Narratives of the General Data Protection Regulation:

Fostering Trust in the Digital Economy

Name: Margriet Miedema

Student Number: 433545

Program: Master International Public Management and Policy

University: Erasmus University Rotterdam

First reader: Dr. S. Grand

Second reader: Dr. K.H. Stapelbroek

Date: August 1, 2019

Word count: 23,036

ERASMUS UNIVERSITEIT ROTTERDAM

EXECUTIVE SUMMARY

Securitization theory, as introduced by the Copenhagen school, offers a discursive understanding of national and international security. This theory has challenged realist notions of security, as it offers a broader definition of the term by including non-military issues. Instead of focusing solely on what constitutes a threat, securitization theory analyses how and when a threat is narrated and successfully perceived by a public. Security may thus also be referenced in a metaphorical way, which is usually done to promote a sense of urgency.

One specific area that has been increasingly securitized is cyberspace, as it has been introduced to the concept of cyber security. As the scope of cyber security has increased, this has included the topic of data privacy. Perceptions on data privacy have become increasingly negative, and trust in online platforms has diminished. Public concern continues to rise on the matter, and governments seem to struggle with the question of how to re-build trust in cyberspace. A promising solution seems to be offered by the European Union, who, in May 2018, enforced the General Data Protection Regulation that sets out to protect the data privacy of all EU citizens. This regulation allows for the testing of the notion that data privacy as a policy area has been influenced by a securitization process.

This research has explored the considerations that shaped the General Data Protection Regulation, including the assumption that a securitization process may have taken place. This has been done by analysing documents and sessions from the three main institutions of the EU using the method of critical discourse analysis. A preliminary analysis found four main discourses used in the EU's narrative on data protection, namely discourses on unity, fundamental rights, security, and the economy. Each institution yielded different results on the presence and dominance of these discourses in their use of language, though some main considerations were found present in each one including, for example, the strong economic motive. The analysis also found evidence of a securitization process, as both implicit and explicit references were made. As the field of the securitization of data privacy is relatively understudied, this research should inspire the further exploration of developments in the field. This is especially encouraged as the role of data in society is likely to vastly increase in the near future.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ALDE	Alliance of Liberals and Democrats for Europe
CDA	Critical Discourse Analysis
DPA	Data Protection Authority
DPO	Data Protection Officer
DSM	Digital Single Market
ECR	European Conservatives and Reformists
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFD	Europe of Freedom and Democracy
EP	European Parliament
EPP	European People's Party
EU	European Union
GDPR	General Data Protection Regulation
Greens-EFA	The Greens–European Free Alliance
GUE-NGL	European United Left – Nordic Green Left
IEC	International Electrotechnical Commission
IR	International Relations
ISO	International Organization for Standardization
IT	Information Technology
JHA	Justice and Home Affairs Council
MEP	Member of the European Parliament
NI	Non-Inscrits
NSA	National Security Agency
S&D	Progressive Alliance of Socialists and Democrats
SMEs	Small and medium-sized enterprises
TFEU	Treaty on the Functioning of the European Union

INTRODUCTION

The global market has been going through many changes over the past decades - especially this last decade it has transformed drastically as consumer habits and trends have changed. Perhaps most evident has been the rise of tech companies, who now make up the five biggest companies in the world based on their global market value. Combined, these companies - including Apple, Amazon, Alphabet, Microsoft and Facebook - account for over 2.2 trillion US dollars in market value ("The rise of the tech giants", 2017). Their growth over the past decade has been immense and fast. Never before has a single sector - the tech sector - had such influence on the global market. This accumulation of power, however, has come with certain negative consequences. In the pursuit of becoming an indispensable service in society's day-to-day life, these tech giants have caused worry among the public regarding, among others, the violation of privacy, tax avoidance, and the rise of 'fake news' (Chadwick, 2017).

So, to what extent do we trust these big tech companies? The words 'trust' and 'tech giants' have made many headlines together, and a critical notion of the relationship between the two words seems to have formed. As demand for information continues to increase - especially now that artificial intelligence is taking off - data has become an increasingly valuable resource. Tech companies have tightened their grip over user data and are hoarding data as it has become a source of market power. This leaves some wondering: Have tech giants turned into "*entrenched, and perhaps abusive, incumbents*" ("The power of privacy", 2019:19)?

A recent article by *The Economist* raised a valid question many governments are currently trying to answer, which is: "How do we tame the tech giants and get them to align with the public interest?". The answer, surprisingly, does not come from Silicon Valley's home of the State of California or the United States. Instead, the European Union is pioneering action in the powerful tech industry, and EU policy makers have gained the title of 'the determinators' ("Europe takes on the tech giants", 2019). This action consists of introducing a unique tech doctrine which is based on two approaches, namely the protection of individual privacy and the boosting of competition in the tech industry.

The first approach draws on the distinct cultures of the EU's Member States, which all seem to value and protect the fundamental right of privacy. This notion of privacy is linked to autonomy, which - regarding personal data - means that you as an individual own your data and therefore can determine how and by whom it can be used. This approach to the privacy of

data has recently been encapsulated in the General Data Protection Regulation (GDPR) - a pioneering comprehensive legal framework that was enforced in May 2018 and sets out to protect the data privacy of all EU citizens. The regulation thereby aims to reshape the way in which organizations take data privacy into account in their operations. In order to achieve this goal, stricter rules and stronger enforcement mechanisms are introduced to guarantee the rights of EU citizens.

The second approach focuses on increasing competition among tech companies, so that large tech companies can no longer lock out competition. This includes the equal treatment of competing firms that use a certain platform, such as Google. It also includes preventing the hoarding of data, as is done by many tech giants. Instead of hoarding data - and thereby increasing a firm's dominance in the tech economy - dominant firms are obliged to share their bulk of collected anonymised data with competitors in the market. The EU has generally had a more sceptical approach to companies that have considerably more market power compared to others in a certain industry. Contrary to the United States - whose antitrust policies have been mostly dominated by free-market thinking - Europe links innovation to competition more so than it does to profit-seeking ("The power of privacy", 2019). In Europe there has thus been more of an ongoing discussion regarding the underenforcement of antitrust policies, and therefore more incentive to introduce such a new approach. Furthermore, the EU generally has more power to regulate antitrust matters, as not only national governments can impose fines, but the European Commission as well. Related antitrust laws regarding the tech industry already exist in, for example, Germany, where tech giants are not allowed to buy up start-ups that could grow to be strong competitors ("Europe takes on the tech giants", 2019). If the EU uses its legal power to increase competition in the tech industry by countering data hoarding, the economy may be boosted as a result. Furthermore, consumers will benefit from a more competitive tech industry, as increased competition tends to result in an increase in available choices and quality.

The EU's tech doctrine of combining the two approaches, offers a new perspective on what a government can do to counter some of the risks that are associated with having only a few large firms control the majority of data. If the doctrine is successful, both consumers and the economy as a whole could benefit. Consumers, thanks to the GDPR, would have regained ownership of their privacy and personal data and have more say in how it is used for commercial benefit. Firms and the economy on the other hand can benefit from the increase in

sharing data and information - which in turn aids the diffusion of power in the industry. This unique combination of both privacy and antitrust regulations offers a 'halfway house' solution: companies are forced to share their bulk of data, which weakens their power and empowers EU citizens ("The power of privacy", 2019).

The European Union thus seems to be taking the lead globally in introducing a new tech doctrine. The notion of the EU being in the lead on this matter, however, is not as surprising as it may seem. Firstly, the EU represents the largest trade bloc in the world and many of the tech giants make a relatively large percentage of their sales in the area. Regulations in the EU thus matter, as they have the ability to influence operations and thereby profits. Secondly, as it represents such a large economic area, EU standards are often copied in other countries - especially emerging economies. Not surprisingly, the GDPR has already led to the re-examination and revision of existing privacy frameworks worldwide.

The EU may not be the home of as many valuable tech companies as the United States, but this does allow the EU to take a more objective stance and thereby take on a more objective leadership role. In the EU, more attention can be given to the public interest as EU regulators will likely be less influenced by tech giants' lobbying efforts compared to the US. It is also argued that Europe is relatively more vigilant about the issue of privacy, due to the relatively recent history of dictatorships on the continent. Its vigilant position on privacy has therefore paved the way to taking a leading role in taming the tech giants ("Europe takes on the tech giants", 2019).

But to what extent is this sentiment shared among the EU public? A recent Eurobarometer survey reports the attitudes of EU citizens towards data protection and related issues. Overall, the results highlight the existence of true concerns among the EU public. 67 percent of the respondents show concern regarding a lack of control over the information they make available online (European Commission, 2015). The majority of the respondents (71 percent) agree that providing information online has become an indispensable aspect of modern-day life. However, this does not mean that providing personal information is not perceived as an issue, as 57 percent of the respondents expressed. A large majority (nine out of ten respondents) agreed on the importance of having rights and protection of their personal data - whether at the national or the European level. The survey furthermore concluded that concerns existed about

the purpose of the processing of their personal data, the potential loss or theft of their information, and the lack of informed consent (European Commission, 2015).

The introduction of the new tech doctrine thus seems to match the general concerns of the European public. These concerns were reflected in the EU's Europe 2020 strategy, under the pillar of a digital agenda for Europe. The digital agenda's main purpose has been to create a Digital Single Market (DSM) to enable smart and sustainable growth in the EU ("Europe 2020 strategy", n.d.). This strategy includes, among others, creating conditions for fair competition, reducing geo-blocking, and solving intellectual property rights issues. Another main element of this strategy consists of building online trust and security, which includes reducing privacy breaches and increasing private data security ("Europe 2020 strategy", n.d.). One of the Digital Single Market strategy's main achievements so far has been the General Data Protection Regulation, which was proposed in 2012 and enforced in May 2018.

One could argue that the European Union has thus been actively responding to the public's concern about the protection of personal data. This notion however may be part of a larger narrative of the EU as a political actor, in which the daunting power of tech giants and technology in society has been securitized. This concept of securitization was introduced by the Copenhagen School – an approach spearheaded by scholars such as Waever and Buzan - and follows social constructivist and post-structuralist thinking. The Copenhagen School introduced securitization as a process in which an actor frames domestic or international interests as a security threat. Therefore, securitization mostly concerns the framing of a threat and steers away from security as an objective concept. This broader understanding of security is in contrast with the traditional realist notion of security, which mostly relates the concept to issues regarding state sovereignty (such as border control or military operations). According to the Copenhagen School, environmental, social, and economic issues, for example, can therefore be influenced by a securitization process.

In this case, it can be argued that the European Union has become a securitizing actor if it has promoted a security narrative regarding the protection of personal data. This may especially be worth analysing, when considering the coined terms of EU regulators being 'pioneers' and 'determinators'. Such a securitization process can be considered successful if the audience is convinced to a certain extent, or if the narrative can motivate political (and/or social) action. Such action can, for example, result in the adoption of new policies and regulations.

Following this line of thought, the adoption of the General Data Protection Regulation could have been influenced by a possible narrative created by the European Union and its institutions. Such narratives can be discovered through the analysis of language use, for which the method of discourse analysis is a fitting choice. Discourse analysis allows for the study of language in use. Using this method, discourses can be found and analysed. The use of this method could also detect the manner in which the public issue has been politically defined.

It is for this reason that this research opts for using the method of discourse analysis to look for the potential narratives that have shaped the GDPR. This research thereby aims to answer the following question: "*What were the main considerations in shaping the General Data Protection Regulation?*". This question is exploratory and open-ended in nature, as it not only examines the possibility of a security discourse, but also any discourse beyond it. The aim is to find these considerations, which become apparent in written or verbal narratives. They therefore do not refer to the factual and technical elements regarding the existence of the GDPR, but to the framing of narratives which have played a dominant role in the discourse on the regulation. In this case, framing would have been introduced by the main institutions of the EU (namely, the Commission, the Council, and the European Parliament) as these actors have the ability to introduce narratives to set the political agenda or implement a certain regulation. The considerations therefore represent those of these institutions (but also the Member States and EP fractions individually).

If evidence of, for example, a security narrative is found, this could have motivated political action which would have shaped the GDPR. Opting for an exploratory research question therefore provides a more comprehensive approach to analysing the underlying considerations for the regulation, which can be found in the form of narratives. This is of relevance, as the GDPR - as a fairly recent development - has been relatively understudied regarding the existence of narratives. Furthermore, the focus on such a recent development could shed light on data protection as a subset of cyber security - a field that has drastically increased in scope since the end of the Cold War. It is therefore possible that the concept of data protection as a security narrative could increase in scope in the near future. Lastly, academic research on the EU as an actor regarding cyber security has been sparse as most research has focused on the United States and other regions (Christou, 2017). Analysing the EU as an actor regarding data protection could thereby partially fill in this gap in literature.

To reach a conclusion on the research question, this research adopts the method of critical discourse analysis. This entails the analysis of documents and sessions of the Commission, the Council, and the European Parliament. Analysing these cases can uncover underlying narratives, which highlight the main considerations of these actors. Chapter 2 is a literature review on the concepts of cyber security and data protection. Chapter 3 will give more information on the General Data Protection Regulation itself, as this will give a better understanding of the regulation before the analysis. Chapter 4 will give an overview of the theories related to the method of critical discourse analysis. The following chapter – chapter 5 – will explain the design of this research. Chapter 6 will constitute the empirical analysis of the selected cases. This will be followed by Chapter 7, which discusses the main findings and limitations of this research. Chapter 8 will provide a general conclusion.

LITERATURE REVIEW

The main objective of the General Data Protection Regulation is to "*protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*" as stipulated in Article 1.2 ("General Data Protection Regulation (GDPR) – Final text neatly arranged", 2018). In striving to do so, the GDPR establishes the legal rules that guarantee the protection of personal data of EU citizens. In order to better understand why such a regulation came to exist, the following section will begin by examining the literature on cyber security as a wider concept within society. As data protection is considered a part of the field of cyber security, the section will continue on with issues related to the processing of personal data - including those of data breaches and data appropriation.

2.1 The Digitization of Society and Cyber Security

The process of digitization has permanently changed and continues to change lives within society. This process involves the transformation of information into a format that is digitally readable, which has advanced the processing and storing of data. Digitization has brought about an increase in ease, speed, and cost-efficiency concerning communication, business processes, and big data (Abolhassan, 2017). Its impact has been remarkable on society, and digitization is often associated with progress and is named the "*digital equivalent of the Industrial Revolution*" (Le Bacon-Gaillard, 2016:para. 2). This progress, however, has raised new security concerns.

Cyber security as a concept evolved and appeared on the political agenda in the post-Cold War era as a response to new technologies and the newly changed geopolitical situation (Hansen & Nissenbaum, 2009). The topic of cyber security first appeared among computer scientists. Though the existence of hackers had been around since the 1950s, it was not until the late 1980s that they were deemed as a threat to national security and as invaders of privacy (Nissenbaum, 2004). These warnings were increasingly echoed by the media and politicians. Simultaneously, cyber technology became more complex and sophisticated. The attention for cyber security reached new peaks following the events of 9/11 (Hansen & Nissenbaum, 2009). Cyberspace was now seen as "*an easy, low-cost, and low-risk*" instrument for terrorist groups and other non-state actors to intensify the effect of their attacks (Silber & Garrie, 2015:para. 2). To this day, the threat of a 'Cyber 9/11' continues to exist, which would encompass a major attack by foreign hackers on national cyber infrastructures.

Cyber security as a definition covers a wide array of practices aimed at protecting computer systems from unauthorized users or attacks. The term is often used as an all-inclusive definition, encompassing *"the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace"* (von Solms & van Niekerk, 2013:101). Cyber security thus serves to protect not only cyberspace itself, but also those that are vulnerable within it, which is any individual that can suffer from tangible or intangible cyber threats. This human element to the definition is what distinguishes cyber security from other types of security, such as information security. This human element also translates to national or state-interests, as states can also have their interests compromised within the realm of cyberspace.

Partly due to these interests, cyber security as a topic has been securitized in political, social, and technical spheres for at least the last three decades (Dunn Cavelty, 2013). According to Nissenbaum (2005), the topic of cyber security has two main conceptions of security - which co-exist within a securitization context of gaining attention and resources from the public, policy makers, and experts. The first concept is considered more scientific and technical, and is therefore labelled 'technical computer security'. This concept is predominantly employed by technical experts, and emphasizes the protection from threats involving the availability, integrity, and confidentiality of information and networks (Nissenbaum, 2005). The second concept - labelled as 'cyber security' - is considered a more recent approach and is influenced by predominantly governments, corporations, and NGOs. These actors link cyber security to the traditional notion of national security. In doing so, they emphasize three main threats, including (Nissenbaum, 2005):

1. The use of computer networks by dangerous or disruptive organizations, such as hate groups, criminal networks, and terrorist networks.
2. Attacks on the infrastructure of vital societal systems, including among other things state administration, banks, healthcare, education.
3. The impairment of the information system itself.

