The Pegasus Spyware scandal and the competences of the European Commission in practice

Verena Feiersinger

Centre for European Integration Research

Working Paper Series

Working Paper No. 02/2024

Centre for European Integration Research
Department of Political Science
University of Vienna

Apostelgasse 23
1030 Vienna/Austria

Telefon: +43-1-4277-49456

Email: eif@univie.ac.at
Web: eif.univie.ac.at

Abstract

This research paper examines the exercise of competences of the European Commission in light of the Pegasus spyware scandal. In 2021, the "Pegasus Project" revealed the illegal surveillance of more than 50000 devices worldwide, including those of EU citizens. The consultation of a combination of publicly available documents, media reports and EU law showed that, on the supranational level, the European Parliament's "Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware" investigated the Pegasus spyware scandal and infringements of fundamental rights, which resulted in the adoption of recommendations for further action. In view of the threat to European values and the rule of law, the Parliament identified a scope of action for the European Commission. Whilst the European Commission is equipped with a wide-ranging toolbox that would allow for an array of legislative actions to be taken, the European Commission is hesitant to act. This lack of response from the European Commission can be attributed to the novelty of the Pegasus scandal itself and its positioning between national security and digital policy. It is the conflicting interests of EU member state governments and the different degrees of being affected by potential EU regulation which impacts national and consequently European positions. Additionally, political and economic framework conditions, such as the elections to the European Parliament from 06 to 09 June 2024, must also be taken into account.

General note: Opinions expressed in this paper are those of the author(s) and not necessarily those of the EIF.

EIF Working Papers are internally refereed scholarly papers.

They can be downloaded at https://eif.univie.ac.at/workingpapers

Authors

Verena Feiersinger is a graduate of the University of Vienna (Master's programme).

Table of Contents

List of Figures

Abbreviations

AIVD	Algemene Inlichtingen- en Veiligheidsdienst, or Dutch Security Service
BKA	Bundeskriminalamt, or German Federal Criminal Police Office
BND	Bundesnachrichtendienst, or German Foreign Intelligence Agency
CJEU	Court of Justice of the European Union
CNI	Centro Nacional de Inteligencia, or Spanish National Intelligence Centre
DG	Directorate-General
DG JUST	Directorate-General
EC	European Commission
EMFR	European Media Freedom Acts
EUCFR	Charter of Fundamental Rights of the European Union
EP	European Parliament
EPP	European People's Party
EU	European Union
EUCFR	European Union Charter for Fundamental Rights
EYP	Ethnikí Ypiresía Pliroforión, or Greek National Intelligence Service
GDPR	General Data Protection Regulation
GISS	Belgian General Intelligence and Security Service
MEP	Member of the European Parliament
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság, or Hungarian National Authority for Data Protection and Freedom of Information
NBSZ	Nemzetbiztonsági Szakszolgálat, or Hungarian Special Service for National Security
NSA	National Security Agency (US)
PASOK	Panhellenic Socialist Movement
PEGA	Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware
PiS	Prawo i Sprawiedliwość, or Polish Law and Justice Party
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

1. Introduction

Over the course of the past decade, the issue of surveillance spyware has gained much traction in relation to revelations of illegal use of the technology and fundamental rights infringements as a consequence. As a result of the advancement of technology, together with the widespread use of smartphones and other similar devices alike, the technological sector and its reach into people's lives has grown tremendously. Therefore, the degree to which targeted monitoring based on technical instruments is being used not only increases but also raises legitimate concerns. One example of this is the use of spyware, more specifically the hacking of smartphones to monitor people's lives covertly (Deibert et al. 2018, p. 7f; Loreggia and Sartor 2022, p. 19f; Marzocchi and Mazzini 2022, p. 4ff; Mildebrath 2022a). This can be traced back to globalisation coupled with technological advancement. However, this rapid advancement of technological development and innovation has created new challenges distinctive to the digital age, because it has also acted as a multiplier of threats and insecurities on the national and supranational level.

The most prominent case of spyware in the last decade is "*Pegasus*", a malware developed by the Israeli company "*NSO Group*" and initially intended for use only by governments to survey criminal activities upon prior legal approval (Loreggia and Sartor 2022, p. 25). However, Pegasus illustrates the dilemma of security and protection of fundamental rights. This is because Pegasus spyware is a new technology representing a challenge as it had never been the case before, but also because it exacerbates already existing concerns for human security and fundamental rights alike.

In the context of increased support and prevalence of authoritarian and other similar regimes worldwide, this new technology creates many more opportunities for illegal and unjustified insights into the private lives of peoples, gravely infringing personal rights and freedoms. From a European perspective, there are many concerns about the state of democracy and rule of law when looking outside of Europe. Governments have a responsibility to maintain security inside their borders, whereas this may include utilising sophisticated surveillance technologies to protect the rights and freedoms of people, defend national security or to uphold the rule of law. Nevertheless, some authoritarian and democratic governments, among

which there are a select number of member state governments of the European Union, have made use of spyware technologies to infiltrate the personal devices of the likes of activists, journalists, and politicians a.o. throughout the world (Feldstein and Youngs 2023, p. 24, 42, 52; Marzocchi and Mazzini 2022, p. 22). Consequently, one may choose to ask whether the domestic situation within the European Union and its member state governments is still upholding its (self)claimed high standards of democracy and rule of law, in return protecting its citizens and residents.

It was several studies, most notably the *Citizens Lab Research Report* and *Forbidden Stories* (see Deibert et al. 2018; Loreggia and Sartor 2022; Mildebrath 2022a), which discovered that Pegasus and similar spyware were being used in an exploitative manner. These reports astonished the world when they revealed the extent to which people's lives had been monitored, including numerous human rights advocates, journalists, academics, and opposition leaders. Furthermore, the reports highlighted the far-reaching scope of the application of spyware technologies, as every individual across the world is a possible target for surveillance purposes if there are no existing restrictions or regulations guiding the use of said technologies. The lack of adequate regulation results in the restriction of fundamental freedoms and human rights, such as the right to free speech and participation in society, as surveillance is set to become more intrusive in what would constitute a sector-specific lawless environment.

The Pegasus Spyware scandal presented a visible breach of fundamental rights. Rights that are granted to every person within the European Union. As protected in the Charter of Fundamental Rights of the European Union (or *EUCFR*), the pillars of the European legal system include fundamental rights such as, but not limited to, the right to privacy, data protection and freedom of speech (Loreggia and Sartor 2022, p. 27; Marzocchi and Mazzini 2022, p. 17). This is besides the fact that restrictions on certain rights are temporarily permissible provided reason, such as, for example, the necessity for law enforcement and intelligence to safeguard national security. Nonetheless, this would be contingent on judicial approval ahead of time. However, one may inquire whether this can realistically be conducted in a moral and legal manner in the absence of suitable, up-to-date regulatory frameworks and supervision mechanisms.

Sophie In t'Veld, a Dutch politician, Member of the European Parliament and the European Political Group "Renew Europe", lamented that "*as soon as national security is invoked, transparency doesn't apply anymore, citizens' rights don't apply anymore. Parliamentary scrutiny or judicial scrutiny doesn't apply anymore. It's basically an area of lawlessness*" (Stamouli and Van Sant 2023, p. 4). In t'Veld's reasoning is precisely the reason why the Pegasus spyware scandal is an important and decisive point for EU policy making with respect to future developments in light of technological advancements digital space. In this regard, the scandal represents policy concerns of the moment and the future alike. This is because spyware does not only concern the digital realm and therefore digital policy, but more importantly fundamental rights and security, therefore crossing over to Justice and Home Affairs and Security policy. It is this intersection of a multiplicity of policy areas that makes it challenging for new legislation to be drafted and implemented as different policy areas are integrated to the supranational European level at different degrees. Therefore, creating consensus among national governments and within the European institutions presents itself as a challenge because neither appears to be willing to relinquish their power and/or competences. This is another point of interest that makes the case of the Pegasus spyware scandal within the context of the European Union an interesting, topical issue with relevance to future governance issues.

In light of this, the Pegasus spyware scandal is more than an unfortunate incident as it calls into question the idea of individual rights, therefore jeopardising the foundation of democratic values and the rule of law. One may therefore ask how spyware was able to gravely breach fundamental rights all EU member state governments have subscribed to when transposing EU law, and whether the spyware scandal may have been the result of the absence of a suitable, up-to-date regulatory framework and lax supervision mechanisms. Furthermore, because of the complexity of the Pegasus spyware scandal and its infringements on common European fundamental rights, an intervention or other formal action under the auspices of the European institutions, more specifically the European Commission, could have been expected as a response to the alleged infractions.

To provide an answer to the question at hand, this author's analysis will be structured as follows. Chapter 2 will outline the research design which will also include the methodological approach with specific focus on the research phases, process and a detailed account of the

author's data collection and data processing procedure. Complementarily, a brief discussion of the theoretical framework, i.e. intergovernmentalism and neofunctionalism and their key arguments to provide a common understanding of the workings of the European Union in theory. In addition, the author will provide an institutional background as a general overview of the functioning of the European Union. In Chapter 3, the author will provide a more detailed examination of the unfolding of events of the Pegasus spyware scandal. This will include a discussion of spyware itself, what it is and what challenges it poses. This will then be followed by an examination of the state of spyware in EU member states dependent on their differing levels of affiliation to the spyware scandal. Having constructed a research design and provided the necessary background information on the Pegasus spyware scandal in reference to the European Union and its member states, the author will then discuss the scandal and its implications for EU politics in Chapter 4. Hence, Chapter 4 will comprise a discussion of the interplay of fundamental rights, different institutional perspectives on the spyware scandal in addition to an evaluation of the spyware scandal based on selected European integration theories. The concluding Chapter 5 will provide a clear and concise answer to the research question in addition to a succinct summary of the most important results and how these results can be classified in the current state of research. Additionally, the author will postulate an assessment of the frontiers of research, whilst giving an overview of recommendations and possible directions for future research.

2. Research Design

As outlined in the introductory remarks by the author, the Pegasus spyware scandal is positioned at the intersection of national security, digital policy and fundamental rights and therefore interconnects different policy areas that differ with regard to the extent they are integrated to a supranational level. This makes formal actions on the European level more complex and sensitive as the balance of power between member state governments and the European institutions can be a challenging path to navigate. Considering the time sensitivity yet relative novelty of the Pegasus spyware scandal, there is a clear research gap as the implications of the Pegasus spyware scandal on the exploitation of competences of the European institutions, more specifically the European Commission, have yet to be examined. Taking into consideration the institutional constellation of the European Union and the

institutional competences of the European Commission, which will be more closely examined in Chapter 4, the author aspires to address the following research question:

> *To what extent does the European Commission utilise its various instruments to exploit, or even increase, its competences in the case of the Pegasus spyware scandal?*

2.1. Methods

To answer the research question, the research design is to follow the logic of first inspecting the Pegasus spyware scandal to understand how events did evolve over the past couple of years with a specific focus on the European Union and member state governments implied in the scandal. The selected timeframe for the author's research will be limited to 01 January 2021 until 15 June 2023. 15 June 2023 is the date when a first formal action by one of the European institutions was taken, i.e. the formal adoption of the *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware* (2023/2500(RSP) [P9_TA(2023)0244]; henceforth: EP Pegasus recommendations) by the European Parliament Plenary Session.

The author's selected method of analysis was process tracing. This method was selected by the author as the Pegasus spyware scandal and its ramifications within the European Union was a relatively new phenomenon, meaning that there no literature specifically addressing it. Therefore, process tracing allows the author to provide a detailed, chronological account of events from the moment the spyware scandal was publicised within the European Union leading up to the EP Pegasus recommendations.

2.1.1. Process Tracing

The author will use the qualitative approach to process tracing modelled after Collier (2011), Bennett and Checkel (2014) and Mahoney (2010 and 2015). As the research project is situated in the field of the European Union and policy making, the author would also like to note that process tracing was recently picked up by Datzer and Lonordo (2023) in their research on EU anti-disinformation policy. As argued by this author in agreement with Datzer and Lonordo (2023), process tracing allows to "*systematically examines[s] the unfolding of*

events over time, identifying key steps in the process, in order to analyse change and gain insight into its causal paths, mechanisms, and outcomes" (Datzer and Lonardo 2023, p. 756, ref. Benett and Checkel 2014 and Collier 2011).

Process tracing can deliver significant contributions to the research project due to its detail-oriented nature. Consequently, this methodological approach allows the author to assess her theory and hypotheses, identify and describe a selected phenomenon in support of an evaluation (Bennett and Checkel 2014, p. 7f; Mahoney 2010, p. 123f; Mahoney 2015, p. 202ff). With these contributions, the author would also like to acknowledge that one of the main challenges of her research project lies in accurately and factually correctly explaining events at specific points in time. Therefore, by breaking down the outcome into smaller pillars and deconstructing the events leading up to the adoption of the EP Pegasus recommendations, the author may draw conclusions by concentrating on how events have developed through time. This detailed examination will provide an understanding of the gravity of the situation that led the European Parliament to the adoption of the EP Pegasus recommendations. Only by doing so can the author avoid ambiguity of results or selection bias.

2.1.2. Data collection

The media research process was conducted for the defined timeframe of 01 January 2021 and concluded with the publication of the EP Pegasus Recommendations on 15 June 2023. This allowed the author to closely follow the chain of events following the revelations of the Pegasus spyware scandal until a formal reaction by one of the institutions of the European Union, i.e. the European Parliament, was adopted.

To gain insight into the inner workings of European Union in the case of the Pegasus spyware scandal, the author prioritised Agence Europe as a first point of information. Agence Europe is a news agency with its headquarters in Brussels and is staffed with specialised journalists. The primary focus of Agence Europe is to provide insight to the European political and economic integration efforts whilst providing both national and supranational (European) perspectives. With its inauguration in 1953, Agence Europe has since published the *European Daily Bulletin* (Agence Europe 2023).

Before the author started with her data collection efforts, keywords and phrases in connection to her research project were collected to provide a starting point. With the Pegasus spyware scandal touching upon different policy areas and principles, the author decided on the keywords "*spyware*", "*Pegasus*", "*spyware scandal*", and "*fundamental rights*". Throughout this collection process, the author ensured for the keywords to be featured in either the title or text to gain the fullest picture possible. This decision was consciously made by the author due to the relative novelty of the spyware scandal, therefore expecting there to be less data when compared to other policy issues, such as the war in Ukraine a.o. However, upon closer consultation, articles based on the defined keywords specifically addressing the spyware scandal, i.e. "*spyware*", "*Pegasus*" and "*spyware scandal*", were few in comparison to articles found based on the keyword "fundamental rights". This is because, having defined the timeframe for the search in Agence Europe, the keyword "fundamental rights" resulted in 3096 articles. In contrast, when the keyword was changed to "spyware scandal", only 2 articles were found, whilst the keywords "Pegasus" and "spyware" resulted in 49 and 63 articles respectively. To understand whether there was an article in the Agence Europe database which addressed the spyware scandal as well as fundamental rights, the author adapted the defined search parameters to include either "*spyware*", "*Pegasus*" or "*spyware scandal*", in addition to "fundamental rights". As a result, 3 articles were identified. An overview of the author's research efforts, including keywords and the number of findings, are summarised in *Table 2-A* (see below).

Figure 0–A: Overview of Agence Europe research process from 01.01.2021 until 30.06.2023 (author's own visualisation)

Keyword	Number of articles
"spyware scandal"	2
"Pegasus"	49
"spyware"	63
"fundamental rights"	3096
"spyware", "Pegasus" or "spyware scandal" + "fundamental rights"	3

Whilst the number of articles found in the author's research process in the Agence Europe database was limited, it did provide the author with a good first overview of how events in relation to the Pegasus spyware scandal unfolded over time. Furthermore, this initial research process allowed the author to gain insight to the reactions of member state governments in light of the revelations made, or more specifically the lack thereof. These findings were thus used as a "stepping stone" for complementary research efforts and provided a first overview of involved EU institutions and implicated national governments. As a next step, the author then chose to search for information regarding the institutional background to have a better understanding of the complexity of EU policy making and the distribution of power among the institutions themselves, but also with respect to national actors. Having laid a focus on European Studies in her MA degree, the research process for literature on the European Union was relatively straightforward and comprised both books and academic articles on the institutional setup and policy making process of the European Union in addition to EU legislation (i.e. TFEU, TEU, a.o.).

To illustrate the complex situation of the Pegasus spyware scandal as holistically and accurately as possible, reports, studies and other publicly available articles (such as European Parliamentary Research Service, Politico, Euractiv a.o.) were consulted and incorporated to

complement the preliminary findings in Agence Europe. With this purpose in mind, the author extended her research efforts beyond the adoption of the European Parliament's recommendations on 15 June 2023. This allowed the author to closely follow actions and responses on the European level and also potentially include any major developments, e.g. the initiation of legislative proposals. As a consequence, should the European Commission have initiated a legislative proposal or made use of its tools in response to spyware after the adoption of the EP Recommendations, this would have been incorporated in the author's work. Therefore, the collection of this additional information was conducted in parallel to all other data collection efforts. Following the discussion of the complexity of the Pegasus spyware scandal, the author will outline and discuss the different tools available to the European Commission. The author will then discuss the EP Pegasus recommendations and compare them with the instruments available to the European Commission. The results of this comparison will then be visualised in a table.

As a next step, a theoretical lens is applied to the Pegasus spyware scandal to perhaps gain more insight into the reasons behind the behaviour of European institutions. For this step of the research design, a neofunctionalist and intergovernmentalist theoretical approach were selected. As will be briefly discussed in the next section, intergovernmentalism and neofunctionalism are two competing theories of European integration that make different predictions of how the integrative process evolves and what the main driving factors are. A short background on the selected theories will be provided in the next section. Lastly, a concluding outlook will summarise the findings, place them in the current state of research, and provide an outlook for future research.

2.2. Theoretical framework

Within the realm of European Integration theory, there is a broad number of theoretical approaches to explaining the state of integration of the European Union. As the author is attempting to gain understanding as to what extent, if so, the European Commission makes use of its tools in the aftermath of the Pegasus Spyware scandal, said integration theories present principles and explanations regarding the Commission's behaviour (or lack thereof). Whilst neofunctionalism, intergovernmentalism, liberal intergovernmentalism, new institutionalism, constructivism and postfunctionalism are all theoretical approaches that

have been linked to European Integration theory, only intergovernmentalist and neofunctionalist approaches will be discussed.

2.2.1. Intergovernmentalism

A first theoretical framework to be of assistance in the authors research project is intergovernmentalism. Within the realm of international relations, there are two core tenets to the intergovernmentalist approach: national governments as the key players, and mutual cooperation being beneficial for national actors based on increased interdependence, especially within Europe. State responses to growing international interdependence are what intergovernmentalism perceives to explain European integration, whereas national governments institute and supervise integrative efforts. Thus, any successes of integration can be traced back to interstate power balances and national policy preferences. This state-centric approach to explaining European integration emphasises the essential position of national governments and their cooperative efforts in this process. This cooperative effort is generally a decision consciously made to advance state interests in an increasingly interdependent global environment (Cini 2019, p. 71f; Schimmelfennig 2018, p. 7f).

Within the context of the European Union, this intergovernmentalist thought places member state governments at the centre of this cooperation effort to advance national interest without having to give up their sovereignty in the process of European integration. Consequently, as argued by Hoffmann and Keohane (1991), rather than a transfer of sovereignty from the national to the supranational level, European integration suggests a pooling or sharing of sovereignty in the spirit of cooperation (Cini 2019, p. 72, ref. Hoffmann and Keohane 1991, p. 277). However, because national governments do not cede (all) their power to a supranational level, any and all decisions are reached by means of intergovernmental (policy) negotiation, which indicates that decisions made with regard to closer cooperation in relation to European integration may only be achieved if member state governments perceive it as beneficial. Therefore, following intergovernmentalist thought, member state governments manage the integration process by deciding collectively on the direction and scope of any future moves towards greater integration (Rittberger and Schimmelfennig 2015, p. 38ff)

Nonetheless, cooperation does not only present benefits. This means that states will have to evaluate the cost and benefit of such a process. Such cooperation will be contingent upon

evaluating the benefits and drawbacks of membership. Consequently, the degree to which European integration enhances is a result of the effectiveness of agreements reached between its constituent states based on a foregone cost-benefit analysis, therefore ensuring the safeguarding of national interest, which remains the primary goal (Cini 2019, p. 70f).

