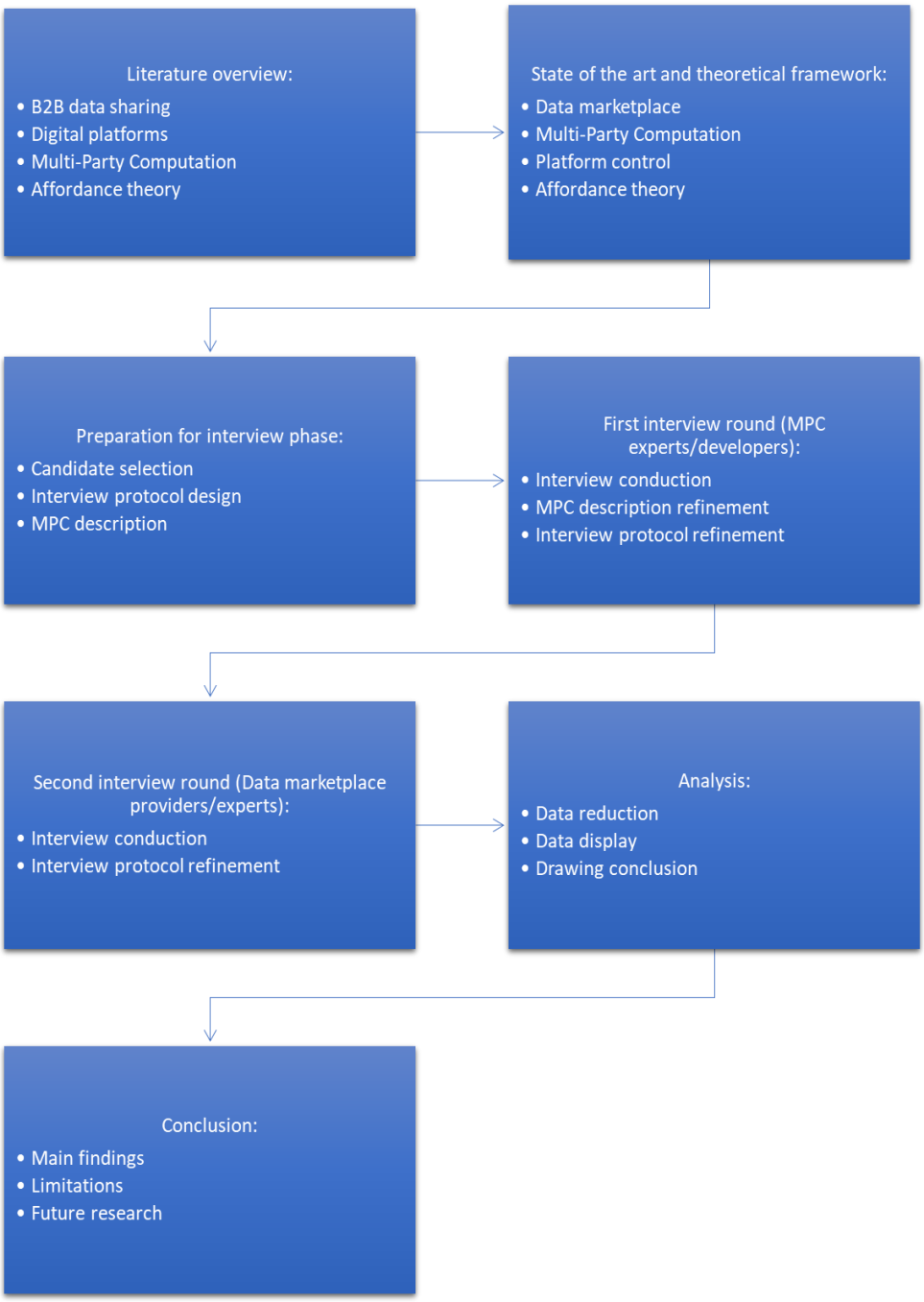

Figure 7: The research framework

In the first phase, a study on the existing literature regarding the data sharing practice, its execution through digital platforms, the MPC technology, and affordance theory was conducted. Afterwards, the core concepts of this research (e.g. data marketplace, MPC, platform control and affordance theory) were analysed. The final output of the literature study is the conceptual model introduced in section 3.3, which represents the base of this research. Afterwards, a qualitative study was conducted through semi-structured interviews to explore how MPC may enable platform control in data marketplaces. Before starting the interview phase, a list of candidates together with the

interview design protocol and the MPC description document were developed. The first round of interviews was conducted among MPC experts and developers to have a better understanding of the technology, improve the MPC description that was sent to the data marketplace providers and experts and validate it. Moreover, the first interviews were also used to refine the questions of the interview protocols. Then, the second round of interviews was carried out among data marketplace providers and experts. Finally, the data collected from the qualitative study were analysed in order to present the results of the research, answer the research questions and provide some potential recommendations for future research.

4.3 Research strategy

The exploratory nature of this research required to conduct a qualitative study to address the practical problem and answer the main research question. In fact, the concept of affordance theory has never been applied to the platform control one, and there is a lack of research on platform control theory in a data marketplace. Moreover, there are few studies regarding the use of MPC in data marketplace settings. The main research strategies that can be undertaken are the followings: "experiment, survey research, observation, case studies, grounded theory, action research, and mixed methods" (Sekaran & Bougie, 2016, p.96).

Given the specific characteristics of this research, including its category, the type of data needed, and the time constraint, the strategy that was adopted was survey research. A survey is a widespread research strategy method commonly undertaken in exploratory and descriptive studies to gather qualitative data and use them to answer several different types of research questions (Sekaran & Bougie, 2016). In this strategy, data can be collected through questionnaires, interviews and observation (Sekaran & Bougie, 2016). Other strategies that were considered are case studies and grounded theory, but they were discarded for several reasons. Since there are no real-world cases where a data marketplace provider uses MPC in his platform, it was not possible to adopt the case study strategy. Moreover, even if the grounded theory can provide several advantages, it requires a considerable time investment, and it can be challenging to be reported.

4.4 Data collection

4.4.1 Data collection method

The research method adopted in this study to collect qualitative data was the interview one. The choice of undertaking interviews instead of a questionnaire can be explained by the fact that the

exploratory nature of the study makes it impossible to do a structured survey. Furthermore, it allows to assess the validity of answers provided by the interviewees by observing nonverbal signals, and it ensures that each informant answers all the questions without receiving any assistance from others (Louise Barriball & While, 1994). Finally, the interview method is usually used in exploratory studies (Sekaran & Bougie, 2016).

Regarding the type of interview, given the limited amount of time available, semi-structured interviews were carried out to answer the sub-questions and lastly the main research question. In fact, the use of a set of questions prepared in advance, accompanied by some follow-up questions in accordance with the answers of the respondent, enables to make the interview more flexible and gather more insights by each informant compared to a structured interview (Sekaran & Bougie, 2016). Moreover, semi-structured interviews are less time and effort consuming compared to the focus group ones (Sekaran & Bougie, 2016).

Due to the wide diversity of locations of each informant, all the interviews were conducted by telephone or video calls. Compared to a face to face interview, several advantages can be achieved by telephone interviews. In fact, it allows to reach a high number of informants in a relatively short timeframe and it avoids that the respondent could feel unease (Sekaran & Bougie, 2016). However, by undertaking telephone interviews there could be the possibility that the informant interrupts the interview in advance (Sekaran & Bougie, 2016). Furthermore, during a telephone interview, it may be more challenging to ensure that the interviewees have correctly understood the question and detect any nonverbal signal from the respondent (Sekaran & Bougie, 2016).

The interviews were carried out among data marketplace providers operating in the mobility domain, data marketplace experts and MPC developers/experts with a high degree of decision-making authority and knowledge regarding the business. The interview questions were based on the conceptual model of section 3.3 and its related sub research questions. The list of the interview questions is shown in the two tables below. In particular, from the tables below it is possible to understand the contribution of every question in answering the sub-research question and their relationship with the affordance theory.

Interviewee: Data marketplace provider	Sub-research questions	Affordance theory step
1. What is your idea about the landscape of data marketplaces?	SQ1, SQ3	Affordance existence
2. From your perspective, what is the meaning of control in the context of data marketplaces? ○ Why or why not do you want to exercise control? ○ What do you want to achieve from it? ○ What could be the main challenges in achieving it?		
3. Which features/aspects of the MPC technology are relevant for you? Why?	SQ4	Affordance perception and actualisation
4. Considering your current situation, how big is your need for this technology? Why?		
5. What are the conditions that would need to be present in order to be able to implement the MPC technology in your platform? Why are these conditions necessary?		
6. Do you think MPC can help you to achieve your ultimate goals? Why or why not? ○ If yes, how do you think this technology can help you? If no, how should it be improved in a way that it can help you? ○ Do you think it will improve your ability in controlling the platform? Why or why not? ○ Who else do you think could benefit from it? Are there any other parties who would benefit from it? Why?		
7. Assuming you have decided to implement the MPC in your platform. How significant will this change be for your platform? Why?		
8. Assuming you have decided to implement the MPC in your platform. How likely will this change the way your platform works? Why? ○ How will this change the way your platform works? ▪ How will the participation in the data sharing process via your platform change? ▪ How will the type of product traded in your platform change? ▪ How will the way your platform store data change?	SQ5	Effects
9. How likely would you adopt the MPC in your platform (now or in the future)? Why?		

Table 9: Interview questions (data marketplace provider)

Interviewee: MPC developers/experts	Sub-research questions	Affordance theory step
1. Could you give a general overview of what MPC is? ○ What do you think about my description of MPC? Is there any relevant aspect missing? If yes, which one is missing?	SQ2, SQ3	Affordance existence
2. How is the MPC process conducted? ○ How does MPC ensure the protection and the privacy of the data? ○ How does MPC provide access to the process and its result? ○ How does MPC ensure that only authorised operations are conducted? ○ How does MPC ensure the proper usage of the data and the purpose of the computation? ○ Can MPC track and record each operation? If yes, how?		
3. What happens if the data inserted by an actor is corrupted? ○ Can MPC detect it? If yes, how? ○ Does the presence of corrupted data affect the result? Why or why not? ○ How is this situation communicated to the actors? ○ Can the computation be resubmitted? If yes, how?		
4. What happens in the presence of a malicious actor? ○ Can MPC detect him? If yes, how? ○ Does the presence of a malicious actor affect the result? Why or why not? ○ How is this situation communicated to the actors? ○ Can the computation be resubmitted? If yes, how?		
5. How do you see the potential implementation of MPC in data marketplaces?	SQ4	Affordance perception and actualisation
6. What are the conditions that would need to be present in order to be able to implement the MPC technology in a data marketplace? Why are these necessary?		
7. What could be the main challenges for an organisation in adopting this technology?		

Table 10: Interview questions (MPC experts/developers)

4.4.2 Participants

Given the low number of data marketplace providers present in the market, and the low number of MPC experts or developers, the type of sampling that was used to select the participants in this research was judgement sampling. Judgment sampling is a category of purposive sampling that is usually adopted if there are few candidates who could provide the information needed for the research (Sekaran & Bougie, 2016). By undertaking this strategy, it is possible to reach the informants who are more easily accessible (Sekaran & Bougie, 2016). Besides, recommendations

about additional potential interviewee were asked at the end of each interviewee, following the snowball sampling method. The following types of candidates were selected:

- Data marketplace providers operating in the mobility domain: people with a high degree of decision-making authority and knowledge regarding the business
- Data marketplace experts: people with expertise regarding the data marketplace field
- MPC experts and developers: people with expertise regarding MPC and its applications, and people who are working in companies that develop MPC solutions

The candidates were invited through email or Linkedin invitations in which was explained the research topic and its aim. Moreover, a brief description of the MPC technology was attached to the invitation. Databases such as Datarade (Datarade, 2020) were used to identify more data marketplace providers. The first round of interviews was conducted among MPC experts and developers. Starting from MPC experts and developers was instrumental in having a better understanding of the technology, improving the MPC description that was sent to the data marketplace providers and validate it. Moreover, in order to achieve a better result, the first interviews were used to refine the interview protocol created at the beginning. The invitations and the interview protocols can be found in the Appendix. Out of 63 invited candidates, the ones who accepted to be interviewed are presented in the table below. In the table it is also indicated their role, the institution where they work and the category of this research to which they belong.

