Bachelor Thesis

B.Sc. Joint Degree "*Public Governance across Borders*"

University of Twente,

Drienerlolaan 5, 7522 NB Enschede, the Netherlands.

University of Münster,

Schlossplatz 2, 48149 Münster, Germany.

Bachelor Circle 3: Socio-Political Aspects of Digital Governance

1st Supervisor: Dr. Azadeh Akbari Kharazi

2nd Supervisor: Dr. A.J.J. Meershoek

Regulating The Invisible Spy

– A Case Study of the Pegasus Spyware examining Surveillance Technology Regulation

Name:

Laura Cristina Dieterle

Wordcount: 11.881 words

Date: 28th of June 2023

WWU MÜNSTER

UNIVERSITY OF TWENTE.

Abstract

This case study of Pegasus Spyware has extensively analysed literature, legal frameworks, judiciary evaluations, and stakeholder dynamics to address the research question regarding technology regulatory bodies' responses to challenges posed by surveillance technologies, particularly the Pegasus Spyware. The findings, based on publicly available documents in governmental databases, reveal that regulatory bodies have acknowledged the need to address the misuse of Pegasus and similar spyware and have identified gaps in existing regulatory frameworks. They identify members of civil society as emerging stakeholders, emphasizing the importance of control mechanisms and the role of “watchdogs” in uncovering and publishing misuse, done by demanding, among others, judicial review, and accountability from both corporate and governmental entities. While the EU as a regional stakeholder has conducted investigations to fill regulatory gaps, the UN as an international stakeholder has recommended a global moratorium on the sale, transfer, and use of surveillance technology until compliance with universal rights and freedoms is assured. National regulatory bodies have responded differently within their respective contexts, and private regulatory bodies, like the NSO Group, face tensions between business interests and upholding human rights. The research underscores the interconnectedness between flawed surveillance technology regulation and the potential chilling effects on human rights.

Contents

List of Images, Tables, Figures, and Abbreviations 1
1. Introduction 2
1.1 Case Background 2
1.2 Research Question and Sub-Questions 3
1.3 Scientific and Societal Relevance 4
2. Literature Review 6
2.1 Technology Regulation 6
2.1.1 Surveillance and Surveillance Technology 6
2.1.2 Surveillance Technology Regulation 7
2.2 Background on the Case of the Pegasus Spyware and the NSO Group 9
2.3 Legal Framework Review: Existing Regulations and Laws 10
2.4 Judicial Review 15
3. Methodology 16
3.1 Description of the Approach 16
3.2 Method of Data Collection 16
3.3 Methods of Data Analysis 17
3.3.1 Stakeholder Analysis 17
3.3.2 Court Case Review 18
4. Analysis: Case Study of the Pegasus Spyware 19
4.1. Stakeholder Analysis 19
4.1.1 Civil Society 19
4.1.2 International and Regional Organizations 20
4.1.3 Governments 23
4.1.4 Private entities 25
4.2 Court Cases 25
5. Discussion of the Findings 29
6. Conclusion 34
7. References 37
Appendix A 41
Appendix B 42

List of Images, Tables, Figures, and Abbreviations

Images

Image 1	*The way Pegasus works on mobile devices.* Srivastava & Bradshaw, 2019

Tables

Table 1	*Legal framework regarding surveillance technology regulation on the national, regional, and international level.* Own presentation

Figures

Infographic 1	*Demands by plaintiffs, infographic based on Table B1, Appendix B* Own presentation

Abbreviations

NSO Group	*NSO Group Technologies limited, and Q Cyber Technologies limited.*
PEGA	*Pegasus Committee.*
UN	*the United Nations.*
EU	*the European Union.*
UK	*the United Kingdom of Great Britain and Northern Ireland.*
USA	*the United States of America.*
i.e.	*id est.*
PA	*Public Administration.*
ICCPR	*International Covenant on Civil and Political Rights.*
Convention 108+	*Convention for the Protection of Individuals regarding Automatic Processing of Personal Data*

1. Introduction

"When […] technology is sold to a government without sufficient oversight, it will eventually be misused" (Scott-Railton et al., 2017, p.28).