The respective national interests of member states and the assertion thereof largely depends on power dynamics within intergovernmental negotiations connected to a state's standing. To simplify this, "*the outcome of international negotiations […] depends on the relative bargaining power of the actors, on one hand, and on the effects of international institutions on the negotiation process, on the other*" (Rittberger and Schimmelfennig 2015, p. 40). This may be traced back to national interest remaining the primary driving force of integrative processes in intergovernmentalist thought. As a result, European integration may only occur if member state governments should perceive this effort to be beneficial for national interest. Nevertheless, the intergovernmentalist approach to integration presumes national interests and policy preferences to be predetermined, meaning they are neither created nor altered by means of negotiation. Therefore, member state governments do not alter national interests in the time leading up to talks, during talks or afterwards. Whilst member states will engage in a cost and benefit analysis with regard to the pursuit of their policy preferences, the content of these interests and goals remains unaffected (Cini 2019, p. 70; Rittberger and Schimmelfennig 2015, p. 40f).

2.2.2. Neofunctionalism

Within a neofunctionalist approach, however, one may identify a functional and institutional dynamic. This means that successes and/or shortcomings in reference to the European integration may typically be traced back to transnational and supranational actors as they are argued to be the main drivers of integrative efforts. The neofunctionalist thought anticipates integration to follow a gradual, self-reinforcing process that is guided by the mechanisms of spillover. This means that with a gradual process of political integration, first cooperative attempts are identified in one policy areas whereas the interconnectedness of policy areas results in more cooperation in other policy areas as well. Based on these increased levels of integration through cooperation, the creation of supranational organisations may be a result of this cooperation, whereas said institutions may grow to become more autonomous. This

means that despite initially consenting to political integration, with the transfer of power to a supranational level as a consequence, member states may find themselves in a situation where even more integrative steps are required as a result. Therefore, neofunctionalists perceive member states to eventually succumb to supranational interest following a path dependent logic of European integration (Strøby Jensen 2019, p. 58ff, Schimmelfennig 2018, p. 15; Rittberger and Schimmelfennig 2015, p. 47).

As already mentioned, spillovers are the main source of transformational change within neofunctionalist thought. Whereas said spillovers were first identified by Ernst Haas (1968, p. 283ff), this conceptual approach was then picked up and further expanded by Schmitter (1969, p. 162), who reclassified the elements of integrative steps into functional, political and cultivated spillover. Following Schmitter's approach as further differentiated and researched by subsequent authors, there are three distinct ways spillovers can solidify.

First, the *functional spillover*. This type of spillover occurs when an initial policy objective can only be guaranteed by completing further integrative acts in interconnected policy areas. In this case, national governments are motivated to implement further measures to integrate said interrelated policy area to ensure national interest can be realised and any welfare losses are avoided. As is the case within the European Union, most policy areas are complexly intertwined therefore making it difficult to separate certain issues and challenges to distribute competences and duties. This, in return, would serve as an incentive for policymakers to undertake further integrative actions to fulfil their initial objectives based on national interest (Demosthenes and Niemann 2015, p. 198; Haas 1968, p. 297; Lindberg 1963, p. 10; Rittberger and Schimmelfennig 2015, p. 48; Schmitter 1969, p. 162).

Second, the *political spillover*. A political spillover happens when national actors, i.e. bureaucrats, political players or interest groups a.o., prefer the resolution of significant challenges, even when they appear on a national, at a supranational level, in case of uncertainties regarding their successful resolution domestically. By means of referring decisions to the supranational level, the European Union is attributed more autonomy and responsibility in the decision-making process. With every decision that is referred to the supranational level, the European Union is therefore gradually ascribed more competence, which requires the European Union and supranational institutions to increase their capabilities to meet added responsibilities. Furthermore, this interest in shared problem-

solving is likely to cause elites to gradually change their political actions and expectations towards the new supranational centre, i.e. the European Union. This approach is likely to increase as integration advances, whereas the extent of integration increases the likelihood actors will achieve their political goals at the supranational level as opposed to the national level (Demosthenes and Niemann 2015, p. 198f; Rittberger and Schimmelfennig 2015, p. 49; Schmitter 1969, p. 162 f.).

Third, the *cultivated spillover*. This type of spillover is initiated by supranational institutions as they attempt to strengthen their own positions by acting as integrators. These supranational institutions can help the integration process by, for example, taking on the role of policy initiatiors or facilitating agreements above the lowest common denominator (Demosthenes and Niemann 2015, p. 199; Rittberger and Schimmelfennig 2015, p. 49). In the case of the European Union, the institutions to initiate this third type of spillover are the European Commission, the European Parliament and the Court of Justice of the European Union (CJEU).

To summarise, neofunctionalism typically anticipates gradual and self-reinforcing integration following the logic of path dependency. This means that member states may be willing to take some integrative steps in the beginning. However, spillover mechanisms may create transnational dependencies. As a result, integrative steps may not be limited to what member states had previously agreed on and supranational actors may also gain substantial autonomy and capabilities (Schimmelfennig 2018, p. 15).

2.3. Institutional background

Based on the research design as applied by the author, the discussion part in Chapter 5 will draw upon knowledge of the inner workings of the implicated institutions of the European Union. Therefore, the author will provide a first impression of the competences of the European Commission and the European Parliament as they are the key players with regard to the Pegasus spyware scandal on the European level.

2.3.1. The European Parliament

The European Parliament is one of the supranational EU institutions. It is the only supranational institution in the European Union that is directly elected by European voters,

every five years, and it consists of 705 Members of European Parliament (number of seats will increase to 720 with the European elections on 06 to 09 June 2024), which are divided into European Political Groups (EPG). Furthermore, the European Parliament acts as an important link in reference to the cooperation with national parliaments as well as the supervision of other EU institutions. Whilst its position may appear strong in the current state, during the early stages of integration, the European Parliament's involvement in the policy-making process was minimal and limited to consultation only.

Following the entering into force of the Treaty of Lisbon in 2007, the European Parliament saw an increase in its powers and competences as it gradually gained legislative authority (Burns 2019, p. 178f; Wallace and Reh 2015, p. 87). These revisions granted the European Parliament consultative powers in a select number of additional policy areas, which means that the European Parliament receives policy proposals by the European Commission for the Council for an opinion. Whilst formalising its opinion, the European Parliament may propose changes, postpone passing a resolution, or refer subjects back. The most valuable addition to its competences is the power of co-decision with the Council of the European Union. Co-decision, by way of explaining, is referred to as the Ordinary Legislative procedure and requires the agreement of both the European Parliament and the Council for legislative proposals to be adopted. Another competence of the European Parliament is that of consent, meaning that it can approve or reject legislative proposals a.o. without being able to give its opinion (Burns 2019, p. 180f; Reh and Wallace 2015, p. 85ff).

Additionally, the European Parliament has progressively acquired new competences that allow for more authority with regard to the European Commission. This is mostly in reference to the installation, confirmation, and the possibility of censure of the College of Commissioners and the Commission (Burns 2019, p. 179; Raunio 2015, p. 254). Tied to this closer connection to the European Commission, there is one more key competence that the European Parliament possesses, i.e. the right of inquiry. This competence means that "*in the course of its duties, the European Parliament may […] set up a temporary Committee of Inquiry to investigate, without prejudice to the powers conferred by the Treaties on other institutions or bodies, alleged contraventions or maladministration in the implementation of Union law […]*" (Article 226 Treaty on the Functioning of the European Union, or *TFEU*).

The European Parliament is therefore attributed a competence which is an integral component of its political control powers that pertain to the investigation of any violations or improper conduct in the application of EU law. In other words, should any infractions of EU legislation, discrimination, neglect or other issues arise, then the European Parliament may make use of its right of inquiry and establish a committee for investigative purposes. Said Committees of inquiry have the authority to request relevant information as part of a fact-finding mission in case of suspected violations or shortcomings with regard to the implementation of EU legislation, in which case they may formally request relevant witnesses and/or experts for testimonials. While the European Parliament may file with the Court of Justice of the European Union (CJEU) in case a European institution or agency does not comply with the Committee's request for a testimonial, the European Parliament must rely on the European Commission for support if a member state refuses to cooperate with such a request. The Committee generally ends within a year of its establishment, culminating in the presentation of a report to the European Parliament Plenary Session, which may then serve as a starting point for a resolution that includes recommendations for other EU institutions and/or member states alike (Article 226 TFEU; Best 2019, p. 244; Fromage 2020, p. 7ff.; Pollack 2020, p. 31f.).

2.3.2. The European Commission

The second relevant European institution is the European Commission. The European Commission is the one supranational institution that is perceived as the driving force behind European integration as it is said to have an institutional interest in increasing its influence with regard to EU policy making and politics. In other words, the European Commission aims to extend its own supranational competences through harmonisation, regulation and standardisation to more policy areas that are not yet integrated to a supranational level, therefore remaining under national jurisdiction (Reh and Wallace 2019, p. 89; Wonka 2015, p. 98).

One of the main responsibilities of the European Commission is to make legislative policy proposals, which in return presents the Commission with the ability to influence both the direction and content of EU policies. This enables the European Commission to advance integrative efforts if it deems just to do so. This means that the European Commission may

contribute to and oversee EU policy making from beginning to end. Furthermore, the Commission often releases working papers and communications to "test the waters" regarding political challenges to its objectives (Egeberg 2019, p. 144f; McCormick 2017, p. 82f; Wonka 2015, p. 84).

Additionally, the European Commission is also tasked with supervising the implementation of EU legislation, which means that whilst respective member states are responsible for the translation of EU legislation into national legislation, the European Commission nonetheless is involved in implementation criteria and standards. These are determined based on the legislative status, i.e. regulations, directives, decisions, recommendations, opinions and recommendations. One essential aspect of the competences of the European Commission is its responsibility to oversee the adherence to EU law and the treaties alike. In case a member state is thought to have violated or neglected to either implement EU legislation or adhere to EU primary and secondary law, the European Commission has the authority to bring infringement actions against them by referring the case to the Court of Justice of the European Union (Egeberg 2019, p. 145; McCormick 2017, p. 82f; Wonka 2015, p. 84).

3. The Pegasus Spyware Scandal

The "*Pegasus Project*" was organised by Forbidden Stories in collaboration with Amnesty International's worldwide Security Lab and involved seventeen worldwide media outlets. The effects of the investigation are still being felt around the world. The global probe discovered that Pegasus, an advanced spyware programme marketed by the Israeli company *NSO Group*, may have affected over 50,000 people based on an extraordinary data breach.

Forbidden Stories compiled and summarised all available information about the Pegasus Project and its international ramifications in the form of maps containing important facts and figures. This for example includes the number of confirmed victims per country among others. Their work facilitates overview and illustration efforts of the events that unravelled and the shockwaves that followed the project's publication. The data upon which their research is based on was derived from publicly accessible sources, including publications by Pegasus Project partners, participants and other media outlets. Amnesty International and Citizen Lab reports are the key source documentation in cases of verified infections. As can be imagined, the findings made a stark impression on civilians and officials alike.

Considering the magnitude of the revelation made by the Pegasus Project in July 2021, the scandal is the most comprehensive cybersurveillance scandal since the Snowden revelations. The Snowden revelations centred around Edward Snowden, former employee of the US National Security Agency (or *NSA*), who publicised the extensive and intrusive nature of surveillance of persons by the NSA. As explained by Leloup (2023) in Le Monde, "*[…], the NSA set up mass surveillance tools giving it access to insane quantities of information: emails, telephone data, social media messages, geolocation*"(Leloup 2023). The revelations did not only raise questions in reference to the interplay of national security and human right, but also highlighted the close cooperation with the tech sector in light of digitalisation.

Despite the global reach of the NSO Group's spyware technology, it is important to take a look closer to home: the European Union. Therefore, this chapter will be organised as follows: First, the author will discuss spyware in a general manner, i.e. what it is and what main challenges it presents. Among these challenges will be that of the protection of fundamental rights. Therefore, the subsequent section will focus on fundamental rights and their framework in the European Union. Having established a common knowledge on

spyware and identified risks in reference to fundamental rights, the author will then move to inspect the EU member states and their respective alleged (non)use of spyware. With this chapter, the author aims to provide a comprehensive starting point for the analysis that will follow in Chapter 4 based on the research method and process as already outlined by the author in Chapter 2.

3.1. Spyware technology: a brief introduction

When speaking of "*spyware*", one is referencing a specific kind of malware. The word malware itself is derived from malicious software, whereas the word malware literally consists of a combination of the two words. In the case of spyware, malware code is covertly placed on a person's device with the intention of obtaining the users personal data. Because the code can be installed covertly, as in the manner of a spy, this type of malware is referenced as spyware. The compromised smartphone then transmits the targeted information to the relevant operator overseeing the malware. This authorises the operator to monitor any and all activities on said smartphone in real time. The personal data accessed by the operator usually includes valuable private information (Gurijala 2021; In t'Veld 2023, p. 4; Maciejewski and Marzocchi 2023, p. 45ff.; Marzocchi and Mazzini 2022, p. 4f.).

One important aspect of the technology that is important to know in reference to spyware: it has the ability to grant complete access to files and messages, even ones that had been sent in the past, passwords, and other personal information (In t'Veld 2023, p. 4). Because of this unique characteristic, spyware is in very stark contrast to traditional, real-time monitoring, which, when compared in scope with spyware is limited. Even if the use of the spyware is based on a court ruling, for example, it nonetheless raises questions regarding its ethicality and the protection of one's fundamental rights such as the right to privacy. This is because of the aforementioned retroactive, nearly unlimited, access to personal data upon its application.

In addition to the undetectable placement of the spyware code, this type of malware could, both theoretically and in practice, also infiltrate one's devices after the installation of software from a different source, e.g. games or other system utilities. If the newly installed software lacks the necessary security precautions it can act as a trojan horse. In this case, the installed programme may be a modified version of the original. By the means of consenting to the download of the software, one inadvertently gives access to one's personal data. The same

goes for software that is downloaded unintentionally by means of pop-up advertisements or even opening a compromised email attachment. The same is applicable to digital music and video files. As is the case with images, when songs, videos or other types of recording are circulated among friends, one may unknowingly infect their devices as well. One additional option may be for other devices to be infected by the malware when they are connected to the home network. Consequently, if files are continued to be distributed or an infected device is connected to a different network, the malware may continue to spread uncontrollably. The result: a domino effect (Gurijala 2021; In t'Veld 2023, p. 4f.; Maciejewski and Marzocchi 2023, p. 45ff.; Marzocchi and Mazzini 2022, p. 4f.; Mekhennet et al. 2021).

To simplify this: almost anything in the digital realm could be used for spyware to covertly infiltrate someone's device. These are just a few examples that highlight the simplicity with which spyware can infiltrate someone's personal data regardless of the security precautions being taken. What these examples have highlighted is the following: when spyware or other malware is not immediately (upon discovery) dealt with adequately, a domino effect is initiated, and the consequences may be extensive and grave.

3.2. Pegasus as the latest prominent example of spyware

Having provided a brief introduction on spyware and related malware, there is one more question that needs to be answered before the author can move forward to discussing its ramifications within the European Union: What is Pegasus and where did it come from?

Pegasus is quite possibly the best-known product from NSO Group based on the waves it has made since the publication of the findings by the Pegasus Project. The Israeli cyber-intelligence company NSO Group created Pegasus, a technology which has all the characteristics of spyware as outlined in the previous section. Nonetheless, with the development and market launch of their product, the NSO Group has repeatedly asserted that their product is only supplied to law enforcement and government security organisations. In line with this, the company reiterates that its technology is solely used to support rescue efforts and combat criminals including terrorists, sex and drug traffickers among others (Farrow 2021, p. 5f.; The Washington Post 2021). This is despite statements made by Shalev Hulio, co-founder and former CEO of the NSO Group, in a The New Yorker Feature (Farrow 2021). In the feature, it is argued that the purchase of Pegasus is restricted to governments,

intelligence agencies and law enforcement. Furthermore, as Farrow quotes Hulio, the company and its leadership "*have repeatedly cooperated with governmental investigations, where credible allegations merit, and have learned from each of these findings and reports, and improved the safeguards in our technologies*" (Farrow 2021, p. 6). Regardless, as shown by the Pegasus Project, the spyware has found other purposes for application and has consequently raised contentiousness as persons apart from criminals, e.g. politicians, government officials, human rights advocates, dissidents, and journalists, have been targeted.

According to reports made by different outlets, such as The Washington Post (2021) and The New York Times (Bergman and Mazzetti 2021; Bergman et al. 2023) among others, Pegasus may be remotely deployed so that a target never has to take any action. This means it can be installed without downloading a software, viewing a document or accidentally clicking on a pop-up window or an infected link. Consequently, after having intruded one's device, everything can be monitored by basically mirroring the device. This in turn essentially means that any and all activities a person undertakes on the device, regardless of whether it is a personal or business device, are recorded (Bergman and Mazzetti 2021; Bergman et al. 2023; Mekhennet et al. 2021).

What this means is the following: when a person accesses their image library to look at pictures, or when that person facetimes colleagues or loved ones, or important messages and/or emails are being drafted, the person in charge of the spyware reportedly can see every detail as if looking at the device themselves (Marzocchi and Mazzini 2022, p. 4f.). On top of this, Pegasus may also covertly activate a phone's cameras and microphone to make new recordings rather than "only" surveying a person's device (Cutler and Pegg 2021, p. 3; Farrow 2021, p. 17). The result: a total loss of privacy in the digital realm.

Considering that most mobile devices now offer very comprehensive and regular software updates as well as two-factor authentication, one would expect for these security measures to provide some protection at the least. However, that is not the case. Even though these security measures can help deter ordinary hackers, offering protection against skilled and well-funded attackers with access to the adequate technology who focus their efforts on a single target is extremely difficult. Furthermore, Pegasus disables security updates and defence systems once it has gained access to the device. Determining whether spyware has been used to compromise the target, however, is quite challenging. It is exceedingly difficult to identify

the perpetrator of the assault when spyware is identified on the target's device since it leaves little to no trace behind (Bergman and Mazzetti 2021; Cutler and Pegg 2021, p. 3; Farrow 2021, p. 32).

Additionally, because of this "*zero-click*" technique, Pegasus may infect a device via a message or a call through WhatsApp or another service, in contrast to social engineering approaches that require the user to click a link or visit a website that covertly installs the virus. If one would think that by refusing to accept a call or deleting a message the spyware would be thwarted from infiltrating personal data, one would assume wrong. As reported by The Washington Post (2021) and The New York Times (Bergman and Mazzetti 2021; Bergman et al. 2023), spyware has the ability to self-install even if the user deletes the message and misses or ignores the call (Washington Post 2021; Bergman and Mazzetti 2021; Bergman et al. 2023). Because Pegasus can capture communications and data before they are encrypted, it may even read encrypted data. The NSO Group's technology has also made use of a procedure known as "*rooting*", as reported by Cutler and Pegg (2021) as well as Bergman and Mazzetti (2021). This makes it possible for whoever installs it to alter the phone further because of having admin privileges (Cutler and Pegg 2021, p. 3). Should this zero-click access fail, however unlikely this may be based on the information gathered by the author, Pegasus is likely sophisticated enough to employ social engineering strategies to attempt tricking people into giving total access (Access Now 2024).

3.3. A tale of implication at the national level

Worldwide, the NSO Group claims to have 40 client states. Of these 40 client states, research conducted by the Pegasus Project has yet to confirm a majority. This may be partly traced back to the persistent refusal of the NSO Group to publicise, or at the least confidentially share select "*clients*", i.e. governments that have purchased the spyware, with the Pegasus Project. Therefore, even though it has been a few years since the Pegasus Project was able to first identify breaches in reference to legal surveillance, new victims are continuing to come forward. With the identification of new victims, there remains the possibility of more, to this point unidentified countries, to be implicated in the Pegasus spyware scandal.