Interviewee (I)	Role	Institution	Category
I_1	Cryptography specialist	Independent research organisation	MPC expert
I_2	Post-doc researcher	University	MPC expert
I_3	CPO	MPC company	MPC developer
I_4	Full professor	University	MPC expert
I_5	Senior cryptography engineer	Independent research institute	MPC expert
I_6	Software developer	MPC company	MPC developer
I_7	CTO	Data marketplace	Data marketplace provider
I_8	Datamatch advisor	Data marketplace	Data marketplace provider
I_9	Head of adoption	Association	Data marketplace expert

I_{10}	Scientific assistant	Research institute	Data marketplace provider
I_{11}	Senior research scientist	Independent research institute	Data marketplace expert
I_{12}	Founding partner	Independent advisor	Data marketplace provider
I_{13}	Partner	Independent advisor	Data marketplace provider

Table 11: Interviewees

4.4.3 Interview process

As previously discussed, the interviews were all conducted by telephone or video calls. Each interview was recorded and subsequently transcribed and submitted to the interviewee and asked to be validated. A word document containing the description of the MPC was sent in advance attached to the invitation in order to prepare each informant. The reason to choose a word document and let them read it themselves instead of using a PowerPoint presentation and explaining the MPC at the beginning of each interview was to reduce the length of the interview and have more time for asking the questions. All the interviews started with a brief introduction of the research's topic and its purpose in order to make the interviewee understand the core concepts. Before starting the interview, each interviewee was asked if they had the chance to read the document. In case they did not read it, a brief description of the research and the relevant concepts were verbally explained. Following the semi-structured approach, each interview was conducted by asking a set of previously prepared questions and some follow-up questions depending on the interviewee's answers.

The criteria adopted for interrupting the data collection phase was the saturation principle, when no additional insights or information emerge from the interviews, or when the answers become repetitive (Miles & Huberman, 1994). Regarding the first round of interviews with MPC experts and developers, the theoretical saturation principle was reached. On the other hand, it was not possible to reach the saturation principle concerning the fourth sub-research question of this study during the second round of interviews because of the limited timeframe available for the data collection phase and the difficulty in reaching informants.

4.5 Data analysis

Each interview was immediately transcribed after it was conducted in order to capture insights, refine concepts and use them in the subsequent interviews. Thanks to this, it was possible to

improve the quality of the interview protocol during the collection data phase. Despite this, the data analysis phase started after conducting all the interviews.

The collected data were analysed following the steps described by Sekaran and Bougie (2016): "data reduction, data display and drawing conclusions" (p.333). Firstly, given the large amount of data gathered, the data reduction phase was carried out through coding and categorisation. During this phase, the qualitative data collected were analysed in order to create codes and categories. Codes are labels that assign a symbolic meaning to a specific piece of text and can be grouped to develop categories (Sekaran & Bougie, 2016). An initial list of codes and categories was generated inductively thanks to sections 2.2, 3.1 and 3.2 (see the table below).

Categories	Codes
Preserving the data	Accuracy
	Privacy
	Completeness
	Integrity
	Encryption
	Information-theoretic security
	Computational security
	Secret sharing
Enabling data ownership	Access control
	Terms and conditions
	Usage control
	Agreement protocols regarding the participants before starting the computation
Preserving the process	Audit trail
	Autonomous computing system
Perception of the technology	Knowledge of the technology
	Recognition of the affordances
Degree of effort required	Change of the system required
	Difficulty of the implementation
Need for the technology	External demand
	Contribution for achieving ultimate goals
	Willingness to adopt the MPC
Impacts on the control-related elements of the business model	Degree of openness
	Product traded
	Data storage

Table 12: Initial list of codes and categories

However, the initial list was changed and refined deductively during the qualitative data analysis process since, for example, new categories and codes emerged, and definitions of initial categories and codes changed. As argued by St John and Johnson (2000), the data reduction performed through qualitative data analysis software, such as Atlas.Ti and Nvivo could introduce several concerns such as prioritising of coding, distractions during the data analysis, time and energy spent to learn how to use the software and focusing on the amount of the data instead of its meaning. Therefore, in this research, it was decided to conduct the qualitative analysis by using Word. Following the data reduction process, each transcript was carefully analysed, and each code was assigned to its corresponding unit of text by using the comment function. The data reduction process was composed of three rounds. During the first round, all the transcripts were carefully read without coding in order to become more familiar with all the documents. Afterwards, two rounds of coding were carried out to generate codes and categories and update the initial list. An example of how the coding process was conducted via Word is provided by the figure below.

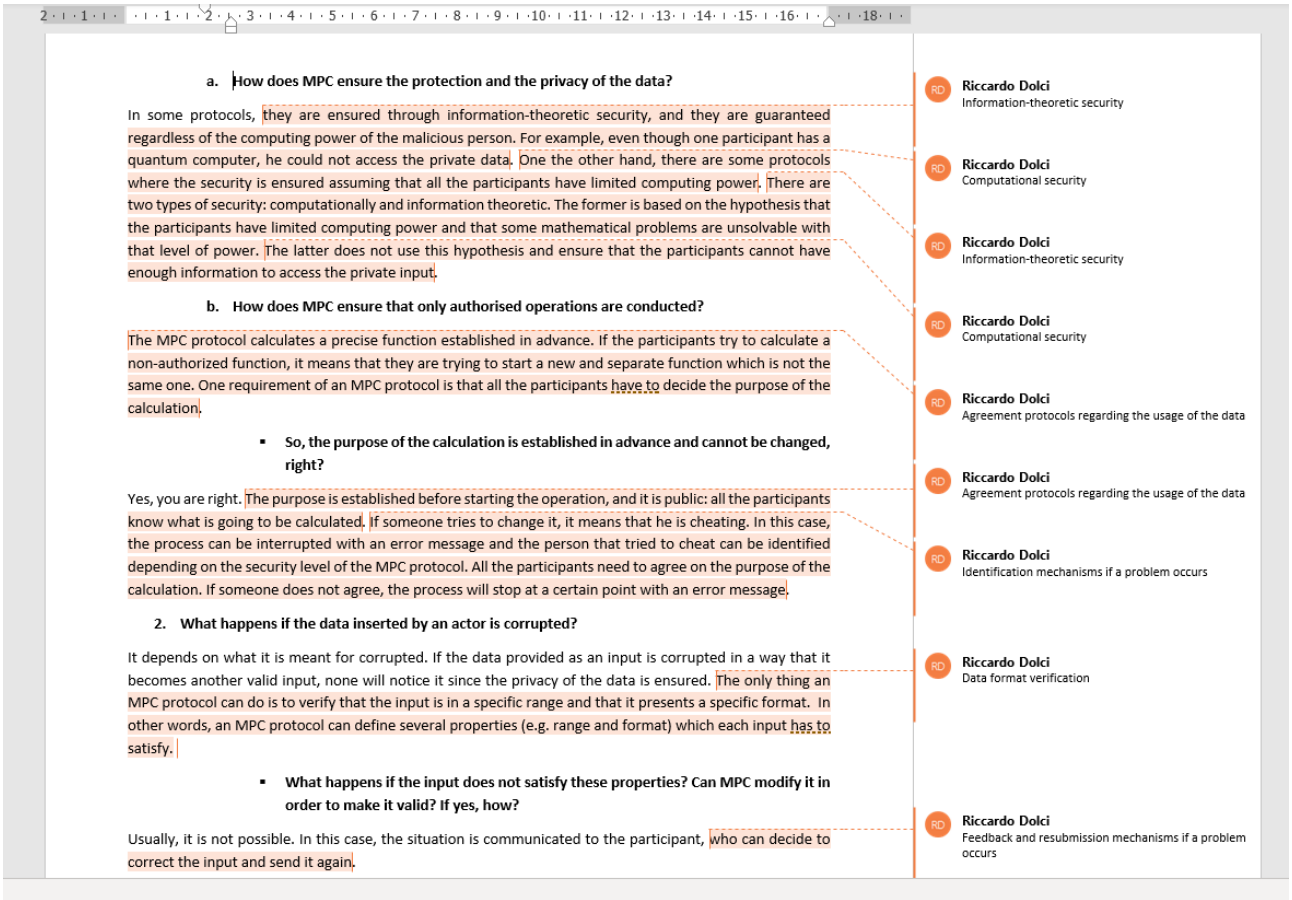

Figure 8: Coding process example

As already mentioned, the entire data reduction phase was conducted via Word by reading and analysing the interview transcripts, comparing the findings with the initial list of codes and

categories and updating it. The final updated list of codes and categories is presented in the table below. In this table, the new or updated categories and codes are characterised by a bold-face font. Finally, in the table, it is also described which informant mentioned the corresponding code.

Categories	Codes	Mentioned by
Preserving the data	**Data security**	I_1, I_2, I_3, I_4, I_5, I_6, I_7, I_{10}, I_{13}
	Data privacy	I_1, I_2, I_3, I_4, I_5, I_6, I_7, I_{12}, I_{13}
	Encryption	I_1, I_2, I_4, I_5, I_6
	Information-theoretic security	I_1, I_3
	Computational security	I_1, I_3
	Secret sharing	I_1, I_2, I_3, I_5, I_6
Enabling data ownership	Access control	I_7, I_8, I_{10}, I_{12}
	Terms and conditions	I_8, I_{10}
	Usage control	I_8, I_9, I_{10}, I_{12}
	Agreement protocols regarding the participants before starting the computation	I_1, I_2, I_3, I_4, I_5, I_6
Preserving the result of the computation	**Correctness of the output**	I_1, I_2, I_3, I_4, I_5, I_7
	Identification mechanisms if a problem occurs	I_1, I_2, I_5, I_6
	Data format verification	I_1, I_4, I_5, I_6
	Feedback and resubmission mechanisms if a problem occurs	I_1, I_2, I_4, I_5, I_6
Perception of the technology	**Lack of understanding of the technology**	I_1, I_2, I_4, I_6, I_8, I_{11}
	Challenging to demonstrate MPC features	I_2, I_4, I_6, I_{11}
	Lack of information about the technology	I_2
Degree of effort required	Change of the system required	I_7, I_8, I_{10}, I_{11}
	Difficulty of the implementation	I_1, I_4, I_{10}, I_{11}
	Low technology maturity level	I_1, I_5, I_7, I_{11}
	No standardisation	I_5, I_{11}
Need for the technology	**Benefited parties**	I_7, I_{10}, I_{11}, I_{12}
	Marketing strategy	I_7
	Possibility for new offerings	I_{10}, I_{12}, I_{13}
	Relevance of MPC features	I_7, I_8, I_{10}, I_{12}, I_{13}
	Improve the current service	I_7, I_{10}, I_{12}
	Contribution for achieving ultimate goals	I_7, I_{10}, I_{12}, I_{13}

	Willingness to adopt the MPC	I_7, I_8, I_{10}, I_{12}, I_{13}
Impacts on the control-related elements of the business model	Degree of openness	I_7, I_{10}, I_{12}
	Product traded	I_7, I_{10}, I_{12}, I_{13}
	Data storage	I_7, I_8, I_{10}, I_{12}, I_{13}
	Additional overhead	I_5, I_{11}

Table 13: Updated list of codes and categories

Regarding the data display, in this research, the data gathered are shown in a qualitative way (e.g. relevant statements) in contrast to the most common instruments used to display the data such as charts and diagrams (Sekaran & Bougie, 2016). Thanks to this, it was possible to facilitate the organisation of the data and the description of the results on which the drawing conclusions section is based.

Drawing conclusions was the last step of the qualitative data analysis process conducted in this study. In this phase, an answer to each sub research questions of the study was provided based on the information gathered in the previous analysis. Thanks to this, it was possible to collect all the information necessary to answer the main research question of this study and fill out the conceptual model generated in section 3.3.

5. Results

In this chapter, the results obtained from the analysis of the interviews are presented. Following the conceptual framework of this research, the chapter is divided into the following sections: affordances, factors and impacts. Firstly, the affordances arisen by the potential use of MPC as a mean to achieve platform control are described. Afterwards, the factors that could affect the realisation of these affordances are presented. Finally, the impacts that the realisation of the affordances could cause on the control-related business model characteristics of a data marketplace are illustrated.

5.1 The affordances

The analysis conducted identified three affordances that MPC could offer to a data marketplace provider in order to realise platform control: (1) preserving the data, (2) enabling data ownership, and (3) preserving the result of the computation. Even though there is no specific grammar for labelling affordances, it has been decided to label affordances as gerunds in accordance with previous researches present in the literature (e.g. Bobsin et al. (2019)). Following the conceptual model of section 3.3, every affordance is described as a potential benefit in terms of platform control that a data marketplace provider could achieve with the use of secure MPC. In particular, in each subsection, it is presented the feature of MPC and the goal of a data marketplace provider which could raise the affordance.

5.1.1 Preserving the data

Preserving the data can be described as the possibility for a data marketplace provider to protect the data exchanged and processed through its platform. This affordance is constituted by the relation between the following data marketplace provider's goal and MPC feature.