Therefore, what differentiates cyber security from the more technical conception of computer security, is its broader scope. Furthermore, the two approaches demand different responses. Technical computer security discourse often evokes a response that can be considered similar

to responses to unethical or criminal activities. Cyber security on the other hand, calls for prioritized, and even extraordinary measures that go beyond policy practices that are in place at that specific time (Nissenbaum, 2005). Cyber security can therefore be considered extra powerful, as the concept has the ability to evoke non-conventional responses. This is in line with the concept of securitization as introduced by the Copenhagen School, which argues that the framing of an issue can generate political (and/or social) action. Policy efforts regarding cyber security can be traced back to the 1980s, which marked the beginning of the securitization of cyberspace. As the domain of cyberspace was not one to be exposed to physical military threats, much of its link to national security was based on the protection of critical infrastructure. This led to the recognition of the vulnerabilities of society - and more importantly, the state - which completed the securitization process (Deibert & Crete-Nishihata, 2012).

Regarding cyber security, political motives can easily be concealed as security or technical ones (Hansen & Nissenbaum, 2009). Nissenbaum (2005) argues that the securitized strategy of cyber security can be well applicable in urgent situations. Caution, however, must be taken when this type of securitization happens outside of this urgent context, as it can increase the power of governments or other authorities and thereby can increase the risk of a possible repression of society. Despite this caution, the link between national security and cyber security has become stronger over time and resulted in political and budgetary consequences. According to Dunn Cavelty (2013), the cyber security discourse consists of a number of subcategories, for example those of cyber-war, terrorism, and cyber-crime. What differentiates these subcategories is the object they refer the threat to. All, however, have in common that they are influenced by the overall security of the computer network. Dunn Cavelty (2013) categorizes three main threats that are found within cyber security discourse: the technological cluster, the socio-political cluster, and the human-machine cluster. Each cluster yields a different response and calls for different countermeasures.

The technological threat discourse for example mainly opened the door for the antivirus industry to grow and evolve. The socio-political discourse on the other hand is mainly linked to the increase in legal tools revolving around cyberspace. Lastly, the human-machine cluster - which involves the complexity and insecurities associated with the modern technology infrastructure - has yielded mostly protective and risk-management measures (Dunn Cavelty, 2013). Cyber security as a whole thus consists of a ‘reservoir’ of different approaches to the

representation of threats, of which political actors can make use. Their use is mainly to mobilize further political discourse and action. This need for mobilization continues to increase as there is little knowledge on which cyber risks could actually lead to a cyber 'doomsday'. From the standpoint of a policy maker, an expansion of political action regarding cyber security is thus necessary to prepare for this brewing threat (Dunn Cavelty, 2013).

2.2 Privacy and the Protection of Data

Privacy is recognized as a fundamental human right. This has been acknowledged by the Universal Declaration of Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union - which defines privacy as the right "*to respect his or her private and family life, home and communications*" (European Union, 2000:10). It is followed by Article 8 of the Charter, which highlights the freedom to protect personal data. Under this article (European Union, 2000:10): *"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".* Privacy is thus considered a fundamental right and an essential individual freedom.

The extent to which we value our privacy comes into question when one considers the potential benefits of the collecting and processing of data. Especially in this new age of information and technology, it has become difficult to balance these benefits with the potential threat of losing the freedom of privacy. The question of to what degree we value our privacy has become increasingly complex, as there has been a continuous increase in the power imbalance between the entities that process data, and the individuals whose data, and thereby privacy, are at risk. People therefore face a trade-off between using popular online platforms and misuse of their data. A recent example of such misuse is the unconsented harvesting of 1.5 million emails by Facebook (Doffman, 2019). Not only are such actions a breach of privacy due to the absence of consent, they are also often commercially exploiting.

Data processing is the collecting, managing, storing, recording, using, or making available of personal data (European Union, 2016). When such processing is done without consent, or when data is accessed by unauthorized actors, one can speak of a data breach. A formal definition is offered by the International Organization for Standardization (ISO) and the International

Electrotechnical Commission (IEC) who defines a data breach as a *"compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed"* (ISO/IEC, 2015:para. 3.7). In the media, data breaches are often credited to hackers and malware. Other incidents that can occur consist of data theft or loss, non-consensual disclosures, phishing, or insider attacks. Those that compromise people's personal data are part of a diverse group of actors, including individual criminals or hackers, organized groups, state-sponsored groups, and insiders (Huq, 2015).

The public disclosure of data breaches has steadily increased since the 1980s - partly due to laws that require private companies to disclose certain information to their consumers. Such information has recently included the notification of when consumers' personal information may have been compromised. A frontrunner regarding such breach disclosure laws, has been the state of California - which passed the S.B. 1386 bill in 2003, which required organizations to notify those individuals whose information had been compromised (Schwartz & Janger, 2007).

Reports on how often data breaches have occurred over time differ. Some reports reveal that the rate at which data breaches appear has increased since 2009 and emphasize that data breaches are here to stay (Huq, 2015). Data made available by the Privacy Rights Clearhouse reports that since 2005, 8.804 data breaches have been made public - which involved a speculated 11.575.804.706 records (Privacy Rights Clearhouse, 2019). A study by Edwards, Hofmeyr and Forrest (2016) however argues that neither the size or frequency of breaches have increased over the last decade. According to the authors, a possible explanation for this is that data privacy practices have improved at roughly the same rate as data attackers have. It thus may be that society is in an arms race with hackers and other rogue elements, and must continuously evolve its protective practices in order to defend privacy.

Data breaches can occur in a number of different institutions. Garrison and Ncube (2011) examine six types of institutions based on United States' data from 2005-2009, consisting of business, education, medical, local/state government, financial, and federal/military. Their findings conclude that education suffers the most amount of breaches - which can be explained by the relatively larger amount of personnel that have access to information. When considering the total amount of breached records however, the business sector has suffered most, closely

followed by the federal/military institutions, and financial institutions. When data breaches at these types of institutions do occur, they thus usually entail a larger amount of breached records. Such breaches can become very costly, as the average cost per record lost is 148 US dollars (Ponemon, 2018).

Despite the costs associated with data processing, it can be a lucrative activity. Especially those actors on the social web - including technology companies and social media platforms - have been known to utilize personal data for commercial purposes. As users of these platforms, one contributes to increased knowledge of one's interests and preferences. Those organizations that collect, utilize, and sell such data, argue that data is "*valuable property to which they have justifiable legal rights*" (Reyman, 2013:516). They base this argument on the idea that user data is not necessarily created by the user itself, it is more a by-product of technologically created processes such as algorithms, which are inherent to the - predominantly free - services these organizations offer online.

This practice has had led to the coining the term 'data appropriation' which refers to the creation of commercial value by these companies without any compensation to users. Data appropriation is only expected to grow as its commercial value has created an arms race for the collecting of data. This capitalist mindset toward data has been embraced by leading tech companies such as Amazon, Google, and Facebook, who have grasped the notion of data as an asset (Sadowski, 2016). These companies have thus started the hoarding and monetizing of as much data as possible.

Data appropriation has, however, become a considerable ethical discussion. As the term 'appropriation' implies, much of the data of individuals is collected without consent or compensation. Moreover, many people seem to be unaware of the fact that their data is collected and used, and "*the generation, collection, and use of data occur with a surprising lack of transparency*" (Reyman, 2013:518). Companies like Facebook have been known to leverage user data for commercial advantage in non-transparent ways (and often in contrast with their public statements) (Doffman, 2019). When these organizations do seek consent, it typically happens through terms-of-use agreements - which are required by law. These agreements, however, can be rather lengthy and difficult to read for the average user, and thus users are often surprised to discover that their personal information is used for commercial ends (Reyman, 2013). It can therefore be considered a breach of their expectations as to their privacy

on such online platforms. The industry of collecting and processing data generates an estimated annual revenue of over 200 billion US dollars (Sadowski, 2016). These amounts are likely to increase over time, and it has been argued that better policies of data ownership and protection are needed to reflect the new role of information and data in society (Sadowski, 2016).

THE GENERAL DATA PROTECTION REGULATION

The recent European response to the question of data privacy has been the General Data Protection Regulation - which entered into force in May 2016. The regulation has been fully implemented by all EU Member States since May 2018. The GDPR would come to replace the Data Protection Directive that was adopted in 1995 and arrives at a time when more and more data is entrusted to the cloud. As data breaches have become more frequent, the GDPR is designed to protect the privacy and security of EU citizens. It does so by imposing strict requirements on organizations - which need to be met in order to avoid hefty penalties. These organizations can be from anywhere in the world, as long as they offer goods or services to - and process personal data of EU citizens.

The following section will focus on what the General Data Protection Regulation represents and how it is designed. This is an important step preceding the discourse analysis, as it sheds light on the functioning and purpose of the regulation, but also on who this regulation particularly serves. Furthermore, this section will look into the functioning and the relative effectiveness of the regulation in its first few active months. Lastly, as the GDPR marks a considerable change regarding the processing of data, its global influence will be given attention.

3.1 Principles

The GDPR was built on a number of principles related to the processing of data, which serve to ensure protection and accountability. As defined in Article 5.1 and 5.2 of the GDPR, these principles are as follows (Irwin, 2018):

1. Lawfulness, transparency and fairness: Data processing needs to be lawful, fair, and transparent.
2. Purpose limitation: Data processing can only be done for a specific purpose.
3. Data minimization: Data processing should only go as far as needed for its purpose.
4. Accuracy: Data must be kept accurate and complete.
5. Storage limitation: The storage of data must be limited, meaning that data must be deleted when it is no longer in use.
6. Integrity and Confidentiality: Data must be kept secure from unauthorized users or losses.

A seventh principle refers to the accountability of organizations that process data. Those individuals within an organization that are responsible for the processing of data are required to demonstrate compliance with the GDPR. One way of ensuring compliance, is by appointing a Data Protection Officer (DPO) - which the GDPR requires for some organizations. A DPO is appointed to be the GDPR expert for an organization and is there to provide knowledge on laws and practices regarding data protection. Such tasks include informing employees of the organization, monitoring compliance, and performing impact assessments. Though every organization should have an individual tasked with the monitoring of GDPR compliance, Data Protection Officers are only required if certain criteria are met. These criteria include that the organization is a public body, performs large-scale monitoring of data subjects, or processes specific categories of data ("Everything you need to know about the GDPR Data Protection Officer," n.d.).

3.2 Supervision

Article 68 of the GDPR establishes the European Data Protection Board (EDPB), which is an official body of the European Union based in Brussels which has a legal personality. The EDPB has come to replace the Article 29 Working Party, which functioned under the 1995 Data Protection Directive. The Board is comprised of the European Data Protection Supervisor (EDPS) - which is an independent supervisory authority for EU institutions and bodies specifically - and the heads of data protection authorities (DPA) from each Member State. The Board mainly functions to contribute to the correct application of the GDPR throughout the EU, and to promote cooperation among DPAs. Another important task is that of advisory to the Commission, mainly concerning data protection in international organizations or third countries (de la Torre, 2019).

3.3 Fines and Penalties

Non-compliance with the GDPR can be quite a costly move for organizations, as GDPR fines are considered relatively high. The amounts, however, differ per organization, depending on the size of the firm or for example the scale of the data breach. As Article 83 of the GDPR states, there are two tiers of fines. The first tier concerns the less severe non-compliances, with fines up to ten million Euros or two percent of an organization's total global turnover from the previous financial year - whichever is the higher amount. The second-tier concerns more severe infringements, which mostly concern violation of the GDPR's core principles regarding privacy and the right to be forgotten. The second-tier fines can go up to twenty million Euros

or four percent of the total global turnover from the previous financial year. These fines can also be given when additional Member State laws are violated or when there is non-compliance with an order from a supervisory authority, such as the DPAs. Besides these fines, any individual who suffers material or non-material damage from an infringement can seek compensation from those controlling or processing his or her personal data ("What are the GDPR Fines?", n.d.).

Since the GDPR came into force in May 2018, the regulation has proven to be a relatively effective tool in guaranteeing the protection of personal data. Recent figures published by the European Data Protection Board show that over 95.000 complaints by individuals and organizations concerning suspected violations of their rights have been filed to data protection authorities. Most of these complaints have concerned the telemarketing and video surveillance industry, and promotional emails (Zorz, 2019). Moreover, the Board released that over 41.000 data breaches have been notified by companies to national DPAs. Most of these breaches have occurred in the Netherlands, Germany, and the UK (Zorz, 2019).

Data from February 2019 reveal that over 90 fines have been issued so far under the GDPR (Zorz, 2019). Since the regulation came into force in 2018, the number of fines that are handed out has steadily increased. This marks the end of the 'amnesty period', which characterized the transition period in which organizations were granted some leniency and time regarding the implementation of the regulation (Mittel, 2019). While many organizations spend time and resources to ensure they are GDPR compliant, fines have been handed out to organizations for what can be considered basic errors - mostly regarding access to personal data, password encryption, and CCTV notifications (Mittel, 2019). Some heftier fines have been handed out for lack of transparency and consent, such as the fifty million Euros fine for Google - handed out by a French DPA. In this case, Google failed to provide transparency and get valid consent from its users regarding personal ads (Simberkoff, 2019).

These first few months of the GDPR's operation and the accompanying fines provide organizations with some important lessons. First, it is important to cover the basics of data protection in order to avoid fines. Second, organizations must realize that ultimately, their headquarters location or server location does not matter in terms of which DPA issues the fine. This aspect was highlighted in the Google case, as it was the US location of Google LLC which was responsible for the processing of EU data - which was then fined by the French DPA

(Mittel, 2019). A final take away from the first months of the GDPR is that the amnesty period to implement the regulation seems to be over. Organizations can thus expect an increase in the amount of fines and can expect heftier fines. This is also partly because it is likely that courts will reference competition law and jurisprudence on which to base the GDPR fines, and EU competition law has imposed hefty fines on big tech companies in the past (Zorz, 2019).

Despite the relatively effective first months of the GDPR, some critical notes have been added to the functioning of the GDPR. The GDPR's short-term effect has been that European technology ventures have received less investments, relative to those investments made in the US (Jia, Jin & Wagman, 2018). Jia, Jin and Wagman's research furthermore shows that mainly newer technology startups have suffered, which leads the authors to anticipate a future drop in technology employment in Europe. This assumption is somewhat in line with what tech giants have been suspecting before the regulation came into effect, which has been that the new EU regulation would be significantly more difficult for smaller companies as compared to larger ones. Larger companies have sufficient resources and legal power to easily comply with the regulation, and therefore the GDPR may have actually favoured tech giants like Google and Facebook. A counter argument to this may be that the GDPR is moving companies away from investing in data plundering activities and toward other innovative fields. This has the potential to positively influence the competitiveness of the European Union (Bershidsky, 2018).

3.4 Global Influence

The EU's General Data Protection Regulation has led organizations around the world to evaluate their own privacy policies. The regulation marks an evolution regarding the balance of power between organizations and citizens, built on the fundamentals of privacy (Goddard, 2017). What makes it especially innovative is its wide jurisdictional scope which goes beyond that of the European Union. This wide territorial scope could make the GDPR a data protection model for the rest of the world, as many global organizations have to adapt to the regulation as many of them serve EU citizens. Companies such as Facebook have already hinted that it might expand its new GDPR-compliant policies worldwide (Chakravorti, 2018).

The GDPR, however, does not provide an answer to non-EU countries and their citizens. First, some countries may opt to free ride on the EU regulation. Nonetheless, support for such regulation varies from country to country. For example, in countries such as the United States, an argument against having more stringent rules is based on protecting competitiveness

(Chakravorti, 2018). Companies, it is argued, must have the ability to collect and analyze personal data in order to ensure the innovativeness of the digital industry - and thereby the competitiveness of the US economy. The question of data privacy thus does not yield a united answer across the globe, as views vary on the possible trade-off between privacy and other (economic) benefits.

Furthermore, the degree of data protection in a certain country can lead to a new form of inequality between the developed and developing world. Users from developing countries were found to be more trusting of online platforms, and generally are more prone to be manipulated or lack information - making these users a vulnerable group. This group moreover seems to continuously grow, as many companies such as Facebook now have the largest amounts of users in developing countries. Safeguards are thus needed in developing countries, but they might be wary of extensive regulations such as the GDPR as it does have the power to harm smaller firms (Chakravorti, 2018). What could potentially happen, is a world divided into what can be considered safer digital zones - predominantly in developed countries - and zones consisting of predominantly developing countries in which individuals are more at risk.