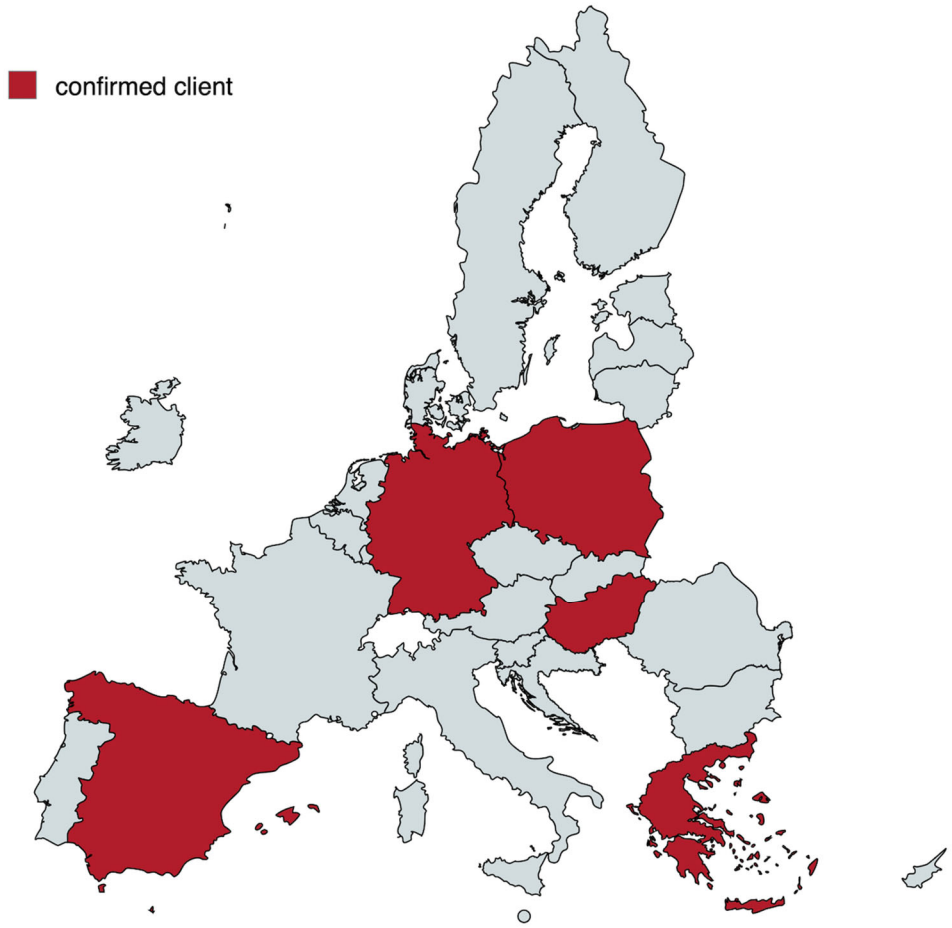
In this section, the author will take a look at EU member state governments that have been implicated in the spyware scandal. As there are differences with respect to the extent and

gravity to which respective EU member state governments are implicated in the scandal, the author has decided to group said member states based on their similarities. Each of these categories was established by the author upon consultation of research conducted and published in reference to the Pegasus Project, the project's partners and various other country and media reports throughout her data collection process. A more detailed account of the author's categorisation will follow in the subsequent subchapters. The author would also like to acknowledge that for this section, sources consulted extend beyond those defined in Chapter 2 due to a lack of information and relevant media reporting for the defined timeframe.

3.3.1. Confirmed clients

Within the European Union, there are five confirmed clients of the NSO group, i.e. Germany, Greece, Hungary, Poland and Spain. Each EU member state government, which is categorised as a "*confirmed client*", has either purchased and used, or purchased the technology without any (public) evidence of its application. In addition, the purchase of the technology has been confirmed by member state governments or confidential sources from bespoke member state governments which then shared the information with the Pegasus Project or other media contacts. The extent to which spyware was used nonetheless differs in each of the five member states. Therefore, the author will provide a concise overview of country-specific conditions for each of the member states. The following paragraphs will comprise said undertaking in alphabetic order. A visualisation of confirmed clients has been provided in *Figure 3-A* (see below for reference).

Figure 0–B: EU member states confirmed as spyware clients (author's own visualisation)



3.3.1.1. Germany

To begin with, Germany. According to an investigative report published in 2021 by a consortium of news outlets in Germany, such as Zeit Online and Süddeutsche Zeitung among others, the German Federal Criminal Police Office (Bundeskriminalamt, or *BKA*) purchased Pegasus for investigative purposes for the federal police in reference to organised crime and terrorism in late 2020. This was eventually formally acknowledged by the authorities during a meeting of the German Bundestag. In this meeting, the BKA acknowledged that it had begun discussions with a delegation of the NSO Group in 2017 and completed its acquisition of the technology in 2019 (Stark 2021; Süddeutsche Zeitung 2021). For the purpose of mitigating the risk misuse and to reduce the likelihood that German legislation would be

abused, as Stark (2021) and Süddeutsche Zeitung (2021) reference their sources, the German government did acquire a restricted version of Pegasus.

This may be traced back to already existing legislation on the use of surveillance technology in Germany dating back to 2017. The German Act on the Restructuring of the Federal Criminal Police Office Act (Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes, 2017), more specifically Para. 51, allows for the use of surveillance technologies. However, the use thereof is dependent on very specific circumstances. "*The Federal Criminal Police Office may, without the knowledge of the person concerned, monitor and record the telecommunications of a person in order to avert an urgent danger to the existence or security of the Federation […], or to the life, limb or freedom of a person or property of significant value, the preservation of which is in the public interest*" (Para. 51, Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes, translated by the author). Furthermore, the use of said technologies is also dependent on whether "*the prevention of the danger or the prevention of the crimes would otherwise be hopeless or significantly more difficult*" (Bundesministerium der Justiz 2017, translated by the author).

This framework had to also be respected by the German Foreign Intelligence Agency (Bundesnachrichtendienst, or *BND*), who also purchased the spyware in the beginning of October 2021. Consequently, as was the case with the BKA, the BND purchased an altered version of the contentious programme. The deployment of the spyware reportedly was, however, contingent on prior approval by the German Chancellery and then-Chancellor Angela Merkel (Stark 2021; Mascolo and Obermaier 2021).

Following the revelations in Germany, human rights advocates filed a data protection complaint with the purpose of challenging the use of Pegasus by the BKA. A thorough inquiry, more legislative oversight, and an examination of the extensive capabilities of covert monitoring were additionally demanded by civil society organisations. Parallel to this, then-German Chancellor Angela Merkel advocated for additional limitations on the spyware trade referencing national security concerns considering NSO Group's headquarters in Israel and all surveillance being conducted through non-German servers. Both the BND and BKA claimed to be able to rule out the possibility that Israel might have knowledge of the surveillance activities despite a former NSO staff member's claim that NSO servers also processed the collected data (Stark 2021).

In light of the existing legal framework in Germany, as well as the public outcry following the revelations, the author would like to note that Pegasus is not the first instance of spyware in Germany. The BND had relied on spyware and related surveillance technologies already in 2008, where it had monitored about 2500 devices (Stark 2009). In addition, FinFisher provided its technology FinSpy to the BKA in 2012 and 2013. However, as reported by the Frankfurter Allgemeine Zeitung (2023) among others, the technology was never used in Germany and had only been contracted for testing purposes. This is because during that time period, the use of said technologies had been prohibited under German law and the German Federal Ministry of Interior had only managed to create the necessary legislative environment for the use of spyware with the German Act on the Restructuring of the Federal Criminal Police Office Act in 2017 as mentioned above. By then, however, the contract with FinFisher had been terminated, which resulted in the BKA never making use of the technology (Hanfeld 2021; Meister 2019; Frankfurter Allgemeine Zeitung 2023).

3.3.1.2. Greece

Greece is among the nations whose government has made use of Pegasus and other similar malware. The consequences of using spyware to track opposition politicians and journalists certainly have been felt in Greece. A number of incident reports about the use of spyware impacted Greece throughout the end of 2021 and 2022. Numerous reports during that time revealed journalists were under surveillance by the Greek National Intelligence Service, which was followed by disclosures made by CitizenLab in reference to spyware having compromised the phone of an investigative journalist, lawmakers and other journalists (Ethnikí Ypiresía Pliroforión, or *EYP*) (Mildebrath 2022b; Samaras 2022; Stamouli 2022a; Stamouli 2022c).

The EYP and the government both refute the idea that the Greek government has ever acquired or utilised Pegasus, more specifically in relation to the monitoring of journalists and politicians. However, it did acknowledge in August 2022 that the EYP had been monitoring two individuals: Nikos Androulakis, a member of the European Parliament and the leader of the Greek opposition party (*Panhellenic Socialist Movement*, or *PASOK*), and financial writer Thanasis Koukakis. Both individuals had, prior to the confirmation by the EYP, contacted CitizenLab to verify the suspected infection of their respective phones with spyware. Around

this time, other instances of EYP surveillance surfaced (In t'Veld 2023, p. 40; Schmitz 2022; Stamouli 2022a).

Following these disclosures, EYP director Panagiotis Kontoleon and the Greek government's General Secretary Grigoris Dimitriadis resigned. According to reports by Becatoros (2022) and Stamouli (2022b; 2022c), Dimitriadis was in charge of fostering collaboration between the Greek government and the EYP, as well as the spyware. According to these reports, Dimitriadis was in charge of spyware, which includes the purchase as well as the supervision of the technology. In line with this, Dimitriadis had communicated with the NSO Group in 2019 to formally acquire Pegasus. As to whether the technology was eventually purchased and by whom is not public information (Becatoros 2022; Stamouli 2022a). In addition to the use of the spyware, Greece has allegedly offered a training facility for non-European agents with the purpose of learning more about the spyware and permitting the export of said spyware to states with a history of violating human rights, as reported by In t'Veld (2023, p. 62).

In a digital statement released in August 2022, Greek Prime Minister Kyriakos Mitsotakis declared that whilst spyware use had been legal, it was politically unacceptable. Additionally, Mitsotakis stated that if he had known about the monitoring, he would not have approved of it (In t'Veld 2023, p. 39; Schmitz 2022; Stamouli 2022b). Nonetheless, he failed to address other instances of the alleged use of spyware by the Greek authorities.

3.3.1.3. Hungary

One EU member state which has had multiple reports in reference to the use of spyware is Hungary. Amidst the European spyware scandal, Hungary was among the initial member states to "fall victim". According to information shared by the Pegasus Project based on an investigation conducted by Direkt36, a media partner of the Pegasus Project, over 300 Hungarians, including political activists, investigative journalists, attorneys, business owners, and politicians may have suffered from the maladministration of Pegasus. Despite being targeted, none of the people reportedly were subject of any criminal inquiries or charges (Agence Europe 19.07.2021; Birnbaum et al. 2021; Walker 2021; Panyi 2022).

After the news first surfaced in July 2021, there was a brief moment during which the Hungarian government refrained from commenting on or denying the use of Pegasus. It was Lajos Kosa, head of the Hungarian Parliament's Defence and Law Enforcement Committee, who confirmed in November 2021 that Pegasus had been acquired by Hungary. However, the Committee reiterated that all the legal procedures had been followed, meaning the surveillance was undertaken following the authorisation from a judge or the Minister of Justice (Panyi 2022).

A formal inquiry into the use of Pegasus by Hungarian authorities was initiated in August by the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság, or NAIH), the data protection authority of Hungary. Following an investigation, the NAIH ruled in January 2022 that the monitoring it had looked into posed no legal problems, thus indirectly raising questions about the autonomy of the EU's data protection authority (Bayer 2018; Panyi 2022; Pfenniger 2023).

The inner workings of the spyware's introduction in Hungary were revealed by Direkt36 in September 2022, along with a list of front firms and middlemen. Accordingly, the Hungarian Parliament's national security committee held a vote in 2017 about the potential purchase of specific surveillance equipment by using the standard public procurement process. As a consequence, the Hungarian Parliament authorised the purchase of a highly advanced spyware at the request of the Hungarian Special Service for National Security (Nemzetbiztonsági Szakszolgálat, or *NBSZ*) (Panyi 2022). Even though the purchase of the spyware had been authorised, Pegasus was acquired in a rather untransparent manner as argued by Panyi (2022), Birnbaum et al. (2021) and In t'Veld (2023, p. 25). Instead of a direct transaction between the Hungarian government and the NSO Group, Pegasus was allegedly purchased by a Hungarian middleman from a Luxembourg-registered business that had ties to the NSO Group (Bayer 2021; In t'Veld 2023, p. 25; Panyi 2022).

Furthermore, there is a strong possibility that Hungary is also deploying other spyware technologies, such as Candiru, as according to research conducted by CitizenLab and Direkt36 (Deibert et al. 2018; Panyi 2022). Furthermore, based to their research, the Hungarian government is believed to have already used spyware before the market launch of Pegasus, as it allegedly acquired potentially intrusive surveillance tools prior to 2017 (Bayer

2018; Deibert et al. 2018). Taking these factors into consideration, the author would argue that there are signs of an egregious use of spyware in Hungary.

To conclude, the author would like to reiterate that Pegasus and the use of similar spyware in Hungary is nothing new as found in her research. The employment of Pegasus and related spyware may likely present an apparent and purposeful effort to curtail media freedom and freedom of expression taking into account the democratic backsliding of Hungary under the current Orban-led government. Due to the government's near total control over all offline and broadcast media channels in Hungary, it is able to maintain its narrative and prevent public scrutiny of independent media outlets from reaching a large portion of the Hungarian population. Furthermore, not only did the Hungarian government acquire and use the spyware against its citizens, but Hungary has also hosted other intelligence-related businesses in the past, e.g. Black Cube and Cytrox, therefore presenting a clear tendency in favour of the use of spyware regardless of a legal justification thereof (Bayer 2021; Birnbaum et al. 2021; Spike 2021; Walker 2021).

3.3.1.4. Poland

In recent years, Poland, similar to Hungary, has significantly increased its surveillance capabilities, eroding or eliminating monitoring and protection mechanisms. Even though 2018 saw the earliest known instances of the use of the Pegasus spyware in Poland, the country has experienced a crisis of the rule of law, which may be traced back to 2015. It was the then Polish government under the leadership of the ruling party Law and Justice (Prawo i Sprawiedliwość, or *PiS*), that began to dismantle the judicial system. This was exemplified in significant institutions being restructured and newly appointed with the objective of having party loyalists occupying all critical positions to create a coherent and highly effective use of the spyware. However, additional accusations surfaced in 2021 regarding the use of spyware against Polish journalists and politicians among others. Furthermore, in early January 2022, it was reported that the NSO Group had sold its spyware to Hungary and Poland's anti-corruption agency following a meeting with Israeli Prime Minister Benjamin Netanyahu. Shortly after this revelation, Jarosław Kaczyński, head of Poland's then ruling party PiS, acknowledged that Pegasus had been purchased by the Polish government. Nonetheless,

Kaczyński strongly refuted using the programme to target opposition lawmakers in the run-up to the 2019 parliamentary election (Deibert et al. 2018; In t'Veld 2023, p. 19).

In her research, the author found media reports that identified three key persons who had been targeted by the spyware. These three persons are Krzysztof Brejza, Roman Giertych, and Ewa Wrzosek. Senator Krzysztof Brejza fell victim to the spyware throughout the run up to the elections in 2019. Back then, Brejza was leading the Polish opposition party Civic Platform in both the European and national elections. While Brejza has categorically rejected any involvement in "suspected crimes", whilst Kaczynski has made accusations linking the senator to illegal activities. Allegedly, however, Brejza has yet to receive any formal charges and was never called upon to provide a statement (Agence Europe 07.01.2022; Bajak and Gera 2021; Cerulus 2021; Cienski 2021; Guerrini 2023; In t'Veld 2023, p. 16 and 18; Wanat 2022). Roman Giertych was reportedly also a victim of Pegasus in the last weeks of the 2019 Polish parliamentary election. According to his statement at a hearing of the European Parliament, the majority of cyberattacks against him did occur in the run up to the election, i.e. between September and December 2019. In light of this the author would like to note that at this time, Giertych was representing former President of the European Council and former Prime Minister, Donald Tusk. Giertych also represented Radek Sikorski, who back then served as a Member of the European Parliament (*MEP*) for the European People's Party (or *EPP*) and is serving as Foreign Minister in the Polish government led by Tusk at the time of writing in early 2024. Lastly, prosecutor Ewa Wrzosek. Pegasus malware was used to attack prosecutor Wrzosek up to six times between June and August 2020. As a prosecutor, Wrzosek reportedly supported the autonomy of the Prosecutor's Office (Bajak and Gera 2021; Cerulus 2021; Cienski 2021; European Parliament 2022a; Walker 2021; Wanat 2022).

Considering what is known about the targets of spyware in Poland, i.e. opponents of the then Polish ruling party PiS, activists, independent attorneys, and government critics, the author would question the legality of the use of spyware. Furthermore, in reference to the three examples of people targeted by the spyware, the then-Polish government refrained from acknowledging or denying any involvement in the matter. Taking into consideration the circumstances of the Pegasus scandal, i.e. the crisis of the rule of law, Pegasus may have arguably been key in the undertakings of PiS, especially with regard to the surveillance of the opposition and critics. It was the current Polish Prime Minister Tusk who called the

Pegasus scandal the biggest and deepest crisis for democracy since 1989, and in light of present circumstances as unprecedented in Polish history (Bajak and Gera 2021; Cerulus 2021; Cienski 2021; Guerrini 2023).

3.3.1.5. Spain

A substantial number of suspected targets in Spain were revealed by the Pegasus Project in July 2021. Citizen Lab revealed in April 2022 that mercenary malware has infected or targeted at least 200 people. Pegasus was the spyware that was utilised most frequently, while Candiru was also employed occasionally. While CitizenLab did not identify a particular entity as the source of the assaults, it did imply that there was a strong nexus with one or more entities within the Spanish government based on circumstantial evidence (Anstis et al. 2022; González 2020; Jones 2020; Pfenniger 2023;).

Among the people targeted, Pegasus infected the phones of sixty-three Catalan lawmakers and pro-independence activists, according to research conducted by CitizenLab. The lab found circumstantial evidence indicating that the Spanish government was engaged in the monitoring. This is now the biggest known cluster of Pegasus monitoring targeting a single political organisation. Consequently, the targeting of Catalan lawmakers and activists is referred to as "*CatalanGate*". The scope of the CatalanGate monitoring was not made public until April 2022, when CitizenLab concluded their extensive study following a collaborative investigation by The Guardian and El País (Agence Europe 19.04.2022; Anstis et al. 2022; González 2020; Jones 2022a).

Speaking on the subject before the Spanish Parliament, Prime Minister Sánchez reaffirmed that all actions taken by the government had been taken in compliance with Spanish law and that the Spanish Parliament and other governmental entities have jurisdiction over matters of national security. In a feature with The New Yorker, Shalev Hulio, co-founder and former CEO of the NSO Group , also asserted that Spain's use of Pegasus was acceptable because of the country's strong adherence to the rule of law and the need for Supreme Court approval (Farrow 2022, p. 32ff.).

The disclosures caused a political crisis in Spain, with numerous parties threatening to withhold their parliamentary support for Sánchez's minority administration and vetoing a

parliamentary investigation into the Pegasus scandal. This may be largely traced back to the timing of the revelations, as this was being perceived as a smoke screen to conceal the involvement of the Spanish National Intelligence Centre (Centro Nacional de Inteligencia, or *CNI*) in the issues investigated by CitizenLab. It was also a rare instance of a government revealing details on monitoring programmes that had not been previously disclosed by businesses, NGOs, or investigative journalists. Following appeals from politicians and civil society organisations alike to re-establish trust in the nation's intelligence establishment, Paz Esteban, Director of the CNI, was dismissed. A parliamentary investigation committee has not been established to investigate the matter (Anstis et al. 2022; In t'Veld 2023, p. 85).

Due to legal and national security concerns, however, the Spanish government has only provided a limited amount of information about their involvement in this targeting. Nonetheless, the majority of the intercepts from around the CatalanGate are related to, or at least coincide with, significant political events, issues, or persons. Examples include the acceptance of the Catalan Parliament's disconnection laws, legal proceedings against Catalan separatists, and Roger Torrent, the speaker of the Catalan regional parliament, as well as two other pro-independence activists in 2019 (González 2020; Jones 2022a; Manancourt and Van Sant 2022).

The author would like to note that the purchase of Pegasus by the Spanish government was not the first instance of the use of spyware in Spain. Back in 2001, the Spanish government purchased Telecommunications Interception Tools and the procurement of SITEL (Systems for the Lawful Interception of Telecommunications). Additionally, the Spanish government acknowledged that in 2010, the Ministry of the Interior, the CNI, and the Spanish National Police had contracted "*Hacking Team*", another company developing spyware, to provide spyware services as part of the implementation of the Integrated Telecommunications Interception System, which gave the State Security and Corps' operational units the ability to intercept and record electronic communications that were legal. Furthermore, the CNI has been suspected of obtaining or using FinFisher and other forms of spyware in the past (Anstis et al. 2022; González 2020; Jones 2022a; Jones 2022b; Manancourt and Van Sant 2022).