Goal: ensuring the privacy and security of the data

"[…] Ensuring the privacy and security of the data are paramount for us, and this is related to the monitoring of the platform". (I_7)

"The main challenge is to guarantee that the algorithm applied to the data will not copy the raw data somewhere. Since the data itself is not computed through a multi-party computation in the sense that it is not encrypted, but it is just guarded in a cage, somebody might write a malicious algorithm and obtain the raw data […]". (I_7)

"I think it is important to ensure data value preservation and the protection of data. (I_{13})

MPC feature: information-theoretic security or computational security

"There are two types of security: computational and information-theoretic. The former is based on the hypothesis that the participants have limited computing power and that some mathematical problems are unsolvable with that level of power. The latter does not use this hypothesis and ensure that the participants cannot have enough information to access the private input." (I_1)

"[…] You can have an MPC setup where you need an honest majority, or there is also actively secure MPC where, even with only one honest party, privacy is still guaranteed […]" (I_3)

As expected, ensuring the security of the data is a prior task for a data marketplace provider to build a safe and trustworthy ecosystem, especially if some analyses are conducted on sensitive or competitive data. In this scenario, the use of MPC could be instrumental in providing the mathematical guarantee (e.g. information-theoretic security) that none can obtain the original input shared by a data provider. However, in order to obtain an unconditional secure MPC protocol it is necessary to assume at least one honest party.

5.1.2 Enabling data ownership

Enabling data ownership can be described as the possibility for a data marketplace provider to enable the data owner to have complete control over its data. In other words, thanks to MPC, it would be possible to let the data provider decide if someone can access its data and enforce directly from the execution of the protocol the rules concerning the usage of its data, thus increasing the level of control over its data. This affordance is constituted by the relation between the following data marketplace provider's goal and MPC feature.

Goal: guarantee that the data owner has full control over its data

"*[…] the seller of the data needs to have control over his data in such a way that, at any time, he can decide who can access the data, how he can use the data and for how long. […]"* (I_8)

"[…] the data provider needs to have full sovereignty over its data […] We are constructing smart contracts where there are rules regarding how to access and how to control single usage, multiple usages, and different type of usage " (I_{12})

"[…] We are currently thinking about introducing usage control mechanisms in our platform" (I_{10})

MPC feature: agreement protocols among the participants before starting the computation and identification mechanisms if someone deviates from it

"The MPC protocol calculates a precise function established in advance. If the participants try to calculate a non-authorised function, it means that they are trying to start a new and separate function which is not the same one. One requirement of an MPC protocol is that all the participants have to decide the purpose of the calculation. […] The purpose is established before starting the operation, and it is public: all the participants know what is going to be calculated. If someone tries to change it, it means that he is cheating. In this case, the process can be interrupted with an error message and the person that tried to cheat can be identified depending on the security level of the MPC protocol". (I_1)

"This is determined by the protocol. For example, in the millionaire problem, the protocol is tailored to tell us who has more money. In other words, with information you have, you cannot do anything else, you can just run that function" (I_2)

The results of the interview showed that the decision concerning who is allowed to participate or not in the process is not part of the MPC. In contrast, they could be described as two different phases; in the first phase it is established who can participate to the process, while in the second one the MPC protocol it is executed. Thus, additional access control techniques should be added to the MPC protocol to decide who can access to the process.

"[…] The decision regarding the participation of an actor is not part of MPC. However, new protocols and practical solutions of MPC that can have the ability to verify the authenticity of an actor have recently been developed. This can be achieved through the combination of standard security access techniques and the MPC protocol. It is important to underline that these techniques are independent and separate from the MPC. In this case, the process can be divided into two different phases: verification of the authenticity and MPC execution. In the first one, it is decided who can participate or not, while in the second one the MPC protocol is executed. Thus, in this case, a list of authorised participants would be provided to the MPC." (I_1)

However, the data provider will submit its data only in the second phase after the list of participants of the process is defined. Therefore, the data owner would be still able to decide to send its data or not for the execution of the protocol depending on the intended usage of the data and the actors participating in the process.

"In order to achieve security, we will have to know the inputs and the computation beforehand. In this case, users provide their consent to use their health data for the computation. Each time we want to make a computation, all these users have consented to use their data." (I_6)

"[…]You can say that we know who has to participate in this protocol, and we know who is able to receive the results at the end." (I_6)

From the interviews, it also emerged that enabling the data owner to decide how its data can be used is instrumental for a data marketplace provider to guarantee that the owner of the data has complete control over its data. This ability is usually called usage control, and it is considered a complementary aspect of access control to ensure data ownership. Usage control has also been underlined by I_9 as a crucial aspect for a data marketplace to increase the level of trust in the platform.

"If I translate control to my hemisphere, it can be referred to usage control. Usage control is crucial for the trust that a customer has in the marketplace. Therefore, control is the ability to put rules to my data sets in a way that the other participants are forced to stick to these rules". (I_9)

Therefore, in this scenario, thanks to the adoption of MPC, the data marketplace provider will ensure that the rules set in advance by the data owners regarding the access and usage of the data will be respected. Thus, it will be possible to prevent any data misuse and detect any potential misbehaviour, thus contributing to the achievement of data ownership.

5.1.3 Preserving the result of the computation

Preserving the result of the computation can be described as the possibility for a data marketplace provider to ensure that the computation over the data sets will be executed correctly. This affordance is constituted by the relation between the following data marketplace provider's goal and MPC feature and is related only to data marketplace providers that offer the opportunity to perform analyses on the data.

Goal: ensure the correct execution of the computation

"[…] There must be completely operational measurement and monitoring all those tasks and guarantees that everything is secure and works as planned […]" (I_7)

"*The aim is to ensure that the computation was done correctly and that during the computation none sent or downloaded some data […]"* (I_7)

MPC feature: execute the computation correctly

"Regarding the correctness, the minimum is that the participants do not accept an incorrect output, but then you can also ask for stricter measures. For example, you can require that the participants always receive a correct output and if the output is not correct, you can require to identify who has cheated or other similar things". (I_1)

"When we talk about secure MPC, secure is meant in the sense that that the computation is carried out correctly and you have the privacy of the input of the players". (I_2)

The interviews conducted among data marketplace providers underlined the importance of ensuring the correct execution of the computation if a data marketplace provider offers the opportunity to perform analyses on the data. In this context, MPC could be used by a data marketplace provider as a tool to achieve this target. There are several features of MPC that enable this functionality and detect if a problem occurs during the different phases of the process. Firstly, during the input phase, the MPC can verify the quality of the data (e.g. range format), and in case the data does not satisfy the requirements, it will be requested to resubmit the input.

"The only thing an MPC protocol can do is to verify that the input is in a specific range and that it presents a specific format. In other words, an MPC protocol can define several properties (e.g. range and format) which each input has to satisfy." (I_1)

"In this case, they would just discard the input, and they will not use it for the function. They will ask to try again; otherwise, they will ignore him." (I_6)

Secondly, during the computation phase, MPC offers the possibility to detect if someone is deviating from the protocol, identify the cheater, and, if necessary, exclude it. Then, this situation will be communicated to all the other parties through feedback mechanisms. However, it is essential to underline that this event does not necessarily cause the abortion of the protocol. Therefore, the successful execution of the process and the correctness of the result can always be ensured.

"If one party acts maliciously and he wants to compute something else, the other parties will be able to see that he acted maliciously. So, they will stop the computation, and they will exclude him from the next one. […] This will be revealed to him and to the other parties. In some protocols, the honest MPC nodes can continue the computation after excluding the malicious node, meaning the computation can finish even if someone is malicious. So, a single node cannot necessarily kill the entire computation." (I_6)

5.1.4 Conclusion

The interviews conducted showed that the use of MPC could offer three affordances to a data marketplace provider in order to realise platform control. These affordances are summarised in the table below. Each row of the table can be read as the following example: since a data marketplace provider wants to ensure the privacy and security of the data exchanged and processes through its platform and the MPC offers information-theoretic security or computational security, then a data marketplace provider would have the possibility to preserve the data exchanged and processed through its platform.

Affordance	Description	Data marketplace provider's goal	Feature of MPC
Preserving the data	The possibility to protect the data exchanged and processed through its platform	Ensure data privacy and security	Information-theoretic security or computational security
Enabling data ownership	The possibility to guarantee that the rules established by the data owner regarding its data will be respected	Guarantee that the data owner has full control over its data	Agreement protocols among the participants before starting the computation and identification mechanisms if someone deviates from it
Preserving the result of the computation	The possibility to ensure that the computation over the data sets will be executed correctly	Ensure the correct execution of the computation	Execute the computation correctly

Table 14: Affordances

In conclusion, the adoption of the MPC would enable a data marketplace provider to set the procedures that every participant has to follow and introduce the control mechanisms necessary to preserve the data, the final result of the computation and enable its data providers to achieve data ownership by ensuring that all the participants will respect the data usage rules they decide to set. This result will be instrumental in realising platform control, thus increasing the level of security and trust of the data marketplace and bringing more data providers to participate in the ecosystem. Finally, based on the aforementioned findings, it was possible to fill the first three constructs present in the affordance existence phase of the conceptual model described in section 3.3.

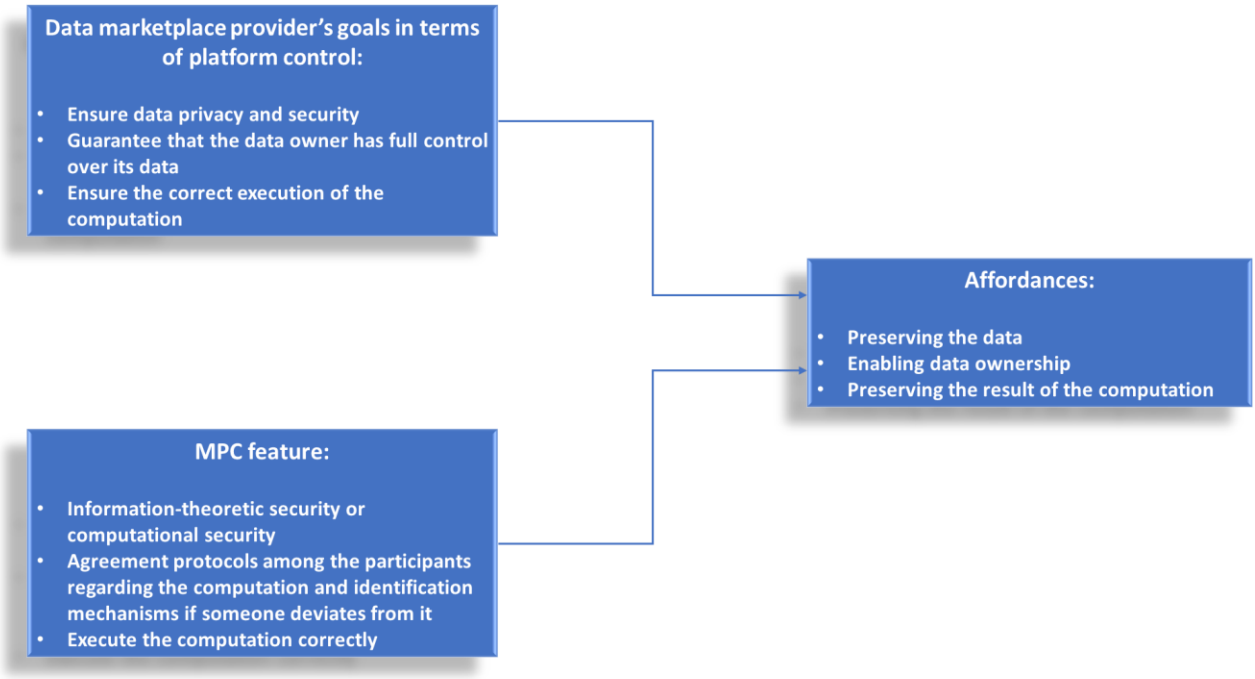

Figure 9: Affordance existence

5.2 The factors

In the previous section, three key benefits that the use of MPC would bring to a data marketplace provider have been presented. However, the realisation of these benefits could be affected by several factors. The interviews conducted identified the following factors: (1) perception of the technology, (2) need for the technology, and (3) degree of effort required. Following the affordance literature, each factor is described as a constraint or an enabler for a data marketplace provider to adopt the MPC technology. The distinction between constraint and enabler depends on the specific characteristics of the data marketplace provider. In fact, a factor could be a constraint for a data marketplace provider, but, at the same time, could be an enabler for another one. All the factors will be described in detail in the next subsections.

5.2.1 Perception of the technology

The perception of the MPC is a crucial factor that could affect the decision of a data marketplace provider to adopt this technology or not in its platform. According to the MPC experts, there is commonly a lack of information and understanding regarding the MPC technology among companies. As a result, firms may not perceive the full potentiality of this technology and, in some cases, they do not believe that the MPC can really offer what it promises. In fact, as the MPC experts

and developers argued, for most of the companies, the MPC technology could be perceived as magical.