This citation from a Citizen Lab Report in 2017, has shown to be widely accurate for the usage of the Pegasus spyware, an intrusive interceptive surveillance technology, distributed by the NSO Group. The NSO Group, a public Israeli-based cyber-technology firm, is mostly known for the invention and distribution of Pegasus spyware (Chawla, 2021). Pegasus is a highly intrusive, practically undetectable spyware, capable of remote zero-click surveillance of smartphones and mobile devices (Chawla, 2021). Its intrusiveness becomes visible by its capability of remotely accessing personal core identity data, by intruding data saved in the mobile cloud, without the target's awareness of this (Marczak et al., 2023; Marx, 2021). This kind of surveillance technology has shown to be vulnerable to unlawful use, especially in connection to fundamental rights and freedoms (Richard, 2022).

Technologies, furthermore, tend to emerge faster than regulatory b*odies can establish control mechanisms or integrate them into legal frameworks (Fenwick et al., 2017). This bachelor thesis aims to map and interpret relevant regulatory stakeholder responses regarding the challenges of regulating surveillance technology by investigating the case of Pegasus spyware.

1.1 Case Background

The case which is subject to this research is Pegasus spyware, an intrusive cyber-surveillance technology, that is designed to access data undetected on mobile devices. This spyware has been subject to a major investigative journalistic publication, in which a critically high number of Pegasus abuses have been uncovered. These misuses were frequently linked to human rights violations, since Pegasus has been used, among others, against members of the press, human rights activists, businesspeople, oppositional political leaders, and even lawyers (Richard, 2022). Since the NSO Group only sells its spyware to governments, the explanation of governmental misuse of surveillance technology seems to be evident (Richard, 2022). Regulation in this area can be described as untransparent, and fragmented, enabling misuse and creating an unregulated environment (Burton, 2023). Ball et al. establish that there are

available institutional possibilities to effectively regulate surveillance technology, which will be investigated in the scope of this research (2012).

There is a broad range of publications on Pegasus from numerous disciplinary approaches. They have frequently issued the company creating Pegasus, i.e., the NSO Group, modus operandi (Kaster & Ensign, 2022), investigations of whom the spyware is sold to (Marczak et al., 2023), or what implication these kinds of espionage tools might have on international law (Alexander & Krishna, 2022; Burton, 2023). However, there is little existing research on how regulatory bodies on national, regional, and international levels have reacted to the misuse of this surveillance technology and how these regulatory mechanisms work.

1.2 Research Question and Sub-Questions

With these considerations in mind, a research question, as well as a set of sub-questions, are formulated. Thus, *To what extent are technology regulatory bodies responding to challenges posed by surveillance technologies, regarding the Pegasus Spyware, considering the national constitutions, regional agreements, and universal rights and freedoms?*, is the research question aimed to be answered in the scope of this bachelor thesis. The focus thereby lies on identifying relevant stakeholders and their position within global regulatory responses, considering the private as well as the public sphere. Due to the notion of Pegasus being used by national governments since it is only distributed to governments, sub-question one has been formulated: *How are national governments and courts responding to documented misuse of Pegasus?* To further put the issue of cyber-surveillance technology in global scope, sub-question two has been formulated: *How are the European Union, as a regional stakeholder, and the UN, as an international stakeholder, responding to documented misuse of Pegasus?* Since civil society has had a crucial role in uncovering the misuse and these publications have evoked a discourse regarding public companies selling intrusive spyware, sub-question three has been established: *Are private entities and civil society responding to misuses of Pegasus, if yes, how?* The misuse of surveillance technology by governmental agencies has different notions. It implies gaps in regulatory frameworks but simultaneously can have influences on privacy and data protection questions. Thus, sub-question four is formulated: *What implications does the misuse of Pegasus have on universal rights and freedoms?*

The research is designed as a single-case study of the Pegasus spyware. It is thereby focused on the responses of regulatory stakeholders regarding challenges posed by surveillance technology. To map the responses of relevant stakeholders, a stakeholder analysis is conducted, focusing on identifying, differentiating, and categorizing stakeholders into interest groups, and investigating relationships between stakeholders in their function as regulatory bodies. This is done while considering international, regional, and national legal frameworks. Additionally, publicly accessible court cases regarding the Pegasus spyware are mapped and examined to review judicial responses regarding challenges to universal rights and freedoms. Finally, findings from these different approaches are connected to identify relevant gaps in international and regional legal frameworks and evaluate whether judicial reviews have been accurate regulatory measures regarding the misuse of surveillance technology.