Furthermore, following the disclosures of the CatalanGate, the Spanish government also announced that Spanish Prime Minister Pedro Sánchez, Defence Minister Margarita Robles, and Interior Minister Fernando Grande-Marlaska, also had their phones targeted by Pegasus

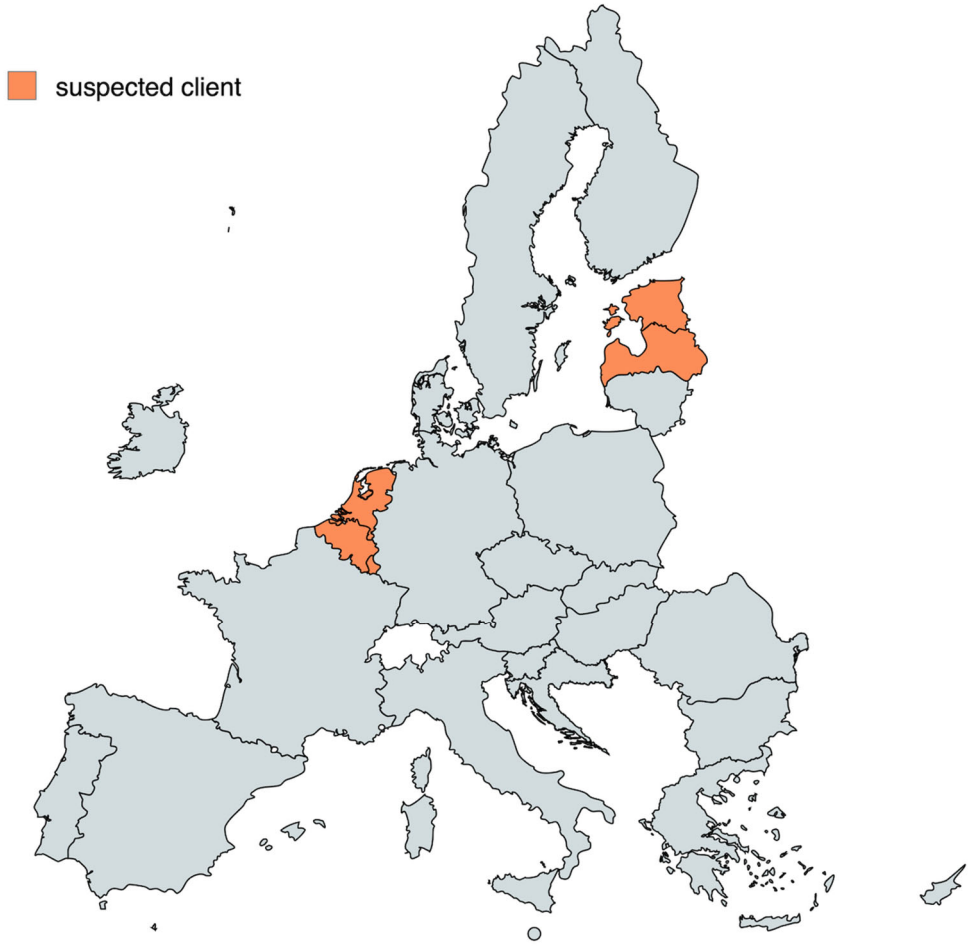
in 2021 (Agence Europe 02.05.2022; Jones 2022b). The author found that, based on her research process, the Spanish Prime Minister was the first official confirmation of the use of spyware against a head of government. However, it has yet to be revealed who or what entity targeted these Spanish officials. This in return highlights that whilst member state governments may purchase spyware for reasons of national security, they may nevertheless also fall victim to the technology. This may be traced back to spyware being difficult to detect whilst being installed covertly and effortlessly.

3.3.2. Suspected clients

The second categorisation, "*suspected clients*", includes EU member state governments that are suspected of either having purchased and used the spyware, or having purchased the spyware without public evidence of its application. It is worth noting that these member states have been categorised as "*suspected*" by the author based on her research in reference to the Pegasus Project and similar information that had been made available for the public.

In reference to suspected clients of the Pegasus spyware, the case for categorisation as either using the spyware or not is a little more difficult than first meets the eye. This may be traced back to diverging reports in the media and other information available in the digital sphere. As already stated earlier, due to a lack of information provided by the defined media outlets as defined in the author's research design in Chapter 2, the author had to expand her research to other media outlets in order to acquire adequate information. Whilst the author did attempt to find detailed information that is reliable, in some cases, the use of the spyware by member state governments cannot be proven – but the non-use cannot be proven either. Therefore, the author has categorised the following EU member states as "*suspected clients*" of the technology: Belgium, Estonia, Latvia, Luxembourg, and the Netherlands. As was the case with confirmed clients, the author will provide an account of the suspected use of the spyware nationally, once again in alphabetical order, whilst a visualisation is provided for a facilitated overview of suspected clients (*Figure 3-B*, see below).

Figure 0–C: EU member states suspected as spyware clients (author's own visualisation)



3.3.2.1. Belgium

According to statements made by Shalev Hulio, co-founder and former CEO of the NSO Group, in an April 2022 feature in The New Yorker, Belgian federal police employ Pegasus in their operations. However, the Belgian federal police reportedly did not confirm using the NSO Group's technology despite Hulio's statement. Regardless, the Belgian federal police responded to the claims by stating that they adhered to a legal framework in reference to the use of intrusive methods in private life. Though Belgian federal police declined to clarify if the Belgian intelligence agency is a client of NSO or employs said spyware to target criminals, Vincent Van Quickenborne, the Belgian Minister of Justice, acknowledged that Pegasus may generally be used in a legal manner by the intelligence services (Farrow 2022; In t'Veld 2023, p. 96; Klingert 2022; Realfonzo 2023).

Whilst it is one of the EU member states suspected of having purchased the spyware, Belgium has reportedly also fallen victim to spyware. As reported by the Pegasus Project, the spyware had been discovered on a number of phones of Belgian residents. A majority of the residents reported of having been targeted were activists, journalists and also politicians. These include Jean-Paul Nsonzrumpa and Carine Kanimba, both connected to Rwandan activist Paul Rusesabagina, as well as the phones of journalist Peter Verlinden and his wife Marie Bamutese, specialising in local and regional affairs in Central Africa. These breaches, as reported by the Pegasus Project, were formally validated in September 2021 by the Belgian General Intelligence and Security Service (or *GISS*). Furthermore, in July 2021, the Pegasus Project also disclosed that a client of the NSO Group apparently had selected Charles Michel, President of the European Council as of 2019, for monitoring in the same year. The same NSO customer reportedly also designated Charles Michel's father, Louis Michel's phone for monitoring. Both the Moroccan and the Rwandan government, which had been suspected behind the spyware attacks, have denied any participation (Klingert 2022; Realfonzo 2023).

The author would like to note that, even though Belgian residents and citizens have been targeted, there is no conclusive proof that it was the Belgian government that conducted the surveillance efforts. The author would argue that, considering the activist activities of some of the victims, there is a probability of Central African governments having purchased the spyware with the purpose of surveying people abroad. Considering there is no publicly available list of clients of the NSO Group's spyware, a concise determination of who is behind the surveillance efforts seems unlikely.

3.3.2.2. Estonia

As reported by the Washington Post and the New York Times, sources familiar with NSO conduct claimed that the NSO Group had licenced Pegasus to Estonia. However, the business afterwards placed limitations on the use of the technology. Allegedly, before Russia invaded Ukraine, Estonia had wanted to purchase Pegasus in order to have access to Russian phones as part of intelligence operations. Although the precise nature of possible limitations is unclear, sources acquainted with Estonia's Pegasus licence claim that the country is unable to target Russian phones (Bergman and Mazzetti 2022; Harris et al. 2022). This is because, as reported by the New York Times, selling the programme to "Russian enemies" was

something Israel believed would sour relations between itself and the Kremlin (Bergman and Mazzetti 2022).

3.3.2.3. Latvia

Similarly to Estonia, Latvia is also under suspicion of being in possession of and using the spyware in reference to the surveillance of Russian or Russia-friendly person's devices as a response to national security concerns. According to a joint investigation by Access Now and the Citizen Lab, Galina Timchenko, founder and editor-in-chief of Meduza, a well-known independent Russian media organisation with its headquarters in Latvia, had Pegasus spyware installed on her iPhone. Timchenko reportedly received a warning from Apple in June that potentially state-sponsored spyware was targeting her personal device. According to the research conducted by Access Now and CitizenLab, Russia, one of its allies, or a state belonging to the European Union might have been the source of the assault (Hammoud and Krapiva 2023; Kirchgaessner 2023).

In light of this evaluation, the author would like to note that the notification came shortly after the Russian government designated Meduza an undesirable organisation due to its critical reporting on the war in Ukraine and Putin himself. This was after the decision was made by Meduza to relocate to Latvia to be able to use the internet and continue independent reporting whilst keep communicating with its Russian readers. In addition, one should acknowledge that the timing of the use of spyware was in the run up to a meeting of Russian journalists in exile (Deibert et al. 2018; Hammoud and Krapiva 2023; Kirchgaessner 2023). As a consequence, it cannot be confidently stated that Latvia has used the technology as the surveillance of the Timchenko may likely be traced back to Russia. This does raise the point that only because some residing in a state, this does not mean that said member state government is responsible for the surveillance. Nevertheless, this does not exclude Latvia from being suspected of having purchased the spyware and using it to promote its national security.

3.3.2.4. Luxembourg

The Pegasus Project noted in July 2021 that OSY, the parent firm of NSO Group, was based in Luxembourg. Accordingly, the NSO Group has two branches in Luxembourg. This was

confirmed by Luxembourg's Minister of Foreign Affairs, Jean Asselborn, who made this confirmation a few days after the revelations. However, Asselborn stated that the company had not applied for export licences for cybersurveillance equipment. The Luxembourg government further stated that there was no proof that Pegasus had been used to infect any residents. The same day, Asselborn wrote to the management of the NSO Group's firms residing in Luxembourg to inform them that Luxembourg would not accept any activity on their part that would support human rights violations overseas (Harwell 2021).

During a live-streamed event in October 2021, Luxembourg's prime minister, Xavier Bettel, hinted that the country had purchased Pegasus, acknowledging that the technology had been bought for state security reasons (In t'Veld 2023, p. 105f.; Manancourt 2022a). The Luxembourg government stated that the Grand Duchy could not put the NSO Group on a blacklist as there is no mechanism to do so. As already mentioned in the section on Hungary and based on information gathered from Direkt36, the NSO Group sold Pegasus to Hungary through an intermediary in Luxembourg. Furthermore, following the assassination of Saudi dissident and journalist Jamal Khashoggi in 2018, The Washington Post revealed that Saudi Arabia had transacted with the NSO Group through one of its Luxembourg-based subsidiaries, Q Cyber Technologies (Harwell 2021). This was complemented by the report of the PEGA committee from May 2023, in which Luxembourg is stated to serve as a significant business base for the NSO Group (In t'Veld 2023, p. 105f.).

3.3.2.5. The Netherlands

The Dutch Security Service (Algemene Inlichtingen- en Veiligheidsdienst, or *AIVD*) reportedly employed Pegasus in the investigation of the criminal Ridouan Taghi, according to a June 2022 story by the Dutch media source *de Volkskrant*. The report claims that the individual "Ridouan T" became a prime suspect in several murders connected to organised crime, drug trafficking, and leading a criminal organisation. Consequently, then-Minister of Justice and Security, Ferd Grapperhaus, requested assistance from the AIVD in finding the criminal Taghi, who had been the primary suspect in the case (Modderkolk 2022). It should be noted that there is no confirmation of the purchase of the spyware, and that the AIVD did not comment on the claims regarding the use of such technologies. Despite the legality of using Pegasus against an individual on the wanted list, the case provoked a public discussion

about the AIVD's involvement in an internal Dutch police investigation and resulted in calls for a re-examination of the spyware's use in the Netherlands (Modderkolk 2022; Stuart Leeson 2022).

3.4. EU member states facilitating the spread of spyware

Having outlined EU member state governments that are confirmed or suspected clients of spyware, there are some EU member states that do not fit either criterion of these first two groups. In the case of these member states, governments are not linked to having purchased the technology. However, they are nonetheless connected to the spyware scandal by either having an alleged connection to the NSO Group or other spyware companies. This includes Bulgaria, Cyprus, Italy and Malta (see *Figure 3-C* for reference). The extent to which the NSO Group and other spyware companies may have been able to establish a corporate structure in a number of EU member states, as found by the author, is alarming.

Bulgaria and Cyprus both have parent or daughter companies of the NSO group located on their territory. This is because export licences for the NSO Group's technology had been obtained from firms in both, Bulgaria and Cyprus. However, the two governments have refuted any involvement in the facilitation of the trade of spyware. In addition, Taylor (2023) raised the question as to whether said export licences were given to NSO companies with names that may not be easily attributed to the NSO Group (Kambas 2022; Manancourt 2022b; Taylor 2023).

A case similar to Bulgaria and Cyprus is Italy. The most prominent case: Hacking Team. As reported by Howell O'Neill (2019), similar to the spyware used for surveillance now by the NSO Group, Hacking Team employed its monitoring system to steal information covertly from whomever the client desired. People targeted back then also included journalists and human rights advocates. Whilst Hacking Team may be the most well-known example considering its revelations in 2014, another spyware company with its headquarters in Italy is Cy4gate, which was founded in 2014 and provides broad-spectrum intelligence and cybersecurity (Howell O'Neill 2019; In t'Veld 2023, p. 106).

However, in the case of Italy, Pegasus is reported to have targeted former Italian Prime Minister and former President of the European Commission, Romano Prodi. The information

became public in 2021 after the Washington Post revealed that Pegasus had infected Prodi's phone at the request of Moroccan secret services. In reference to this, the author would like to acknowledge that Prodi had been appointed as a UN Special Envoy to the Sahel regarding the matter of Western Sahara, a disputed region between Morocco and the Sahrawi Arab Democratic Republic (Birnbaum et al. 2021; In t'Veld 2023, p. 106). Once again, the author would like to reiterate that pinpointing the attacker is impossible due to the covert nature of spyware technology. Additionally, the author would like to acknowledge that whilst Italy is host to some spyware companies as outlined earlier, there is no public record of the Italian government having acquired spyware by the time of writing.

Lastly, Malta. Whilst there is no public record of spyware companies having settled on the island, a number of prominent players in the spyware industry, e.g. the CEO of Intellexa, were either able to attain a Maltese passport or register businesses on the island. Even though there appears to be little activity in reference to the trade of spyware in Malta, the issuing of passports at least indicates to some degree that a select number of persons are free to distribute goods and services within the European Union, therefore at the least facilitating the trade in spyware (Deibert et al. 2018; In t'Veld 2023, p. 99 and 108; Taylor 2023).

As a consequence, looking at the number of cases that facilitate the distribution, purchase and use of spyware in perspective, the author would argue that there is a distinct tendency of spyware companies settling in EU member states over time. This in return allows said companies to establish a well-functioning work base with unlimited access to the internal market.

Figure 0–D: EU member states facilitating the spread of spyware (author's own visualisation)

3.5. EU member states as victims of spyware

The last few subchapters have highlighted EU member state governments that acted as "perpetrators" in reference to having acquired or being suspected of having acquired spyware technology, as well as facilitating the distribution of spyware across the European Union. There is, however, one more group of EU member states that must not be forgotten in the author's research: EU member states that have become "victims" of spyware. In this case, member state governments have reported the use of spyware against its citizens and residents without the government having been accused of, or being a confirmed client of spyware technology. This list of countries includes Finland and France (for a visualisation see *Figure 3-D*).

3.5.1. Finland

To begin with, Finland. The situation in reference to the connection between Finland and spyware is relatively simple to describe when compared to the other EU member states in this group. In Finland, there is no record and no report of the government using or acquiring the spyware technology, nevertheless the country was affected by the use of spyware. An announcement was made by the Finnish Ministry of Foreign Affairs in January 2022 that Pegasus had targeted Finnish diplomats abroad (Ministry of Foreign Affairs of Finland 2022; Vanttinen 2022). However, the ministry did not provide any further details in reference to the security breach. Therefore, whilst the accusation of its nationals being illegally surveyed was made, there is no mention of the number of diplomats that were the target of the breaches, in addition to information regarding when said breaches occurred, or who had been responsible for the attack. Additionally, considering the covert nature of the technology, it is difficult to pinpoint who is behind the attack once again highlighting the transnational aspect of spyware.

3.5.2. France

Second, France. The Pegasus Project disclosed in July 2021 that it had identified French president Emmanuel Macron, his former prime minister Edouard Philippe, and fourteen other French officials for possible Pegasus surveillance. It was one further instance in which an inquiry exposed the possible use of spyware developed by NSO Group against a head of government while said head of government held office. In the wake of the Pegasus Project's revelations, Macron reportedly changed his phone number. This was then superseded by an urgent cybersecurity meeting before the French government opened diplomatic talks with the Israeli government. This is because the French government perceived the Israeli government to have sway over the list of targeted phone numbers, consequently requesting that French phone codes be removed (In t'Veld 2023, p. 101ff.; Leloup and Untersinger 2021a). To what extent the NSO Group is directly linked, if so, to the Israeli government, remains unclear and subject to speculation.

Whereas the author made the decision to group France with other European member states that had fallen victim to the abuse of spyware, she would like to acknowledge an interesting piece of information that surfaced parallel to the revelations of the Pegasus Project in

reference to France. This is because it was also revealed that France had been engaged in talks with the NSO group to purchase Pegasus. In line with this, the author found that Le Monde reported that the NSO Group made approaches to France in 2019 and 2020 in reference to said spyware purchase. However, the government eventually formally declined to contract the spyware as reported by Le Monde. The French government has since then officially stated that it backed out of the purchase when the first revelations of the abuse of the Pegasus spyware were being publicised in 2020 (In t'Veld 2023, p. 101ff.; Leloup and Untersinger 2021a; Leloup and Untersinger 2021b). Based on her research, the author could not find any evidence that would question the French government's "innocence".

Figure 0–E: Citizens and/or residents targeted by the use of spyware (author's own visualisation)

3.6. Remarks on the presence of spyware in the European Union

As the author has seen throughout her research process, it is indeed challenging to categorise every member state when there is no access to a complete picture, i.e. adequate and well-rounded information regarding the purchase and use of the Pegasus spyware. Considering the NSO Group refuses to publicise its client list, whether or not someone is a client, suspected client or a victim of spyware will remain uncertain with room for speculation unless official sources have confirmed the purchase. The cases of Belgium and Latvia, among others, have highlighted this difficulty in clearly differentiating the different categories as established by the author. This is because one does not exclude the other. As exemplified in the case of Belgium, whilst its citizens and residents have fallen victim to the use of spyware against the backdrop that the government had purchased the spyware, there is virtually no way to determine who targeted Belgian citizens and residents and this remains a topic for speculation. In the case of Italy, for example, citizens and residents have also been targeted whilst there is no (public) record of the Italian government having purchased spyware despite having hosted spyware companies in the past.