In sum, the GDPR has not produced a domino effect yet and it might not ever as the regulation's basis on the fundamental right to privacy is challenged by economic arguments which may influence the interests of countries such as China and several states in the United States (Baxter, 2018). However, a domino effect may still occur, as the EU's largest trading partners may find it easier to adopt similar regulations. So far, countries such as Japan, Brazil, Australia, and the state of California are moving towards similar regulations (Baxter, 2018). Whether the GDPR will serve as a blueprint for the rest of world's data protection regulations thus remains debatable. However, the influence the GDPR has had as yet, is that is has caused the re-examination of - and debate on - existing privacy frameworks worldwide.

THEORETICAL FRAMEWORK

In order to better understand the underlying considerations that shaped the General Data Protection Regulation, this research adopts the method of discourse analysis. This chapter will give an overview of the theories from which this method originated. These include social-constructivism and post-structuralism. Furthermore, a closer look will be taken at securitization theory - a concept originated by the Copenhagen school - which offers a different perspective on the concept of security.

4.1 Social Constructivism and Post-Structuralism

Social constructivism as described by Alexander Wendt lends itself well to the study of international politics and the interactions between states - though it in itself is not a theory of international politics. According to Wendt, social constructivism became more popular in the post-Cold War era, as more mainstream international relations theories such as realism could not fully explain how the Cold War ended (Wendt, 1999). Social constructivism offered a more holistic approach to interpreting international relations and helped shed new light on concrete issues dominating international politics. Wendt's social constructivist approach to IR deviates from realist theories such as realism and neoliberalism in how it approaches the collective action problem. Both realist and neoliberal theories fail to treat state interests as something that is endogenous to state interaction. Whereas realism considers state interests to be dominated by self-interest and thereby exogenous to interaction, neoliberalism has rather neglected the notion. Wendt's social constructivism reframes the collective action problem to one where state interests are endogenous to state interaction (Wendt, 1994). It thereby offers a constructivist argument, which is that states and their interests are shaped by "*historically contingent interactions*" (Wendt, 1994:385). In that sense, constructivism can contribute to the liberal focus on the transformation of state identities and interests (Wendt, 1992). In doing so, social constructivism takes these identities and interests as the dependent variable for analysis. In sum, three core claims of constructivism can be identified (Wendt, 1994:385):

1. "*States are the principal units of analysis for international political theory;*
2. *The key structures in the states system are intersubjective, rather than material; and*
3. *State identities and interests are an important part constructed by these social structures, rather than given exogenously to the system by human nature or domestic politics*".

The state as the central unit of analysis and as a social construction can take on two types of identities. These identities are distinct and therefore non-rivalrous, in the sense that each form can explain different interests that motivate (collective) action. A first identity is that of corporate identity. A state's corporate identity constitutes their intrinsic individuality - as shaped by shared beliefs and institutions. Four interests can be identified that are inherent to this sense of identity (Wendt, 1994:385):

1. "*Physical security, including its differentiation from other actors;*
2. *Ontological security or predictability in relationships to the world, which creates a desire for stable social identities;*
3. *Recognition as an actor by others, above and beyond survival through brute force; and*
4. *Development, in the sense of meeting the human aspiration for a better life, for which states are repositories at the collective level*".

These interests influence states' motivations for engagement in (collective) action. The concept of corporate identity however must not be confused with that of self-interest, as these interests are in relation to 'the other' - in IR this concerns mostly other states.

The second type of identity of the state is that of the social identity. Social identities refer to the meanings the state assigns itself, depending on 'the other' and their perception of the state (Wendt, 1994). A state can thus have multiple social identities, depending on the number of 'others' the state engages with. This allows states to engage with one another and maintain their individuality, while simultaneously being aware of underlying expectations and mutual understandings. It can thereby influence the way in which states define their interests and thereby their actions. These social identities furthermore are continuously reshaped as interactions take place, making them fluid and not fixed - as is assumed by other theories such as realism. Social constructivism, however, does not assume that social identities automatically lead to collective action choices. It very much co-exists with self-interest, making the motivation for action differ per issue. Social identity does, however, determine the boundaries to how the 'self' in self-interest is identified.

The European Union makes for an interesting case, as it presents itself as a collective actor, while also having numerous individual Member States who each possess several social identities. This research to an extent hypothesizes that the EU has taken on the role as a

securitizer concerning the data - and privacy protection - of its citizens. This collective role has shaped the interests which have led to the creation of the GDPR as it is today. A discourse analysis, as will be discussed below, can help identify these interests and their underlying understandings.

This type of analysis is also related to post-structuralist theory. Post-structuralism finds its origins in French philosophy, where it marked itself as a deviation from structuralism in the 1960s and 70s. Structuralism essentially was a structural linguistic approach, where language could be studied by focusing on its underlying structures as part of a larger system (Olssen, 2003). Language was studied as a system, as it represented a social institution belonging to a collective of individuals - meaning that the language of individuals was defined in relation to that of others. Following this logic, what constitutes a language is determined by "*a system of differences, and the kinds of differences that a language embodies*" (Olssen, 2003:190). These differences can account for the way in which reality is understood in society.

Post-structuralism takes on a more critical perspective and allows for the critical evaluation of "*social institutions, cultural beliefs and political arrangements*" (Wylie, 2006:298). Post-structuralism constitutes a more sceptical approach, which rejects the idea that truth can be deemed obvious or or be deemed as common sense. It thereby represents quite a radical approach, even when compared to theories such as Marxism, as it assumes that nothing in society is fundamental. Society is plural and complex, and requires one to question its deepest beliefs.

It was writers like Foucault and Derrida who deviated from traditional structuralist theory. Though inspired by structuralism in his early works, Foucault rejected many notions that were central to the original theory (Olssen, 2003). Foremost was that underlying structures were both universal and ahistorical. According to Foucault, these were neither: identified regularities in the understood meaning of language were specific to particular time periods and places. This shifted the focus to the micro-scale of individuals' lives. What distinguished Foucault from other post-structuralist writers was his focus on power, which made his work resemble a more materialist conception. Meaning - as in how reality is understood in society - is affected by "*historical and social context, and within such a context, by power*" (Olssen, 2003:194). Reality furthermore does not only consist of the discursive level, but also that of the pre-levels of reality. Foucault argues that any reality is shaped by relations between forces. Reality is thus

not only shaped by the result of those forces - but also by how these forces were shaped externally before entering the relation.

Derrida on the other hand is best known for the development of the term deconstruction. Deconstruction is both an ongoing process as well as a method that is used to understand the relationship between language and its meaning. According to Derrida, there is no actual definition of the term. Rather, deconstruction is what simply happens (Royle, 2003). It thereby is inherent in language, but it also constitutes more than a language. This allows for deconstruction to undermine that what society believes constitutes the truth (Wylie, 2006).

4.2 Securitization Theory

A discursive understanding of national and international security has been offered by the Copenhagen school - one which has challenged realist notions of security. Traditionally, the concept of security refers to the state and its national security. Realist theory takes on a rather narrow view of the concept and emphasizes military affairs such as the protection of borders and countering foreign military attacks. This narrowness has been criticized as it only concerns matters related to state sovereignty, and attempts have been made to approach the concept of security in a wider manner (Waever, 1996). The danger of increasing the scope of the concept is that, potentially, everything could be considered a security issue.

A notable attempt has come from the Copenhagen school, which offers a broader understanding of security by going beyond border and military threats (Nissenbaum, 2005). The Copenhagen School has thereby tried to create a concept that lies "*somewhere between the narrow (always state, only military) and the wide (everything people worry about)*" (Waever, 1996:106). This has led to the definition of security not being an objective matter, but "*a way to frame and handle an issue*" (Waever, 1996:108). The Copenhagen School argues that security carries a sense of urgency, which allows for any security discourse to bring in non-military issues, as long as it is accepted by the audience as a national or international security concern which is a result of the framing process. This ability has led to the coining of the term 'societal security' - meaning "*the ability of a society to persist in its essential character under changing conditions and possible or actual threats*" (Waever, Buzan, Kelstrup & Lemaitre, 1993:23). This marked a clear distinction from security-thinking in only a state or military way. Moreover, securitization does not for the most part concern what actually constitutes a threat. Instead, it is predominantly about how to successfully portray a threat as a threat and what that

entails. Key contributors to the Copenhagen School such as Waever and Buzan were predominantly interested in highlighting conditions in which the securitization of a threat appears and when the process is successfully achieved (Nissenbaum, 2005). This perspective suggests that framing a threat as a security issue can be a decision made by, for example, politicians.

What is central in a security discourse is a sense of emergency, which demands prompt measures (Hansen & Nissenbaum, 2009). This has allowed for a broadened understanding of what security may entail in a discourse that goes beyond conventional security concepts. Instead, any referent object that resembles the concept of security semantically can be considered part of a securitized discourse. Security as a term thus does not indicate a definitive criterion for securitization, as it may also consist of "*only a metaphorical security reference*" (Buzan, Waever & De Wilde, 1998:27). A key feature of threats that can be securitized is therefore that they are presented in a way that mark their emergency, by emphasizing their imminent, harrowing, and existential nature (Nissenbaum, 2005). Whether this sense of emergency is established successfully or not, depends on how it is received by the audience. This audience usually consists of the public but can also be made up of policymakers, technocrats, and bureaucrats.

Within the Copenhagen School, security concepts tend to lean towards the collective understanding of the term. An often-found concept is that of national security, which highlights the relational characteristic of security as one between individuals and states (Hansen & Nissenbaum, 2009). National security is then articulated as individual security that is provided by the state. It is thus not uncommon that within political discourse the individual is often addressed on a collective basis, and it is unlikely that specific individuals become the object of securitization. This is in line with the works of Waever and Buzan, who argue that "*only general collectives or collective values count*" as the referent objects of securitization (Nissenbaum, 2005:66). Exceptions to this notion can however be made when a clear link can be established between the specific individual interests and those of the collective.

Those who have the power to securitize are considered securitizing actors. First, to be a securitizing actor, one must have the capacity to do so. Actors who have the ability to do so typically include a range of state actors, including government officials, politicians, government agencies, military officials, and heads of state. Other non-state sources of

securitization can consist of the media, jurists, (large) corporations, and pressure groups (Nissenbaum, 2005).

Within the context of this research, the European Union is highlighted as the securitizing actor. The existential threat that is being narrated is that of the vital need to protect all EU citizens from privacy violations and data breaches. EU citizens have thus become the referent object of securitization, as they consist of the objects that need protection from these privacy breachers and appropriators. The audience that must accept this narrative in order for the securitization to be considered successful consists of EU citizens - both directly and indirectly through the European Parliament (EP) - and the EU's Member States. The EU's GDPR thus fits within the context of what a securitization process entails.

RESEARCH DESIGN AND METHODOLOGY

Following the literature review and the theoretical framework, it can be hypothesized that data protection - as a subset of cyber security - may have been securitized. Taking on the example of the GDPR, the EU is considered the securitizing actor as it has designed and adopted the regulation. Whether in fact the EU's policy on data protection has been part of a larger trend of the securitizing process of cyberspace, can be examined by adopting critical discourse analysis as the method of research. This method does not solely focus on finding evidence for securitization, as it takes into account all possible discourses. Any outcome beyond that of securitization can thus be possible, which allows for the exploration of all considerations that played a role in establishing the GDPR. The following sections will discuss this research's method of approach, which include how to perform a critical discourse analysis; the decision to conduct preliminary research; and the selection of cases.

5.1 Critical Discourse Analysis

Discourse analysis is considered the study of language in practice. It studies how language differs in its meaning and the actions that follow it. Discourse analysis can be considered a branch of linguistics, but it also contributes to social sciences due to its ability to study language in social contexts - e.g. historical, political, institutional, and so on (Gee & Handford, 2012). It is therefore that discourse analysis as a research method is often used in a wide range of disciplines, including that of political science. Many different forms of discourse analysis exist. A form that is predominantly interested in "*tying language to politically, socially, or culturally contentious issues and in intervening in these issues in some way*" is called critical discourse analysis (Gee & Handford, 2012:5).

Critical discourse analysis (CDA) contributes to critical social analysis because of its specific focus on discourse and its relation to other social elements such as institutions, identities, and power relations (Fairclough, 2012). This type of analysis is both normative and explanatory in nature. Its normative character relates to its ability to not only describe reality, but also assess to what extent it matches society's values. On the other hand, its explanatory character is able to highlight the underlying forces behind existing structures or mechanisms. Within CDA, discourse is defined as the "*ensemble of ideas, concepts, and categories through which meaning is given to social and physical phenomena, and which is produced and reproduced through an identifiable set of practices*" (Hajer, 2005:300). Discourse thus refers to concepts that structure individual or groups of participants' contributions to any discussion. These

concepts resemble structures, which can be found through analysis. Though perhaps not immediately obvious, once a structure is found, a discourse can be easily recognized (Hajer, 2005).

When translating the concept of CDA to the political arena, it mostly concerns the manner in which a political issue is defined. The definition of a political issue is usually part of a grander narrative which is formed by an actor or group of actors. The way a political actor narrates a political issue matters, as "*language has the capacity to make politics, to create signs and symbols that can shift power-balances and impact … institutions and policy-making*" (Hajer, 2005:300). Discourse therefore has a direct ability to shape policy.

Critical discourse analysis allows for the observation of present discourses, but it is also able to highlight the dominance of each discourse. CDA, it is important to keep in mind, does not constitute a linguistic theory and thus does not provide any predetermined grammar or linguistic characteristics of discourses. However, what it is able to do is highlight those features of a (written or spoken) narrative that seem to be manipulated in order to pursue a certain purpose. A critical discourse analysis involves several different levels, for which Huckin (1997) provides concepts and guidelines. Huckin argues that textual manipulations are often most powerful when considering the text as a whole. Texts often represent a certain genre, e.g. a policy document. Manipulation of such a genre can occur when the writers or speaker use deviations from neutral language if it matches their objective. Such objectives can also become clear through the manner in which the text is framed - which refers to how a text is presented and which perspective it takes on. Other features of CDA to keep in mind when considering a text, are foregrounding, omission, and presupposition. Foregrounding refers to the concepts that are emphasized relative to others that are not. Omission on the other hand refers to what is entirely left out - and thus what is explicitly left out of the reader's perception. Finally, presupposition points to the use of language in which certain things are taken for granted or are presented as the only truth (Huckin, 1997).

Critical discourse analysis also takes sentences and words into account. In sentences for example, manipulations can also take on foregrounding, omission, and presupposition. Special attention at this level can be given to agent-patient relations, which distinguishes actors from (passive) recipients. In sentences, a focus can thus be on recipients - e.g. victims of a certain event or phenomena - or those that have exerted some form of power. Furthermore, certain

suggestive language can be used. At the more detailed level of words, indicators such as word connotation, labels, metaphors, and formality can be used to analyse a text (Hucking, 1997).

To be able to start the analysis of a text, one can opt for preliminary research as a useful tool. This step can provide a baseline of discourses that can be used to identify similar discourses in the selected cases. A next step is to accompany those found discourses with a set of indicators, which will help aid the discourse analysis, and will provide consistency throughout the analysis. A last step is to perform the discourse analysis on the selected cases. This step also consists of analysing which discourses have been most dominant, which can be done by calculating percentages of found discourses by using the preliminary discourses as a guideline. The literature review and theoretical framework leads to the hypothesis that the EU's data protection discourse may have been securitized. The method of discourse analysis allows for the testing of this notion, as it is able to identify whether securitization is an existing discourse at all, and to what extent it has been present.

5.2 Preliminary Analysis

When performing a discourse analysis, it is important to be able to distinguish separate discourses. One way of distinguishing such discourses is to build these on assumptions, which for instance have been gathered through literature and theory. Another method is to perform a preliminary analysis, which is an exploratory method to find out which pre-existing discourses can be found within a certain context. This discourse opts for the latter, as literature on discourses present in data protection policies are scarce.

When selecting the documents for a preliminary research, it is important to keep in mind that these no longer can be used for the actual discourse analysis. Such documents thus need to be of less importance for this analysis, which can for example be because the documents are relatively dated. These documents do, however, need to be relevant to the topic, in order for them to be considered representative. Once used for the preliminary research, these documents will no longer be used for the discourse analysis, as these would not yield new results.