Research question and sub-questions:

RQ: To what extent are technology regulatory bodies responding to challenges posed by surveillance technologies, regarding the Pegasus Spyware, considering the national constitutions, regional agreements, and universal rights and freedoms?

SQ1: How are national governments and courts responding to documented misuse of Pegasus?

SQ2: How are the European Union, as a regional stakeholder, and the UN, as an international stakeholder, responding to documented misuse of Pegasus?

SQ3: Are private entities and civil society responding to misuses of Pegasus, if so, how?

SQ4: What implications does the misuse of Pegasus have on universal rights and freedoms?

1.3 Scientific and Societal Relevance

From a scientific perspective within the scope of Public Administration (PA) research, it is important to research regulatory bodies, since the regulation of new technology can be named as an emerging field in PA. Mainstream regulatory mechanisms and processes are not designed to regulate undetectable technology and therefore not fitting for regulation of this kind of intrusive spyware. To adequately regulate surveillance technology, it is crucial to

identify possible gaps and shortcomings in public regulatory frameworks while investigating the influence such technologies might have on universal rights and freedoms. To prevent further misuse of Pegasus and similar surveillance technology, it is essential to evaluate national, regional, and international frameworks regarding surveillance technology. As reports have shown, misuse of Pegasus is frequently connected to human rights violations, which indicates a fragmented regulatory framework (Richard, 2022). To further prevent chilling effects on universal rights and freedoms caused by and connected to surveillance technology, research regarding regulatory mechanisms is crucial. The societal relevance can additionally be observed within the recent EU-adapted resolutions regarding furthering regulation of surveillance technology (in ´t Veld, 2023). The EU has thereby acknowledged gaps regarding the regulation of surveillance technology and put in place a committee to detect those and establish possible ways to address them.

2. Literature Review

To analyze this research question in an adequate scope, it is crucial to examine the existing academic literature. Therefore, a literate review of, for this research relevant topics, has been conducted.

2.1 Technology Regulation

New forms of technology have emerged rapidly over the last decades. In many cases, regulations do not keep up with this fast-changing landscape, which leaves certain aspects of technologies with no or little regulation (Ball et al., 2012). Even though there is almost no aspect of daily life that has not yet been conquered by new technologies, the regulation of these is often left to judiciary branches. When developing legal frameworks and policies concerning this field, it is relevant to consider that the required responses must be adaptable to change, while minimizing risks of harm and including an ethical perspective (Moses, 2015). This cannot be achieved by limiting regulations to singular and very specific technical policy responses, but rather by planning potential risks and including them in a broader policy framework (Moses, 2015). Other scholars suggest shaping policy-making more flexible and inclusive by involving multiple stakeholders, and by that, multiple perspectives from different areas in regulation recommendations, following the French example (Fenwick et al., 2017). The French government has included multiple stakeholders in a conference concerning internet rights in the past, where public officials, private sector actors, and civil society spokespeople had the opportunity to be in dialogue for policy recommendations, allowing all stakeholders to be heard (Ball et al., 2012).

2.1.1 Surveillance and Surveillance Technology

The following paragraph presents a small overview of current academic discussions regarding surveillance and surveillance technology.

Cyber-surveillance can be defined as an information technology mechanism that serves the purpose of surveilling persons, groups of people, institutions, or processes, to impose a certain kind of influence over them, while being operated from data networks (Lyon, 2014). There have been extensive discussions revolving around the term surveillance in the academic sphere, focusing mainly on the way data is collected, by whom, for what surveillance is

conducted, and the intersection between the private and the public sector in the surveillance context (Lyon, 2015).