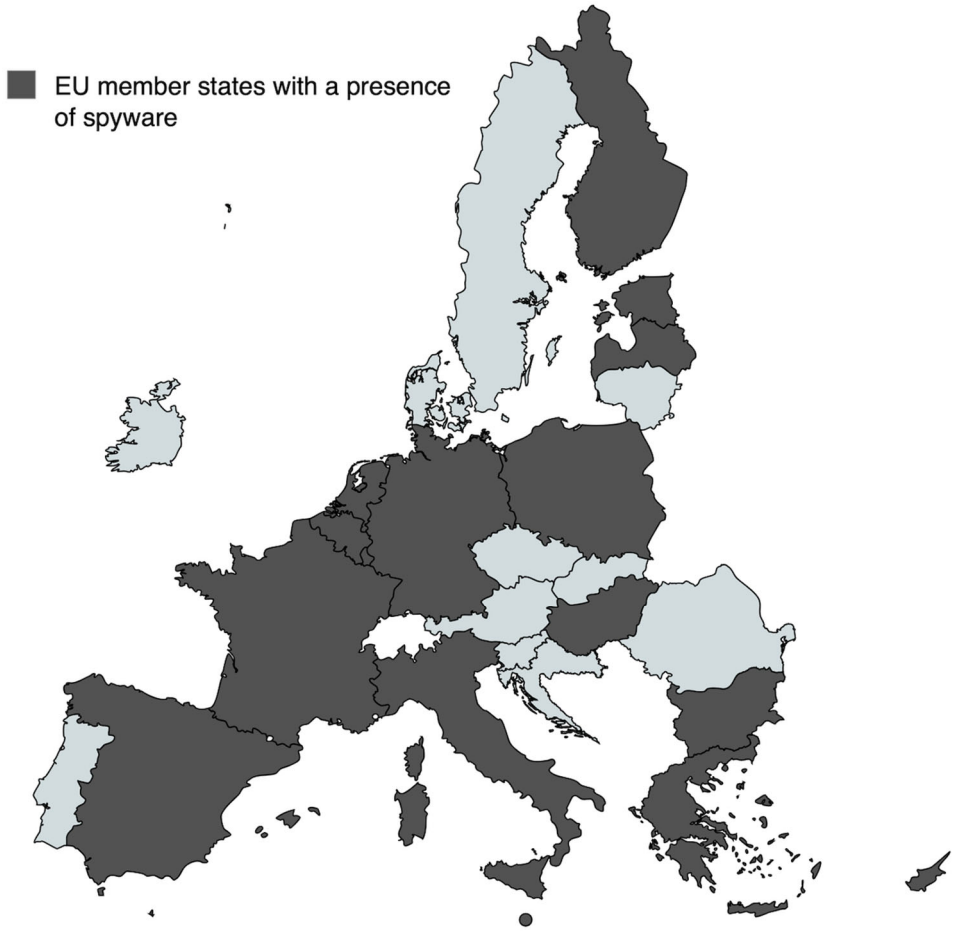
Moreover, should citizens and residents of a EU member state be targeted by spyware, the scandal may also present itself as a necessity for the member state government to opt to purchase spyware in an attempt to strengthen national security as a direct measure. This in return could further promote the spread of spyware in the European Union and beyond.

Even though the author would like to refrain from generalising "perpetrators" and "victims" among EU member states in reference to the spyware scandal, the outlined country-specific subchapters have shown that a significant number of EU member states are in a way connected to the spyware scandal. Based on this, the author would argue that there are indicators that the use of spyware is much more present within the European Union than initially anticipated. Especially looking at some member states, e.g. Germany and Italy among others, there is a history of spyware companies settling within their respective borders.

With the purpose of visualising this, the author has highlighted all EU member states that have been affected by the spyware scandal, whether it be by means of having purchased and/or used the spyware, having been suspected of the previous action, having facilitated the spread of the malware as well as having fallen victim to its application. *Figure 3-E* (see below

for reference) underscores the urgency with which the spyware scandal ought to be addressed. This is because, when disregarding the differentiation between perpetrating and victimised EU member states, spyware affects 17 of 27 EU member states already by the time of writing in early 2024. Consequently, the author would argue that, whether or not national governments want to admit it: citizens and residents, which evidently also includes citizens from other EU member states, are being affected by this technology and will remain at risk in the future. To this extent, the author would expect for the European institutions to become active with reference to the respect of fundamental rights and European values.

Figure 0–F: Overview of the presence of spyware in the European Union (author's own visualisation)



4. Spyware and the European Union – a story of complicity?

The previous chapter has highlighted the intrusiveness with which spyware may grant access to one's personal life and data without one's consent. Furthermore, the country specific subsections have highlighted the willingness of EU member states to engage in the surveillance of its residents, as well as the willingness to facilitate the spread of spyware technology within the European Union by means of hosting spyware companies. Consequently, the author would argue that it is necessary to take a closer look at the European Union and its member state in reference to the market for spyware.

4.1. Reflections on the European Union and the market for spyware

The spyware industry in the European Union appears to flourish despite the EU's comparatively strict regulations controlling the export and sale of spyware. Some European member states, such as Bulgaria, Cyprus, Italy and Malta as outlined in Chapter 3.4, are home to a number of local commercial spyware enterprises that create and market cutting-edge invasive technologies both domestically and internationally (Kot and Feldstein 2023, p. 15f; Riecke 2023, p. 698f.).

In the European Union, the Dual-Use Regulation (*Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*) regulates the export, transfer, and transit of dual-use commodities whereas dual-use commodities are items and/or technologies that may be used for both, civilian and military purposes. Considering that such items do present some level of risk, the regulation aims to ensure a responsible handling and distribution of said items and/or technologies and therefore protect people. Although the European Union theoretically maintains tight export regulations by means of this Dual-Use Regulation, there has been a growing trend among member states to try and attain a competitive advantage.

This may be achieved with a flawed transposition of legislation from supranational to national level, therefore creating an environment permissible for spyware distribution thanks to lax regulations. Whilst the European Union does have the Dual-Use in place, which in theory should provide a regulatory framework for spyware and the protection of private

information, the regulatory environment is still more favourable in the European Union compared to other countries (Baruch and Leloup 2023; Tar 2023).

In t'Veld (2023) traces this back to the consciously incomplete national implementation of the Dual-Use Regulation, as well as other EU regulations in relation to the use of spyware such as the General Data Protection Regulation (GDPR). With this attitude towards EU law, EU member state easily circumvent export regulations which in return facilitates the introduction of a product into the market. Therefore, companies such as the NSO Group set up subsidiaries in one EU member state, therefore gaining access to the internal market and facilitating the distribution and export of the technology. As argued by In t'Veld, this is precisely what some companies have decided to do (Baruch and Leloup 2023; In t'Veld 2023, p. 73 and 108; Tar 2023).

This may perhaps be traced back to the reputation of the Single Market itself as one reason for subsidiaries of larger companies to relocate to the European Union. Export regulators are said to believe that having established subsidiaries in the European Union provides adequate assurance of adherence to the highest human rights standards, which would exempt companies within the European Union from additional due diligence in reference to the respect of human rights (Kot and Feldstein 2023, p. 15; Riecke 2023, p. 698). Looking back a few years, the number of businesses that relocated their export divisions to Europe, specifically to Cyprus, increased whenever for example Israel's export licencing regulations became more stringent. In addition, a number of well-known figures in the spyware sector have become citizens of the EU in order to conduct business freely both inside and outside of the European Union (Baruch and Leloup 2023; Tar 2023).

Furthermore, as argued by Riecke (2023) and Kot and Feldstein (2023), the political economy of the spyware industry is a contributing factor in the seemingly effortless spread of spyware. In other words, the perceived need for spyware technology is still quite significant, whether it comes from commercial or government clients. This means that there is enough financial incentive for other suppliers to step in and cover shortfalls in case other spyware suppliers were to be sanctioned. This means that despite the backlash the NSO Group has faced in since the revelations, the spyware market is unlikely to collapse even if a majority of companies were to go out of business – an implausible scenario in and of itself at present (Kot and Feldstein 2023, p. 15; Riecke 2023, p. 698). Looking back at the spyware scandal,

most of the attention from the public had been directed on commercial vendors such as NSO Group, which are backed by global private equity companies or in some cases even states. As highlighted in Chapter 3.5.2 in reference the situation of the use of spyware in France and French politicians being targeted, there is speculation that the NSO Group is backed by Israel. This could indicate that high value connections enable new opportunities, perhaps also for firms that sell the most advanced programming, including zero-click malware that are hard to detect and rather expensive to purchase.

Looking closer at the demand perspective itself, EU member state governments do have an existing history of purchasing spyware as shown in case of some EU member states throughout Chapter 3. The conflicting signals democratic governments have given about their dedication to rein in intrusive technologies therefore does pose an issue. This is largely because there is no public statement on any legislative actions that would curb spyware in the European Union. Considering the relevance of the European Union as a market, one may as well refer to the Union as a "*spyware hub*" for these technologies.

As is the case with other policy areas, there is no consensus among EU member states in reference to the regulation of spyware. According to Kot and Feldstein (2023, p. 18), some member states are unwilling to enforce the fundamental rights perspective that, as further elaborated on in the subsequent chapter, has to be respected when transposing supranational to national legislation. Consequently, member states which are reluctant to implement a stricter regulatory framework may present themselves as safe havens for spyware companies. Within the European Union, this includes member states Bulgaria, Cyprus, Greece, Hungary, and Malta among others (Baruch and Leloup 2023; Kot and Feldstein 2023, p. 18; Szpunar 2020, p. 403).

Considering the public outcry following the revelations of the Pegasus Project, it becomes evident to the author that public campaigns, privacy crises, and regulatory mandates have not succeeded in controlling the market. To the contrary: the spyware market in the European Union seems to be expanding despite the aforementioned Dual-Use Regulation in place. That being said, given the pattern of abuse of spyware that has taken place across the European Union in the past few years, the overall assumption of member states' compliance in transposing EU law obviously falls short in reality. More than that, the examination of member states' situations as provided in Chapter 3 has shown that surveillance is frequently

carried out by both, authoritarian governments and democratic countries alike, against a variety of illegitimate targets. And, as can be seen in the case of Spain, Hungary and Poland, among others, these targets also include political competitors and journalists. Furthermore, more than half of the EU member states are connected to spyware, whether in the role or perpetrator, facilitator or victim (see *Figure 3-E* for reference). Consequently, as would be argued by the author, an examination of the market would be necessary for long-term strategies aimed at reducing the spread and misuse of spyware technology.

4.2. Fundamental rights as a balancing act

Having established the intrusive nature of Pegasus and other, similar spyware technology and all its challenges in reference to the regulatory framework in the European Union, one must also look at why this has caused the extensive public outcry as it did in reference to the disregard for fundamental rights. Rights which are supposed to be applicable to all residents of the European Union and which are derived from what could be interpreted as common values. Whilst international law uses the term of human rights in reference to all rights that are inherent to an individual that must not be violated based on their respective attributes, i.e. nationality, religion and gender among others, European Union legislation references the idea of fundamental rights. Even though fundamental rights significantly overlap with human rights, and they are anchored in EU law, there are shortcomings with regard to their implementation considering their limited applicability in reference to EU member states. For this purpose, the author will discuss fundamental rights in the context of the European Union whilst highlighting plausible challenges and inadequacies.

Looking back in history, the European Union was established on the principles of respecting human rights, especially those of minorities, freedom, democracy and the rule of law. To this extent, the European Union is a "union of values" (Art. 2 TEU), which must be upheld by all actors while enforcing EU law. The Charter of Fundamental Rights of the European Union (henceforth referenced as *Charter* or *EUCFR*) defines said rights in the European Union and stands on equal footing with the Treaty of Lisbon and the Treaty on European Union (TEU) as of 2009. With its adoption, the Charter establishes a new phase in the development of European integration by making fundamental rights visible, but also combining and

systematising the sources of inspiration dispersed throughout several national and international legal instruments into a single text (Lenaerts 2012, p. 356ff.).

Furthermore, the Charter functions as an aid to interpretation in the same way as the general principles of EU law. Any national law coming under the purview of EU law that violates the Charter must be set aside, and any EU legislation found to be in violation of an Article of the Charter will be declared null. Nonetheless, it is essential to state that private parties are not included in Article 51(1) EUCFR, which declares that the Charter applies to EU institutions and EU member states when implementing EU legislation. Consequently, the cornerstone of adherence is the Charter's area of applicability.

As the provisions of this Charter are directed toward EU institutions and member states, this means the following: the EUCFR is applicable to the European Union's institutions, bodies, offices, and agencies with proper consideration for the subsidiarity principle, and to member states when they are implementing EU legislation, and only then, according to Article 51(1) EUCFR. In other words: member states are only to respect the EUCFR when they are implementing EU law. Whilst this presents a shortcoming of the European Union in reference to the general applicability of fundamental rights in its framework, the EUCFR nonetheless formalises the commitment of a EU polity to fundamental rights. Moreover, the Charter establishes a solid foundation for the creation of a set of rights as prerequisites for the formation of the EU political community, which is made up of national structures, supranational organisations, and private parties (Lenaerts 2012, p. 376f.).

This strict applicability of the EUCFR may be traced back to concerns raised by several member states that an EU catalogue of fundamental rights would undermine their national sovereignty throughout the Charter's development process. These concerns also included the fear of the CJEU utilising the Charter as a federalising mechanism, which would in return replace the basic rights provided by the national constitutions with a federal one, similar to that of the United States of America (Council of the European Union 2023, p. 5; Denman 2014; Frantziou 2015).

This ambiguity may be traced back to, as argued by Spaventa (2018), the absence of an all-encompassing fundamental rights competence. Even though the rule of law crisis in recent years has demonstrated that some commonality of fundamental rights is essential to the core

functioning of the European Union itself, there remains a lack of unanimity regarding what constitutes fundamental rights. Because of this, fundamental rights are dispersed over many policy domains and legislative forms, each with different objectives and necessities. Because of this, every policy domain has a different standard of fundamental rights whilst of course respecting the base line as defined by the EUCFR (Spaventa 2018, p. 1000f.).

Looking at the European Union at this very moment, it is no surprise that there are different interpretations of what constitutes fundamental rights nationally considering a tendency of nationalist, right-wing parties gaining popularity. Furthermore, looking back in time, EU member states have had respect for democracy and rule of law for differing timespans. Considering the narrow interpretation of the EUCFR and its positioning within the European Union, fundamental rights are important to some and not as important to others. In line with this, democratic discourse and compromise may account for the present situation. Over the past decade, fundamental rights have become the focal point of political and judicial contestation, which is mirrored in many dynamics between the national and supranational level. As a first consequence, consensus to find a common definition of fundamental rights is challenging which results in a fragmented interpretation and protection of fundamental rights in the European Union (Spaventa 2018, p. 998).

Against the backdrop of the rapid development and technological advancement, application (and misuse) of digital technologies, challenges to democracy and the rule of law are increasing. In the case of spyware, this also affects fundamental rights. Therefore, the author would like to reiterate that it is crucial to keep in mind that, despite the fact that digital technologies haven't altered the moral foundation of the EU, rights and freedoms now do appear to demand fresh perspectives in order to protect basic rights. Here, the spyware scandal in addition to other circumstances such as the COVID pandemic has brought attention to the ongoing need to uphold fundamental rights. This may largely be traced back to challenges in safeguarding the rule of law and democracy, widespread misinformation campaigns, racism, mistreatment, and many other challenges in safeguarding vulnerable populations.

4.3. European institutions in gridlock?

In early 2022, the European Parliament established a Committee of Inquiry in accordance with Article 226 TFEU in response to the ramifications of the growing spyware scandal. The purpose of the Committee was to scrutinise claims of maladministration or violations in the application of EU law pertaining to the use of Pegasus and similar surveillance spyware (Agence Europe 15.02.2022, 10.03.2022 and 19.04.2022). Because the Committee of Inquiry was established as a direct response to the spyware scandal, it has been dubbed the *PEGA Committee*, formally known as the "*Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware"* (henceforth referenced as PEGA Committee or Committee). Despite the PEGA Committee carrying out its mandate and responsibilities with diligence, one must acknowledge that there are flaws to the Committee's effectiveness. This is because neither the Committee nor the European Parliament itself can call witnesses or have them testify under oath, nor can either one of the two access restricted material.

Thus, when compared to national parliaments, the European Parliament does not have the same extent of investigative authority, regardless of its right of inquiry as enshrined in the TFEU. Considering the extent to which the European Union has seen the use of spyware, or at the least the cooperation with companies developing spyware, the European Parliament had no choice but to rely on interinstitutional synergies and the good cooperation with the other European institutions because of its own flawed investigative authority. From what the author could gather in her research process, it indeed was challenging for the European Parliament to gather enough information via hearings and its own fact-finding missions whilst being confronted with a lack of responses to its information requests. Additionally, a lack of transparency in reference to the public access to information on both, the national and supranational level, was a challenge in and of itself.

Oftentimes, the pretence of national security is used to avoid responsibility, and likely even accountability, at a supranational level. This is possible because, as enshrined in Article 4(2) of the Treaty on European Union (TEU), "*[the European Union] shall respect [member states'] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State*" (Art. 4(2) TEU).

Consequently, in light of the revelations of the use of spyware in the European Union, member states have used this provision in the TEU to justify the use thereof, as reported by In t'Veld (2023, p. 144). The author would like to acknowledge that whilst this is reported by the European Parliament's PEGA Report and Recommendations, there are no official statements from EU member state governments that unequivocally state this. Because of this, the author would argue that it is difficult to comprehend the rationale behind the use of national security because of the lax definition of the term and the expansive interpretation of its reach by the national authorities.

Nonetheless, case law from the Court of Justice of the European Union (or *CJEU*) indicates that national security concerns must be balanced with the democratic values and basic rights that are deeply ingrained in what are often understood as EU values and are thus expected to be respected when transposing supranational to national law. In line with this, the CJEU has also argued that "*the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law*" (In t'Veld 2023, p. 4, ref. Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, C-623/17 (2020)). Member states must nonetheless define their essential national security interests and adopt appropriate measures to ensure their internal and external security. The *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ruling also clarified the criteria member states must adhere to when defining matters falling under the umbrella of national security.

However, the limitation of fundamental rights cannot be justified as being under national security when member states use the latter as a reference to refrain from being held accountable or having to provide information if one were to follow the European Parliament's line of argumentation. Without exception, EU legislation, with all its protections, has to be followed even when national security is under threat. Spyware misuse for purposes not directly related to said threat national security, as outlined in the case of Hungary and Poland, for example, is well documented.

As was seen in the previous chapter, the maladministration of spyware exposed EU citizens and residents, which in some cases may be directly traced back to the member state government itself. This essentially means that checks and balances within a democratic

society had been rendered inoperable, at least temporarily. Whilst a few member states had arrived at this stage, others had "only" hosted spyware companies or experienced the illegitimate use of spyware from a third party against its citizens and residents. Luckily, however, a majority of EU member states has so far refrained from taking this course of action, i.e. relying on spyware for political or other, illegitimate purposes.

With this being said, however, when member states do decide to utilise said technology, the European Union's existing institutional and political framework is flawed to the extent that it lacks the necessary tools to stop, or even prevent, the use of the technology (see Chapter 4.1 for reference). This in return results in the European Union's legislative vulnerabilities being exposed by spyware. This is precisely where the European Parliament's PEGA Committee is situated.

As a result of an investigation, the European Parliament adopted the EP Pegasus recommendations to the Council and the Commission on 15 June 2023. The recommendation includes proposals for legislative and non-legislative actions at the supranational level to regulate the use of spyware, with the goal of defending European Union law, and with it the rights enshrined in the European Union Charter of Fundamental Rights that are to be respected when transposing Union to national law. Following the line of argumentation as outlined in this section, the European Parliament, in its recommendations, asked the European Commission to take a closer look into the maladministration of spyware in EU member states (European Parliament 2023).

Consequently, the author would argue that, should member states be allowed to not face any consequences with regard to serious spyware violations by using the pretext of national security, this would certainly set a concerning precedent. Before moving to the subsequent section on the European Commission, the author would like to remind that the use of spyware is not exclusively a national issue. This is because spyware has both, direct and indirect, effects on the European Union, its institutions and member states. Indirectly because of the misadministration on a national level which resulted in European citizens and residents being targeted; directly, because members of the European Commission, the European Parliament, and the European Council were also among those targeted. Furthermore, spyware is not a solely national issue as it does not respect traditional borders, and the surveillance of citizens and residents is not limited to state borders. As a result, because spyware does not respect

traditional borders, it is a transnational and therefore European problem that needs to be addressed at all levels, the supranational included.

A discussion of the recommendations made by the European Parliament in relation to the tools available to the European Commission will follow in the subsequent section.

4.3.1. The European Parliament's recommendations to the European Commission: a discussion

Translated to the tools available to the European Commission as attributed to it by the treaties, the author decided to use *Figure 4-A* (see below) to help visualise what requirements the European Parliament has established for actions to be taken by the European Commission in the aftermath of the Pegasus spyware scandal. In this table, the European Commission's tools have been ordered from less to more formalised and more impactful, as follows: First, the European Commission has the possibility to consult with civil society, experts and other bodies to gather information, as well as holding conferences as food for thought on topical issues. This first step may then be complemented by the creation of centres of excellence and other institutions to streamline knowledge and provide expertise to the European Commission. Another tool of the European Commission is the establishment of specific monitoring procedures, which is a form of communication between the Commission and national authorities with the purpose to assist member state governments in the successful implementation, progress and attainment of goals and objectives. These monitoring procedures may include fact finding missions and follow up reports among others. Next is the European Commission's competence in reference to the initiation and creation of EU legislation. Should said EU legislation be improperly implemented, the European Commission then has the opportunity to initiate infringement proceedings with the purpose of controlling and enforcing EU law. Should this not be enough to incentivise the member state to implement EU law, said member state would then have to face financial penalties. Should all these measures fail to make member state governments compliant with EU legislation once again, there is one last resort for the European Commission, and the European Union as a whole, to hold said member state accountable: Article 7 Procedure (as enshrined in the Treaty on European Union, or *TEU*). The author would like to note that the tools of the European Commission do depend on the policy area. This is because of the

different levels with which policy areas are integrated at the supranational level, therefore attributing the European Union and its institutions differing competences. For the purpose of the author's research, this section focuses on all tools available to the European Commission regardless of policy area as this allows to visualise all possibilities in reference to an adequate response in the aftermath of the spyware scandal.