The documents selected for the preliminary analysis are based on the predecessor of the GDPR, which is the Data Protection Directive of 1995. This directive was the EU's first step towards regulating personal data within the European Union. It mainly focused on the protection of individuals' personal data and - perhaps more so - ensuring the free movement of data across

Member States. It is thus likely that these two goals have become prominent discourses within the Data Protection Directive narrative. Furthermore, it is important to keep in mind that since 1995 the pervasiveness of information technology (IT) has considerably increased, which heightened the importance of data protection as an ongoing discourse. This vast difference in the influence of IT on society can indicate that securitization may have been less of a dominant discourse in the earlier days of data protection regulations. Furthermore, considering that the securitization of cyberspace drastically increased after the events on 9/11 in 2001, it may be especially difficult to find a strong presence in this 1995 directive. However, what this preliminary analysis of these documents does reveal, is a range of possible discourses that may be found in the 2016 General Data Protection Regulation.

For this preliminary analysis, the documents analysed can be found in table 1. The selection of the documents has been made based on their relevance to the final directive. Furthermore, the availability of the documents was considered (which led to the Council document being based on the Council's position at first reading and not the second). The used documents include the first proposal for the directive that was drafted by the Commission, and the common position that was adopted by the Council. Lastly, two additional documents of the Commission were included as they provided more linguistic evidence for the discourses that were found.

Table 1. Preliminary Research Document Selection

Actor	Date	Content
The Commission	July 27, 1990	The Commission first proposal was drafted in 1990, which concerned the protection of individuals regarding the processing of personal data.
The Commission	July 18, 1990	One of the Commission's first press releases regarding the protection of personal data called for 'community action' on the matter.
The Council	February 20, 1995	The Council reached a common position in 1995 on the amended proposal of the Commission.
The Commission	February 21, 1995	The Commission's response to the Council's common position.
The Commission	July 25, 1995	The Commission's response to the definite adoption of the directive.

It must be noted that this preliminary research does not use EP documents. This is due to the lack of availability of EP documents regarding the 1995 directive. Furthermore, the European Parliament represents a wide range of political parties and thereby ideologies. These ideologies tend to result in different discourses in terms of problem - and solution - definitions. This results in a less uniform voice for the EP, whereas one could argue that the Commission and the Council individually represent a more united voice. However, what can be hypothesized for the EP is that the dominance of certain discourses may differ between right-wing and conservative political parties, and left-wing parties. Whereas left-wing parties might stress fundamental rights and economic gains, security might be more of a concern for right-wing parties. Furthermore, euro sceptical parties might be wary of more European regulations, and therefore may use little of a unity discourse as can be found in table 2. These are, however, assumptions, and whether these hold for the policy field of data protection is yet undetermined. This discourse analysis, however, may shed more light on these differences between European political parties.

5.3 The Discourses

The preliminary research resulted in four discourses, as can be found in table 2 below. Each discourse can be distinguished based on how the problems and solutions are defined, and which keywords and sentences are most frequently used. It is important to keep in mind that some discourses can overlap to a certain extent. For example, the unity discourse and the economic discourse both emphasize the Single Market and the completion thereof. Furthermore, as expected, securitization proved to be the least used discourse in these preliminary documents. It is thus possible that in the new policy documents of the GDPR, the securitization discourse may have evolved and may appear different from those in these early 1990s documents. The analysis of the GDPR documents should, however, show the evolution of the discussion around technology and data privacy.

In total, four discourses were found, including a unity, fundamental rights, security, and economy discourse. The unity discourse mostly represented the need to establish a common set of rules, as divergences in regulations were deemed an obstacle to the full completion of the Single Market. The discourse was thus mostly problem based as it often referred to the issues of having heterogeneous regulations. The second discourse concerned fundamental rights, and predominantly referred to the fundamental rights of EU citizens. The discourse was neither problem- nor solution- based. More so, the discourse established why regulating data protection at the EU level was an obvious and fundamental need.

The third discourse was named the security discourse as it showed signs of securitization. It thus not referred to the traditional notion of security, but rather the broader understanding of the concept which is offered by the Copenhagen School. It therefore included any references to a threat narrative. The security discourse was clearly in its infancy at the time of the 1995 Directive. The discourse was mostly problem-based, though often referring to more abstract issues such as the vulnerability of modern society in a world that is becoming increasingly dominated by IT. Lastly, the economy discourse somewhat overlapped with the unity discourse, as its problem definition also concerned the Single Market. The discourse, however, distinguished itself by focusing more on businesses and consumers, and how these would benefit from having EU rules on the protection of data. The economy discourse was thus predominantly solution-based, and overall presented a positive outlook on the introduction of an EU directive.

The table below provides a guideline for the interpretation of the GDPR documents. Key words or synonyms thereof are easy recognizable and can hint to a certain paragraph or part of the text being part of a certain discourse. The problem - and solution - definition are part of narratives and should be relatively consistent within a certain discourse. When performing a discourse analysis on a policy document in its entirety, it can be useful to use such keywords or narratives in order to find the key pieces of text that point towards a certain discourse. A method that can then be used to determine each discourse's dominance, is to compare the frequency of discourses relative to one another.

In order to compare discourses, each time a piece of text - or in the case of a debate, a section of speech - is considered to refer to a certain discourse, it will receive a point. It can, however, occur that a certain piece of text or paragraph contains more than one discourse. In such a case, both discourses will receive a point. What results is a range of different scores per discourse, which can be summed up as the total amount of discourse-indicators found. Each discourse's dominance can afterwards be calculated by dividing its score by the total amount. For example, if a Member of the European Parliament refers to the unity discourse once and to the economy discourse three times, the unity discourse is represented by 25 percent, whereas the economy discourse is by 75 percent.

Table 2. Preliminary Discourses

Discourses	Keywords and Sentences	Problem Definition	Solution Definition
Unity	- Obstacles - Homogeneous (standards) - Common rules - Throughout the Community - Minimizing differences between Member States - Narrowing divergences - The full realization of the Single Market - The development of the Community	- Differences in Member State rules on the protection of personal data makes it impossible to fully realize the Single Market.	- A Union-wide approach is needed in order to fully develop the Community as it is meant to be. - The directive allows for a union-wide approach, while leaving some 'room for manoeuvre'.
Fundamental Rights	- The individual - Freedom - Ensuring privacy - Giving consent - Preventing abuse - The creation of a 'citizen's Europe' - The right to access	- Strict conditions are needed to protect the individual's information and consent. - Individuals must have the right to access information concerning him or her.	- The directive provides a legal basis that ensures a high level of protection for individuals' privacy.
Security	- The vulnerability of modern societies - Individual security vs. interests of the public at large - Dependence on IT - A jeopardy to the establishment - Safeguards - Creating trust	- A jeopardization of an area without internal borders that is becoming increasingly dependent on IT systems.	- Safeguards need to be established to boost trust - which is needed to counter society's vulnerability and dependency.
Economy	- Efficiency gains - Competitiveness gains - Essential to business activities - Fostering consumer confidence - Free flow - A problem for multinational companies - Valuable market opportunity	- An obstacle to the pursuit of economic activities. - A need to match the needs of consumers.	- Common rules are needed to establish the free flow of services. - The free flow of services will enhance consumer confidence.

5.4 Case Selection

This following section will discuss the cases selected for the final discourse analysis on the General Data Protection Regulation, as can be found in Table 3. These cases are arranged based on their date of publication or the date of the event (e.g. when a debate took place). Following the table, a brief explanation and justification will be given for the selection of the documents per institution.

Table 3. Document Selection for the Discourse Analysis

Actor	Date (of publication)	Content
The Commission	January 25, 2012	Proposal for a regulation for the protection of individual's personal data and the free movement thereof.
The Commission	January 25, 2012	Press release on the proposed reform of the EU's data protection rules from 1995.
The Commission	January 28, 2013	Press release on the European Data Protection Day of 2013, which mentions the progress of the negotiations on the proposal.
The European Parliament	March 11, 2014	Debate on the protection of individuals regarding the processing of personal data, including that for the purposes of preventing crime, which was held in Strasbourg.
The Council	June 15, 2015	Public session of the Justice and Home Affairs Council. In this session, the Council aimed to reach a general agreement on the proposed regulation on the protection of personal data.

One of the Commission documents consists of the founding document for the regulation, which is the initial proposal. Analysing this proposal is therefore of great importance, as it allows for the analysis of the regulation based on its first official document. Though this document may contain many legal elements which are not necessarily used to promote a certain discourse, some elements of the considerations for the proposed regulation should be traceable. Other documents from the Commission include press releases. Though these are officially published by the institution at hand, the language used in these press releases may be considered less formal compared to an official proposal. They may therefore provide different insights, as narratives can be more easily created. The few press releases were selected based on their

relevance, and therefore mostly concerned official updates on the progress of the proposal. These updates were mostly published on the annual Data Protection Day.

The two other selected documents are video recorded sessions from the European Parliament and the Council of the European Union. The EP session is the official debate which was followed by a voting session and preceded its official opinion at first reading. Compared to the debate that preceded the second reading, the first debate gives a better overview of the Parliament's and its parties' initial thoughts on the proposal, without having made any compromises and amendments yet.

The Council session of the Justice and Home Affairs Council was selected for different reasons. The session on June 15, 2015 was aimed at reaching a general agreement on the Council's stance on the proposal. This was confirmed by the Council session on October 9, 2015, in which it was expressed that in June, the Council reached an agreement on its position on the GDPR after which the Council began talks with the European Parliament. Moreover, earlier sessions of the Council dealt with different legislative deliberations per session, making it difficult to combine several of these three-hour sessions into one general analysis. The June 15th session therefore provided a more comprehensive analysis, as it was an attempt to reach a final position. Lastly, it also appeared to be the only session where all 28 Member States were present and active, and thus allowed for the analysis of all EU Member States.

EMPIRICAL ANALYSIS

This chapter will consist of the analysis of the selected cases, which include the documents from three institutions of the EU involved in the ordinary legislative procedure on the GDPR, namely the Commission, the Council, and the European Parliament. Each piece of text or recording is analysed using the discourses that were found in the preliminary analysis. These are used to provide an indication of their presence and dominance in the GDPR-related texts. Each analysis per institution is accompanied by a table or graph which indicates the overall use of the discourses. For the Council and the European Parliament, Member States and political parties are analysed separately.

6.1 Analysis of the Commission Documents

The following section will discuss the analysis of the Commission Documents. These represent both more formal legal documents - such as the official proposal for the GDPR - as well as relatively less formal pieces of text, which include press releases. All documents will be analysed based on the references made to the discourses as found in the preliminary analysis.

6.1.1 Cases

Data for the analysis of the Commission's position on the GDPR consists of the official proposal for the regulation from 2012, and two press releases from 2012 and 2013. The data thus includes a more formal legal document as well as relatively less formal pieces of text. The Commission's proposal consists of an introductory chapter followed by sections on legal elements. The press release of January 25, 2012, coincided with the day of the official proposal and therefore served as an introduction of the proposed regulation towards the press and public. The press release of January 28, 2013, coincided with the annual European Data Protection Day, and mostly discussed the progress on the GDPR.

6.1.2 Main Findings

This analysis tests for the presence and dominance of discourses used by the Commission. It thereby uses the discourses found in the preliminary analysis as a baseline. From the analysis, the results can be summed up as follows:

- The proposal strongly emphasized the fundamental rights discourse as it contained many references to the legal basis of the proposed regulation. These references were also made in the press releases, though to a less extent.

- The unity discourse was used to highlight the need for legal unity across the European Union to overcome the divergences in rules between the Member States.
- The context of the proposal introduced the security narrative, which emphasized the rapid developments and increase in scale regarding the processing of data. Eurobarometer data was mentioned to reflect the perception of the EU public.
- The economy discourse was used least in the Commission's proposal. The importance of the GDPR to the EU economy was, however, strongly emphasized in the press releases. The discourse mainly touched upon cost-efficiency and consumer confidence.

6.1.3 Empirical Support

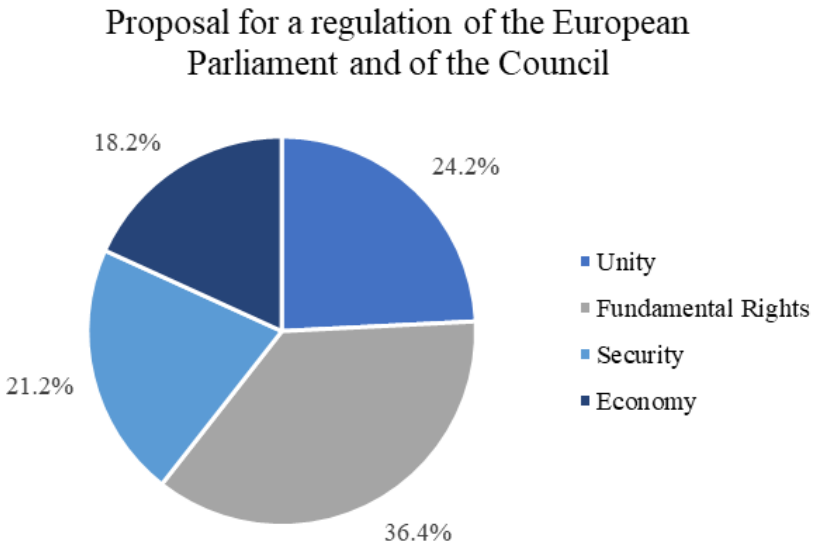

Figure 1. Percentage Use of Discourses of Commission's Proposal

As can be seen in figure 1 above, a first analysis of the Commission's proposal shows that it is predominantly dominated by the fundamental rights discourse, which constitutes over a third of all present discourses (for full scores, see the coding table in Appendix A). The context the Commission sets the proposal in, however, was dominated by the unity and security discourses. The unity discourse emphasized the need to introduce a harmonized set of rules which would ensure unity in terms of applying it as EU law. Furthermore, this unity discourse presented solutions such as a "*consistency mechanism for cooperation between the supervisory authorities themselves and the Commission*" (European Commission, 2012b:33). Evidence of the unity narrative was also found in the chapter on the legal elements of the proposal, which justified the choice for a regulation (instead of a directive). According to the proposal, a

regulation would ensure direct applicability and more legal certainty, which would benefit the harmonization of rules.

The security narrative was less present in the chapter on legal elements but was relatively quickly introduced in the context of the proposal. Here, a narrative was put forward which emphasized the new challenges society faces as a result of rapid developments in technology. The narrative thus introduced a threat, which came as a result of a dramatic increase in the scale of the collecting and processing of personal data by both private and public organizations. This narrated threat was supported by Eurobarometer data, which showed that there was "*a widespread public perception that there are significant risks associated notably with online activity*" (European Commission, 2012b:2). The solution this security narrative offers was, however, rather vague and only merely referred to a need to build trust in the online environment. This may also explain why little evidence of it was found beyond the proposal's introduction.

The fundamental rights discourse, however, was especially dominant in the proposal's legal chapters. The context setting of the proposal only made mention of the proposal's legal basis, which include Article 16 of the Treaty of the Functioning of the European Union (TFEU) and Article 8 of the Charter of Fundamental Rights of the EU. The document proceeded to build on this legal basis, which was extended by a number of fundamental rights issues, of which the most dominant was the invasion of privacy. Other threats this narrative highlighted, were the possible negative effects on, for example, the freedom of expression, the protection of intellectual property, and the freedom to conduct a business. The solution that was offered to counter these threats mainly covered the entire proposal, as the proposal was directed towards the rights of EU citizens. It thus may not be surprising then that the fundamental rights discourse was especially dominant in such a document that contained a lengthy legal framework.

Lastly, the economy discourse was notably less dominant. Some context was given on the link between data protection and economic development, which was linked to the security discourse in its explanation of how a lack of trust in the online environment could lead to lower consumer confidence. This, in turn, would negatively impact the innovative capacity of the technology sector, and thereby the economy of the EU. The economy discourse is extended in the chapter on consultations and impact assessments, where the proposal was said to be preceded by two

phases of public consultation. This included consulting the private sector, including business organizations and consumer organizations. The problem the economy narrative highlighted is one which was actually put forward by economic stakeholders themselves - who had "*asked for increased legal certainty and harmonization of the rules on the protection of data*" (European Commission, 2012b:4). According to these stakeholders, the complexity and vast difference between rules were considered a real impediment to their operations - both within the EU and the rest of the world. The way in which the economy problem was defined in this document thus matches the preliminary findings rather well, as it too referenced consumer confidence and the challenges fragmentation pose to companies. Some of these concerns were included in the legal elements of the document, where Member States and their supervisory authorities are encouraged to consult regularly with small and medium-sized enterprises to consider their needs. To some extent, it can be argued that the economy discourse represented a merger of interests, between those of the EU and businesses operating inside and beyond EU borders. Despite these overlapping interests, the economy discourse was the least dominant - though still significant - discourse in the Commission's proposal.