The need to differentiate between the agent who carries out surveillance, and the subjects, i.e., those who are being surveilled, while considering that these categories can in some instances also merge, for example in a context of co-surveillance, are broadly agreed on within the field (Marx, 2021). The balance of power between the agent and the subject determines, according to Marx, the normative scope of judgment within society (2021). Hence, the targeting of an individual's unique identity (for example an indicator of the current geographical position) or core identity (for example political beliefs) plays a crucial role in the societal acceptance of surveillance, since the surveillance of a person's core identity is perceived as more intrusive (Marx, 2021). Furthermore, according to Marx, surveillance should first and foremost be normatively evaluated from the culture and the context, meaning the situations in which it is used, instead of evaluating it in a bigger and generalized scope (2021).

Consequently, it is crucial to look at international, regional, and national agreements, considering the regulation of surveillance.

2.1.2 Surveillance Technology Regulation

Building upon these insights, the focus will lie on different ways of regulating surveillance technology. The issue of institutionally controlling and regulating surveillance technology has been an ongoing debate in the political as well as the academic community since the 1960s when surveillance technologies first emerged and the private sector, as well as governments, started to have an increased interest in data collection (Ball et al., 2012). The challenges arising from regulating new surveillance technology are numerous and deeply interconnected with human rights issues (Kaldani & Prokopets, 2022).

Regan identifies four different **institutional regulation models** that can proclaim regulatory responses to surveillance technology issues (Bell et al., 2012).

First, and most evident, one must name the **regulation by national governments**, so executive, legislative, and judicial responses to issues of technology regulation. However, when examining national governments, the contextualization of said government is essential, since every state, and therefore its regulatory powers is a product of its political culture,

history, location, and further factors (Ball et al., 2012; Vennesson, 2008). This becomes visible when examining national governments and their institutions, the placement of the institutions, or even the lack of institutions in place to regulate surveillance technology. Scholars argue that, since the government's interest in a strong surveillance apparatus is too high, it is crucial for effective regulating institutions to be independent of the legislative and executive branches (McAllister, 2012). Following this logic, it becomes evident that an independent judiciary branch is a key element of strong protection against new technologies, that have not yet been regulated by the government (Ball et al., 2012).

The second form of institutional regulation Regan introduces is **extra-governmental organizations and regulatory arrangements** such as watchdogs, ombudspersons, and commissions (2012). Within this category, one might introduce the group of civil society. The term “civil society” is widely discussed in academia but will be used in this research for actors who are part of non-governmental institutions and organizations that strengthen the interests and will of citizens (Fenton et al., 2010). Meaning the sphere between state and society inhabited by those promoting civic duties and political rights, for example, independent press, and human rights activists (Fenton et al., 2010). These kinds of non-governmental actors can carry out studies, evaluate new technologies independently and, based on this, make policy recommendations, in the areas of surveillance and privacy (Ball et al., 2012).

Furthermore, **international agreements** play an important role in regulating technological issues, since they oftentimes directly influence national regulations to meet international standards, or are binding treaties between states (Ball et al., 2012).

Another way of regulating surveillance technology is by considering **self-regulation arrangements** by industry. This, however, is a difficult endeavor, since self-regulation can lead to competition and uncertainty, as well as the lack of ethical boundaries, especially in the surveillance sector (Ball et al., 2012). Nevertheless, a combination of self- and government regulation, meaning co-regulation between the private sector and the government has been considered in the past and is still widely discussed among stakeholders. The suggestion of multi-stakeholder approaches includes hearing representatives from multinational enterprises that produce or sell cyber-spyware technologies to cooperate with civil society

groups, such as Amnesty International, as well as state representatives (Chan, 2019). This is done to achieve viable policy recommendations (Chan, 2019).

However, one must add that there is no model among the above-mentioned that fits all states since it is important to acknowledge the differences in the political culture, government structure, and historical influences on surveillance technology policies and regulations in different countries. What can be concluded more generally, is a need for active attention on the institution in charge of regulating surveillance technology, as well as its evolvement (Fenwick et al., 2017).

2.2 Background on the Case of the Pegasus Spyware and the NSO Group

This research focuses on the specific case of Pegasus spyware, a specific interceptive intrusion spyware.

To understand what makes the case of Pegasus different from other surveillance technologies, one must consider two main points.