Figure 0–G: Overview of the European Commission's tools and recommendations of use made by the European Parliament (author's own visualisation)

Tools available to the European Commission	***Recommendations by the EP***
Consultation and conferences	Yes
Creation of centres of excellence and other institutions	Yes
Establishment of specific monitoring procedures	Yes
Initiation and creation of EU legislation	Yes
Infringement proceedings (control and enforcement of EU law)	Yes
Financial penalties	No
Art. 7 procedure	No

In the Recommendations adopted by the European Parliament, the European Commission was directly called upon 27 times. Of these 27 remarks, 22 are in reference to the Commission's tools as visualised in *Figure 4-A*. The other five instances the European Commission is addressed in the EP Recommendations are in reference to what the Parliament perceives as the Commission's inaction in the aftermath of the revelations. These five remarks do not include recommendations for European Commission to make use of its tools and are therefore not included in the next section.

As can be seen in *Figure 4-A*, the European Parliament recommended the European Commission to use five of the seven tools available to the Commission, i.e. consultation and conferences, the creation of centres of excellence, the initiation and creation of EU legislation as well as the initiation of infringement proceedings with the purpose of the enforcement of EU law. Whilst this provides a simplified overview, each of the tools referenced in the European Parliament's recommendations will be addressed more in detail in the subchapters below.

As a first step, the author will outline the recommendations as made by the European Parliament in its recommendations. This will follow the order of the European Commission's tools as listed in *Figure 4-A*. Having established the European Parliament's expectations of the European Commission's response to its report, and the Pegasus spyware scandal as a whole, the author will then move to discuss measures taken by the European Commission in response to the European Parliament's proposal for action.

4.3.1.1. Consultation and conferences

To begin with, the European Parliament argues that it would be a positive (first) step for the European Commission to engage in a consultative process with relevant actors with the purpose of providing food for thought on the issue of spyware (mis)use. Six of the 22 recommendations are in relation to the European Commission's competence to engage in consultative processes and conferences.

Among the recommendations were the call to action for the Commission to adapt its annual rule of law report to allow comparisons of spyware usage across member states in addition to being provided national reports from the responsible national actors regarding spyware in the internal market (European Parliament 2023a, Para. 32 and 39). In relation to the market aspect of spyware, the European Parliament also called on the European Commission confer with member state governments in reference to the issuing of export licenses for the use of spyware under the Dual-Use-Regulation; this information is in return to be reported to the Parliament (European Parliament 2023a, Para. 57 and 63). Furthermore, the Commission is expected to also investigate any statement of invoking national security in cases where spyware abuse is suspected (European Parliament 2023a, Para. 42). Lastly, the European Parliament also calls the Commission to lead in organising an interinstitutional conference

wherein the Commission, Council, and Parliament work towards governance reforms with the purpose of effectively countering, perhaps even preventing, internal threats to democracy and the rule of law (European Parliament 2023a, Para. 132).

4.3.1.2. Creation of centres of excellence, other agencies or institutions

In line with the tools available to the European Commission, in this case the creation of a centre of excellence as well as other agencies or institutions, the European Parliament recommended the Commission establish said bodies in two instances. First, the Commission is asked "*to initiate, without delay, the creation of an independently run European interdisciplinary research institute, with a focus on research and development at the nexus of information and communication technology, fundamental rights and security*" (European Parliament 2023a, Para. 113). The European Parliament envisions this research centre to serve the purpose of collaborating with academics, civil society, and experts in the field of information and communication technology. Second, the Parliament also recommended the Commission to form a special taskforce with representation from the national electoral commissions to safeguard the European election 2024. This is supported by the Parliament arguing that the elections could be impacted by the improper use of spyware tools like Pegasus, especially considering that spyware does not abide by traditional borders (European Parliament 2023a, Para. 125).

4.3.1.3. Establishment of specific monitoring procedures

More than half of the recommendations by the European Parliament addressed to the European Commission are in reference to the latter establishing specific monitoring procedures, assessments and implementation reports. As argued in the European Parliament's recommendations, the lack of activity from the Commission is worrisome, based on which it "*urges [the Commission] to make full use of all its powers as guardian of the Treaties, and to conduct a comprehensive and in-depth investigation into the abuse of and trade in spyware in the Union*" (European Parliament 2023a, Para. 123). In addition, the European Parliament pleas for the Commission to look into and report on the improper implementation and enforcement of EU law in reference to regulations and directives regarding technological advancement, such as the Dual-Use Regulation among other, with the purpose of developing

a roadmap to correct them (European Parliament 2023a, Para. 52). Following this call to action, the recommendations also call upon the Commission to have the resources to adequately monitor and implement existing legislation (European Parliament 2023a, Para. 59). In particular, the Commission should monitor the rule of law more closely and include recommendations specific to each country regarding the illegal use of spyware by member states in its annual Rule of Law Report. It should also evaluate how responsive state institutions are to providing redress to those who are targeted, and it should expand the scope of its Annual Rule of Law Report to include all threats to democracy, the rule of law, and fundamental rights (European Parliament 2023a, Para 121(a)). For example, Para. 75 (European Parliament 2023a) recommends the Commission to establish a coordinated strategy for obligatory vulnerability disclosures from member state governments.

4.3.1.4. Initiation and creation of legislation

The fourth tool part of the European Commission's competences is the initiation and creation of EU legislation. In Para. 35, the European Parliament calls on the Commission to propose legislation, as the Parliament would expect a new approach in reference to regulating "hacking as a service". This is to prevent any support of surveillance efforts by hacking as a service that would violate the European principles, such as the principle of necessity and proportionality. Especially since the actor in charge is granted access to an excessive amount of personal, sensitive data (European Parliament 2023a, Para. 35). Another recommendation made by the Parliament was in reference to the initiation of a general call to legislative action referencing the EP PEGA recommendations as a whole (European Parliament 2023a, Para. 136).

4.3.1.5. Infringement proceedings

One step beyond establishing specific monitoring procedures is that of initiating infringement proceedings. Four of the 22 recommendations call on the European Commission to precisely do so in cases of persistent noncompliance. In the case of infringement proceedings, the Commission may initiate infringement proceedings if a member state fails to adequately transpose new EU legislation, or if said member state fails to rectify an alleged breach of EU law. If this is the case, the European Commission would send a formal notice to the member

state. Upon the member state's response, the Commission will then, dependent on whether the issue had been resolved, issue a reasoned opinion. Should the member state, even after this step, be in breach of EU law, the Commission then has the option to refer the matter to the CJEU. As argued by the European Parliament, these competences are in line with the Commission's key role in enforcing EU law and ensuring its uniform application throughout the Union. In case of non-compliance with existing EU law, the European Parliament argues the Commission shall therefore make use of this option if the matter is not resolved by any other means (European Parliament 2023a, Para. 14, Para. 53, Para. 90 and Para. 121(b)).

4.3.2. The European Commission's response to the European Parliament's recommendations

In response to inquiries from the PEGA Committee and the vast number of media allegations regarding the use of spyware in member states, the Commission reportedly sent letters to a select number of member state governments asking for clarity on the spyware controversy (In t'Veld 2023, p. 135). According to the report by In t'Veld (2023, p. 135), "*the Commission itself points out […] 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness. It is up to the Member States, however, to 'demonstrate that national security would be compromised in the case at issue'*" (In t'Veld 2023, p. 135). According to In t'Veld, no further action had been taken in response to the Commission's letter. The author would like to acknowledge that this letter from the European Commission to the select number of member state governments (Cyprus, France, Greece, Hungary, Poland and Spain) is not publicly accessible and there is no relevant media reporting by the time this MA thesis was concluded. As a consequence, the author had to rely on the information as provided by the *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (A9-0189/2023)*.

However, there is one additional instance in which the Commission decided to address member state governments in an attempt to gather information in reference to the use of spyware. However, in this case, the letter was addressed to all member states in a general manner. Whilst the author had been unable to publicly access the letters referenced by In t'Veld (2023, p. 135) in the European Parliament's Report, the author was able to find a copy

of said general letter addressed to all member state governments with the request to provide information. The letter itself reads like a questionnaire and contains questions such as "*For what purpose is the use of spyware permitted under national law*", "*What are the conditions for the use of spyware […]? Please explain the type of safeguards that exist under national law*" and "*Please specify if the use of spyware […] requires prior authorisation by a court or an independent administrative authority*." (Gallego 2022). Considering the contents of the letter, one may presume that the European Commission's Directorate-General for Justice and Consumers (or *DG JUST*), sent the letters as an opportunity to map out the situation in each member state and try to understand national positions. Member state governments were asked to return a response by 31 January 2023 (Gallego 2022). In a meeting of the PEGA Committee on 28 March 2023, the European Commissioner for Justice, Consumers and Gender Equality Didier Reynders, informed that the Commission was still gathering member state responses. Only upon having received all replies would the Commission then assess the questionnaires. The author would like to note, however, that Reynders did not provide a timeframe for said assessment (In t'Veld 2023, p. 136).

Since the European Parliament adopted the Recommendations in June 2023, the European Commission adopted two documents that hint to possible legislative acts in reference to the use of spyware in the European Union: the 2023 Rule of Law Report (European Commission 2023a) and the Communication on Defence of Democracy (European Commission 2023b).

In its *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On Defence of Democracy (COM(2023) 630 final)* on 12 December 2023 (henceforth referenced as *Communication* or *Communication on the Defence of Democracy*), the European Commission acknowledges that democracy itself is not without its obstacles and adversaries. The Commission traces this back to authoritarian regimes perceiving the plurality of opinions and diversity of democracy as a threat. Furthermore, the Commission also acknowledged that some of these authoritarian regimes had deliberately pursued policies to weaken democratic institutions, exert pressure on the media, and thus diminish the independent space available for civil society. In addition, the Communication also acknowledge that the strategic weakening of democracy may take many different forms, whether it be taking advantage of social divisions to incite mistrust in established institutions, or silencing the voices of its own

citizens and civil society. In line with this, the Commission also recognised manipulation and disinformation campaigns in direct relation with electoral campaigns (European Commission 2023b, p. 1).

This Communication signals that the Commission does see challenges and worrisome trends in reference to democracy, most notably efforts to weaken public support for or faith in representative democracy and democratic institutions. This would also include the illegitimate use of spyware in relation to attempts to eliminate, or at the least weaken, democratic checks and balances as well as election campaign instability. Considering what the author has shown based on the examination of the use of spyware by EU member state governments, the Commission nevertheless refrains from directly addressing any member state that had utilised the technology to weaken democratic principles. Nevertheless, the author did find that the Commission acknowledged the need for action on the supranational level: "*recent experience shows […] the need for the EU to be in the vanguard of countering such destructive forces*" (European Commission 2023b, p. 1).

In this communication, the European Commission also addresses the use of spyware, whereas it argues the following: "*Surveillance tools may be used by public authorities, under certain conditions, for reasons of national security, but the use of spyware to gain political advantage is very different*" (European Commission 2023b, p. 10). This is because fair play and legality are prerequisites for democratic discourse. This phrase, as argued by the author, clearly highlights the European Commission's concern for the misuse of technology. Nevertheless, the Commission also acknowledges that member state governments are the sole authority in reference to national security. Regardless, the Commission emphasises that it is improper for member state governments to employ said technology with the purpose of targeting journalists and political figures, among others, for political advantage. Looking at the European Commission's Communication, the Commission does argue for the consideration of EU case law and its standards when inferring national security, as also highlighted in the European Parliament's Report.

In its communication, the European Commission also references the *2023 Rule of Law Report* (European Commission 2023a), which had been published in July 2023. Here, the Commission reaffirms that national checks and balances are necessary to guarantee that security measures are in place, even in cases when the use of spyware is connected to national

security. According to EU legislation, whereas the Commission here directly references the EUCFR, fundamental rights such as the protection of personal data and the freedom of speech, among others, should all be protected. In its report, the Commission expands on the findings from the previous years, and notes the developments in relation to the "*alleged illegal use of spyware (such as 'Pegasus', and equivalent surveillance spyware)*" (European Commission 2023a, p. 27).

As in the case of the Commission's Communication on the Defence of Democracy, the 2023 Rule of Law Report also underlines that, while ensuring national security is within the purview of member state governments, member states are required to adhere to EU law. Consequently, the use of surveillance tools such as spyware must adhere to strict regulations and uphold EU law. This is because EU law, as argued by the Commission's 2023 Rule of Law Report, protects basic rights including the privacy of individuals' data and freedom of speech as well as the security of journalists (European Commission 2023a, p. 27).

In the same 2023 Rule of Law Report, the Commission did also address the insufficient oversight over the use of covert surveillance techniques outside of legal proceedings. As argued by the Commission, this has led to increased concerns about the deployment of spyware against journalists and opposition politicians, most notably in Hungary and Poland (European Commission 2023a, p. 27). In reference to this, in order to establish universal EU protections to ensure media freedom and plurality, the Commission struck new ground in September 2022. In addition to safeguards against political meddling, the European Media Freedom Act (or *EMFA*) is also set to contain particular regulations prohibiting the use of spyware against journalists in addition to guidelines preserving media plurality and independence in the European Union. Furthermore, it emphasises transparency as well as the openness about media ownership and the distribution of public service advertising (European Commission 2023a, p. 30).

The European Commission further acknowledged that the European Parliament's recommendations contained other suggestions for actions at the supranational level, i.e. the initiation and creation of EU legislation to remedy grievances with regard to member state shortcomings when implementing and respecting EU law. This could include the revocation of export licences that violate EU law, the conditional sale and use of spyware within the EU, and the creation of uniform EU standards to control the use of spyware among others.

Consequently, the European Commission states that "*[the European Commission] is now carefully assessing the final position and recommendations of the European Parliament*" (European Commission 2023a, p. 30). Whilst there has been no formal proposal for further action in reference to making use of its tools from the Commission by the time of writing in early 2024, this may well be subject to change in the future.

Therefore, to understand why the European Commission has responded in the manner it did as outlined in this subchapter, the following section will discuss said response in light of integration theories as outlined in Chapter 2.2.

4.3.3. Discussion of the European Commission's behaviour drawing on insights from European integration theory

Whilst the author has shown that the use and distribution of spyware within the European Union is not necessarily a novelty per se, the Pegasus spyware scandal was much more extensive and involved more than half of all EU member states. Consequently, even though spyware had been found in the European Union prior to the revelations surrounding NSO Group's Pegasus, there is a difference in the sheer scale of the scandal based on the information derived from publicly available sources as outlined in Chapter 3.

The author found that whilst in the case of the European Union there is one vocal actor in support of "systemic reform" with regard to the exploitation of spyware, i.e. the European Parliament, there is little to no willpower to implement a narrower regulatory framework. Neither on the national nor on the supranational level. The European Parliament conducted a thorough investigation based on the restricted amount of information that had been made available. The investigation was concluded with the publication of the Parliament's recommendations for actions to be taken by different actors among which most prominently the European Commission.

As also seen in Chapter 4, the European Commission has taken some steps to acknowledge the gravity of the spyware scandal and the illegitimate use of the technology, i.e. the *Rule of Law Report 2023* and the *Communication on the Defence of Democracy* of the same year. In these documents, the European Commission acknowledged the need for the sensitive

assessment of the situation on the European and national level, as well as the proposals made by the European Parliament in reference to its tools and competence.

The author would like to note that this is the second time the European Commission has acknowledged the use of spyware and its challenges to fundamental rights and the rule of law in its Rule of Law Report. The *2022 Rule of Law Report* was the first to address spyware. In this document, the Commission provided a succinct summary of the spyware scandal whilst acknowledging the existence of spyware and its implications for fundamental rights for the first time. As the document reads, "*[spyware] has gradually gained importance over last year: while linked to national security, there is a need for national checks and balances to ensure safeguards are in place and fundamental rights are respected*" (European Commission 2022, p. 25). The author also consulted the 2021 Rule of Law Report as well as the 2020 Rule of Law Report, in which the topic of spyware was not referenced.

This would indicate that the European Commission has taken note of the events surrounding the spyware scandal and revelations made by the Pegasus Project. Therefore, considering the order in which the author had ranked the European Commission's tools, from less to more formalised and more impactful, the author would argue that the steps taken by the European Commission as outlined above are represented in step one, i.e. a consultative process for an informational exchange with experts on spyware, civil society a.o.

In reference to the 2022 and 2023 Rule of Law Report, the main arguments of both documents, i.e. the respect for fundamental rights, EU law and the need for rule of law and adequate checks and balances, also in reference to national security, are similar albeit being placed in a different order. Even though both paragraphs are similar, the inclusion of spyware and its challenges nevertheless does indicate that the European Commission recognises the scandal and its ramifications for fundamental rights as both, a challenge and an opportunity. Whilst no new monitoring procedures were established, the inclusion of the maladministration of spyware in the Rule of Law Report could outline an axis for future measure. This means that, whilst not yet having done so, the European Commission could perhaps use the existing language for a gradual amplification over time in case member states refrain from addressing national shortcomings as outlined in this paper. This could very well indicate a willingness of the European Commission to expand its existing rule of law

monitoring procedures to include spyware. As to whether this is the case remains to be seen considering the European election from 06 to 09 June 2024.

Figure 0–H: Overview of the European Commission's tools, recommendations of use made by the European Parliament and actions taken by the European Commission (author's own visualisation)

Tools available to the European Commission	***Recommendations by the EP***	***Actions taken by the EC***
Consultation and conferences	Yes	Yes
Creation of centres of excellence	Yes	No
Establishment of specific monitoring procedures	Yes	No
Initiation and creation of EU legislation	Yes	No
Infringement proceedings (control and enforcement of EU law)	Yes	No
Financial penalties	No	No
Art. 7 procedure	No	No

Looking at the author's ranking of the European Commission's tools and taking into consideration what the author's research has shown, the author does acknowledge that any steps except infringement proceedings require the support of member state governments. Consequently, the author would argue that the Commission's response was hesitant, considering that it has been close to a year since the European Parliament adopted its recommendations. However, it is important to note that legislative proposals and other initiatives require time to be prepared.

When placed into the political and geopolitical context, i.e. the war in Ukraine and the surge of right-wing, anti-European politics post-Covid, one may argue that the European Commission may have seen a need to prioritise and focus on a select number of policy areas and topics where it can more easily reach consensus. This reminds the author of aspects of an intergovernmentalist outlook on the world. In intergovernmentalist thinking, member state governments are the main drivers of integration while placing emphasis on their sovereignty with regard to policy- and decision-making processes. This in return also means that as a default rule, decisions are made at the national level by means of bilateral or multilateral negotiation. Only in the case of shared interest will governments agree to cooperate as the

intended result must be perceived as beneficial (Cini 2019, p. 70f., p. 72, ref. Hoffmann and Keohane 1991, p. 277; Rittberger and Schimmelfennig 2015, p. 38ff).

Based on this intergovernmentalist logic, EU policy would have to reflect national interest in each and every single case. Looking at the Pegasus spyware scandal more specifically and taking into consideration the number of member state governments that have either purchased, used or facilitated the purchase and use of spyware, it would appear unlikely to the author at present that cooperation in this context would be fruitful. This is because, in order for member states to either continue the use or spread of spyware for national benefit or not be held accountable for their past infringements of EU legislation, it is essential to refrain from promoting a tighter regulatory framework.

Furthermore, rather than enabling the European Commission as a supranational actor to promote the integration of the relevant policy areas and expand its competences, the intergovernmentalist perspective would place emphasis on member state sovereignty. In the case of spyware, digital policy is located in very close proximity to national security, whereas the latter has yet to be integrated to the supranational level. Considering that spyware technology also presents a possibility to strengthen national security, it becomes a topic of national interest. In this case, member state governments would be more reluctant to delegate more autonomy and competences to the supranational level, i.e. the European institutions, regardless of integrative advances in the realm of EU digital policy in the last few years (e.g. the EU General Data Protection Regulation or the European Media Freedom Act a.o.). Therefore, the author would argue that the spyware scandal and its ramifications underscore the contentious struggle of dividing competences between the European institutions and member states. Looking at the European Commission and the requirements for its legislative proposals to be adopted in line with EU policy-making processes, unless there is some sense of forthcoming consensus on the common challenges posed to the European Union by spyware, there is little hope for the European Commission to advance proposals. This may in part account for the European Commission's hesitant use of its tools.