"One challenge is that for the company itself, but also for the customer, it is hard to be convinced that MPC is a good solution and that it does what it does. For someone that is not of this field or does not know about MPC and crypto, it is very hard to understand what MPC does and what it does not do. This solution is so powerful that for many people, it is even hard to believe that it is possible. […]" (I_4)

"Nowadays, the main challenges regard the level of information and the understanding of technology. Usually, people do not understand how it works and does not trust or do not like things that they do not understand. MPC is not trivial to understand for someone who does not work with it. Sometimes, it sounds like magic." (I_2)

According to several MPC and data marketplace experts, indeed, one of the main challenges to spread the adoption of the MPC is to convince people that MPC is secure as it promises to be. Since most of the people are not familiar with the MPC concept and the cryptology field, it is difficult to explain to someone the MPC aspects, demonstrate them practically and convince people that MPC does what it claims to do.

"Since it is an emerging field, you would have to convince people that they can actually trust this. Even if MPC is 100% mathematically proved secure, how can we make people believe that there is nothing fishy going on and they can trust it. This is an obstacle to tackle. It is all about security. So, it is important to convince them that this technology is as good as it promises to be." (I_6)

"The problem is how to convince stakeholders, providers, consumers, and operators, that the guarantees provided by MPC are important, and they are actually enabled in a verifiable way by the technology" (I_{11})

This challenge could be explained by the novelty of this technology and its only recent development. Some data marketplace providers interviewed, indeed, were not familiar with the concept of MPC. Therefore, a data marketplace provider may not perceive the MPC technology as secure as it promises to be. However, only one of the data marketplace providers interviewed did not perceive the MPC technology as secure.

"I am not really familiar with the MPC concept. […] Our clients do not like to have a third party where your data is flowing. If you have two hospitals that want to share data between each other, they are

not willing to share through whatever system that can see the data. Even if it is encrypted and you might think it is secure, you never know what can happen." (I_8)

5.2.2 Need for the technology

The need for the MPC is another crucial factor that could affect the decision of a data marketplace provider to adopt this technology or not in its platform. The previous chapter showed that secure MPC could offer several advantages in terms of platform control to a data marketplace provider. However, a data marketplace provider could decide to adopt the technology or not only if it considers the MPC features relevant for its company and if it believes that MPC could improve its current situation and contribute to achieving its ultimate goals. The interviews showed that MPC technology could be relevant to a data marketplace provider for different reasons.

"The important aspect is that competitors can connect to a multi-party computing device server. Thanks to this, they can trust the service that MPC will use the data only according to what they agreed […] So, MPC would enable us to run computations on competitive data securely and to amalgamate data, merge data, analyse data, and transform data from different databases." (I_{12})

"Ensuring the security and privacy of the data traded would be a relevant and interesting feature which we would like to offer […] Monitoring the data usage would also be important for us […]" (I_{10})

Only in one case, in fact, a data marketplace provider claimed that the MPC would not be relevant for its company.

"From our side, we have different ways of implementing a data marketplace. For us, I do not really see any relevance […]" (I_8)

The results of the interviews showed that, in most of the cases, the MPC could satisfy several different needs of a data marketplace provider depending on its current situation. In order to better understand the results, it is essential to distinguish two types of data marketplaces: data marketplaces that focus only on data exchange offerings and data marketplaces that also offer to make computations on the data present in the platform. In the first case, in addition to the aforementioned affordances, the use of MPC would provide to the data marketplace providers to offer a new service in its platform, thus opening to new opportunities for achieving its ultimate goals. Secure MPC, indeed, would enable to perform meaningful computations on the data provided by the data owners and sell the result to an interested party, while maintaining the security and privacy of the data.

"[…] Regarding the business level, it would greatly improve our abilities. We could offer services or also data, which we are not currently able to offer, and it would open up many new opportunities". (I_{10})

Our ultimate goals are to improve road safety as well as efficiency. I think that this technology can contribute to achieve those goals. The reason why we offer this platform is that we want to improve and enable data exchange in order to make road users and automated vehicles better informed and make the road safer and more efficient. So, I think MPC could contribute in achieving this." (I_{10})

In case a data marketplace provider is already offering the possibility to run computations over the data, the use of MPC would improve the current service by providing the mathematical guarantees regarding the privacy and security of the data during the computation. Currently, indeed, there are no solutions other than secure MPC that can ensure this level of security during a computation. As a result, a data marketplace provider cannot run computations over competitive or sensitive data sets and, at the same time, maintain a high level of security.

"Currently, we are doing it through a third-party partner, and we are doing it through technological or engineering techniques where we rely on the firewalls and the network configurations. In contrast, what we would like is to rely on mathematics and cryptography. Thus, this is why we think it is a better solution" (I_7)

"We believe that it would be possible to buy data and doing something with it while keeping the data of the companies private. There are not many ways of how this can be achieved. To my knowledge, only homomorphic encryption and multi-party computation can do this job" (I_7)

"At the moment, we are not able to provide a trustworthy, intermediate platform like the MPC one. This result means that there are a couple of applications which are not possible at all. For example, computing between competitors is not possible at the moment. If we have the MPC technology, we will be able to have insights creation from competitive fields which is a totally important and necessary aspect. […] In conclusion, it is a prerequisite for creating successful data markets." (I_{12})

Thus, MPC could be used by a data marketplace provider as a mean to improve the current service offered by the platform and as a marketing message for its customers, thus possibly increasing the level of trust perceived by them towards the platform and bringing more participants.

"[…] it will definitely be a future technological and marketing message for the customers that we can offer mathematical guarantees regarding the privacy of the data. This could bring more participants." (I_7)

Even though a data marketplace provider could offer different new opportunities to its platform, the results showed that the majority of them believe that the adoption of the MPC technology could also generate advantages for all the parties involved in the system (e.g. data providers and data buyers). By creating a safe and trustworthy environment, data providers could sell and monetise safely sensitive or competitive data, while data buyers could benefit from the analysis that they want to compute on the data. This belief could play a crucial role in the adoption of MPC by a data marketplace provider. In fact, since the success of the marketplace strongly depends on the number of data providers and data buyers present in the platform, a data marketplace provider would decide to adopt this technology only if it believes that the MPC could benefit its customer.

"I think there are several parties who could benefit from it, especially in the mobility sector. It could be relevant for vehicle manufacturers. They receive data from their car sold, and they have connected systems that allow to collect much data. However, they cannot really sell the data because they could be personal. So, MPC would provide several advantages for them. They could execute an algorithm on the data, get the result and then sell that. The parties who would benefit from it are the data provider that could be the vehicle manufacturers who own the data. On the other side, the data consumers such as private navigation providers could get several benefits." (I_{10})

"All the stakeholders will gain benefits from this technology. The data marketplace provider can get advantages. The data provider can be sure that its data is safe. Finally, the data buyer can be sure that what he receives is really quality data." (I_{12})

Finally, the need for this technology is underlined by the fact that the majority of the data marketplace providers interviewed claimed that they would adopt the MPC technology very likely in their platform. Only in one case, the data marketplace provider claimed that it would not adopt the MPC.

"We would adopt it very likely because I believe that it is the correct mathematical way to guarantee the privacy of data during the computation run on this data." (I_7)

"We will implement very likely because we need the MPC." (I_{12})

"I do not think we will use that because I do not see the benefits right now. I see more problems than benefits" (I_8)

5.2.3 Degree of effort required

The degree of effort required to adopt the MPC technology represents a crucial factor that could affect the realisation of the affordances. At the current technological maturity level, the adoption, implementation and usage of MPC require several resources such as time, energies, expertise and costs. Thus, nowadays, the implementation of MPC technology in a data marketplace could represent a difficult task. This result could be explained by the fact that MPC is not a type of off-the-shelf technology, and it is not standardised, but it has to be tailored according to the individual needs of each customer.

"[…] MPC is not a type of off-the-shelf technology; it is not immediately available, but it is still under development. There are several different types, and it is not easy to understand which one presents the best properties or which one is the most efficient. The adoption, implementation and usage of MPC require a lot of resources such as time, energies and cost." (I_1)

"[…] Another difficulty is that MPC techniques have to be implemented in a computer language. Thousands of lines of codes have to be written, and specific choices of the different parameters need to be made […] (I_4)

"I think it is kind of difficult to implement MPC technology in a data marketplace. Currently, it does not present a sufficient level of maturity where any developer can easily make it works. It has a relatively high learning curve, and I think that this technology has a low usability level. […] In addition, there is no standardisation, as far as I know in this area. At this stage, it is not a very mature and usable technology." (I_{11})

"There are no new standardisation or RFC standardisation for MPC. It is so new that it is not standardised." (I_5)

For all the aforementioned reasons, the interviews showed that a data marketplace provider might consider that secure MPC does not currently present an adequate level of maturity for deciding to adopt it in its platform. As a result, a data marketplace provider could prefer to wait that the MPC technology becomes easier to use, more widespread, and that provides a higher level of performance.

"[…] Until it is not proven that multi-party computation or homomorphic encryption are usable in practice, provide a high level of performance, give good results and have a proven track record, we will not adopt them […] Currently, we are still in the research phase; we do not see the maturity of the technology and the readiness level of multi-party computation. […] We are also not seeing that other companies are using it. Before adopting the MPC, we have to wait first that the technology becomes ready, more popular and easier to use." (I_7)

Besides the high number of different resources required, from the technical side, the adoption of MPC could cause a significant change to the current system. If the data marketplace offers only data exchange services, the adoption of MPC will cause a change in the structure and the business model of the marketplace. Since MPC enables data aggregation other than running computations on data to produce meaningful insights, a data marketplace provider could have to face issues related to data aggregation. In fact, before computing the data, it would be necessary to transform the data in the right format.

"[…] Data aggregation is quite complex, and it is totally different than just sharing the data. There are some issues in aggregating data because you need to define how data fit with each other, what is the relation between the data, and you need to define the structure of the data. This is not always easy to do, especially if the data is coming from different systems. […] I also strongly believe that if you want to do data aggregation, you need a standard for sharing data […] There are so many types already of data, and if you want to make standards to comply with, that can be difficult." (I_8)

"[…] we need a different plugin modules interfaces to bring the data in one format and then compute them in one because very often data is unstructured and heterogeneous. Sometimes it is difficult to put data together; before the MPC, you need to transform data in the right format, and then you can compute it in one platform." (I_{12})

"The impact will be quite high because if you have a standard, every data shared has to be reworked to comply with the standards". (I_8)

Moreover, if the current system is not compatible with the MPC technology and its encryption mechanisms, it would have to be completely redesigned. This result will cause a radical change in the platform.

"The most important condition is that we would need a budget for that. From the technical side, we would need a service running on different sites to enable the MPC technology. I also think that the

system would have to be completely redesigned since it is not built for the encryption mechanisms of MPC. This is not just a thing on the application layer, but it would be a very deep implementation. […]" (I_{10})

On the other hand, a data marketplace could, instead, present a modular and modern system which could make the MPC technology more compatible with the current platform. In this scenario, the MPC would represent a new add-on module of the system, thus reducing the impact of the change and the degree of effort required.

"Our platform is modular, it is based on microservices, and it has a quite modern architecture. So, we do not expect that the change will be big […] In this particular case, it will not change our platform a lot; it will just provide mathematical guarantees. It will not change a lot because we already simulate a sort of multi-party computation […]" (I_7)

5.2.4 Conclusion

The interviews conducted showed that the realisation of the affordances might be affected by three main factors: (1) perception of the technology, (2) need for the technology, and (3) degree of effort required. These factors are instrumental in understanding how likely a data marketplace provider would adopt the MPC technology in its platform. Even though the interviews showed that secure MPC could satisfy several needs of a data marketplace provider, there are still some constraints that could negatively affect the adoption of MPC among data marketplace providers. A data marketplace provider, indeed, could not perceive the MPC as secure as it promises to be because of the difficulty to understand the technology. Moreover, since the adoption, implementation and usage of the MPC require several resources such as time, energies, expertise and costs a data marketplace provider may prefer to wait that the technology becomes more mature and widespread. Besides, since the adoption of MPC could affect the overall structure of the present system significantly, a data marketplace provider could prefer to maintain its current business model in order to avoid a radical change. However, in some cases, it could be possible to reduce the degree of effort if the data marketplace presents a compatible architecture with the MPC. Finally, based on the aforementioned findings, it was possible to fill the second phase (e.g. affordance perception and realisation) present in the conceptual model described in section 3.3.