First, the NSO Group provides and sells Pegasus exclusively to vetted governments for the purpose of "lawful interceptions", such as the detecting of terrorism or pedophilia rings, which have been successfully done in the past (Chawla, 2021). This, however, makes potential misuses difficult regulatory issues, since they indicate governmental misuse, which is rarely detected, and difficult to persecute (Chawla, 2021).

Second, Pegasus can initiate total surveillance on the targeted device, meaning that the spyware can access nearly every part of the targeted "digital life. It is a "zero-link" technology, meaning that the target is not required to click on a link to install the spyware on their device, but the device is infected immediately (Chawla, 2021). The instance Pegasus is installed on the device, NSO lets their clients access the infected devices, giving them access to every digital data the targeted device has ever produced, as well as every current activity performed on the mobile device, including access to geographical and communications data, able to secretly turning on the microphone and camera, as well as providing real-time recordings of the targeted individual (Chawla, 2021; Kaster & Ensign, 2022). This way the usage of Pegasus presents an active decision by the NSO client to subordinate the privacy of an individual by mining all its data. The way Pegasus works is additionally demonstrated in Image 1.

Image 1: *The way Pegasus works on mobile devices.* (Srivastava & Bradshaw, 2019).

The spyware is highly intrusive and only detectable when conducting specific forensic tests on the infected mobile device (Marczak et al., 2023). Since the NSO Group claims to only sell Pegasus to governments, the misuse of this spyware implies that governments might not meet their regulations regarding surveillance technology (NSO Group, 2023). The other implication such abuses have is that the regulatory bodies and regulations in place are not strong enough to avoid misuse. These misuses, furthermore, have implications for the human rights situations in according countries since the right to privacy and other fundamental rights are put in question (Rueckert, 2021).

The Forbidden Stories consortium, which uncovered the scope of misuse, is an important factor within the case of Pegasus, due to the revelations around their journalistic work, which has impacted several policy decisions and put the issue of surveillance technology on the global agenda.

2.3 Legal Framework Review: Existing Regulations and Laws

To analyze which regulation and protection mechanisms are in place and to demonstrate, that the issue of surveillance technology is a global one, a summary of legal regulations regarding surveillance technology has been conducted on international, regional, and national levels,

which is illustrated in detail in Table 1. It is observable that all cases demonstrated have laws and regulations in place to safeguard privacy and regulate surveillance technologies. However, even with these regulations in place, violations by Pegasus Spyware were not isolated incidents (Richard, 2022). Due to the limited scope of this research, there will not be an extensive elaboration on all regulations, and a focus will lie on international agreements since these have the most influence on global developments.

India, the UK, Spain, Greece, Mexico, Saudi Arabia, Israel, and the USA, have been selected to demonstrate that the challenges surveillance technology regulation pose, are global issues (Alexander & Krishna, 2022). Moreover, these countries have been selected due to their connection with the Pegasus spyware. There have been documented misuses in India, Spain, Mexico, the UK, India, the USA, Israel, and Saudi Arabia, while there are additionally pending lawsuits in the UK, India, and the USA concerning Pegasus and the NSO Group (Richard, 2022). Greece has not experienced Pegasus misuse, but issues with similarly intrusive surveillance spyware. Israel, the country from which Pegasus is distributed, is featured as well.

The following international agreements influence national legislation regarding surveillance technology regulation.

Firstly, the **International Covenant on Civil and Political Rights (ICCPR),** emphasizes the right to privacy and freedom of expression, which legally binds governments and regulatory bodies to use surveillance technology with the principles of legality and expresses that states must apprehend their duty to protect human rights (Alexander & Krishna, 2022; *International Covenant on Civil and Political Rights*, 1967). Secondly, the **Budapest Convention on Cybercrime** is a binding treaty and emphasizes the fight against cybercrime. Similar to the ICCPR, it does not directly regulate surveillance technology but rather implies regulations for them in a cybercrime context. These are mainly the criminalization of cybercrime impacting the usage of surveillance technology in investigations. It further emphasizes data protection and privacy, which impacts the use of surveillance technology (*Convention on Cybercrime*, 2001; Le Nguyen & Golman, 2021). Thirdly, the **Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (Convention 108),** and the amendment of this**, Convention 108+**, are legally binding international treaties, that safeguard and protect data. After the amendment, individual rights are more emphasized, empowering individuals to exercise stronger control over their data (Alexander & Krishna, 2022; Convention 108 +:

Convention for the Protection of individuals regarding the processing of Personal Data, 2018). Fourthly, the **Wassenaar Arrangement,** regulates export controls for conventional arms and dual-use goods and technologies, meaning civilian, as well as military goods and technology, in a non-binding way (Alexander & Krishna, 2022; Kaster & Ensign, 2022; *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, 1995). The objective is to ensure the responsible and transparent transfer of these items, so they do not contribute to destabilizing regional or international security, but since not all states have incorporated the arrangement into national legislation yet, or are even part of it, there has been inconsistency in controlling states acquiring dual-use technologies (Alexander & Krishna, 2022). There are, furthermore, reasonable doubts about whether the Pegasus spyware can be seen as dual-use technology. While some categorize Pegasus as a cyberweapon, which would make it part of the Agreement, Israel, if it was part of the Arrangement would have to decide whether this was the case for Pegasus and act accordingly (Burton, 2023). It is further argued that surveillance technologies, like Pegasus, do not fall under the Wassenaar Arrangement, since intrusion software is not restricted to the same degree as other technologies (Burton, 2023). Consequently, according to Burton, "it controls software toolkits that companies sell to clients to conduct operations with intrusion software, but not the software itself" (2023, p. 35), meaning that the NSO Group is allowed to sell its spyware in conformity with the Wassenaar Arrangement.

	India	United Kingdom	Spain	Greece	Mexico	Saudi Arabia	Israel	California, USA
International	**ICCPR. Budapest Convention on Cybercrime. Wassenaar Arrangement.**	**ICCPR Budapest Convention on Cybercrime Convention 108+. Wassenaar Arrangement.**	**ICCPR, Budapest Convention on Cybercrime, Convention 108+, Wassenaar Arrangement.**	**Convention 108. Budapest Convention on Cybercrime. Wassenaar Arrangement**.	**ICCPR. Budapest Convention on Cybercrime. Convention 108+. Wassenaar Arrangement**.	none	**ICCPR. Budapest Convention on Cybercrime. Not** part of **Wassenaar Arrangement** but claims that all its approvals for Pegasus exports have not violated the **Arrangement.**	**ICCPR. Budapest Convention on Cybercrime. Wassenaar Arrangement.**
Regional	none	**European Convention on Human Rights (ECHR)**: Signatory to ECHR, international human rights treaty which protects fundamental rights and freedoms, including the right to privacy. The ECHR (court) interprets and enforces the ECHR, and its decisions impact the UK's surveillance practices.	**Charter of Fundamental Rights of the European Union:** As a member state of the European Union, Spain is bound by the Charter, which recognizes fundamental rights, including the right to privacy. The Charter impacts surveillance practices within the EU. **ECHR.**	**Charter of Fundamental Rights of the European Union. ECHR.**	**American Convention on Human Rights:** Mexico is signatory to this regional human rights treaty including the right to privacy. The Inter-American Court of Human Rights interprets and enforces the Convention, influencing Mexico's approach to surveillance practices.	none	none	none
National	**Information Technology Act, 2000 (IT Act):** Governing various aspects of electronic communications, including surveillance and interception, provides legal provisions for	**Regulation of Investigatory Powers Act 2000 (RIPA):** UK legislation governs "lawful interception" of communications and the acquisition of communications data by public authorities, sets out the legal framework for surveillance activities and use of surveillance	**Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD):** This law provides regulations on data protection and privacy rights, including provisions related to surveillance activities	**Law 4624/2019 on the Protection of Personal Data:** Law aligns with the General Data Protection Regulation (GDPR) and provides regulations on the protection of personal data, including provisions	**Ley Federal de Protección de Datos Personales en Posesión de Particulares (Federal Law on Protection of Personal Data Held by Private Parties):** specifies rules for data storage and use only for natural	**The Basic Law of Governance 1992:** This foundational law defines privacy as a right related to dignity of an individual, guarantees the privacy of communication, generally	**The Protection of Privacy Law, 1981:** law regulating privacy in Israel (privacy in general and privacy in computerized databases). **Data Security Regulations 2017:** determine the level of security to be implemented in	**4th Amendment of US Constitution:** Protects individuals from surveillance activities by government. **Electronic Communications Privacy Act (ECPA**): Federal Law governing interception of electronic communications by government entities.