Contrary to this, neofunctionalism typically anticipates gradual and self-reinforcing integration following the logic of path dependency as the supranational institutions promote integration as a means of furthering self-interest and expanding its own competences and autonomy. This means that even though member states may be willing to take some

integrative steps in the beginning, it is the supranational actor that drives subsequent integration. Whereas this may initially be the case in one policy area, because of spillover mechanisms, other policy areas will be affected and therefore create new (transnational) dependencies and the need for further integration. Having created a common market, there may be functional pressure to jointly regulate the "product", i.e. spyware (Strøby Jensen 2019, p. 58ff, Schimmelfennig 2018, p. 15; Rittberger and Schimmelfennig 2015, p. 45ff.). As a result, integrative steps may not be limited to what member states had previously agreed on and supranational actors may also gain substantial autonomy and capabilities (Schimmelfennig 2018, p. 15). Should this be the case, the author would expect the European Commission to act for the good of all its European Union citizens and residents, therefore not limiting itself to steps one and perhaps three, i.e. consulting with experts and introducing language to acknowledge the ramifications of the spyware scandal.

Furthermore, considering digital policy and national security are policy areas in which there are precedents of the European Commission showing initiative, the spyware scandal would present itself as an opportunity to use and expand its competences. Nevertheless, this has not happened by time of writing in early 2024, therefore contradicting neofunctionalist thinking.

Nevertheless, the author would argue that spyware does present a challenge and that it will be an important precedent for future challenges in reference to the rapid technological advancement. As shown in Chapter 3.6, when the differentiation between perpetrating and victimised EU member states is not taken into account, spyware affects more than half of all EU member states (see *Figure 3-E* on p. 45 for reference). This is because it is difficult to precisely categorise EU member states based on their affiliation with spyware. This means that whilst a member state has purchased the technology, for example, it can still nonetheless fall victim to the technology by another state. Therefore, as seen in the cases of Belgium or Latvia, among others, it is impossible to pinpoint who targeted citizens and residents. Even though some EU member states have confirmed the purchase of the spyware, and some are suspected of having purchased it, this does not guarantee that said member states are the only actors capable of surveying citizens and residents. This is because spyware does not respect traditional borders. As a result, the author would argue that the challenges posed by spyware, coupled with rapid technological advancement and digitalisation, concern all EU member states and that a regulatory framework would be beneficial.

Considering that 17 of 27 EU member states are affected by spyware and this presents a majority, one may preclude that there must be factors beyond the concern for rule of law and the protections of fundamental rights that impede the establishment of a common regulatory framework. This in return may also explain why the European Commission has so far preferred to refrain from "getting involved" by means of initiating or advancing policy proposals, or alternatively holding member states accountable.

As can be seen by the line of argumentation by the European Parliament as well as the statements made by the European Commission, there is some level of agreement among both European institutions that more responsibility and supervision are needed in reference to the spyware sector and the illegal surveillance of persons. This is because there are some factors that should be established among EU member states: democratic values, a common understanding of fundamental rights and a common market. This would indicate that there are arguments to be made for the European Commission to take action. However, so far, the Commission does not perceive it beneficial to promote legislative proposals on the European level as perhaps the Commission was not confident in achieving the necessary votes in the Council.

This may be traced back to different explanations. To begin with, one may call into question the resolve of the European Commission and its commissioners to initiate change. When this is placed into the context of the European elections on 06 to 09 June 2024, one may interpret the inaction of the Commission as an indicator for the phasing out of office. Furthermore, as previously argued, legislative proposals take time. This would mean that there is a possibility of the Commission initiating a legislative proposal that, due to the EU policy-making process, may not be adopted before the European election, therefore outdating the Commission's time in office and predetermining the first official acts of the new Commission. Additionally, if the Commission were to initiate more regulations to be transposed to national law, even if it had achieved the votes in the Council, nationalist right-wing forces may voice their criticism of a perhaps tighter regulatory framework. The author would like to reiterate that whilst Commissioners do serve the Commission, they are nominated by member state governments before being subjected to a hearing and vote in the European Parliament. As a result, this may account for the current Commission refraining from following legislative steps as suggested in the European Parliament's recommendations, which were published in June 2023.

Since it is impossible to determine who is behind illegal surveillance attempts, this certainly raises questions in reference to national security and the protection of its people for all EU member states *Figure 3-E* (see p. 45) shows. Furthermore, in the case of France and Spain, high level politicians and even heads of state or government had been targeted, as well as the President of the European Council, Charles Michel. As a result, the illegitimate use of spyware does affect EU member states and the European institutions alike. The author would argue that the establishment of an adequate regulatory framework for the protection of fundamental rights and the strengthening of already existing regulations in reference to the protection of privacy and personal data would be of shared interest to both, the European institutions and member states that have fallen victim to the illegal use of spyware.

In line with this, Roussi (2024) reported that France and other EU member states have voiced their support to establish an international regulatory framework to restrain the fast-paced spread of spyware across the globe, as "*governments have struggled to stop the spread of commercial hacking tools*" (Roussi 2024). Their initiative is supported by tech companies such as Apple, Google and Meta among others. These tech companies had continuously voiced their opposition to the lack of a regulatory framework in addition to challenges posed to their products due to the malignant nature of spyware and its rapid development. It is their support that led the US to blacklist Pegasus and the NSO Group already in 2021 (Bergman et al. 2021; Kirchgaessner 2021; Roussi 2024). As to when this may spill over to a tighter European regulatory framework and if this will result in a legislative proposal from the European Commission remains to be seen. If there is a change in stance on the national level in favour of EU legislation, there may be hope yet.

5. Conclusion

Spyware is more than just a technical instrument that is occasionally used for very specific purposes. What the author has found in her research process is that spyware functions as a crucial component of a system subverting democratic principles and fundamental rights in both autocratic and democratic countries alike. Even though the use of such surveillance technology, in theory, could be regulated by means of different protection mechanisms, controls for supervision and examination, research reveals that such regulatory frameworks such as the Dual-Use Regulation are insufficient. Even though the rapid advancement of

technology may be partly to blame for lax or missing regulations, there have been instances where the current situation of facilitated surveillance based on the use of spyware was purposely created. In these cases, e.g. Hungary, Poland, Spain and Greece, among others, the technology was used as a means to an end with the purpose of either strengthening political power, or exerting influence.

Since the Pegasus Project was published in July 2021 and the revelations made waves around the globe, civil society, businesses, and the media have all given targeted malware a great deal of attention. Just like governments one would presume. Yet that is not necessarily the case. As shown by the author, EU member state governments have yet to formally address the causes of the maladministration of spyware and implement some sort of systemic reform to avoid ambiguity.

The research conducted by the author, more specifically the examination of EU member states in relation to spyware in Chapter 3, has clearly indicated that the use of spyware is on the rise across the European Union, and it has been for a while. However, as argued by the European Parliament and followed up by the European Commission, the use of spyware in reference to the protection of national security had been used as an argument to avoid the supranational institutions from trying to claim their competences. And even though the European Commission did ask member state governments to respond to a questionnaire in reference to the spyware scandal, there has been no distinct movement of the Commission towards effectively making use of the tools it applies in other policies. Nevertheless, the European Commission has consulted experts and included said information in its 2022 and 2023 Rule of Law Report.

Beyond this, the Pegasus Project has demonstrated the inadequacy of the legal frameworks and oversight bodies currently in place, both at the national and European level. Considering the tools available to the European Commission as established in Chapter 4, there is potential for the Commission to incite (positive) change and hold member states accountable by setting a precedent. Furthermore, as outlined in the European Commission's Communication on the Defence of Democracy and the 2023 Report on the Rule of Law, the supranational institution does possess the awareness of spyware being a threat to democracy and the rule of law, just as much as its illegitimate use is a threat to fundamental rights that are supposed to be respected when transposing European to national legislation. Additionally, by introducing

new language in its 2022 and 2023 Rule of Law Reports, one may argue that the European Commission has opened a door for the gradual expansion of its monitoring mechanisms to include spyware technologies. As to whether the European Commission will initiate legislative proposals in the future remains to be seen. This may be traced back the availability of the European Commission's tools being dependent on the policy area, as of course the level to which a policy is integrated defines to what extent, if at all, the Commission is attributed competences.

Looking at the situation of spyware in the European Union and taking into consideration the author's research as outlined in this paper, it goes without saying that the situation is intricate. This is because when one couples the covertness of spyware with a lack of transparency and the lack of willingness of member state governments to cooperate in regard to information sharing to address systematic shortcomings and the infringement of fundamental rights, an unfortunate chain of events may even further deteriorate democratic values and principles. The author would argue that the lack of willingness by the European Commission to make maximal use of all potential tools in its overall toolbox is connected to different reasons outlined in the preceding subchapter, such as the geopolitical environment, the European elections and different national interests in reference to the member states differing relationship with spyware.

Furthermore, as shown in the author's research, the free movement and internal market of the European Union facilitate the trade in spyware. Regardless of the preconceived notion of the European Union being a strict regulator, a number of member states are being used as export hubs due to lax enforcement of export laws. Because of an inapt protection of fundamental rights at the EU level, as outlined above in Chapter 4, and perhaps more importantly because of a delicate balance among member states that is required for fundamental rights to be upheld, at least at the lowest common denominator, the EUCFR has a very narrow interpretation and application.

To conclude, the author would like to emphasise that against the backdrop of technological advancement, the digital revolution will underline both, its advantages and disadvantages. Therefore, in addition to making use of the advantages and disadvantages of the digital revolution, the European Union and its member states must act to keep up with technological developments outside the EU. Considering the position of the European Union, more

specifically that of the Single Market on the global stage, EU member states and EU officials will likely have to determine whether they want to prioritise market power over democratic principles and fundamental rights. It cannot be ignored that select EU member state governments do have vested interest in a tighter regulatory framework regarding the use, and trade, of spyware considering their residents and citizens had been targeted illegally, with France being one of the most vocal supporters thereof (Roussi 2024).

If the European Union is to remain a place where people may enjoy their rights and freedoms whilst living in harmony, European institutions and member state governments alike will have to find a consensus on how to address challenges raised and exacerbated by digitalisation and technological advancement. The Pegasus spyware scandal has highlighted the ease with which fundamental rights are so easily harmed, partly even with the intent of limiting democratic principles. As shown by the author, this exploitation included the surveillance of journalists, politicians and activists, among many others, therefore infringing on fundamental rights and what the author would argue is the cornerstone of democracy: diversity and plurality of voices and opinions. A tight regulatory framework would not only have to be introduced, but more importantly be enforced in a manner that would leave little to no incentive to member state governments to disregard EU law. Furthermore, considering the rapid advancement of technological innovation, the author would also argue that the European Union and its member states would have to invest in more efficient and secure cyber security systems to protect the personal data and privacy of their residents. Otherwise, a tight regulatory framework may only curb the spread of spyware within the European Union whilst devices remain vulnerable to spyware operators outside of the European Union.

Considering the investments that would have to be made in reference to security measures in support of European citizens and residents being able to guard their privacy and personal data, one may also argue that the European Union may opt to "disregard" its high standard in reference to the protection of fundamental rights to maintain, or even enhance, its position as a market power on the global stage. Should the European Union wish to cement its place as a market power internationally, it must consider potential pitfalls. This is because, contrary to the European Union, other market powers such as China, for example, are typically less concerned about the respect for fundamental rights. Therefore, they may act without

restrictions for the benefit of a competitive advantage which might lead to a global downward cycle. Either way, the European Union must find a constructive way forward soon.

6. Outlook and topics for further research

Looking back at her research design and process, the author must acknowledge that, whilst the European Parliament's Recommendations were adopted more than six months ago in June 2023, there still is little information available in reference to the position of the European institutions apart from the Parliament, but also regarding that of member state governments. The author did find an adequate number of documents for the examination of the situation at the national level as outlined in Chapter 3, consisting of relevant articles that are publicly accessible as well as the results of the PEGA Committee. What the author struggled with in her research process was the analysis of the European Commission's competences, more specifically with regard to the author's initial plan of analysing these competences in light of European integration theory as outlined in Chapter 2. In the end, what the author found in terms of publicly available documents were different actions taken and statements made by the European Parliament, most notably the PEGA Committee, and a handful of statements and communications from the European Commission. On a national level, the information gathered by the author is limited to a select number of statements by national governments as outlined in Chapter 3 in addition to newspaper articles provided by different media outlets and the Pegasus Project.

Nevertheless, based on her research project and lessons drawn from it, the author does see potential for further research based on her own. This is because any and all advances and efforts made in reference to the regulation of the technology and the digital realm are precedents. First, the author would argue in support of a comparative analysis of a select number of EU member states that had been implicated in the spyware scandal. By doing so, one could then enter into a detailed examination on the state of democracy and the rule of law. This would perhaps then allow the possibility to engage in a discussion of legal principles and the role of the CJEU more in detail. Second, one may investigate already existing EU legislations such as the Dual-Use Regulation in reference to the spread of spyware across the European Union. Considering the gridlock in reference to the recommendations made by the Parliament and the lack of information regarding the European

Commission's stance on the issue, this might be an interesting example of a case study in which process tracing could possibly highlight the extent to which the European Commission makes use of its tools in reference to already existing legislation in digital policy. Additionally, the author would argue that comparing the response of the European Union and its institutions to other important international actors, e.g. the United States of America, could add valuable insight in reference to how a legislative response, or the lack thereof, affects the development of spyware in the aftermath of its maladministration.

7. References

Access Now (2024). *Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan*, 01 February 2024. Available at: https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/ [last accessed: 16 February 2024].

Agence Europe. *'Europe Daily Bulletin* ', Brussels: Agence Europe S.A.

Amnesty International (2021). *Hungary: The government must provide a meaningful response to the Pegasus scandal*. Amnesty International, Press Release, 20 July 2021. Available at: https://www.amnesty.org/en/latest/press-release/2021/07/hungary-the-government-must-provide-a-meaningful-response-to-the-pegasus-scandal/ [last accessed: 30 November 2023].

Anstis, S., Böcü, G., Campo, E., Deibert, R., Marczak, B., Razzak, B. A., Scott-Railton, J. and Solimano, S. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*. The Citizen Lab, Research Report #113, 18 April 2022. Available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ [last accessed: 30 November 2023].

Bajak, F. and Gera, V. (2021). *AP Exclusive: Polish opposition duo hacked with NSO spyware*. The Associated Press (AP), 21 December 2021. Available at: https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e [last accessed: 30 November 2023].

Baruch, J. and Leloup, D. (2023). *In Cyprus, a cyber-surveillance conglomerate benefits from legal opacity and tax optimization*. Le Monde, 16 November 2023. Available at: https://www.lemonde.fr/en/investigations/article/2023/11/16/in-cyprus-a-cyber-surveillance-conglomerate-benefits-from-legal-opacity-and-tax-optimization_6261166_231.html [last accessed: 31 December 2023].

Bayer, L. (2018). *Israeli intelligence firm targeted NGOs during Hungary's election campaign*. Politico, 06 July 2018. Available at: https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ [last accessed: 30 November 2023].

Bayer, L. (2021). *Hungarian spyware scandal bolsters fears of Orbán critics*. Politico, 19 July 2021. Available at: https://www.politico.eu/article/hungarian-spyware-scandal-bolsters-fears-of-orban-critics/ [last accessed: 30 November 2023].

Becatoros, E. (2022). *Greece's intelligence chief resigns amid spyware scandal*. The Associated Press (AP), 05 August 2022. Available at: https://apnews.com/article/technology-greece-software-spyware-2c42b9496f7b3e227080daba150c86c6 [last accessed: 30 November 2023].

Bennett, A. and Checkel, J. T. (2014). Process tracing: From philosophical roots to best practices. In Bennett, A. and Checkel, J. T. (eds.) *Process Tracing: From Metaphor to Analytic Tool*, Cambridge: Cambridge University Press, pp. 3-38.

Bennett, A., and Checkel, J. T. (eds.). (2014). *Process Tracing: From Metaphor to Analytic Tool*, Cambridge: Cambridge University Press.

Bergman, R. and Mazzetti, M. (2022). *The Battle for the World's Most Powerful Cyberweapon*. New York Times, 31 January 2022. Available at www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [last accessed: 23 December 2023].

Bergman, R., Mazzetti, M. and Stevis-Gridneff, M. (2023). *How the Global Spyware Industry Spiraled Out of Control*. The New York Times, 08 December 2022. Available at: https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html [last accessed: 30 November 2023].

Birnbaum, M., Chastand, J.-B. and Pethő, A. (2021a). *In Orban's Hungary, spyware was used to monitor journalists and others who might challenge the governmen*t. The Washington Post, 19 July 2021. Available at: https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ [last accessed: 30 November 2023].

Birnbaum, M., Harwell, D., Sabbagh, D. and Timberg, C. (2021b). O*n the list: Ten prime ministers, three presidents and a king*. The Washington Post, 20 July 2021. Available at: https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/ [last accessed: 03 March 2024].

Bundesministerium der Justiz (2017). *Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017* [1354]. Bundesgesetzblatt, Jahrgang 2017, Teil I, Nr. 33. Available at: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27943142%27%5D&skin=pdf&tlevel=-2&nohist=1&sinst=9672FD22 [last accessed: 31 December 2023].

Burns, C. (2019). The European Parliament. In Cini, M. and Pérez-Solórzano Borragán, N. (eds.) (2019). *European Union Politics*, 6th Edition, Oxford: Oxford University Press, pp. 177-188.

Cerulus, L. (2021). *Polish spyware scandal stokes tensions with Brussels*. Politico, 21 December 2021. Available at: https://www.politico.eu/article/polish-spyware-scandal-stokes-up-tensions-with-eu/ [last accessed: 30 November 2023].

Cienski, J. (2021). *Polish opposition politician accuses government of phone hack*. Politico, 24 December 2021. Available at: https://www.politico.eu/article/poland-opposition-politician-accuses-government-phone-hack-krzysztof-brejza/ [last accessed: 30 November 2023].

Cini, M. (2015). The European Commission after the reform. In Magone, J. M. (ed.), (2015). *Routledge Handbook of European Politics*. London and New York: Routledge, pp. 235-247.

Cini, M. (2019). Intergovernmentalism. In Cini, M. and Pérez-Solórzano Borragán, N. (eds.) *European Union Politics*, 6th Edition, Oxford: Oxford University Press, pp. 69-82.

Cini, M. and Pérez-Solórzano Borragán, N. (eds.) (2019). *European Union Politics*, 6th Edition, Oxford: Oxford University Press.

Collier, D. (2011). *Understanding Process Tracing*. PS, Political Science & Politics, 44 (4), pp. 823-830.

Consolidated version of the Treaty on European Union [2012] OJ C326/13 (TFEU). Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF [last accessed: 13 January 2024].

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU). Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN [last accessed: 13 January 2024].

Council of the European Union (2023). *Presidency conclusions – The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 21 October 2020 [11481/20]. Available at: https://www.consilium.europa.eu/media/46496/st11481-en20.pdf [last accessed: 29 December 2023].

Cutler, S. and Pegg, D. (2021). *What is Pegasus spyware and how does it hack phones*?. The Guardian, 10 July 2021. Available at: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [last accessed: 06 March 2024].

Datzer, V. and Lonardo, L. (2023). *Genesis and evolution of EU anti disinformation policy: entrepreneurship and political opportunism in the regulation of digital technology*. Journal of European Integration, 45 (5), pp. 751-766.

De Burca, G. (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator. *Maastricht Journal of European and Comparative Law MJ*, *20* (2), pp. 168–184.

Deibert, R., Marczak, B., McKune, S., Scott-Railton, J., and Razzak, B.A. (2018). *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, CitizenLab Research Report No. 113, University of Toronto, September 2018. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ [last accessed: 29 December 2023].

Demosthenes, I. and Niemann, A. (2015). *European economic integration in times of crisis: a case of neofunctionalism?*. Journal of European Public Policy, 22 (2), pp. 196-218.

Denman, D. (2014). *The EU Charter of Fundamental Rights: How Sharp are its Teeth?*. Judicial Review : JR : Mapping the Developing Law and Practice of Judicial Review., 19 (3), pp. 160–172.