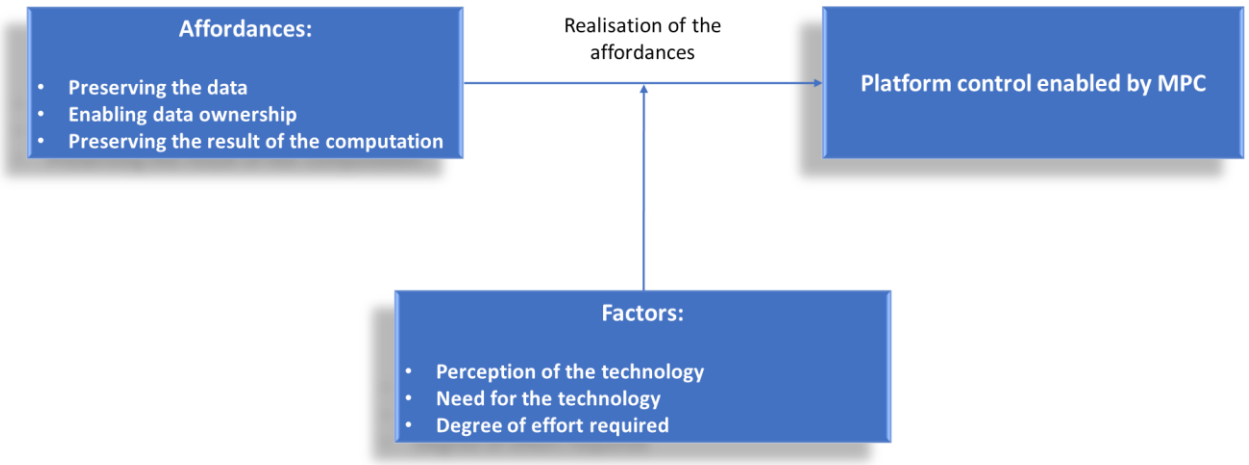

Figure 10: Affordance perception and realisation

5.3 The impacts

The adoption of the MPC technology by a data marketplace provider could cause several impacts on its platform. Considering the data marketplace taxonomy presented in section 2.1.3, the main control-related attributes that could be affected are the following: (1) market access, (2) architectural design, and (3) transformation.

Regarding the market access, the interviews showed that each data marketplace presents a different degree of openness. Data marketplace providers, indeed, regulate the access to their platform by merely using registration mechanisms or selecting the participants depending on some requirements that they have to fulfil. In this case, it resulted that the use of MPC would not affect the degree of openness of their platform.

"We want to have as many as possible data providers on the platform. So, we do not want to have restrictions now for accessing the platform for data providers or data buyers. At the moment, everyone who wants to come can come. However, we want to keep a listing process which means that a data provider needs to go through a couple of steps to show its trustworthiness. If your organisation satisfies a certain threshold of the quality check, then you can provide how many data sets you want." (I_{12})

"The access to the platform is not restricted at the moment. The only restriction we use is that the user has to register. Even if we adopt the MPC, we would maintain this restriction" (I_{10})

"[…] We will stay in this sort of B2B closed consortium context with selected partners […]" (I_7)

Concerning the architecture of the data marketplace, it is necessary to distinguish two different cases. A data marketplace, indeed, can have a centralised or a decentralised structure. Since the MPC technology allows a data provider to keep its raw data, if a data marketplace presents a decentralised structure, there will be no change in the way the platform stores the data. In contrast, if a data marketplace has a centralised structure, the data will not be stored in the platform, but they will remain with the data provider.

"There will be no changes in this case. With MPC, the data storage will be decentralised, and the data will remain with the data provider." (I_{12})

"Since we do not store data, it will not change." (I_8)

"For sure there will be a change because it will be much more secure, and I expect that there will be much more requirements related to the data storage. Now the data are stored in the platform; we have data feeds, so it is always real time data. If new data comes from the data provider, then the old data is overwritten. The data are temporarily stored in the platform but there is not a large storage of data." (I_{10})

Moreover, depending on the service offered by a data marketplace, there could be a change in the type of product sold in the platform. If a data marketplace provider focuses only on data exchange offerings, it would be able to offer a new type of product in its platform (e.g. transformed data). Otherwise, if a data marketplace provider already offers to make computations on the data present in the platform, the product will not change.

"In this case the data would not be sold in the same form, but in another form such as transformed data or a different type of data." (I_{10})

"Since in our company we have some kind of undercoat simulation of MPC it will not change much" (I_7)

Finally, the results from the interviews showed that the introduction of the MPC in a data marketplace could cause a negative impact on its functioning. In order to ensure the security of the computation, several secret shares have to be generated and shared among the parties involved. These operations require a high computational power which can slow down the run time. Therefore, at the current stage, the introduction of MPC in a data marketplace could create an additional overhead in the functioning of the platform.

"It could bring some additional complexity […] In principle, it can create additional overhead." (I_{11})

Based on the aforementioned findings, it was possible to fill the last phase (e.g. affordance effects) of the conceptual model described in section 3.3. As it can be inferred from the figure below, depending on the current situation of the data marketplace, the introduction of MPC in a data marketplace could cause up to three organisational changes.

Figure 11: Affordance effects

6. Discussion and conclusion

In this chapter, the final remarks regarding the study are outlined. Firstly, the main findings of this research are discussed in order to answer the sub and main research questions of this study and determine the achievement of the research objective. Moreover, a comparison between the findings and the existing literature is provided. Secondly, another comparison between the MPC technology and other types of secure technologies currently used in data marketplaces is provided. Thirdly, the theoretical and practical contributions of this research are described. Afterwards, the limitations encountered during the study are illustrated. Finally, recommendations for future research are provided.

6.1 Main findings

This research has a primary objective to investigate how MPC can enable a data marketplace provider to realise platform control in its marketplace. The findings showed that the framework provided by the affordance theory can be used to understand the contributions that the adoption of MPC can offer to a data marketplace provider to govern its platform and manage the interdependences among its participants. In order to achieve the goal of this study, one main research question and five sub-questions were addressed. In the following paragraphs, it is provided with an answer to all of them.

SQ1: "What goals are perceived to be important for data marketplaces providers in terms of platform control?"

The interviews showed that a data marketplace provider has three main goals related to platform control: (1) ensure the security and the privacy of the data; (2) guarantee that a data provider has complete control over its data; (3) ensure the correct execution of the computation. All these goals were expected since they are necessary for the creation of a trustworthy environment in which each participant (e.g. data provider and data buyer) can operate safely and in line with their own interests. Moreover, these results are in line with the existing literature of control both from a platform theory and computer security perspective. Regarding the former, data marketplace requires defined rules that determine how data should be used and effective mechanisms that monitor all the operations, including the quality of the data and detect any mistrustful activity (Koutroumpis et al., 2017). In this case, the rules are established exclusively by the data owners. Concerning the latter, the goals in terms of control are in line with the ones described by Fink (1994)

(e.g. integrity and privacy) and with the concept of usage control presented by Park and Sandhu (2004).

SQ2: "What are the key features/aspects of MPC that could enable platform control in data marketplaces?"

The results showed that three key features of the MPC technology could enable platform control in a data marketplace: (1) information-theoretic security or computational security, (2) agreement protocols before starting the process and identification mechanisms if someone deviates from it, (3) and correct execution of the computation. The main features resulted from the interviews are in relation to the ones retrieved from the literature study. However, from the interviews, it emerged the possibility to create a protocol where even if a problem occurs during the process (e.g. incorrect data format or misbehaviour), it will not necessarily cause the abortion of the process; on the contrary, the process will still be executed and the correct result delivered to the interested party. This additional aspect could be really relevant in the data marketplace context since it ensures successful execution of each transaction.

SQ3: "What are the affordances that secure MPC could offer to a data marketplace provider in order to realise platform control?"

The results from the interviews showed that the adoption of MPC could generate three main affordances for a data marketplace provider in terms of platform control: (1) preserving the data, (2) enabling data ownership and (3) preserving the result of the computation. These affordances are generated by the relationship between the aforementioned data marketplace provider's goals in terms of platform control and the key features of the MPC technology. These results confirm that MPC could realise control in a data marketplace from both a platform theory and computer security perspective. Regarding the former, the results showed that the MPC could be used as a mean to achieve process control in a data marketplace by establishing the procedures that every participant has to follow to operate in the platform. Thanks to this technology, it will be possible to align the behaviour of the participants with the platform provider's goals. Concerning the latter, the MPC could introduce the proper mechanisms for enforcing the policies that regulate the usage of the data exchanged and processed through the system, thus protecting the data from harm, theft, and unauthorised usage. The aforementioned benefits (e.g. data security and usage control) are in line with the ones offered by other security technologies such as blockchain (Banerjee & Ruj, 2019; Xiao et al., 2019).

SQ4: "What are the factors that could affect the realisation of the affordances?"

As argued by the affordance theory, the realisation of the aforementioned affordances strictly depends on the decision of a data marketplace provider to adopt or not the MPC technology in its platform. The results of the study showed that the realisation of the affordances could be influenced by three factors: (1) perception of the technology, (2) need for the technology, and (3) degree of effort required. These factors are instrumental in understanding how likely a data marketplace provider would adopt the MPC technology in its platform. Each of these factors, indeed, can represent a constraint or an enabler for a data marketplace provider to adopt the MPC technology.

The results of the interviews showed that secure MPC could satisfy several different needs of a data marketplace provider. In fact, secure MPC would allow to perform meaningful computations on the data and sell the result to an interested party, while maintaining the security and privacy of the data. This functionality could enable a data marketplace provider to offer a new service (e.g. secure aggregation and computations on competitive data sets) in its platform, thus opening to new opportunities for achieving its ultimate goals. At the same time, if a data marketplace provider is already offering the possibility to execute computations over the data, the adoption of MPC would improve the current service by providing the mathematical guarantees regarding the privacy and security of the data during the computation. Therefore, MPC could be used by a data marketplace provider as a marketing message for its customers, thus increasing the level of trust perceived by them towards the platform. By offering this unique type of service, it would also be possible for a data marketplace provider to charge it more compared to the other services. What is surprising from this result is that most data marketplace providers want to go beyond data exchange offerings and provide the opportunity to perform computations on competitive data sets in their platform. However, with the current security technology they have, they cannot offer this service and, at the same time, ensure a high level of security during a computation. Thus, the adoption of MPC by a data marketplace provider would contribute to solving this issue and creating a new generation of data marketplaces.

The results from the interviews also identified some barriers that could hinder the adoption of MPC among data marketplace providers. A data marketplace provider, indeed, could not perceive the MPC as secure as it promises to be because of a lack of understanding or information about the technology. Furthermore, nowadays, the adoption, implementation and usage of the MPC require several resources such as time, money, expertise and energies. Therefore, a data marketplace

provider could consider that this technology does not currently present an adequate level of maturity to be adopted in its platform. However, since the interest regarding the MPC is recently increased, and the research is focusing on improving MPC, it is reasonable to assume that this barrier will be overcome in the future. Besides, a data marketplace provider could prefer to wait and see the behaviour of other companies. Thanks to this strategy, indeed, a data marketplace provider may be able to reduce the risks of failure and the costs related to informing the customers about the MPC technology. Therefore, as expected, the current maturity level of the MPC technology and its novelty could represent a barrier for its adoption by a data marketplace provider. As a result, the first mover should be a company with a substantial budget which enable the introduction of the MPC in its data marketplace and a level of reputation sufficient to convince its participants about the potential of the MPC.

As expected, the adoption of the MPC in a data marketplace could affect the overall structure of the system. In fact, if the present system is not compatible with the MPC, it could be necessary to redesign the platform entirely, thus causing a radical change. A data marketplace provider could also prefer to maintain its current business model and focus only on data exchange offerings in order to avoid the problems related to data aggregation. Since data could be unstructured and heterogeneous, it could be challenging to find the right format and transform the data in order to comply with it before the computation. Therefore, a data marketplace provider may be less inclined to adopt the MPC in its platform because of the high degree of effort required. However, a surprising result was that there are currently existing types of modular and modern data marketplace which are already compatible with the MPC technology. In this case, secure MPC would represent a new add-on module for the system, which will significantly reduce the impact of the change and facilitate the realisation of the affordances.

All the factors resulted from the interviews are in line with the ones described by Pozzi et al. (2014) in their literature review regarding the affordance theory, for instance, lack of understanding and the degree of effort required. These factors are also in line with the ones presented by Clohessy and Acton (2019) in their literature study regarding the adoption of blockchain, which is another type of security technology. In fact, in their research, they identified several factors which could affect the adoption of blockchain, including perceived benefits, costs, knowledge, complexity, and technology readiness.

SQ5: "What are the impacts that the realisation of the affordances could cause on the control-related business model elements of a data marketplace?"