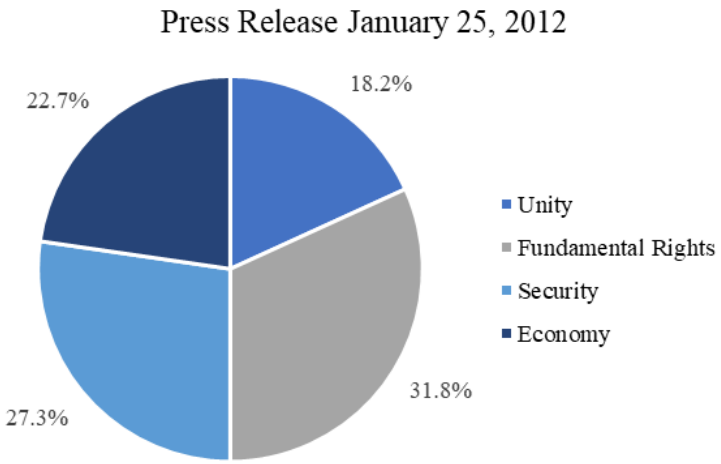

Figure 2. Percentage Use of Discourses of Press Release January 25, 2012

The press release of January 25, 2012 showed relatively similar use of the discourses compared to the proposal itself (see Appendix B for coding). Though the unity discourse was used relatively less, similar references were found that highlighted the divergences in rules between the Member States. Following the implementation of the 1995 directive, Member States implemented different regulations which led to differences in enforcement. The press release therefore mentioned the phenomena of fragmentation, which led to high administrative costs. In a way, these costs would justify the need for a regulation, which - according to the text -

would lead to "*savings for businesses of around €2.3 billion a year"* (European Commission, 2012a: para. 1). This introduced a new aspect of the unity discourse, which was one based on cost efficiency and the benefits to European businesses. Another element which seemed to be based on efficiency gains for businesses, was that companies would only have to deal with a single national data protection authority in the Member State where they operate instead of multiple.

Both of these business-related aspects of the unity discourse seemed to be tied to that of the economy discourse. Not only would companies benefit from less administrative costs due to the proposed regulation, they would also benefit from a more dynamic European economy as the initiative is stated to boost consumer confidence, employment, and innovation. It was thereby implied that the GDPR would be a step forward in unleashing the potential of the Digital Single Market. The economy discourse also touched upon another cost-saving aspect of the regulation, which entailed the increased responsibility and accountability for those processing data, including, for example, the responsibility to provide a data breach notification within 24 hours. Though this would require a more responsible approach to data processing, it could save businesses up to €130 million in total per year (European Commission, 2012a).

The security discourse mostly referred to the dramatic increase in the transferring and exchanging of data. It was furthermore emphasized that this phenomenon is happening in a space without borders, where such exchanges happen across the entire globe. For these reasons, as expressed by a quote from the then-EU Justice Commissioner and Commission Vice President Viviane Reding, "*citizens do not always feel in full control of their personal data"* (European Commission, 2012a:para. 2). To an extent, the security discourse was also tied to the economy discourse based on the notion that an increase in trust among European citizens would lead to an increase in trust in online services, thereby boosting the Digital Single Market. It was therefore implied that it was of importance that consent would become an essential element of the regulation - and that this would also hold for companies based outside the EU - in order to foster trust among EU citizens.

Lastly, the fundamental rights discourse touched upon topics such as Article 8 of the EU Charter of Fundamental Rights, Article 16 of the TFEU, and the right to be forgotten. Overall, this discourse seemed to provide the legal foundation for the other discourses to build on, as a

strong and uniform legal framework would be needed to build trust among European citizens. This in turn would contribute to a boost of the European economy.

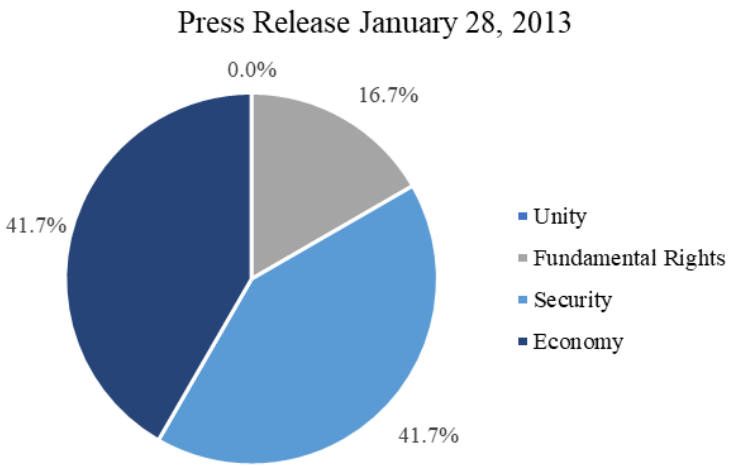

Figure 3. Percentage Use of Discourses of Press Release January 28, 2013

The press release of January 28, 2013, on the progress on the GDPR showed a similar but differently put story compared to the 2012 press release. Here, the economy and security narratives were intertwined to a certain extent. For example, the text stated the 'clear' reason for the regulation was that: "*to flourish, the digital economy needs trust"* (European Commission, 2013:para. 2). Lacking confidence would lead to less use of online services and products. Stronger and more reliable rules were therefore argued to be needed, as *"confidence in turn drives growth"* (European Commission, 2013:para. 2). Therefore, not only personal data, but trust in sharing that personal data has substantial economic value. The GDPR thus implied to be the fitting regulation *"to secure trust and generate growth in the digital single market"* (European Commission, 2013: para. 3).

6.2 Analysis of the Council Documents

The following section will discuss the analysis of the Council's position on the proposed regulation. The analysis will specifically focus on the Council session of the Justice and Home Affairs Council which was held on June 15, 2015. As the Council represents the governments of all Member States, each Member State will be analysed individually on their use of the discourses.

6.2.1 Case

During the June 15, 2015, session, JHA ministers from all 28 Member States were present and actively participating in the session (Council of the European Union, 2015). Figure 4 provides the percentages of the overall use of each discourse per Member State, and thus gives an indication of their considerations. As the session was also attended by the Commissioner for Justice, Consumers, and Equality Věra Jourová - who had considerable speaking time - her use of the discourses was also added to the analysis. Her scores, however, do not represent those of the Council or Member States, but more so represent those of the Commission. All 28 Member States were included in the analysis, but four did not use any of the discourses during their speaking time. These four (Slovenia, Estonia, Slovakia, and Denmark) are therefore not included in figure 4.

Following the Commission's proposed regulation in 2012 and the European Parliament's position at first reading in 2014, the Council set out to reach a 'general approach' - which would entail a political agreement of the Council and its Member States on the proposal in order to finalize the Council's position at first reading. Such a general approach is often agreed upon to speed up the legislative procedure, as it lets the European Parliament know about the Council's position before it publishes its first reading.

The purpose of this specific session was to give the floor to each Member State to express their support for or opposition to adopting a general approach. Though many Member States did express their approval of the general approach, many took the opportunity to address some of their remaining concerns. In general, there seemed to be a mutual understanding of the compromises that were already made after - what were considered - long and complex negotiations the Council had been having since 2012. There therefore seemed to be a general desire to deal with the remaining concerns in the trialogues (with the European Commission and the European Parliament).

Overall, many Member States used their speaking time - which was approximately three to four minutes per Member State - to address first their support of or objection to the general approach, and second to bring up their remaining concerns. In general, there seemed to be little doubt about why the regulation was needed as the regulation's context was already introduced by the Council Presidency and Commissioner Jourová - who both opened the session. This session therefore less concerned the 'why' (why the regulation was needed), but more so

concerned the 'how' (how can we get this proposal through). The analysis of this session thus showed both general and specific considerations for the adoption of the GDPR.

6.2.2 Main Findings

This analysis tests for the presence and dominance of discourses used by the Council and its Member States. It thereby uses the discourses found in the preliminary analysis as a baseline. From the analysis, the results can be summed up as follows:

- There seemed to be wide-spread support for reaching a general agreement.
- A core aspect of this general agreement was the implementation of a single EU-wide framework, which supported the unity narrative.
- The economy discourse was used frequently as many Member States mentioned the benefits of levelling the playing field between European and non-European tech companies.
- A sense of urgency was created by use of the security discourse, as it emphasized a lack of the public's trust in data privacy.

6.2.3 Empirical Support

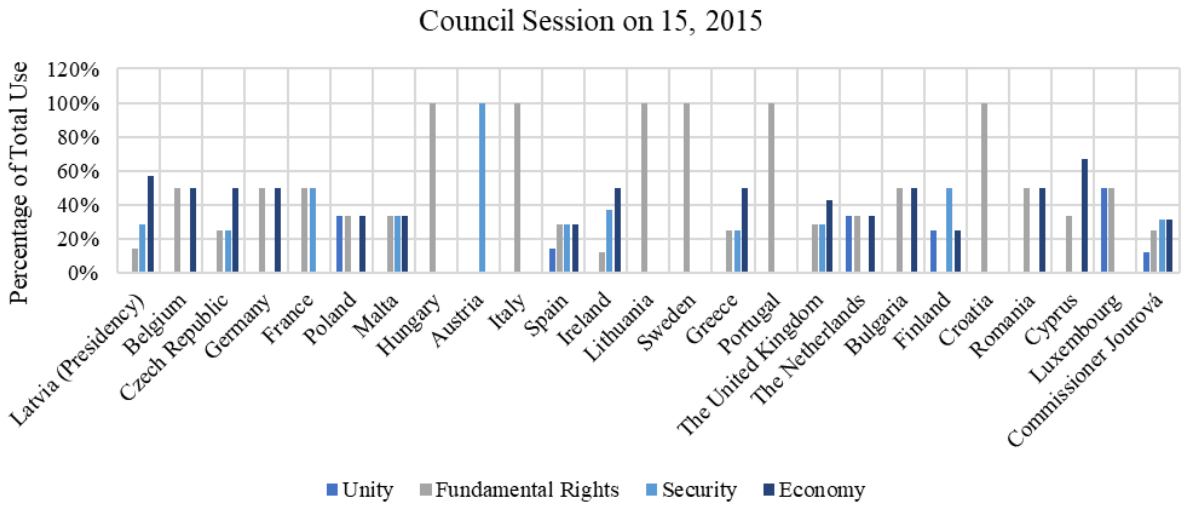

Figure 4. Percentage Use of Discourse of Council Session on June 15, 2015

The least used discourse and therefore the least considered in this session, was the unity discourse. When used, the discourse mostly referred to the negative effects of fragmentation of regulations in the EU. The narrative thus seemed to be predominantly problem-based. Despite the scant use of the discourse in this session, it was made clear in the opening of the session by Commissioner Věra Jourová that there seemed to be a general agreement on the

implementation of a single framework as this was one of the core elements of the proposed regulation. Member States that had expressed their doubts about the proposal being a regulation instead of a directive - such as Denmark - did announce they would support the general agreement since the proposal allowed for enough flexibility for Member States to maintain and adopt national legislation.

The economy discourse on the other hand was referred to often. Common themes included the boost of innovation, the reduced costs for businesses, and the increase in competitiveness of European companies. The latter especially was touched upon frequently in combination with the fundamental rights discourse, as a number of Member States such as Greece and Romania, expressed the need to find the right balance between ensuring the protection of fundamental rights and fostering the competitiveness of the European digital market. The regulation in general seemed to be supported based on the notion that it would be a step forward in the completion of the Digital Single Market. An important argument that was brought forward was that the regulation would 'level the playing field' between non-European and European tech companies - indicating that European tech companies had a disadvantage or less-competitive position compared to non-European tech companies.

The economy discourse was frequently linked to the topic of security, as done by for example Ireland and Finland. The security discourse mostly offered a sense of urgency to finding an agreement on the proposal. According to Ireland for example, a high level of data protection was a must as the digital age is characterized by rapid developments. Therefore, the EU must strive for data protection standards that are able to keep up with emerging technologies and new digital business models. If not, consumer confidence would weaken even further, and trust in the digital economy would diminish. This in turn would mean that the EU would fail in realizing the full potential of its digital market, and thereby miss out on the benefits of innovation, economic growth, and an increase in jobs. The topic of trust was overall frequently used to create a sense of urgency in finalizing the regulation. This sense of urgency was strengthened by referring to EU citizens' sentiments on data privacy as brought forward by, for example, Eurobarometer data. Member States such as Spain therefore implied that action should be taken, as EU citizens would expect the EU to do so. Overall, the security discourse was used to promote a speedy solution for data privacy concerns and the lack of trust. This would entail a speedy adoption of the GDPR.

Lastly, the fundamental rights discourse was also often used in conjunction with the economy discourse. Generally, it was stressed that there needed to be a right balance between the protection of fundamental rights and fostering the digital economy of the EU - for example, the United Kingdom stressed the importance of reaching an agreement that preserved both privacy and opportunity. Statements such as these implied that even though fundamental rights were at the heart of the regulation, protecting them should not be at the expense of innovation and growth for European businesses. Ensuring that the regulation would work and be beneficial for European businesses therefore seemed to be a high priority in the Council.

6.2.4 Finalization of the Session

Overall, there seemed to be a majority support for adopting a general approach during this session. This agreement would, however, be one that was built on the compromises made by all Member States. The compromise agreement would allow the Council to continue with the trialogue phase, in which there would be room to discuss and work on the remaining concerns of the Member States that were mentioned during the session. Some of these concerns, for example, consisted of the protection of minors, transfers to third countries, the formulation of specific articles such as Article 6 on the lawfulness of processing, and ensuring privacy without limiting freedom of expression or research for scientific purposes.

The session concluded that after three years of discussions, a general agreement had been reached. The Council eventually ended up publishing their position at first reading on April 8, 2016. This position was adopted with a qualified majority of 27 votes in favour, and 1 vote against. The latter vote came from Austria, which had already expressed its opposition to the general approach as it worried that the EU regulation would compromise their high-level national data protection rules. Following the adoption of the general approach, the trialogue sessions would start on June 24, 2015, with the first meeting held in Brussels (Council of the European Union, 2015).

6.3 Analysis the European Parliament Debate

The following section will discuss the analysis of the European Parliament's use of discourses. Specific attention will be given to the debate that was held on March 11, 2014 (European Parliament, 2014). As the European Parliament represents a wide range of political parties and thereby ideologies, there will be a distinction made between the parties regarding their scores

per discourse. Before doing so, a short description will be given of the political fractions in the Parliament, their ideologies, and their members that participated in the.

6.3.1 Case and EP Fractions

The debate held in Strasbourg on March 11, 2014, covered the protection of EU individuals' personal data and the processing thereof. A number of MEPs from several EP groups were present at the debate, and each MEP was given on average one to two minutes of speaking time. Depending on the MEP and his or her speech, some MEPs managed to address more discourses than others - but, differences in the scores on discourses were most importantly based on the MEPs' personal and party-related priorities and concerns. Below, the present EP fractions are shortly described. This is done in order of left- to right-wing parties. The Europe of Freedom and Democracy (EFD) party is left out, as no speakers from the party participated in the debate.

6.3.1.1 European United Left - Nordic Green Left (GUE-NGL)

The European United Left - Nordic Green Left is a left-wing party and brings together parties which one could consider socialist or communist in nature. The party values confederalism, meaning they value respecting the diversity of all its members. This could also partly explain why the party is considered Eurosceptic. Other principles include social equality, solidarity, and sustainability ("European United Left / Nordic Green Left", n.d.). The party consisted of 35 MEPs in March 2014. In the debate, one speaker came forward, which was Cornelia Ernst.

6.3.1.2 Progressive Alliance of Socialists and Democrats (S&D)

The Progressive Alliance of Socialists and Democrats is considered a centre-left, progressive, and predominantly social-democratic party. Furthermore, the party can be considered pro-European. The S&D group's priorities have been the fight against unemployment and the creation of a fairer market. Other values consist of social justice, democracy, and sustainability ("What we stand for", n.d.). In March 2014, the Progressive Alliance of Socialists and Democrats was the second largest party in the European Parliament, and had a total of 195 MEPs. Speakers during the debate on data protection were Dimitrios Droutsas, Sylvie Guillaume, Silvia-Adriana Țicău, Claude Moraes, Juan Fernando López Aguilar, Evelyn Regner, Marc Tarabella, Silvia Costa, and Tonino Picula.