Deutsche Welle (2021). *Hungary admits to using Pegasus spyware*. Deutsche Welle, 11 April 2021. Available at: https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217 [last accessed: 30 November 2023].

Deutsche Welle (2022). *Polish leader admits government bought spyware*. Deutsche Welle, 01 July 2022. Available at: https://www.dw.com/en/poland-top-leader-admits-government-bought-pegasus-spyware/a-60361211 [last accessed: 30 November 2023].

Egeberg, M. (2019). The European Commission. In Cini, M. and Pérez-Solórzano Borragán, N. (eds.) *European Union Politics*. 6th Edition. Oxford: Oxford University Press, pp. 143-156.

European Commission (2022). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2022 Rule of Law Report* [COM(2022) 500 final], 13 July 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0500 [last accessed: 24 May 2024].

European Commission (2023a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of*

the Regions, 2023 Rule of Law Report [COM(2023) 800 final], 05 July 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0800&qid=1707693839666 [last accessed: 02 February 2024].

European Commission (2023b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On Defence of Democracy [COM(2023) 630 final]*, 12 December 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0800&qid=1707680803492 [last accessed: 02 February 2024].

European Parliament (2022). *PEGA: Hearing on 'Use of spyware in Poland'*. European Parliament, Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 15 September 2022. Available at: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220915-0900-COMMITTEE-PEGA [last accessed: 30 November 2023].

European Parliament (2023a). *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware* (2023/2500(RSP)) [P9_TA(2023)0244]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf [last accessed: 17 June 2023].

European Parliament (2023b). *European Parliament resolution of 23 November 2023 on the lack of legislative follow-up by the Commission to the PEGA resolution* (2023/2988(RSP)) [P9_TA(2023)0440]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0440_EN.pdf [last accessed: 15 January 2024].

European Parliament (2023c). *Plenary Session, 15 June 2023*. Available at: https://multimedia.europarl.europa.eu/en/webstreaming/plenary-session_20230615-0900-PLENARY [last accessed: 17 June 2023].

European Union (2021). *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*. Official Journal of the European Union [L 206-1-461], 1 June 2021. Available at: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=CELEX%3A32021R0821&qid=1718707367430 [last accessed: 09 April 2024].

Farrow, R. (2022). *How Democracies Spy on Their Citizens*. The New Yorker, 18 April 2022. Available at: www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens [last accessed: 21 December 2023].

Feldstein, S. and Youngs, R. (2023). *Pegasus and the EU's external relations*. European Parliamentary Research Service (EPRS), January 2023. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)741475 [last accessed: 26 March 2023].

Frantziou, E. (2015). *The Horizontal Effect of the EU Charter of Fundamental Rights: Rediscovering the Reasons for Horizontality*. European Law Journal Review of European Law in Context, 21 (5), pp. 657–679.

Fromage, D. (2020). *The European Parliament's Right of inquiry in context. A comparison of the national and the European legal frameworks*. European Parliament, Directorate-General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, March 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648708/IPOL_STU(2020)648708_EN.pdf [last accessed: 03 March 2024].

Gallego, A. (2022). Letter from the Director-General Justice and Consumers to H.E. Ambassador Danielsson [JUST.C.3/CS/ks(2022)9917600], 21 December 2023. Available at: https://cdn.netzpolitik.org/wp-upload/2023/04/Spyware-mapping-excercise-EU-Commission-letter.pdf [last accessed: 7 February 2024].

González, M. (2020). *Spain's intelligence service has spyware program that targeted Catalan politicians*. El País, 16 July 2020. Available at: https://english.elpais.com/politics/catalonia_independence/2020-07-16/spains-intelligence-service-has-spyware-program-that-targeted-catalan-politicians.html# [last accessed: 30 November 2023].

Guerrini, F. (2023). *Pegasus Spyware Scandals Highlight Global Dangers As Activists Demand Action*. Forbes, 24 September 2023. Available at: https://www.forbes.com/sites/federicoguerrini/2023/09/14/pegasus-spyware-scandals-highlight-global-dangers-as-activists-demand-action/ [last accessed: 30 November 2023].

Gurijala, B. (2021). *What Is Pegasus? How Surveillance Spyware Invades Phones*. Scientific American, 9 August 2021. Available at: https://www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/ [last accessed: 29 December 2023].

Hammoud, R. and Krapiva, N. (2023). *Hacking Meduza: Pegasus spyware used to target Putin's critic*. Access Now, 13 September 2023. Available at: https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/ [last accessed: 31 December 2023].

Hanfeld, M. (2023). *Ex-Manager von Finfisher werden angeklagt*. Frankfurter Allgemeine Zeitung, 23 May 2023. Available at: https://www.faz.net/aktuell/feuilleton/medien/tuerkei-verkaufte-finfisher-spionagesoftware-an-den-geheimdienst-18913191.html [last accessed: 30 November 2023].

Harris, S., Kirchgaessner, S., Mekhennet, S., Nakashima, N. and Timberg, C. (2022). *Israel blocked Ukraine from getting potent Pegasus spyware*. The Washington Post, 23 March 2022. Available at: https://www.washingtonpost.com/technology/2022/03/23/urkraine-spyware-pegasus-russia/ [last accessed: 30 November 2023].

Harwell, D. (2021). *How Washington power brokers gained from NSO's spyware ambitions*. The Washington Post, 19 July 2021. Available at: https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/ [last accessed: 09 April 2024].

Howell O'Neill, P. (2019). *The fall and rise of a spyware empire*, MIT Technology Review, 29 November 2019. Available at: https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/ [last accessed: 03 March 2024].

In t'Veld, S. (2023). *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))* [A9-0189/2023]. European Parliament, Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, 22 May 2023. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html [last accessed: 14 January 2024].

Jones, S. (2020). *Spanish government denies spying on Catalan leaders*. The Guardian, 19 July 2020. Available at: https://www.theguardian.com/world/2020/jul/19/spanish-government-denies-spying-on-catalan-leaders [last accessed: 30 November 2023].

Jones, S. (2022a). *Catalans demand answers after Spanish spy chief confirms phone hacking*. The Guardian, 05 May 2022. Available at:

https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking [last accessed: 30 November 2023].

Jones, S. (2022b). *Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy'*. The Guardian, 15 May 2022. Available at: https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy [last accessed: 30 November 2023].

Kambas, M. (2022). *Cyprus MPs launch inquiry into spyware development on the island*. Reuters, 09 November 2022. Available at: https://www.reuters.com/world/middle-east/cyprus-mps-launch-inquiry-into-spyware-development-island-2022-11-09/ [last accessed: 30 November 2023].

Kirchgaessner, S. (2023). Ru*ssian news outlet in Latvia believes European state behind phone hack*. The Guardian, 25 September 2023. Available at: https://www.theguardian.com/world/2023/sep/25/latvia-russia-meduza-phone-hack-galina-timchenko [last accessed: 31 December 2023].

Klingert, L. (2022). *Belgian police reveal use of controversial Pegasus spyware*. The Brussels Times, 21 April 2022. Available at: https://www.brusselstimes.com/218350/belgian-police-use-controversial-pegasus-spyware [last accessed: 30 November 2023].

Kot, B. and Feldstein, S. (2023). Why *Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*. Carnegie Endowment, 14 March 2023. Available at: https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf [last accessed: 29 December 2023].

Lavenex, S. (2020). Justice and Home Affairs. In Pollack, M., Roederer-Rynning, C., Wallace, H., and Young, A. (eds.) *Policy-Making in the European Union*. 8th Edition. Oxford: Oxford University Press, pp. 343-362.

Leloup, D. (2023). Snowden revelations: Ten years on, where are the protagonists now?. Le Monde, 06 June 2023. Available at: https://www.lemonde.fr/en/pixels/article/2023/06/06/snowden-revelations-ten-years-on-where-are-the-protagonists-now_6029230_13.html [last accessed: 26 May 2024].

Leloup, D. and Untersinger, M. (2021a). *«Projet Pegasus»: un téléphone portable d'Emmanuel Macron dans le viseur du Maroc*. Le Monde, 20 July 2021. Available at: https://www.lemonde.fr/projet-pegasus/article/2021/07/20/projet-pegasus-un-telephone-

portable-d-emmanuel-macron-dans-le-viseur-du-maroc_6088950_6088648.html [last accessed: 30 November 2023].

Leloup, D. and Untersinger, M. (2021b). *Malgré les approches de NSO Group, la France a choisi à la fin de 2020 de ne pas acheter le logiciel espion Pegasus*. Le Monde, 26 November 2021. Available at: https://www.lemonde.fr/pixels/article/2021/11/26/malgre-les-approches-de-nso-group-la-france-a-choisi-a-la-fin-de-2020-de-ne-pas-acheter-le-logiciel-espion-pegasus_6103783_4408996.html [last accessed: 30 November 2023].

Lenaerts, K. (2012). *Exploring the Limits of the EU Charter of Fundamental Rights*. European Constitutional Law Review, 8 (3), pp. 375–403.

Loreggia, A. and Sartor, G. (2022). *The impact of Pegasus on fundamental rights and democratic processes*. European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, December 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740514 [last accessed: 26 March 2023].

Magone, J. M. (ed.) (2015). *Routledge Handbook of European Politics*. London and New York: Routledge.

Mahoney, J. (2010). *After KKV: The New Methodology of Qualitative Research*. World Politics, 62(1), 120–147.

Mahoney, J. (2015). *Process Tracing and Historical Explanation*. Security Studies, 24 (2), pp. 200-218.

Manancourt, V. (2022a). *Brussels, EU governments on collision course over Pegasus spyware*. Politico, 15 February 2022. Available at: https://www.politico.eu/article/brussels-eu-government-collision-course-pegasus-spyware/ [last accessed: 09 April 2024].

Manancourt, V. (2022b). Pegasus' complex structure hinders EU spyware probe. Politico, 20 May 2022. Available at: https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/ [last accessed: 09 April 2024].

Manancourt, V. and Van Sant, S. (2022). *EU spyware probe has a problem: Spain*. Politico, 28 November 2022. Available at: https://www.politico.eu/article/hungarian-spyware-scandal-bolsters-fears-of-orban-critics/ [last accessed: 30 November 2023].

Maciejewski, and Marzocchi, O. (2023). *Pegasus and the EU's external relations*. European Parliamentary Research Service (EPRS), January 2023. Available at:

https://www.europarl.europa.eu/RegData/etudes/STUD/2023/741475/IPOL_STU(2023)741475_EN.pdf [last accessed: 26 March 2023].

Marzocchi, O. and Mazzini, M. (2022). *Pegasus and surveillance spyware*, European Parliamentary Research Service (EPRS), May 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_IDA(2022)732268 [last accessed: 26 March 2023].

Mascolo, G. and Obermaier, F. (2021). *Auch BND nutzt umstrittene Pegasus-Überwachungssoftware*. Süddeutsche Zeitung, 08 October 2021. Available at: https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974 [last accessed: 30 November 2023].

Mazey, S., and Richardson, J. J. (eds.) (2015). *European Union: power and policy-making*, 4th Edition, London and New York: Routledge.

McCormick, J. (2017). Understanding the European Union: a concise introduction, 7th Edition, London: Palgrave Macmillan.

Mekhennet, S., Priest, D. and Timberg, C. (2021). *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*. Washington Post, 18 July 2021. Available at: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ [last accessed: 03 March 2024].

Meister, A. (2019). *Berlin hat den Staatstrojaner FinFisher gekauft, wir veröffentlichen den Vertrag*. Netzpolitik.org, 05 August 2019. Available at: https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/ [last accessed: 30 November 2023].

Mildebrath, H. (2022a). *Europe's PegasusGate: Countering spyware abuse*, European Parliamentary Research Service (EPRS), July 2022. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729397 [last accessed: 25 March 2023].

Mildebrath, H. (2022b). *Greece's Predatorgate: The latest chapter in Europe's spyware scandal?*. European Parliamentary Research Service (EPRS), September 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf [last accessed: 30 November 2023].

Ministry of Foreign Affairs of Finland (2022). *Ministry for Foreign Affairs has solved suspected espionage case*. Press Release, 28 January 2022. Available at: https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/ulkoministerio-on-saanut-selvitettya-siihen-kohdistuneen-vakoilutapauksen [last accessed: 30 November 2023].

Modderkolk, H. (2022). *AIVD gebruikt omstreden Israëlische hacksoftware*. deVolkskrant, 02 June 2022. Available at: https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/ [last accessed: 30 November 2023].

Newman, A. L. (2020). *Digital Policy-Making in the European Union*. In Pollack, M., Roederer-Rynning, C., Wallace, H., and Young, A. (eds.) *Policy-Making in the European Union*, 8th Edition, Oxford: Oxford University Press, pp. 275-296.

Nielsen, N. (2023). *MEPs probing spyware 'stonewalled' by EU states*. EUObserver, 17 March 2023. Available at: https://euobserver.com/eu-political/156844 [last accessed: 30 November 2023].

Panyi, S. (2022). *The inside story of how Pegasus was brought to Hungary*. Direkt36, 28 September 2022. Available at: https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/ [last accessed: 30 November 2023].

Pfenniger, K. (2023). *Pegasus Project: What has happened since the revelations*. Forbidden Stories, 17 July 2023. Available at: https://forbiddenstories.org/pegasus-project-impacts-map/ [last accessed: 30 November 2023].

Raunio, T. (2015). The European Parliament. In Magone, J. M. (ed.), (2015). *Routledge Handbook of European Politics*. London and New York: Routledge, pp. 248-262.

Realfonzo, U. (2023). *Focus turns to Belgium over spyware use*. The Brussels Times, 13 October 2023. Available at: https://www.brusselstimes.com/737599/focus-turns-to-belgium-over-spyware-use [last accessed: 30 November 2023].

Reh, C. and Wallace, H. (2019). An Institutional Anatomy and Five Policy Modes. In Pollack, M., Roederer-Rynning, C., Wallace, H., and Young, A. (eds.) *Policy-Making in the European Union*, 8th Edition, Oxford: Oxford University Press, pp. 67-106.

Riecke, L. (2023). *Unmasking the term 'dual use' in EU spyware export control*. European Journal of International Law, 34 (3), pp. 697–719.

Rittberger, B. and Schimmelfennig, F. (2015). The EU as a system of differentiated integration. In *European Union*, 4th Edition, Routledge, pp. 33–62.

Russi, A. (2023). How Europe became the Wild West of spyware. Politico, 25 October 2023. Available at: https://www.politico.eu/article/how-europe-became-wild-west-spyware/ [last accessed: 30 November 2023].

Samaras, G. (2022). *Greece's 'Watergate' explained: why the European Parliament is investigating over a wiretapping scandal*. The Conversation, 08 November 2022. Available at: https://theconversation.com/greeces-watergate-explained-why-the-european-parliament-is-investigating-over-a-wiretapping-scandal-192537 [last accessed: 30 November 2023].

Schimmelfennig, F. (2018). Theorien der europäischen Integration. In Becker, P. and Lippert, B. (eds.) *Handbuch Europäische Union*. Wiesbaden: Springer VS, pp. 1-23.

Schmitter, P. C. (1969). *Three Neo-Functional Hypotheses About International Integration*. International Organisation, 23 (1), pp. 161-166.

Schmitz, F. (2022). *Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not*. Tagesspiegel, 04 September 2022. Available at: https://www.tagesspiegel.de/politik/ein-abhorskandal-bringt-athens-regierung-in-not-8605792.html [last accessed: 30 November 2023].

Scott-Railton, J., Anstis, S., Böcü, G., Campo, E., Deibert, R., Marczak, B., Razzak, B. A. and Solimano, S. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans using Pegasus and Candiru*. Citizen Lab, 18 April 2022. Available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ [last accessed: 29 December 2023].

Spaventa, E. (2018). *Should we "harmonize" fundamental rights in the EU? Some reflections about minimum standards and fundamental rights protection in the EU composite constitutional system*. Common Market Law Review, 55 (4), pp. 997–1023.

Spike, J. (2021). *Hungarian official: Government bought, used Pegasus spyware*. The Associated Press (AP), 04 November 2021. Available at: https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 [last accessed: 30 November 2023].

Stamouli, N. (2022a). *Greece's spyware scandal expands further*. Politico, 05 November 2022. Available at: https://www.politico.eu/article/greece-spyware-scandal-cybersecurity/ [last accessed: 30 November 2023].

Stamouli, N. (2022b). *PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal*. Politico, 05 August 2022. Available at: https://www.politico.eu/article/spying-scandal-envelop-top-greek-government/ [last accessed: 30 November 2023].

Stamouli, N. (2022c). *Spying scandal clouds Greece's political future*. Politico, 13 September 2022. Available at: https://www.politico.eu/article/greece-kyriakos-mitsonakis-spying-scandal-clouds-greeces-political-future/ [last accessed: 30 November 2023].

Stamouli, N. and Van Sant, S. (2022). *Probe slams '4 or 5' EU governments for spyware use*, POLITICO, 08 November 2022. Available at: https://www.politico.eu/article/eu-spyware-probe-slams-government-leaders-as-perpetrators-of-abuse/ [last accessed 28 September 2023]. (pages as printed by author)

Stark, H. (2009). *BND infiltrierte Tausende Computer im Ausland*. SPIEGEL, 07 March 2009. Available at: https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html [last accessed: 30 November 2023].

Stark, H. (2021). *BKA kaufte heimlich NSO-Spähsoftware*. ZEIT Online, 07 September 2021. Available at: https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-nso-israel-bundeskriminalamt-kauf-innenauschuss-bundestag-unterrichtung [last accessed: 30 November 2023].

Stone Sweet, A. and Sandholtz, W. (1997). *European integration and supranational governance*. Journal of European Public Policy, 4 (3), pp. 297-317.

Strøby Jensen, C. (2019). Neo-Functionalism. In Cini, M. and Pérez-Solórzano Borragán, N. (eds.) *European Union Politics*, 6th Edition, Oxford: Oxford University Press, pp. 55-68.

Stuart Leeson, S. (2022). *Dutch intelligence service allegedly uses Pegasus hacking software*. Euractiv, 03 June 2022. Available at: https://www.euractiv.com/section/politics/short_news/dutch-intelligence-service-allegedly-uses-pegasus-hacking-software/ [last accessed: 30 November 2023].

Süddeutsche Zeitung (2021). *Bundeskriminalamt verwendet "Pegasus"*. Süddeutsche Zeitung, 07 September 2021. Available at: https://www.sueddeutsche.de/politik/cybersicherheit-bundeskriminalamt-verwendet-pegasus-1.5404002 [last accessed: 30 November 2023].

Szpunar, M. (2020). *Reconciling new technologies with existing EU law – Online platforms as information society service providers*. Maastricht Journal of European and Comparative Law, 27 (4), pp. 399–405.

Tar, J. (2023). *How Cyprus became the EU launchpad of Israel's spyware companies*. Euractiv, 14 June 2023. Available at: https://www.euractiv.com/section/cybersecurity/news/how-cyprus-became-the-eu-launchpad-of-israels-spyware-companies/ [last accessed: 30 November 2023].

Taylor, A. (2023). *Malta among states lobbying to allow spyware use against journalists*. Euractiv, 13 December 2023. https://www.euractiv.com/section/politics/news/malta-among-states-lobbying-to-allow-spyware-use-against-journalists/ [last accessed: 31 December 2023].

Van Evera, Stephen. 1997. *Guide to Methods for Students of Political Science*. Ithaca, NY: Cornell University Press.

Vanttinen, P. (2022). *Finnish diplomats fall victim to cyber espionage*. Euractiv, 31 January 2022. Available at: https://www.euractiv.com/section/politics/short_news/finnish-diplomats-fall-victim-to-cyber-espionage/ [last accessed: 30 November 2023].Walker, S. (2021). *Viktor Orbán using NSO spyware in assault on media, data suggests*. The Guardian, 18 July 2021. Available at: https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests [last accessed: 30 November 2023].

Wanat, Z. (2022). *Poland's Watergate: Ruling party leader admits country has Pegasus hacking software*. Politico, 07 January 2022. Available at: https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/ [last accessed: 30 November 2023].

Washington Post, The (2021). *Response from NSO Group to the Pegasus Project*. The Washington Post, 18 July 2021. Available at: https://www.washingtonpost.com/investigations/2021/07/18/nso-group-response-pegasus-project/ [last accessed: 14 October 2023].

Wonka, A. (2015). The European Commission. In Mazey, S., and Richardson, J. J. (eds.) (2015). *European Union: power and policy-making*, 4th Edition, London and New York: Routledge, pp. 83-105.