The findings from the interviews also showed that the adoption of MPC technology by a data marketplace provider could cause several impacts on its platform. Concerning the market access, the interviews revealed that the use of MPC would not affect the degree of openness of their platform. Each data marketplace provider, indeed, will maintain its current restrictions, which could vary from registration mechanisms or listing processes. As expected, even though the level of restrictions is relatively low to increase the number of participants, the data marketplace providers want to prove the identity of the party before allowing it to enter the market. Thus, this separate aspect should be integrated with the MPC technology. Regarding the architecture of the data marketplace, if the platform presents a centralised structure, the data will not be stored in the platform anymore, but they would remain with the data provider. Therefore, the architecture would become decentralised. This result is in line with the expectations since MPC enables a data provider to keep its raw data. Concerning the type of product traded, as expected, if a data marketplace provider focuses only on data exchange offerings, it would be able to offer a new type of product in its platform (e.g. insights). In fact, MPC focuses on performing analysis on the data to provide a specific result. Finally, the findings from the interviews revealed that the adoption of the MPC in a data marketplace could cause additional overhead in the functioning of the platform, which can slow down the run time of the process. This result is in line with the limitations of the MPC technology (e.g. low efficiency) identified by Choi and Butler (2019).

The aforementioned impacts are consistent with the ones identified by the existing literature on the introduction of innovative technologies for improving the security of data marketplaces. For example, the introduction of blockchain in a platform, which is currently spreading in the market, would make a marketplace decentralised and since this technology presents several disadvantages such as scalability, inefficiency and energy-consuming (Brett, 2018), the system would become less performant.

MQ: "How does MPC enable a data marketplace provider to realise platform control?"

In conclusion, thanks to the findings obtained by this research and the answer of the previous sub research questions, it was possible to fill the conceptual model of this study, thus answering the main research question. As indicated by the figure below, the realisation of platform control by a data marketplace provider through the adoption of secure MPC follows a time dependent process.

Firstly, the affordances arise from the relation between the features of the MPC and the data marketplace provider's goals in terms of platform control. Secondly, if a data marketplace provider perceives these affordances and decides to adopt secure MPC it will be able to realise platform control. In fact, since the affordances are only opportunities that an organisation with a particular purpose can achieve a technology, their actualisation process, which is the realisation of the potential actions, strictly depends on several factors. These factors, indeed, may facilitate or hinder the realisation of the affordances identified. Finally, the decision of a data marketplace provider to adopt secure MPC in its platform and realise the affordances may affect the architecture of the data marketplace and the product traded in the platform.

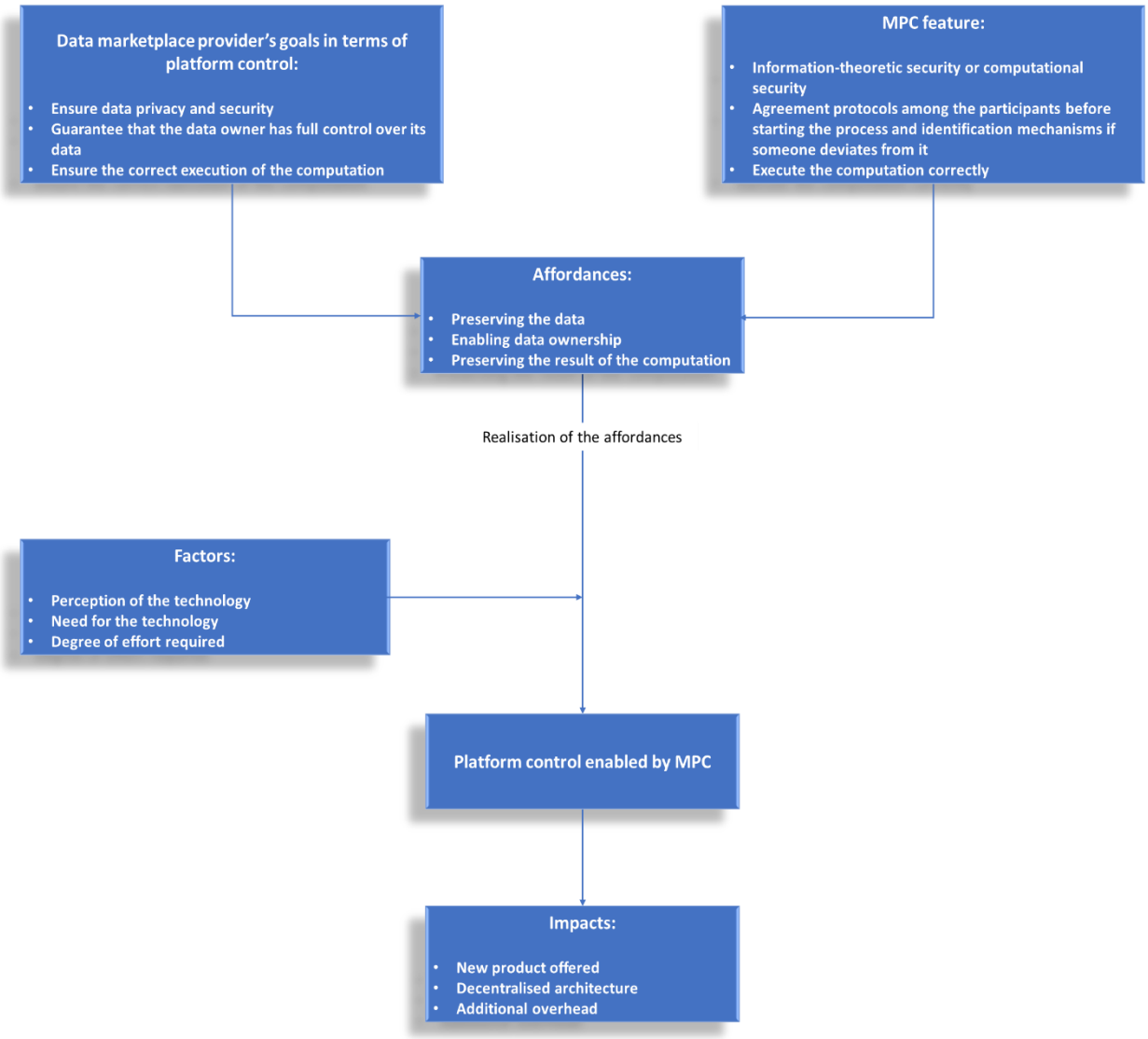

Figure 12: Filled conceptual model

6.2 Reflection on MPC and other security technologies

Even though secure MPC offers a great promise, at the current stage, secure MPC presents several limitations because of its domain-specific expertise required, its poor scalability, its low efficiency and high computational overhead. Moreover, it is important to underline that in order to implement an unconditional secure MPC which delivers a correct output it is still necessary to assume honest majority or at least one honest party. Thus, if all the actors behave maliciously the MPC protocol could be compromised. However, in real-world scenarios where business enterprises are involved there is the possibility to extremely mitigate this risk. In fact, if a party is detected cheating, its reputation will be significantly damaged and will have to sustain financial penalties. Finally, secure MPC cannot verify if the data entered by an actor is fake. Thus, if a data provider sends fake data, the output of the computation would be influenced.

Furthermore, in order to introduce it successfully in the data marketplace context, it would be necessary to add several security mechanisms. Firstly, it would be necessary to verify the identity of each participant before starting the process to make sure that each actor is who he claimed to be. Secondly, there is a need to implement secure channels among all the participants in order to avoid any attack from an external party. Thirdly, it is necessary to integrate MPC with audit trail mechanisms which register all the transactions executed in a data marketplace.

Despite the aforementioned considerations, secure MPC could bring significant contributions to data marketplaces. Nowadays, there are already several security mechanisms which are currently used by data marketplaces. The most common ones could be terms and conditions agreements and standard licensing models which can regulate the access and usage of data. However, these techniques seem to be not sufficient to promote the data sharing practices and establish data marketplace successfully in the market, as shown by the high number of platforms that have failed recently (Spiekermann, 2019). In this scenario, blockchain technology could be another solution to try to solve privacy and security issues and enable data sovereignty. However, secure MPC could offer an added value compared to the current present solutions adopted data marketplace.

Firstly, after the data is exchanged, nothing could prevent a data buyer to copy the data somewhere. Thanks to secure MPC, since the raw data remain always with the data provider and stay encrypted during the computation, it would be possible for a data owner to be sure that none could copy its data. Moreover, none of those solutions offers the possibility to run computations on competitive and sensitive data in a secure way as the MPC one. Therefore, the offerings provided by a data

marketplace could be restricted to only data exchange ones. As a result, data marketplaces could lose customers (e.g. data providers and buyers) that are interested in obtaining insights from the computation over competitive or sensitive data. In conclusion, secure MPC could be integrated into a data marketplace with other technologies (e.g. blockchain) which offer identification mechanisms, audit trail techniques and secure channels in order to contribute in creating the new generation of secure data marketplaces.

6.3 Theoretical and practical contributions

The research provides several theoretical and practical contributions. Firstly, it contributes to the study of a new solution for enabling B2B data sharing. In fact, existing research mainly focuses on data sharing between two defined partners in a determined context. Thus, this research offers more information regarding how the data sharing practice is conducted in open digital platforms and how it differs from commercial and privately managed exchanging platforms (e.g. IOS). Secondly, this study also contributes to data market literature by presenting different types and characteristics of a data marketplace, which could be used to update the taxonomy of data marketplaces. Thirdly, previous research on control mechanisms focuses mainly on the organisational or software platform contexts. This research contributes to the literature of platform control theory by describing a new solution to realise platform control in open ecosystem settings such as data marketplaces. From the results of the study, it can be inferred that secure MPC could be used as a mean to realise control both from a platform theory and computer security perspective.

Fourthly, the study provides insights into the MPC literature by exploring a new possible application of the technology. MPC literature, indeed, currently focuses mainly on how to improve MPC in terms of efficiency and scalability without investigating its possible applications. The results of this research showed that secure MPC could satisfy several needs in the data marketplace context. Fifthly, the research provides insights regarding the factors that could affect the adoption of the MPC in a data marketplace. The results showed that these factors are in line with the ones regarding the applications of security technologies (e.g. blockchain) in other domains. This result could be useful for future experiments concerning this topic. Finally, the research contributes to the study of affordances in the technology domain by considering the adoption of MPC and its features by a data marketplace provider. In fact, there are no studies regarding the affordances of MPC in any setting. Thanks to this, it would be possible to provide a framework by which companies can identify and

capture potential organisation opportunities for gaining value from the MPC, and eventually reaching goals.

This research also provides practical contributions to the business actors involved in data-sharing domains and to MPC developers. Regarding the former, data marketplaces providers could get benefits from this study by discovering a new strategy in governing data marketplaces to increase the number of participants in the platform. By considering the adoption of security technology like MPC, they can also assure data providers to exchange their data safely in the platform, increasing the number and the variety of data. This result may allow data marketplace providers to achieve a sustainable economic success of the company and establish themselves in the market. Concerning the latter, this study could contribute to raising the interest in MPC technology, thus fostering the spread and the application of this technology in different domains. As a result, MPC developers, including the Safe-DEED project, could increase the number of clients and receive more fundings for the development of the technology.

6.4 Limitations

This research presents various limitations which may have affected the findings obtained. Firstly, due to the difficulty of reaching informants, it was not possible to focus the research on data marketplace involved exclusively in the mobility domain. Therefore, it was necessary to include data marketplaces operating in different areas. However, all the data marketplace providers interviewed focused on several types of data, including mobility data. Thus, it can be assumed that there would not be significant changes in the model of the research if data marketplace providers that purely focus on mobility data were interviewed. Moreover, even though the interviews gathered several insights, if more data marketplace providers were interviewed, it might have been possible to gain more information for the research and reach theoretical saturation also for the fourth sub-research question of the study.

There could be several reasons why the candidates were not willing to participate in the interview. It could be that the companies were overwhelmed by the crisis caused by the coronavirus disease. It could also be that they did not want to be interviewed because they did not have any expertise in the MPC field. Another reason could be that they were not interested in the MPC technology. It is essential to underline that these are just assumptions since the candidates selected did not answer to the invitations sent. Thus, it is not possible to provide a real explanation to why they did not accept to be interviewed. However, if the last assumption is correct, it could have affected the

results of the research by reducing the need for the MPC technology in the data marketplace domain.

Secondly, there are some limitations related to the informants interviewed. Two of the data marketplace providers interviewed belong to the same data marketplace, which is not currently operating anymore. Thus, their answerers were based on the assumption that the data marketplace was still running. Moreover, in some cases, it was not possible to interview the candidate initially selected. Thus, it was necessary to interview a person with a different role in the company. This issue could have affected the answers of some questions of the protocol related to the technical aspects of the data marketplace (e.g. How significant will this change be for your platform? Why? or how will this change the way your platform works?). In fact, an informant involved in a technical role in the company could have provided different answers compared to the one involved in another role.

Thirdly, the majority of the interviewees did not have the chance to read the MPC description document before the interview. In this case, the relevant concepts of the research and the description of the MPC were verbally explained. This issue could have affected the validation of the MPC description during the interviews among MPC experts and developers. If the informants studied the MPC description carefully before the interview, they would have possibly provided additional insights for the illustration and validation of the MPC technology. In addition, it could have influenced the understanding of the MPC from the data marketplace providers. In fact, due to the complexity of the MPC field, the participants may not have fully understood the description of the MPC technology and its potential.