6.3.1.3 The Greens-European Free Alliance (Greens-EFA)

The Greens-European Free Alliance represents a mix of both green, regional and minority-based parties. Most of these parties can be considered progressive and relatively pro-European. The group promotes finding sustainable solutions for common issues, and values the protection of the environment, democracy, equality, and social justice ("About Greens/EFA", n.d.). The European Parliament consisted of 58 MEPs from the Greens-EFA group during the time the debate took place. Greens-EFA speakers in this debate consisted of Jan Philipp Albrecht, Judith Sargentini, and Carl Schlyter.

6.3.1.4 Alliance of Liberals and Democrats for Europe (ALDE)

The Alliance of Liberals and Democrats for Europe is a party representing liberal and democrat values of the European Member States. The party is pro-European and prefers a leadership role for the EU in tackling global challenges. Their ideology is furthermore built on liberal principles, such as democracy, rule of law, and human rights (About the ALDE Party", n.d.). These principles are mostly translated into politics and economics. At the time the debate took place, the party was represented by 85 Members of the European Parliament (MEP) out of a total of 766 MEPs. During the debate on the protection of personal data, the following speakers came forward: Nadja Hirsch, Baroness Sarah Ludford, and Sophia in 't Veld.

6.3.1.5 European People's Party (EPP)

The European People's Party, as one of the oldest EP parties, represents predominantly Christian democratic, conservative-liberal, and conservative politicians and views. The EPP promotes centre-right policies, and can be considered relatively pro-European, though some Eurosceptics are members of the party. Current goals of the party consist of increasing the EU's competitiveness, and regaining the trust of the European citizens ("Group of the European People's Party (Christian Democrats)", n.d.). In March 2014, the EPP was the largest EP party, with 274 MEPs in total. It is therefore not surprising that the party was represented by the largest number of speakers in the debate on data protection. The speakers from the EPP were Seán Kelly, Lara Comi, Marielle Boullier Gallo, Axel Voss, Kinga Gál, Wim van de Camp, Carlos Coelho, Csaba Sógor, Anna Maria Corazza Bildt, Zbigniew Zaleski, and Salvatore Iacolino.

6.3.1.6 European Conservatives and Reformists (ECR)

The European Conservatives and Reformists group is a centre-right to far-right political party and represents conservative-liberal views. It is considered a Eurosceptic party as its views on the EU are influenced by Eurorealism, which focuses on reforming the EU (as opposed to pro-European or complete anti-European thoughts) ("European Conservatives and Reformists Group", n.d.). In March 2014, the ECR was represented by 56 MEPs. During this particular debate, speakers consisted of Timothy Kirkhope, Vicky Ford, and Ruža Tomašić.

6.3.1.7 Non-Inscrits (NI)

The Non-Inscrits group represents MEPs that are not members of any of the recognized political groups in the EP. Because of this reason, the group contains many different ideologies. In general, the group can be considered to contain mostly far-right parties. 35 MEPs were members of the group in early 2014, of which two participated in the debate of the protection of personal data. These MEPs were Auke Zijlstra and Franz Obermayr.

6.3.2 Main Findings

This analysis tests for the presence and dominance of the four discourses used by the European Parliament and its political fractions. The main findings can be summed up as follows:

- There was general support for the proposal, though many MEPs used their speaking time to raise remaining concerns.
- The unity discourse was not dominantly present in the debate. When used, this was mostly by MEPs from pro-European fractions.
- The fundamental rights discourse was often used, and mostly promoted a solution-based narrative in which the GDPR would be a monumental step forward in the protection of privacy.
- Securitization did occur in the debate, both implicitly and explicitly. The implicit narrative promoted a sense of urgency, whereas the explicit narrative made mention of the actors involved.
- The economy discourse stressed both positive as well as negative aspects of the proposal.

6.3.3 Empirical Support

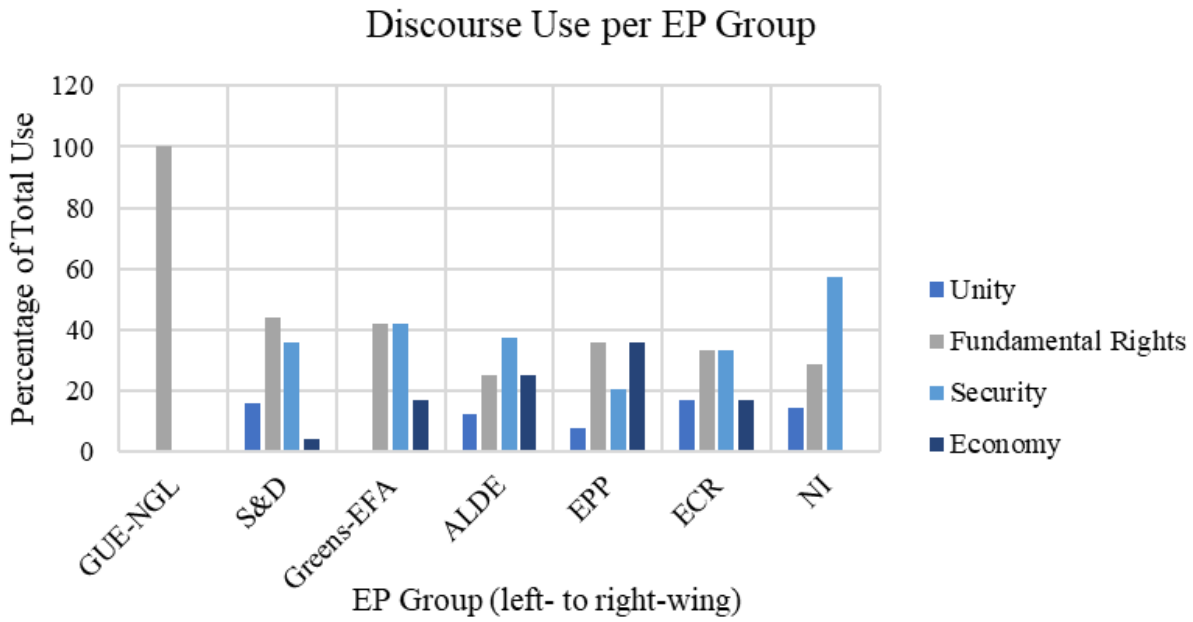

Figure 5. Percentage Use of Discourse of EP Debate on March 11, 2014

6.3.3.1 The Unity Discourse

Overall, the unity discourse was not dominantly present in any particular party. When the discourse was touched upon, it was usually done rather briefly. This made it clear that unity regarding the protection of data was not as much of a concern as the other discourses. Most of the speakers that did speak of unity (as found in Appendix D), were MEPs of the Progressive Alliance of Socialists and Democrats. This included Dimitrios Droutsas, the second rapporteur of the GDPR and directive, who emphasized that the GDPR would provide a comprehensive and consistent single instrument for the protection of personal data. His colleague, Silvia-Adriana Țicău, also showed her support for the legislative proposal as she argued that it would provide a series of common rules. This notion was supported by Claude Moraes, who made mention of the GDPR as a single set of international privacy rights. The need for such a single set of common rules was highlighted by Tonino Picula, who emphasized the importance of harmonizing procedures across the EU.

The unity discourse was also touched upon by a number of MEPs from the European People's Party. For example, Seán Kelly used the unity discourse to give positive feedback on the proposal, as he mentioned the desire to have one set of rules across the entirety of the European Union. According to Kelly, this made 'absolute sense' as the online world knows no borders. His colleague, Carlos Coelho, also made mention of the GDPR as a step in the right direction.

He highlighted the importance of the proposal being a regulation - thus enforceable as law in the entire Union - as he argued that it would provide legal certainty across the entirety of the EU. Anna Maria added to this notion that the regulation would help overcome legal fragmentation between the Member States.

Other MEPs that used the unity discourse came forward with similar comments and arguments. Again, overall, the unity discourse was predominantly absent, and when mentioned it was mostly brief. What can however be noted here, is that when looking at the number of speakers using the discourse (as can be found in Appendix D), most were members of pro-European parties such as S&D and the EPP. In general, one could argue that the mention of having a single framework for the entire EU might have been obsolete, as the proposal of the GDPR was based on the notion of it being an update and improvement of the 1995 Directive. For the 1995 Directive, promoting the need for a single framework may have been of more importance to get the directive through, whereas for the GDPR there may have already been agreement on the need of an update - which presumed it representing a single framework. This presumption may have been supported by, for example, Eurobarometer data which showed high support for an EU-wide solution.

6.3.3.2 The Fundamental Rights Discourse

The fundamental rights discourse proved to be the most popular discourse, as it was used by every EP party. Overall, it was made very clear that the General Data Protection Regulation would be a monumental step forward in the protection of the fundamental right of privacy. The discourse was thus highlighted in mostly a positive way, as the proposal was applauded for its 'revolutionary' character. The rapporteur, Jan Philipp Albrecht from the Greens-European Free Alliance, opened the debate by referring to the Lisbon Treaty, which recognizes the fundamental right of the protection of personal data. According to Albrecht, the proposal of the GDPR would aim to protect this fundamental right across the EU. The second rapporteur, Dimitrios Droutsas from the S&D group, argued that the proposal would send a message to the citizens of the EU that the European Parliament was aware of their concerns and would take the matter very seriously. He furthermore implied that the proposed regulation and the work of the European Parliament had been in line with the interests of European citizens. To a large extent, the opening of the debate by the two rapporteurs indicated that the proposal would be an answer to the concerns of the EU public. The fundamental rights discourse therefore seemed to promote a solution-based narrative.

Most of the references to the fundamental rights discourse came from the European People's Party (as can be found in Appendix D). Seán Kelly specifically pointed out the strengths of the regulation, which he considered to be explicit consent, and the right to be forgotten. Another point he made, is that the regulation would protect the fundamental rights of children, and therefore he applauded the need for permission from parents for the processing of their children's data. This point was backed up by Anna Maria Corazza Bildt, who proposed to add the protection of children in the regulation, as she argued that information needed to be child-friendly and easy for them to understand. Another MEP from the EPP, Kinga Gál, highlighted that often citizens are not even aware of the right to protect their personal data. She therefore argued that it is important to have a system in place that guarantees these rights for all. Her colleague, Carlos Coelho, brought up another fundamental rights-based argument for the regulation, which concerned the unauthorized storing and processing of personal data by states and their security agencies.

Similar notions were expressed by other fractions and their MEPs. Juan Fernando López Aguilar, an MEP of the Progressive Alliance of Socialists and Democrats, emphasized that the regulation would be a 'giant step forward' in regulating the fundamental rights of EU citizens, in particular Article 8 of the Lisbon Treaty. His S&D colleague, Marc Tarabella, even went as far as arguing that the regulation would be a dream come true for EU citizens, who would become responsible for their own personal data. MEPs from other parties overall seemed to use the fundamental rights discourse in a positive and solution-based way. For example, Auke Zijlstra from the Non-Inscrits group argued that consent should be an essential element of data processing, in order to make users more aware of such activities and their purpose. Another example is that of Carl Schlyter from the Greens-EFA group and Cornelia Ernst from the European United Left - Nordic Green Left group, who both emphasized that above all, the regulation would be about providing citizens with the freedom of choice and the freedom to choose where to give consent and where not.

6.3.3.3 The Security Discourse

Another discourse often found was that of security. The security discourse was mainly problem-driven as the use of the discourse did not necessarily promote the GDPR as a solution but rather emphasized it as a step forward in solving the bigger problem: privacy in the modern era. The use of the discourse can be divided into two categories. The first consists of the implicit use of the security discourse, which mainly referred to modern society and its use of technology

and data. The second category consists of a more explicit use of the discourse. When used, MEPs referred to actual actors such as the tech giants.

The first category of the implicit security discourse made up the majority of the use of the overall discourse. Examples of this implicit use were found in every fraction, apart from the GUE-NGL. There were some parties that only used the discourse in this manner, and thereby refrained from any explicit mentions. Each speaker from the ALDE group for example used the security discourse in an implicit way. MEP Sophia in 't Veld, for example, emphasized the need for legislation such as the GDPR as we are living in the era of personal data. Another party that seemed to favour the implicit security discourse was the EPP. Some EPP MEPs referred to lacking trust among citizens. Others mentioned the vulnerability of young people such as children and teenagers, who generate data at an unprecedented scale through the use of apps. Such data could be used by companies to monitor them, which would limit their freedom. Overall, the implicit use of the discourse mostly concerned the difference in scale and importance of data protection which had been caused by major technological developments in this day and age, as Csaba Sógor expressed it. Though such statements did not necessarily provide a strong narrative on what constituted the actual threat, a threat was clearly constructed based on references to lacking trust, society's most vulnerable people, and the immense changes in society brought about by technological developments.

The only parties in which the security discourse was used in an explicit way were the Greens-EFA group, the S&D group, and the Non-Inscrits group. Remarkably, both rapporteurs did not steer away from providing more specific notions on the threat of lacking data privacy and the actors associated with it. Jan Philipp Albrecht opened the debate by stating that European citizens and European companies would not allow the European Parliament and the EU as a whole to continue accepting the undermining of European standards by big global tech companies and third-country authorities. Furthermore, Albrecht stated that European consumer associations and companies were urging the EP to complete the GDPR sooner rather than later. This urgency, he argued, was based on the notion that these companies and consumer associations knew that the only ones to profit from the postponement of the regulation were the big data companies from Silicon Valley. He added to this, that these big data companies had constantly tried to undermine EU market rules, and thereby gained competitive advantages over European tech companies. These notions were backed up by the European public, who Albrecht argued, were looking for data-friendly and trustworthy products and services.

The second rapporteur, Dimitrios Droutsas, also used the security narrative in his opening speech. Droutsas emphasized the need for the data reform package to go through - meaning that both the data protection regulation and the directive would be voted for in favour by the EP. When stressing the importance of the package deal, he asked those who were critical of the directive how they would justify to their constituencies that they would choose to protect them against for example Google, but not against the police and other judicial authorities. He thus implied that voting in favour of the regulation would protect EU citizens against tech companies like Google.

Another MEP who also explicitly mentioned tech companies was Judith Sargentini from the Greens-EFA group, who argued that certain companies do not adhere to the rules and regulations. She therefore called for speedy action to ensure that companies like Google and Facebook do not gain absolute carte blanche to do whatever they like. Moreover, she argued that European tech companies must be given the chance to provide the safest products and services in the world. Two MEPs from the S&D group also came forward with similar notions. Sylvie Guillaume argued that the data protection package was ready to face the challenges of the digital world, despite the great difficulties caused by American tech giants. Marc Tarabella, spoke of the safeguards that were needed to be put into place as, he argued, multinationals were being championed above citizens. He even went as far as mentioning that the National Security Agency (NSA) had been carrying out espionage for large multinationals to benefit their marketing. According to Tarabella, the regulation would be a first step in the process of 'fighting back'.

The implication of espionage seemed to be another element of the security discourse, besides that of the tech multinationals. For example, the NSA was also explicitly mentioned during the speech of the second rapporteur Droutsas. The topic of espionage was also implied by Marielle Boullier Gallo and Kinga Gál - both from the EPP group - who expressed the need to avoid mutual spying between the EU and the US. Overall, such mentions mainly concerned the directive on the processing of personal data for the purpose of crime prevention - which these MEPs argued the Parliament should vote for in favour. This would also entail complying with similar rules concerning third countries. As it was only mentioned by a few MEPs, and was expressed rather vaguely, the true motive of this topic in the security discourse is difficult to find.

All in all, the security discourse varied widely in terms of how explicit the security threat was constructed. Mainly liberal and conservative parties stayed away from explicitly mentioning threatening actors, but many of their MEPs did imply the need for stricter protection of personal data as a result of major technological developments and changes in society. Left-wing parties such as the S&D group and the Greens-EFA group did however opt to call out the tech giants. The difference in the use of the security discourse can possibly be explained by the difference in party ideologies, as left-wing social-democratic parties may be more wary of large multinationals and their impact on society. The fact that tech giants were however mentioned by the two rapporteurs of the data protection package, and the earlier data provided by Eurobarometer which showed a certain level of fear among the EU population, permits speculation that to a certain extent all parties were aware of the impact of the regulation on large multinationals.

6.3.3.4 The Economy Discourse

Lastly, the scores on the economy discourse varied per fraction. Most of the use of this discourse was found in the EPP and ALDE fractions. When using the economy narrative, many MEPs expressed hope that the GDPR would bring about not only high data-protection standards, but also support for innovation and jobs in the digital economy. As ALDE MEP Baroness Sarah Ludford put it, smart companies were aware that their business will only prosper on the basis of trust. She thereby implied that businesses could benefit from the GDPR and stricter compliance regimes, so that companies who *do* play by the rules do not miss out in terms of competitiveness. Other positive mentions of the GDPR related to the economy narrative concerned mostly the advantage of having a Digital Single Market, which the GDPR would bring about. These mentions mostly referred to the completion of the Single Market, which would benefit European businesses, and the creation of fairer competition between European and non-European companies - also referred to as 'levelling the playing field'. Overall, many of the MEPs spoke of striking a balance between the protection of privacy and allowing the internal digital market of Europe to develop. The benefits to consumers the GDPR would bring was a much less mentioned topic. It may however have been implied, combined with the security discourse, that European citizens would benefit from increased trust and safer products that could be provided by European companies.

Not all of the economy discourse was positive as some concerns regarding small and medium-sized enterprises (SMEs) were raised. EPP MEPs Marielle Boullier Galo, Kinga Gál, Anna

Maria Corazza Bildt, and Wim van de Camp expressed their concerns regarding the effect of the regulation on start-ups and small businesses in the EU. How the GDPR could potentially negatively affect SMEs was however not made clear in the debate, and therefore these concerns could have mainly been expressed to ensure a certain level of precaution. All in all, the economy discourse was used to express both hope and concerns regarding the effect of the GDPR on the European economy and European businesses. Furthermore, there seemed to be much less emphasis on the completion of Single Market compared to the 1995 directive. More so, the economy narrative touched upon topics such as innovation, competitiveness, and the digital economy.

6.3.4 Remaining Concerns and Finalization of the Debate

Considering the overall debate on the protection of data privacy, there seemed to be a general support for the proposal even though some concerns were raised. These concerns consisted of, for example, the effect of the regulation on SMEs, as mentioned above in the section on the economy discourse. Others concerns that were expressed regarded the difficulties of protecting the rights of data that are transferred to third countries, the possible negative effects on research in the medical field, and the possible effects on free speech. The last two concerns were mainly brought up by the EPP fraction. Nonetheless, many of the MEPs who brought these concerns up, also mentioned many of the positive aspects of the regulation which mostly concerned the protection of fundamental rights. Furthermore, as many MEPs spoke of the need for a speedy adoption of the regulation, these concerns may have been raised to make a final remark on behalf of their parties or constituencies.

Compared to the regulation, the directive on the processing of personal data intended for crime prevention received notably more scepticism, as many MEPs - including the second rapporteur Droutsas - reaffirmed that the regulation and the directive should be a package deal and hoped that their colleagues would vote in favour of both. All in all, the European Parliament voted largely in favour of the package proposal with 621 votes for; 10 against; and 22 abstentions. The result of the voting was therefore adoption by simple majority (European Parliament, 2014).

DISCUSSION OF FINDINGS

Based on the performed empirical analysis, this chapter will discuss its main findings. The discourse analysis on the General Data Protection resulted in a number of different findings per institution. Though the discourses per institution showed many similarities, differences in use, emphasis and expressed concerns showed different narratives on the establishment of the General Data Protection Regulation. These different narratives, as presented in figure 6 below, show the different considerations per EU institution. The following sections will discuss both the differences, as well as the main similarities between these considerations.

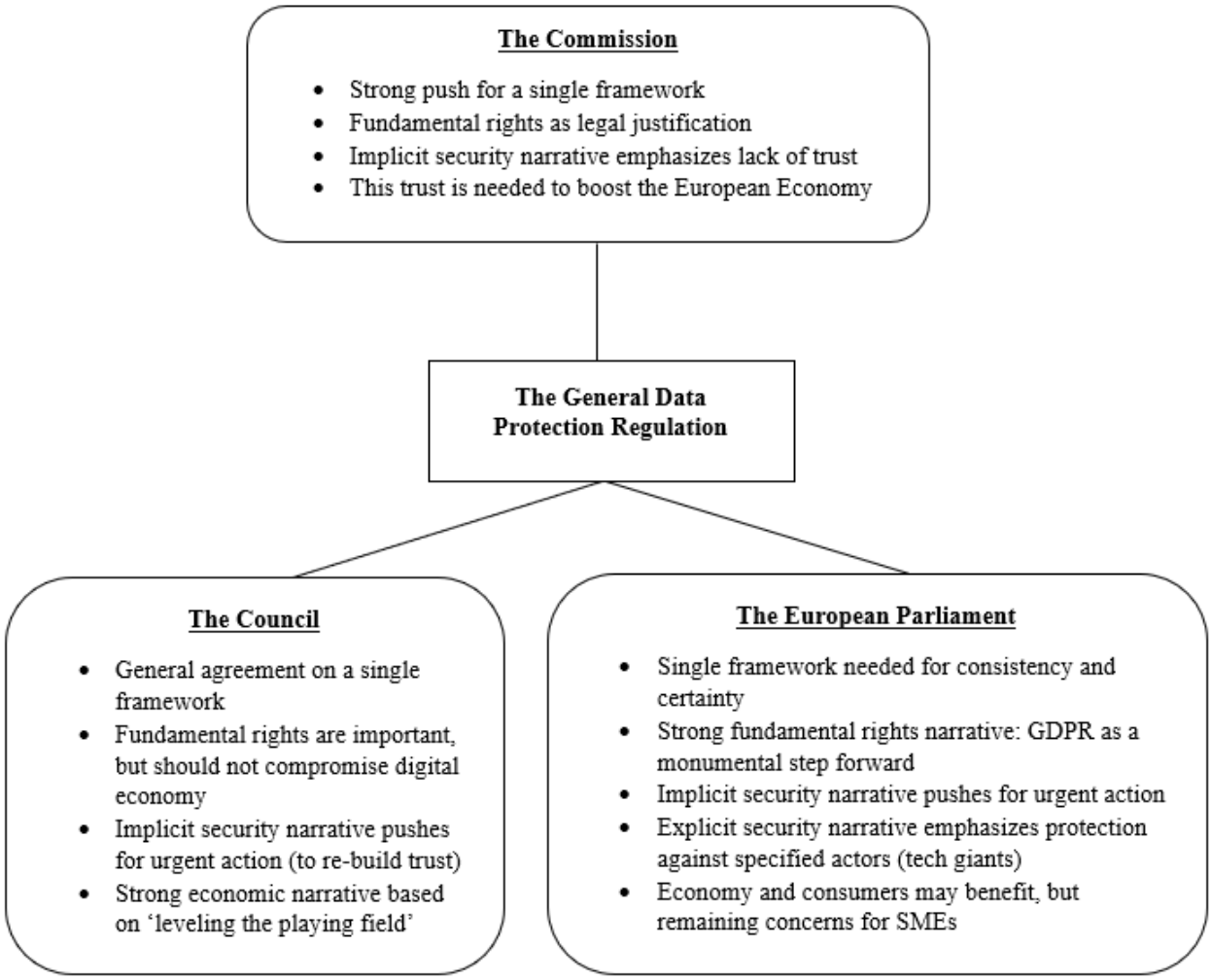

Figure 6. Key Points per Institution

7.1 Differences per Institution

Though each EU institution involved in the ordinary legislative procedure of the GDPR used all discourses from the preliminary analysis (unity; fundamental rights; security; and economy), some nuances can be found. These nuances mainly resulted from the differences in emphasis or the expression of any strong remaining concerns. Each institution therefore offered a different overall narrative on the purpose and ideal formation of the regulation. These differences are not necessarily contradictory. Rather, they emphasize different underlying considerations from the actors within that institution.

First, the unity discourse mostly varied in terms of emphasis. The Commission offered the strongest emphasis on the need for a single framework, with arguments based on the need for legal certainty and the harmonization of rules. Such a single framework was also argued to reduce costs for businesses and would lead to overall efficiency gains. The fact that the Commission expressed the strongest motivation for a single framework may however be less surprising. Compared to the Council and the European Parliament, the Commission represents the general interest of the EU - and therefore does not have a national government or constituency to represent. It may thus be that pushing an EU regulation is in line with the supranational nature of the Commission.

The Council and the European Parliament both offered an overall positive use of the unity discourse. The European Parliament stressed for example the need for a more consistent framework and the need for more legal certainty for EU citizens. The Council, on the other hand, mostly stressed the need to prevent fragmentation of data protection rules in the EU. A regulation therefore seemed to make sense (though a few Member States would have preferred a directive) and a general approach was adopted.

The second discourse of fundamental rights yielded quite different results per institution. Though all seemed to agree on the importance of, for example, Article 8 of the Charter of Fundamental Rights of the European Union, some nuances were found. The Commission's proposal mainly highlighted the importance of legal elements - such as Article 8 - as the foundation of the regulation. The proposal furthermore dealt with other fundamental rights issues in relation to the regulation, such as the expression of freedom. The European Parliament mostly expressed the fundamental rights narrative in a highly positive manner. The regulation was expressed to be a 'revolutionary' and monumental step forward in the protection of

privacy. In general, the notion that the GDPR would be a fundamental improvement for the protection of privacy seemed widely accepted. Other positive aspects that were mentioned included the protection of minors, the importance of consent, and the increase in personal freedom. Contrary to the EP, the Council approached the fundamental rights discourse rather neutrally.

Overall, the regulation was implied to be a good step forward for the protection of citizens' privacy. This positive perspective however did not seem to overrule the other narratives - especially the economy narrative - as several Member States expressed the need to find the right balance between the protection of privacy and economic concerns. The regulation and its protection of personal data were thus considered a positive development, but only if it were to be designed in a way that would avoid it being at the expense of European businesses. To a certain extent, this placed the European economy and European businesses at an equal (if not higher) level of importance as the fundamental rights of European citizens.

The security discourse was found to be much more present in the GDPR considerations compared to the 1995 Directive from the preliminary analysis. As expected, the security discourse has developed since the directive, though its use may have been relatively similar in nature. Each institution used the security discourse to provide context regarding the importance of the regulation. Most referred to the rapid developments in technology and how these have changed society. Another popular theme seemed to be that of the European public's perception of the privacy of personal data, which was supported by Eurobarometer data. The combination of both themes created a narrative that promoted a call to (urgent) action: The European Union needs to respond to the public's concerns regarding their data privacy, and it needs to do so in a timely manner to keep up with rapid developments in the technology sector. The assumption that securitization took place in the discourse on the GDPR was thereby confirmed.

Trust also seemed to be a common theme used in the security discourse. Not only did this concern the public's trust in the protection of their privacy, but also the trust of consumers. If consumers lose trust in the online products and services of tech companies, the economy will be negatively affected. The security discourse was thus often linked to economic motives. This also happened explicitly when certain Members of the European Parliament called out tech giants as key players undermining the trust of EU citizens. These large multinationals were mentioned to have violated European rules and standards; to have been profiting off of

consumers; and to be deemed untrustworthy. To an extent - at least within the European Parliament - these tech giants were framed as a direct threat. This provided strong evidence for the possible securitization of data privacy within the EU,

Overall, the economy discourse seemed to be the most important factor in the shaping of the GDPR, as all other discourses were constantly linked to economic motives. Two groups ultimately motivated the economic importance of the regulation: European consumers and European (tech) companies. Firstly, consumers would benefit from the regulation as it would increase consumer confidence and it would give them access to safe and trustworthy online products and services. This latter argument seemed to be especially dominant in the European Parliament. European (tech) companies on the other hand would benefit from reduced costs and the 'levelled playing field'. The latter concept was mostly used in the Council and by some MEPs, and it referred to fairer competition between European and non-European companies. To an extent, this implied that European tech companies had experienced unfair competition with non-European tech companies - or European tech companies were simply less competitive. Another economic motive consisted of the realization of the Digital Single Market, which is a strategy of the Commission to enable smart and sustainable growth in the EU. It is therefore not surprising that this argument was brought forward by the Commission, especially in their press releases to the public. Lastly, though in general all institutions seemed to portray the regulation as a positive development, some MEPs did raise concerns for SMEs.

7.2 Patterns and Main Consideration

Despite the differences in use of the discourses per institution, a number of factors and considerations formed a consistent thread weaving through the conversations on finalizing the GDPR. The first consists of the acknowledgement of compromise, which was expressed in both the Council session and the European Parliament. Compromises were not only made between the three EU institutions, but also between party ideologies and Member States' interests. Despite the compromises made, there seemed to be general satisfaction about the possible finalization of the regulation. A second factor is that there seemed to be general concern for those vulnerable to the regulation. This group consisted of for example children, start-ups, researchers, and the media (if freedom of expression were to be compromised). The possible negative effects of the proposal for this group provided the main remaining concerns that were expressed in the European Parliament debate and Council session.

The main consideration however seemed to be the strong economic motive, driven by the determination to back up European tech companies by levelling the playing field in the EU. This emphasis on increasing competition in the tech industry coincides with the story of the EU as a 'determinator' and introducer of strict tech doctrines to re-balance the disproportionate power some tech companies have over others. Within the GDPR narrative, the economic benefits of the regulation were also often touched upon. To an extent, it calls into question whether the regulation would have received the wide support it did if it were not for the considerable benefits for European businesses. This is in line with the Council's reasoning that the regulation should not compromise the development of Europe's digital economy.

All in all, the discourses seemed to form an integrated storyline on the creation of the GDPR. More often than not, discourses were linked to one another. The unity discourse – with a main emphasis on a single framework – was positively linked to economic benefits and the public's concern on privacy. The fundamental rights discourse linked its strong legal principles to public demand for better data protection. A sense of urgency was promoted by the security discourse, which also pushed for an increase in trust. This trust would benefit the European economy, which would also benefit from the levelled playing field. Many of these considerations therefore seemed interlinked, and there seemed to be a general 'the sooner the better' approach to finalizing the regulation.

7.3 Limitations, Implications, and Future Recommendations

It is important to mention the limitations and implications of these results. First, the external validity of this research may be limited as it constitutes a qualitative method which has yielded results specific to this policy area. Generalizability of these results can therefore not be assured, as applying the method used in this research may yield completely different results in another area. Not only does this concern differences in policy areas, but also differences in national or regional legislation. As mentioned previously in the section on the global influence of the GDPR, not every country (or region) views the issue of data privacy the same. It is thus possible that when using the same methodology to a similar regulation, different outcomes may still result. This, however, presents the opportunity for future research, as it would be of interest to analyse different global patterns of narratives on the protection of personal data.

Another limitation of this research regards the interpretation of the researcher on the narratives. Though narratives and discourses are relatively easy recognizable, and the use of the

preliminary analysis provided more consistency throughout the discourse analysis, differences in interpretations may still differ per person and could lead to differences in outcomes. This opens up the possibility of researcher bias.

Regarding the interpretation of the security discourse, this limitation can also stem from the boundaries of securitization as a concept itself. Though the strength of securitization as a concept brought forward by the Copenhagen school is its inclusion of concepts beyond traditional security, the boundaries of the concept are rather blurry. To what extent a non-traditional security area has been securitized or not is thus open to interpretation. Therefore, the securitization of data privacy is a new area that needs more exploration, though its link to cybersecurity has indicated the possibility of securitization of the area. The developments of areas such as big data and artificial intelligence may shed new light on how the concept of data protection progresses.

The research implications of this study are limited to only a number of actors as due, to less generalizable results, it is less likely that this research will have broader practical implications. Governments and politicians will continue narrating any cybersecurity-related issues as they see fit, as they have a duty to represent the concerns of their national governments or constituency. The industry of collecting and processing data continues to grow, and it has been argued that better policies of data ownership and protection are needed to reflect the new role of information and data in society, as argued by Sadowski (2016). This, combined with the rapid developments of the technology industry, requires data protection policies to reflect the evolution of technology in society.

7.4 Data Privacy Beyond the GDPR

This research has shed light on an important piece of modern-day legislation and the underlying narratives that were created to help put it into place. As discussed previously in section 3.4, the EU's GDPR has led to the re-examination of - and debate on - existing privacy frameworks worldwide. It seems that the regulation has marked a clear divide between those (national or supranational) governments that put more stringent regulations in place regarding the protection of data privacy, and those that do not. This divide has mainly been caused by economic motives, which can be accounted to, for example, a strong liberal mindset. In the future, however, this may change. This research has argued that the considerations for the GDPR were dominated by a strong underlying economic narrative, which counters the notion

that the regulation predominantly concerned the protection of fundamental rights. This narrative built a case on strong economic arguments, including the (unfair) competition in the tech industry. It therefore does not seem to fuel any existing hesitations regarding the economic considerations for such a regulation.