In order to deal with the aforementioned limitations, some strategies could be undertaken in the future. Firstly, by sharing the final report of the thesis with the informants, it would be possible to increase the rate of response. In fact, data marketplace providers could gain several benefits from the findings of this study. Secondly, other prices, such as gift cards and cash incentives, could be introduced to make the candidates accept the invitation. Finally, alternative ways to illustrate the MPC technology could be used to ensure that the informants are very prepared before the interview. For example, the presence of a short video in the invitations could make the informant more willing to study the material before the interview.

6.5 Recommendations for future research

The research regarding data marketplace and MPC real-world applications is relatively new. Therefore, this study proposes several different directions to undertake future research. Firstly, with more interviews, it could be possible to overcome the main limitation of this research by reaching theoretical saturation also for the fourth sub research question. Secondly, this study is the first attempt to apply the concept of affordance in the MPC domain. Thus, there could be the possibility to identify more factors if more information and insights are gathered. Thirdly, since the final model generated by this study is not tested, future research could be undertaken to validate it through quantitative studies. For example, some experiments could be conducted through MPC prototypes to explore further the introduction of secure MPC within the data marketplace domain. Fourthly, the results of this research provide future directions for updating the taxonomy of data marketplaces, their architecture, and their business models.

Fifthly, future research could be undertaken regarding the introduction of secure MPC in other related data sharing settings. Due to the increasing interest and spreading of the data-sharing practice among different industries, investigating the application of secure MPC in other data sharing settings could further promote the data-driven economy. Finally, the perspective adopted in this research was from the data marketplace providers. However, it resulted that the MPC could also provide benefits to the data providers participating in the platform. Exploring the different perspectives of the actors involved could provide other insights for the implementation of secure MPC in the data marketplace context.

Bibliography

Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From Keys to Databases—Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, *61*(12), 1749–1771. https://doi.org/10.1093/comjnl/bxy090

Arrow, K. (1962). *Economic Welfare and the Allocation of Resources for Invention* (pp. 609–626) [NBER Chapters]. National Bureau of Economic Research, Inc. https://econpapers.repec.org/bookchap/nbrnberch/2144.htm

Aumann, Y., & Lindell, Y. (2007). *Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries* (No. 060). http://eprint.iacr.org/2007/060

AutoMat Project. (2018a, January 18). *AutoMat: Connected Car Data - The Unexcavated Treasure*. https://www.youtube.com/watch?v=uRjvnahJ-9o

AutoMat Project. (2018b, February 13). *AutoMat—The Vehice Big Data Marketplace*. https://www.youtube.com/watch?v=W3kxHd3CdL0

Banerjee, P., & Ruj, S. (2019). Blockchain Enabled Data Marketplace—Design and Challenges. *ArXiv:1811.11462 [Cs]*. http://arxiv.org/abs/1811.11462

Becker, J., Backhaus, K., & Grob, H. L. (2014). The Data Marketplace Survey Revisited. *ResearchGate*. https://www.researchgate.net/publication/260795184_The_Data_Marketplace_Survey_Revisited

Bernhard, E., Recker, J., & Burton-Jones, A. (2013). Understanding the Actualization of Affordances: A Study in the Process Modeling Context. *ICIS*. https://www.semanticscholar.org/paper/Understanding-the-Actualization-of-Affordances%3A-A-Bernhard-Recker/730ea441aac5497565d9ecafd0ac07f7ecc3a180

Bestavros, A. (2017). *Sharing knowledge without sharing data*. https://www.youtube.com/watch?v=P2MmO458xu4

Bobsin, D., Petrini, M., & Pozzebon, M. (2019). The value of technology affordances to improve the management of nonprofit organizations. *RAUSP Management Journal*, *54*(1), 14–37. https://doi.org/10.1108/RAUSP-07-2018-0045

Boudreau, K. J. (2010). *Open Platform Strategies and Innovation: Granting Access vs. Devolving Control*. https://www.researchgate.net/publication/220535085_Open_Platform_Strategies_and_Innovation_Granting_Access_vs_Devolving_Control

Brett, C. (2018, October 15). Blockchain disadvantages: 10 possible reasons not to enthuse -. *Enterprise Times*. https://www.enterprisetimes.co.uk/2018/10/15/blockchain-disadvantages-10-possible-reasons-not-to-enthuse/

Cao, M., & Zhang, Q. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. *Journal of Operations Management*, *29*(3), 163–180. https://doi.org/10.1016/j.jom.2010.12.008

Chida, K., Ikarashi, D., Miyata, T., Takiguchi, H., & Kiribuchi, N. (2014). *R&D on Secure Computation Technology for Privacy Protection*. *12*(7), 6.

Choi, J. I., & Butler, K. R. B. (2019, April 2). *Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities* [Review Article]. Security and Communication Networks; Hindawi. https://doi.org/10.1155/2019/1368905

Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. *Industrial Management & Data Systems*, *119*(7), 1457–1491. https://doi.org/10.1108/IMDS-08-2018-0365

Damgard, I., Pastro, V., Smart, N. P., & Zakarias, S. (2011). *Multiparty Computation from Somewhat Homomorphic Encryption* (No. 535). http://eprint.iacr.org/2011/535

Datarade. (2020). *Datarade*. https://datarade.ai/

DeCoste, B. (2018). *Secret Sharing Explained*. https://medium.com/dropoutlabs/secret-sharing-explained-acf092660d97

Eldefrawy, K., Ostrovsky, R., Park, S., & Yung, M. (2018). *Proactive Secure Multiparty Computation with a Dishonest Majority: 11th International Conference, SCN 2018, Amalfi, Italy, September 5–7, 2018, Proceedings* (pp. 200–215). https://doi.org/10.1007/978-3-319-98113-0_11

Encyclopaedia Britannica, Inc. (2019, January 17). *Computer security*. Encyclopaedia Britannica. https://www.britannica.com/technology/computer-security

European Commission. (2018). *Study on data sharing between companies in Europe*. https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

Evans, D., Kolesnikov, V., & Rosulek, M. (2018). *A Pragmatic Introduction to Secure Multi-Party Computation*. https://securecomputation.org/docs/ch2-definingmpc.pdf

Fink, D. (1994). A Security Framework for Information Systems Outsourcing. *Information Management & Computer Security*, *2*(4), 3–8. https://doi.org/10.1108/09685229410068235

Fricker, S., & Maksimov, Y. (2017). *Pricing of Data Products in Data Marketplaces*. ResearchGate. https://www.researchgate.net/publication/318492802_Pricing_of_Data_Products_in_Data_Marketplaces

Fruhwirth, M., Rachinger, M., & Prlja, E. (2020, January 7). *Discovering Business Models of Data Marketplaces*. https://doi.org/10.24251/HICSS.2020.704

Ghosh, H. (2018). Data Marketplace as a Platform for Sharing Scientific Data. *ResearchGate*. https://www.researchgate.net/publication/323503712_Data_Marketplace_as_a_Platform_for_Sharing_Scientific_Data

Ghotkar, M., & Rokde, P. (2016). *Big Data: How it is Generated and its Importance*. http://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%202/1.%2001-05.pdf

Gibson, J. J. (1979). *The Ecological Approach to Visual Perception*. Houghton Mifflin. https://books.google.it/books?hl=it&lr=&id=8BSLBQAAQBAJ&oi=fnd&pg=PP1&dq=The+Ecological+Approach+to+Visual+Perception+gibson&ots=zOD4aOrt2v&sig=OhecVltOcLprkJP3YPQ0P2miD78&redir_esc=y#v=onepage&q=The%20Ecological%20Approach%20to%20Visual%20Perception%20gibson&f=false

Goldbach, T., Benlian, A., & Buxmann, P. (2018). Differential effects of formal and self-control in mobile platform ecosystems: Multi-method findings on third-party developers' continuance intentions and

application quality. *Information & Management*, *55*(3), 271–284. https://doi.org/10.1016/j.im.2017.07.003

Goldbach, T., & Kemper, V. (2014). Should I Stay or Should I Go? The effects of Control Mechanisms on App Developers' Intention to stick with a Platform. *ECIS*. https://www.semanticscholar.org/paper/SHOULD-I-STAY-OR-SHOULD-I-GO-THE-EFFECTS-OF-CONTROL/f3b868fa5f7be0238c6a2a7055b52c43091b08bf

Gollmann, D. (2010). Computer security. *WIREs Computational Statistics*, *2*(5), 544–554. https://doi.org/10.1002/wics.106

Greeno, J. G. (1994). *Gibson's Affordances*. https://pdfs.semanticscholar.org/1649/eba81f5ee5490322969798af8b82feb8a5db.pdf

Gunasekaran, A., & Sandhu, M. (2010). *Handbook on Business Information Systems*. https://www.researchgate.net/publication/228279757_Handbook_on_Business_Information_Systems

Halevi, S., Ishai, Y., Kushilevitz, E., & Rabin, T. (2018). *Best Possible Information-Theoretic MPC* (No. 913). http://eprint.iacr.org/2018/913

Hausvik, G., & Thapa, D. (2017). What You See is Not What You Get—Challenges in Actualization of EHR Affordances. *ResearchGate*. https://www.researchgate.net/publication/320833440_What_You_See_is_Not_What_You_Get_-_Challenges_in_Actualization_of_EHR_Affordances

Hazay, C., & Lindell, Y. (2010). *Efficient Secure Two-Party Protocols: Techniques and Constructions*. Springer Science & Business Media. https://www-springer-com.tudelft.idm.oclc.org/gp/book/9783642143021

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., … Cybersecurity, S. (2013). *Guide to Attribute Based Access*

Control (ABAC) Definition and Considerations. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf

Hutchby, I. (2001). Technologies, Texts and Affordances. *ResearchGate*. https://www.researchgate.net/publication/240729307_Technologies_Texts_and_Affordances

Kirsch, L. J. (1996). The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. *Organization Science*, *7*(1), 1–21. https://doi.org/10.1287/orsc.7.1.1

Koutroumpis, P., & Leiponen, A. (2013). Understanding the value of (big) data. *2013 IEEE International Conference on Big Data*, 38–42. https://doi.org/10.1109/BigData.2013.6691691

Koutroumpis, P., Leiponen, A., & Llewellyn, D. W. T. (2020). *Markets for Data*. https://www.researchgate.net/publication/338411973_Markets_for_Data

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017). *The (Unfulfilled) Potential of Data Marketplaces*. https://www.etla.fi/en/publications/the-unfulfilled-potential-of-data-marketplaces/

KPMG. (2018, March 2). *Trend 8: The benefits of sharing data become more evident—KPMG Global*. https://home.kpmg/xx/en/home/insights/2018/01/trend-8-the-benefits-of-sharing-data.html

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security*, *1*(1), 3–13. https://doi.org/10.1007/s102070100003

Lazouski, A., Martinelli, F., & Mori, P. (2010). Usage control in computer security: A survey. *Computer Science Review*, *4*(2), 81–99. https://doi.org/10.1016/j.cosrev.2010.02.002

Leonardi, P. M. (2013). When Does Technology Use Enable Network Change in Organizations? A Comparative Study of Feature Use and Shared Affordances. *MIS Quarterly*, *37*(3), 749–775. https://doi.org/10.25300/MISQ/2013/37.3.04

Lindel, Y. (2019). *Secure Multiparty Computation – a Seasoned Technology with Strong Foundations*. Unbound. https://www.unboundtech.com/secure-multiparty-computation-seasoned-technology-strong-foundations/

Louise Barriball, K., & While, A. (1994). Collecting data using a semi-structured interview: A discussion paper. *Journal of Advanced Nursing*, *19*(2), 328–335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Manzi, G. (2017). Big Data and Smart Mobility. *COMPLEX SYSTEMS*, 58.

Markus, M. L., & Silver, M. (2008). *A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit*. https://www.researchgate.net/publication/220580526_A_Foundation_for_the_Study_of_IT_Effects_A_New_Look_at_DeSanctis_and_Poole's_Concepts_of_Structural_Features_and_Spirit

Marr, B. (2018). *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#e4694e760ba9

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. SAGE.