Tough section 3.4 touched upon the debatability of a possible domino effect caused by the regulation, the GDPR may still become known as an important initiative that put stringent rules regarding the protection of personal data in place. The regulation marks a clear territory in which individuals are at low risk of privacy breaches. Due to its innovative nature, the regulation's jurisdictional scope goes well beyond that of the European Union and thereby increases data privacy and safety world-wide. This could mean that, globally, a divide can come to exist between safe and unsafe digital zones - which would be an incentive for governments to implement similar regulations in terms of stringency. In such a scenario, economic arguments may be overruled by the need to provide a risk-free digital zone for both citizens and companies. Therefore - despite initial hesitations on the notion of the GDPR as a game changer – the GDPR may become a blueprint after all for data protection regulations. This hypothetical prediction becomes more plausible if the securitization of data privacy continues to develop, as it has the capacity to call for urgent action.

CONCLUSION

We are living in the digital age, and the process of digitization has permanently changed and continues to change lives within society. Though this process has brought about many positive aspects, there seems to be a relatively recent growing concern about the scale and speed of technological developments – especially those regarding the processing of data – as recent reports show. Trust in online platforms has diminished. Tech giants seem to have contributed to this distrust in their pursuit of becoming an indispensable service in society's day-to-day life. This pursuit has brought about a number of negatively perceived phenomena, such as the hoarding of data and the occurrence of data breaches. As public concern rises, governments seem to struggle with the question of how to re-build trust in cyberspace.

In the past few decades, cyberspace has been securitized with the introduction of cyber security. This process of securitization entails how to successfully portray a threat as a national or international security threat. The process thereby promotes a sense of urgency, as such a threat should be dealt with in a timely manner. Over time, the link between national security and cyber security has become stronger. Furthermore, the scope of cyber security has increased, as recent technological developments and trends seem to become increasingly securitized. This has included the securitization of data privacy, as data appropriation and data breaches continue to increase in size and frequency.

This particular research has looked into the EU's General Data Protection Regulation, as it constitutes an ambitious regulation that is set out to protect the privacy and security of EU citizens regarding the processing of personal data. As the regulation's aim concerns ensuring data privacy, it can be hypothesized that the regulation may show evidence of a securitization process. In order to test this assumption, this research uses the method of critical discourse analysis. Discourse analysis is the study of language in practice and can highlight the differences in meaning and the actions that follow language. Critical discourse analysis specifically focuses on how language is tied to political, social, or cultural issues. Regarding the EU as a political actor, it thus concerns the manner in which the political topic is defined and narrated, which in turn has the direct ability to shape policy.

The critical discourse analysis method, however, does not only test the notion of the securitization of data protection, as it also allows for the exploration of any other discourses. Any considerations that have influenced the final the outcome of the regulation can thus be

uncovered when using this method of research. In order to uncover these considerations, this research opted for the use of a preliminary analysis, which gave an indication of the possible discourses to be found in the discourse analysis of the GDPR. Based on the ordinary legislative process of the regulation, cases from the Commission, the Council, and the European Parliament were selected for the analysis.

The preliminary analysis resulted in a total of four discourses on unity, fundamental rights, security, and economy. Each discourse offered a different narrative on why the regulation was deemed necessary. Based on these four discourses, the documents and sessions from the Commission, the Council, and the European Parliament were analysed. This yielded different results per institution in terms of presence and dominance of the discourses. In general, there seemed to be sufficient support for a single framework, which supported the unity discourse. Fundamental rights considerations were also widely supported, as the regulation was deemed a monumental step forward regarding the protection of personal data. The security discourse promoted urgent action and emphasized trust in the digital era. The assumption that the GDPR to an extent may have been subject to the process of securitization therefore seems to be confirmed as distrust in the digital economy and the urgency of this issue were often emphasized. Perhaps most importantly, the economy discourse emphasized the benefits to European businesses, which would result from fairer competition in the technology sector. The economy discourse was often linked to the other three, and therefore seemed to take a central position in the finalizing of the GDPR.

Though some differences can be found between the institutions, each institution used these four discourses to express different considerations for the establishment of the General Data Protection Regulation. This research has therefore reached its goal of exploring the possible considerations that shaped the GDPR to what it is today. As technology continues to develop, however, it is of future interest to monitor the changes in considerations that occur in the political realm.

BIBLIOGRAPHY

Abolhassan, F. (2017). *Cyber Security. Simply. Make it Happen: Leveraging Digitization Through IT Security.* Cham, Switzerland: Springer.

About Greens/EFA. (n.d.). Retrieved May 15, 2019, from https://www.greens-efa.eu/en/our-group/about-greens-efa/

About the ALDE Party. (n.d.). Retrieved May 15, 2019 from https://www.aldeparty.eu/about/the-alde-party

Baxter, M. (2018, August 24). How GDPR is shaping global data protection. Retrieved from https://gdpr.report/news/2018/08/24/how-gdpr-is-shaping-global-data-protection/

Bershidsky, L. (2018, November 14). Europe's Privacy Rules Are Having Unintended Consequences. Retrieved from https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are

Buzan, B., Waever, O. & de Wilde, J. (1998). *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner.

Chadwick, P. (2017, February 27). The Rise of the Tech Giants. Retrieved from https://www.iedp.com/articles/the-rise-of-the-tech-giants/

Chakravorti, B. (2018). Why the Rest of the World Can't Free Ride on Europe's GDPR Rules. Retrieved from https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules

Christou, G. (2017). The EU's Approach to Cybersecurity. *University of Essex Online paper series, Spring/Summer 2017*

Council of the European Union. (2015, June 15). *Justice and Home Affairs Council (Justice) - Public Session* [Video file]. Retrieved from https://video.consilium.europa.eu/en/webcast/a3e69074-109a-4c84-802d-f8b3fa75d622

Deibert, R.J. & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance, 18,* 339-361.

Doffman, Z. (2019, April 18). 1.5m Users Hit By New Facebook Privacy Breach As Extent Of Data Misuse Exposed. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/04/18/facebook-illegally-harvested-data-from-1-5m-users-as-it-leveraged-its-data-machine/#688c4c016a2e

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15,* 105-122.

Edwards, B., Hofmeyr, S. & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cyber Security, 2*(1), 3-14.

Europe 2020 strategy. (n.d.). Retrieved May 24, 2019, from https://ec.europa.eu/digital-single-market/en/europe-2020-strategy

Europe takes on the tech giants. (2019, March 23). *The Economist, 430*(9135), 11.

European Commission. (2005). Special Eurobarometer 431: Data protection. Retrieved from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

European Commission. (2012a, January 25). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* [Press release]. Retrieved from http://europa.eu/rapid/press-release_IP-12-46_en.htm

European Commission. (2012b, January 25). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved from http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

European Commission. (2013, January 28). *European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws* [Press release]. Retrieved from http://europa.eu/rapid/press-release_IP-13-57_en.htm

European Conservatives and Reformists Group. (n.d.). Retrieved May 15, 2019, from http://www.europarl.europa.eu/elections-2014/en/political-groups/european-conservatives-and-reformists-group/

European Parliament. (2014, March 11). *Sitting of 2014-03-11* [Video file]. Retrieved from http://www.europarl.europa.eu/plenary/EN/vod.html?mode=chapter&vodLanguage=EN&startTime=20140311-15:02:19-783#

European Union. (2000, December 18). Charter of the Fundamental Rights of the European Union. *Official Journal of the European Communities.* Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union. (2016, April 27). General Data Protection Regulation. *Official Journal of the European Union.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=NL

European United Left / Nordic Green Left. (n.d.). Retrieved May 15, 2019, from http://www.europarl.europa.eu/elections-2014/en/political-groups/european-united-left-nordic-green-left/

Everything you need to know about the GDPR Data Protection Officer. (n.d.). Retrieved May 1, 2019, from https://gdpr.eu/data-protection-officer/

Fairclough, N. (2012). Critical discourse analysis. In J.P. Gee & M. Handford (Eds.), *The Routledge Handbook of Discourse Analysis* (pp. 9-20). London, UK: Routledge.

Gee, J.P. & Handford, M. (2012). *The Routledge Handbook of Discourse Analysis.* London, UK: Routledge.

General Data Protection Regulation (GDPR) – Final text neatly arranged. (2018). Retrieved from https://gdpr-info.eu/

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

Group of the European People's Party (Christian Democrats). (n.d.). Retrieved from http://www.europarl.europa.eu/elections-2014/en/political-groups/group-of-the-european-people's-party-(christian-democrats)/

Hajer, M. (2005). Coalitions, Practices, and Meaning in Environmental Politics: From Acid Rain to BSE. In D. Howarth & J. Torfing (Eds.), *Discourse Theory in European Politics: Identity, Policy, and Governance* (pp. 297-315). Basingstoke, UK: Palgrave Macmillan

Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53,* 1155-1175.

Hucking, T.N. (1997). Critical Discourse Analysis. In T. Miller (Ed.), *Functional Approaches to Written Text: Classroom Applications* (pp. 78-92). Washington, DC: United States Information Agency.

Huq, N. (2015). Follow the Data: Dissecting Data Breaches and Debunking Myths. *TrendMicro Research Paper.* Retrieved from https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf

Irwin, L. (2018, January 31). The GDPR: Understanding the 6 data protection principles. Retrieved from https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

ISO/IEC. (2015). International Standard ISO/IEC 27040. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en

Jia, J., Jin, G.Z. & Wagman, L. (2018). The Short-Run Effects of GDPR on Technology Venture Investment. *NBER Working Paper Series No. 25248.*

Le Bacon-Gaillard, A. (2016, December 1). How Young People View The Impact Of Digitization On The World [INFOGRAPHIC]. Retrieved from https://www.digitalistmag.com/future-of-work/2016/12/01/young-people-view-impact-of-digitization-04723399

Mittel, M. (2019, February 14). What We Can Learn From the GDPR's First Fines. Retrieved from https://www.cmswire.com/information-management/what-we-can-learn-from-the-gdprs-first-fines/

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7,* 61-73.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society, 6*(2), 195-217.

Olssen, M. (2003). Structuralism, post-structuralism, neo-liberalism: assessing Foucault's legacy. *Journal of Education Policy, 18*(2), 189-202.

Ponemon, L. (2018, July 11). *Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT.* Retrieved from https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Privacy Rights Clearinghouse. (2019). *Data Breaches.* Retrieved April 4, 2019 from https://www.privacyrights.org/data-breaches

Reyman, J. (2013). User Data on the Social Web: Authorship, Agency, and Appropriation. *College English, 75*(5), 513-533.

Royle, N. (2003). *Jacques Derrida.* London, UK: Routledge.

Sadowski, J. (2016, August 31). *Companies are making money from our personal data - but at what cost?* Retrieved from https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon

Schwartz, P.M. & Janger, E.J. (2007). Notification of Data Security Breaches. *Michigan Law Review, 105*(6), 913-984.

Silber, M. & Gerrie, D. (2015, April 16). Guarding against a 'cyber 9/11'. *Wall Street Journal.* Retrieved from https://search-proquest-com.eur.idm.oclc.org/docview/1673303622?accountid=13598

Simberkoff, D. (2019, January 23). Will Google's $57M Fine Finally Push the US Toward Comprehensive Privacy Regulations? Retrieved from https://www.cmswire.com/information-management/will-googles-57m-fine-finally-push-the-us-toward-comprehensive-privacy-regulations/

The rise of the tech giants. (2017, June 26). Retrieved from https://finfeed.com/features/rise-tech-giants/

de la Torre, L.F. (2019, March 8). What is the European Data Protection Board (EDPB)? Retrieved from https://medium.com/golden-data/what-is-the-european-data-protection-board-edpb-dbe0ba0ceb3e

The power of privacy. (2019, March 23). *The Economist, 430*(9135), 19-22.

Von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97-102.

Waever, O. (1996). European Security Identities. *Journal of Common Market Studies, 34*(1), 103-132.

Waever, O., Buzan, B., Kelstrup, M. & Lemaitre, P. (1993). *Identity, Migration, and the New Security Agenda in Europe*. London, UK: Pinter.

Wendt, A. (1992). Anarchy is what States make of it: the Social Construction of Power Politics. *International Organization, 46*(2), 391-425.

Wendt, A. (1994). Collective Identity Formation and the International State. *The American Political Science Review, 88*(2), 384-396.

Wendt, A. (1999). *Social Theory of International Politics.* Cambridge, UK: Cambridge University Press.

What are the GDPR Fines? (n.d.). Retrieved May 1, 2019, from https://gdpr.eu/fines/

What we stand for. (n.d.). Retrieved May 15, 2019, from https://www.socialistsanddemocrats.eu/what-we-stand-for

Wylie, J.W. (2006). Poststructuralist Theories, Critical Methods and Experimentation. In S. Aitken & G. Valentine (Eds.), *Approaches to Human Geography* (pp. 298-310). Thousand Oaks, CA: SAGE Publications.

Zorz, Z. (2019, February 7). 8 Months of GDPR: 59,000+ reported breaches, 91 fines. Retrieved from https://www.helpnetsecurity.com/2019/02/07/gdpr-numbers-january-2019/

APPENDICES

Appendix A: Coding table of the European Commission proposal

Section	Unity	Fundamental Rights	Security	Economy
Context of the Proposal	4	3	4	2
Legal Elements of the Proposal	4	9	3	4
Total	8	12	7	6

Appendix B: Coding table of the European Commission press releases

Case	Unity	Fundamental Rights	Security	Economy
Press Release January 25, 2012	4	7	6	5
Press Release January 28, 2013	0	2	5	5

Appendix C: Coding table of the Council session on June 15, 2015

Member State	**Unity**	**Fundamental Rights**	**Security**	**Economy**
Latvia (Presidency)	0	1	2	4
Belgium	0	1	0	1
Czech Republic	0	1	1	2
Germany	0	1	0	1
France	0	1	1	0
Poland	1	1	0	1
Malta	0	1	1	1
Hungary	0	1	0	0
Austria	0	0	2	0
Italy	0	1	0	0
Spain	1	2	2	2
Ireland	0	1	3	4
Lithuania	0	1	0	0
Sweden	0	1	0	1
Greece	0	1	1	2
Portugal	0	1	0	0
Slovenia	0	0	0	0
The United Kingdom	0	2	2	3
The Netherlands	1	1	0	1
Bulgaria	0	1	0	1
Finland	1	0	2	1
Croatia	0	1	0	0
Estonia	0	0	0	0
Slovakia	0	0	0	0

Member State	Unity	Fundamental Rights	Security	Economy
Romania	0	1	0	1
Cyprus	0	1	0	2
Denmark	0	0	0	0
Luxembourg	1	1	0	0
Commissioner for Justice, Consumers and Gender Equality, Věra Jourová	2	4	5	5

Appendix D: Coding table of the European Parliament debate on March 11, 2014.

	Unity	Fundamental Rights	Security	Economy	Total
ALDE					8
Nadja Hirsch	0	1	1	0	
Baroness Sarah Ludford	1	0	1	2	
Sophia in ‘t Veld	0	1	1	0	
Total	1	2	3	2	
ECR					6
Timothy Kirkhope	1	1	1	1	
Vicky Ford	0	0	0	0	
Ruža Tomašić	0	1	1	0	
Total	1	2	2	1	
EPP					39
Seán Kelly	1	2	1	2	
Lara Comi	0	0	1	1	
Marielle Boullier Galo	0	1	1	1	
Axel Voss	0	1	0	1	
Kinga Gál	0	1	1	1	
Wim van de Camp	0	2	0	3	
Carlos Coelho	1	1	1	0	
Csaba Sógor	0	1	1	0	
Anna Maria Corazza Bildt	1	3	0	2	
Zbigniew Zaleski	0	1	0	0	
Salvatore Iacolino	0	1	2	3	
Total	3	14	8	14	
Greens-EFA					12
Jan Philipp Albrecht	0	2	3	1	
Judith Sargentini	0	1	2	1	
Carl Schlyter	0	2	0	0	
Total	0	5	5	2	
GUE/NGL					2
Cornelia Ernst	0	2	0	0	
NI					7
Auke Zijlstra	0	2	3	0	
Franz Obermayr	1	0	1	0	
Total	1	2	4	0	
S&D					25
Dimitrios Droutsas	1	1	2	0	
Sylvie Guillaume	0	2	2	0	
Silvia-Adriana Țicău	1	1	0	0	
Claude Moraes	1	0	1	1	

Juan Fernando López Aguilar	0	2	1	0
Evelyn Regner	0	1	0	0
Marc Tarabella	0	1	3	0
Silvia Costa	0	1	0	0
Tonino Picula	1	2	0	0
Total	4	11	9	1