Mukhopadhyay, S., & Bouwman, H. (2019). Orchestration and governance in digital platform ecosystems: A literature review and trends. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/DPRG-11-2018-0067

Mukhopadhyay, S., de Reuver, M., & Bouwman, H. (2016). Effectiveness of control mechanisms in mobile platform ecosystem. *Telematics and Informatics*, *33*(3), 848–859. https://doi.org/10.1016/j.tele.2015.12.008

Muschalle, A., Stahl, F., Löser, A., & Vossen, G. (2013). Pricing Approaches for Data Markets. In M. Castellanos, U. Dayal, & E. A. Rundensteiner (Eds.), *Enabling Real-Time Business Intelligence* (pp. 129–144). Springer. https://doi.org/10.1007/978-3-642-39872-8_10

Okamura, T., & Teranshi, I. (2016). Enhancing FinTech Security with Secure Multi-Party Computation Technology: NEC Technical Journal. *NEC*. https://www.nec.com/en/global/techrep/journal/g16/n02/160211.html

Park, J., & Sandhu, R. (2004). The UCONABC Usage Control Model. *ACM Transactions on Information and System Security (TISSEC)*, *7*(1), 128–174. https://doi.org/10.1145/984334.984339

Parker, G., & Van Alstyne, M. (2017). Innovation, Openness, and Platform Control. *Management Science*, *64*(7), 3015–3032. https://doi.org/10.1287/mnsc.2017.2757

Pedersen, T. B., Saygın, Y., & Savas, E. (2007). *Secret Sharing vs. Encryption-based Techniques For Privacy Preserving Data Mining*. 11.

Pozzi, G., Pigni, F., & Vitari, C. (2014). Affordance Theory in the IS Discipline: A Review and Synthesis of the Literature. *ResearchGate*. https://www.researchgate.net/publication/263642241_Affordance_Theory_in_the_IS_Discipline_a_Review_and_Synthesis_of_the_Literature

Roman, D., & Vu, K. (2018). Enabling Data Markets Using Smart Contracts and Multi-party Computation. *ResearchGate*. https://www.researchgate.net/publication/330085470_Enabling_Data_Markets_Using_Smart_Contracts_and_Multi-party_Computation

Roth, A. E. (2008). What Have We Learned from Market Design?*. *The Economic Journal*, *118*(527), 285–310. https://doi.org/10.1111/j.1468-0297.2007.02121.x

Rouse, M. (2014). *What is access control?* SearchSecurity. https://searchsecurity.techtarget.com/definition/access-control

Safe-DEED. (2019). *Safe-DEED*. https://safe-deed.eu/

Santos, M., & Faure, A. (2018). Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption: *Social Media + Society*. https://doi.org/10.1177/2056305118795876

Sarfo, F. A. (2019). Use of Digital-Physical Security System in a Developing Country's Port: A Case Study of Ghana. *ResearchGate*. https://www.researchgate.net/publication/333700848_Use_of_Digital-Physical_Security_System_in_a_Developing_Country's_Port_A_Case_Study_of_Ghana

Schreieck, M., Hein, A., Wiesche, M., & Krcmar, H. (2018). The Challenge of Governing Digital Platform Ecosystems. *ResearchGate*. https://www.researchgate.net/publication/319773199_The_Challenge_of_Governing_Digital_Platf

orm_Ecosystems#:~:text=Multi%E2%80%90sided%20platforms%20(MSPs),to%20disrupt%20long%E2%80%90established%20industries.&text=The%20results%20indicate%20that%20platform,in%20different%20shapes%20and%20characteristics.

Schreieck, M., Wiesche, M., & Krcmar, H. (2016). Design and Governance of Platform Ecosystems – Key Concepts and Issues for Future Research. *ResearchGate*. https://www.researchgate.net/publication/303924671_Design_and_Governance_of_Platform_Ecosystems_-_Key_Concepts_and_Issues_for_Future_Research

Sekaran, U., & Bougie, R. (2016). *Research Methods For Business: A Skill Building Approach*. John Wiley & Sons. https://www-wiley-com.tudelft.idm.oclc.org/en-gl/Research+Methods+For+Business:+A+Skill+Building+Approach,+7th+Edition-p-9781119266846

Sharemind. (2020). *How does Sharemind MPC work? A short introduction to secure multi-party computation technology*. https://sharemind.cyber.ee/sharemind-mpc/

Spiekermann, M. (2019). *Data Marketplaces: Trends and Monetisation of Data Goods*. https://www.intereconomics.eu/contents/year/2019/number/4/article/data-marketplaces-trends-and-monetisation-of-data-goods.html

St John, W., & Johnson, P. (2000). The pros and cons of data analysis software for qualitative research. *Journal of Nursing Scholarship: An Official Publication of Sigma Theta Tau International Honor Society of Nursing*, *32*(4), 393–397. https://doi.org/10.1111/j.1547-5069.2000.00393.x

Stahl, F., Schomm, F., Vossen, G., & Vomfell, L. (2016). A classification framework for data marketplaces. *Vietnam Journal of Computer Science*, *3*(3), 137–143. https://doi.org/10.1007/s40595-016-0064-2

Steinfield, C. W. (2014). Inter-Organizational Information Systems. *ResearchGate*. https://www.researchgate.net/publication/275351047_Inter-Organizational_Information_Systems

Strong, D. M., Volkoff, O., Johnson, S. A., Pelletier, L., Tulu, B., Bar-On, I., Trudel, J., & Garber, L. (2014). A Theory of Organization-EHR Affordance Actualization. *J. AIS*, *15*, 2. https://doi.org/10.17705/1jais.00353

The Economist. (2017). *Regulating the internet giants—The world's most valuable resource is no longer oil, but data | Leaders | The Economist*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The MPC Lounge. (2013). *Secure Supply Chain Collaboration*. The MPC Lounge. https://mpclounge.wordpress.com/2013/04/15/secure-supply-chain-collaboration/

Tiwana, A. (2013). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. https://www.semanticscholar.org/paper/Platform-Ecosystems%3A-Aligning-Architecture%2C-and-Tiwana/df103a485ec19c3463f40bbe9294c44ca05c424f

Volgushev, N., Schwarzkopf, M., Getchell, B., Varia, M., Lapets, A., & Bestavros, A. (2019). Conclave: Secure multi-party computation on big data (extended TR). *Proceedings of the Fourteenth EuroSys Conference 2019 CD-ROM on ZZZ - EuroSys '19*, 1–18. https://doi.org/10.1145/3302424.3303982

Volkoff, O., & Strong, D. M. (2013). Critical Realism and Affordances: Theorizing It-Associated Organizational Change Processes. *MIS Quarterly*, *37*(3), 819–834. JSTOR.

Wiseman, E. (2019). *Why data is the world's most valuable resource*. https://www.paysafe.com/en/blog/the-worlds-most-valuable-resource-not-oil-but-data/

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2019). Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution. *ArXiv:1904.07275 [Cs]*. http://arxiv.org/abs/1904.07275

Yao, A. C. (1982). Protocols for secure computations. *23rd Annual Symposium on Foundations of Computer Science (Sfcs 1982)*, 160–164. https://doi.org/10.1109/SFCS.1982.38

Zammuto, R. F., Griffith, T. L., Majchrzak, A., Dougherty, D. J., & Faraj, S. (2007). Information Technology and the Changing Fabric of Organization. *Organization Science*, *18*(5), 749–762.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y. (2019). Secure Multi-Party Computation: Theory, practice and applications. *Information Sciences*, *476*, 357–372. https://doi.org/10.1016/j.ins.2018.10.024

Appendix

Appendix A: Invitations

Invitation for data marketplace providers

Good morning,

My name is Riccardo Dolci and I am a master student at the Management of Technology program at Delft University of Technology. I am currently attending my master thesis entitled: “Realising platform control in data marketplaces through Secure Multi-Party Computation”, which aims to understand how MPC technology may (or may not) enable control in data marketplaces.

I would like to conduct an interview with you to hear your perspective about the landscape of data marketplaces, the importance of control mechanisms, and the relevance of security technology like MPC for data marketplaces. The interview will last around one hour and will be conducted via Skype.

I would be grateful if you can inform me about your availability in the following weeks. I also attached the interview protocol and a brief description of the MPC technology for your reference as a preparation for the interview. Give me this opportunity would hugely contribute to my work as well as the existing research on data marketplaces and MPC.

I would be happy to answer your questions if you need any further information. Thank you very much and I look forward to hearing from you.

Kind regards,

Riccardo Dolci

Invitation for MPC developers/experts

Good morning,

My name is Riccardo Dolci and I am a master student at the Management of Technology program at Delft University of Technology. I am currently attending my master thesis entitled: “Realising platform control in data marketplaces through Secure Multi-Party Computation”, which aims to understand how MPC technology may (or may not) enable control in data marketplaces.

I would like to conduct an interview with you to hear your perspective about the landscape of MPC and the key features/aspects of MPC that could contribute to the security of data marketplaces.

Finally, I would appreciate your opinion to validate my description of the MPC technology. The interview will last around one hour and will be conducted via Skype.

I would be grateful if you can inform me about your availability in the following weeks. I also attached the interview protocol and a brief description of the MPC technology for your reference as a preparation for the interview. Give me this opportunity would hugely contribute to my work as well as the existing research on data marketplaces and MPC.

I would be happy to answer your questions if you need any further information. Thank you very much and I look forward to hearing from you.

Kind regards,

Riccardo Dolci

Appendix B: interview protocols

Interview protocol MPC experts/developers

Introduction

This interview aims to understand how MPC technology may (or may not) enable control in data marketplaces. Before starting the interview, I will briefly introduce my description of the data marketplace and the MPC technology, in case you will not have the chance to read the description I have sent to you.

The interview will be recorded depending on your consent, transcribed and analysed to complete my work. I ensure the full confidentiality of your personal information, and that the information you will provide me will be used only for academic purposes.

Interview questions

1. Could you give a general overview of what MPC is?
    a. What do you think about my description of MPC? Is there any relevant aspect missing? If yes, which one is missing?
2. How is the MPC process conducted?
    a. How does MPC ensure the protection and the privacy of the data?
    b. How does MPC ensure that only authorized parties can access to the process and its result?
    c. How does MPC ensure that only authorized queries are conducted?
    d. How does MPC ensure that the function of the computation does not change during the process?
    e. Can MPC track and record the computation that is made and its users? If yes, how?
3. What happens if the data inserted by an actor is corrupted?
    a. Can MPC detect it? If yes, how?
    b. Does the presence of corrupted data affect the result? Why or why not?
    c. How is this situation communicated to the actors?
    d. Can the computation be resubmitted? If yes, how?
4. What happens in the presence of a malicious actor?
    a. Can MPC identify the malicious actor? If yes, how?
    b. Does the presence of a malicious actor affect the result? Why or why not?

c. How is this situation communicated to the actors?
d. Can the computation be resubmitted? If yes, how?

5. How do you see the potential implementation of MPC in data marketplaces?
6. What are the conditions that would need to be present in order to be able to implement the MPC technology in a data marketplace? Why are these necessary?
7. What could be the main challenges for an organisation in adopting this technology?

Final note

I would like to thank you again for your participation to this interview. Your expertise and opinion would hugely contribute to my work as well as the existing research on data marketplaces and MPC.

Kind regards,

Riccardo Dolci

Interview protocol data marketplace providers

Introduction

This interview aims to understand how MPC technology may (or may not) enable control in data marketplaces. Before starting the interview, I will briefly introduce my description of the data marketplace and its relationship with the concept of control. Moreover, I will also illustrate the MPC technology, in case you will not have the chance to read the description I have sent to you.

The interview will be recorded depending on your consent, transcribed and analysed to complete my work. I ensure the full confidentiality of your personal information, and that the information you will provide me will be used only for academic purposes.

Interview questions

1. What do you think about the landscape of data marketplaces?
    a. What kind of functionalities should be provided by data marketplaces?
    b. What are the payment models that you prefer to adopt in your platform? Why?
2. From your perspective, what is the meaning of control in the context of data marketplaces?
    a. Why or why not do you want to exercise control?
    b. What do you want to achieve from it?
    c. How do you currently exercise control?

    d. What could be the main challenges in achieving it?
3. Which features/aspects of the MPC technology are relevant for you? Why?
4. Considering your current situation, how big is your need for this technology? Why?
5. What are the conditions that would need to be present in order to be able to implement the MPC technology in your platform? Why are these conditions necessary?
6. Do you think MPC can help you to achieve your ultimate goals? Why or why not?
    a. If yes, how do you think this technology can help you? If no, how should it be improved in a way that it can help you?
    b. Do you think it would improve your ability in controlling the platform? Why or why not?
    c. Who else do you think could benefit from it? Are there any other parties who would benefit from it? Why?
7. Assuming you have decided to implement the MPC in your platform. How significant will this change be for your platform? Why?
8. Assuming you have decided to implement the MPC in your platform. How likely will this change the way your platform works? Why?
    a. How will this change the way your platform works?
        i. How will the participation to the data sharing process via your platform change?
        ii. How will the type of product traded in your platform change?
        iii. How will the way your platform store data change?
9. How likely would you adopt the MPC in your platform (now or in the future)? Why?

Final note

I would like to thank you again for your participation to this interview. Your expertise and opinion would hugely contribute to my work as well as the existing research on data marketplaces and MPC.

Kind regards,

Riccardo Dolci