	the monitoring and interception of electronic communications by government authorities. **Telegraph Act, 1885:** Legislation empowers the government to intercept and monitor telecommunications, including phone calls and messages, for specified purposes (national security, public safety).	technologies. **Investigatory Powers Act 2016 (IPA):** IPA is comprehensive surveillance law, which establishes powers and safeguards related to the interception of communications, bulk data collection, equipment interference, and access to communications data.	and the use of surveillance technologies. **Ley de Enjuiciamiento Criminal (Criminal Procedure Act):** This law outlines the procedural rules for criminal investigations in Spain, including provisions related to surveillance measures, such as wiretapping and electronic surveillance.	related to surveillance technologies and privacy rights. **Hellenic Telecommunications and Post Commission (EETT):** EETT is regulatory authority, responsible for overseeing telecommunications and electronic communications.	persons and private entities. **Article 16 of the Mexican Constitution:** affirms the right to protection of personal data, access, rectification and elimination, only federal judicial authority has power to authorize monitoring of any private communication. **Federal Telecommunications and Broadcasting Law 2014:** establishes principles and requirements for the protection of personal data in the possession of private entities.	prohibits surveillance unless an exception applies. **Anti-Cyber Crime Law of 2007 (Royal Decree), the E-commerce Law of 2019:** establish the regulatory powers of the National Cybersecurity Authority and the Communications and Information Technology Commission ('CITC') and contain privacy provisions. **Personal Data Protection Law (PDPL):** ensure the privacy of personal data, regulate data sharing, and prevent the abuse of personal data.	computerized databases. **Transfer Regulations 2001:** regulate the transfer of personal data from Israeli databases outside the State of Israel. *CYBERSECURITY*: **Privacy Law and the Data Security Regulations** set out the obligation to safeguard personal data maintained in a computerized database and the standards of security. **Computers Law, 1995**: criminalizes unlawful computer-related misconduct, hacking or making malicious use of computers.	**Computer Fraud and Abuse Act (CFAA):** federal law addresses and crimilizes forms of unauthorized access to computer systems **California Electronic Communications Privacy Act (CalECPA**): state law extends privacy protections to electronic communication. **California Invasion of Privacy Act (CIPA):** establishes interception of communication as civil and criminal penalties for privacy violations. **California Consumer Privacy Act (CCPA**): grants consumers rights regarding personal information imposes obligations on businesses handling consumer data. **Comprehensive Computer Data Access and Fraud Act:** Criminalizes accessing computers if intent to cause harm.
Documented Pegasus Misuse against citizens of these states	**Yes**	**Yes**	**Yes**	**No, but similar Predator spyware**	**Yes**	**Yes**	**Yes**	**Yes**

Table 1: *Legal framework regarding surveillance technology regulation on the national, regional, and international level*. (source: own presentation)

2.4 Judicial Review

As Ball et al. state, an independent and strong judiciary is crucial regarding the misuse of surveillance technology and the protection of human rights and democratic values (2012). This is true, especially for new technologies, that have not yet been regulated by national law.

Additionally, judicial deference to governments is often based on democratic legitimacy concerns, especially when government actions are in question (Popelier et al., 2021). Since the Pegasus Spyware misuses have occurred, among others, within democratic states, the democratic legitimacy of government agencies is put in question, and courts are expected to voice the publics sentiment regarding these concerns (Popelier et al., 2021). Judicial review of certain administrative processes, for example, how the usage of spyware has been handled, requires the courts to confront tensions between values and concerns issued by civil society and administrative decision-making (Donnelly, 2017). This means that courts have the power to review certain policy decisions from an, to a degree, independent perspective.

The strength of judicial institutions becomes evident when looking at past cases and their implications for the regulation of surveillance. Considering the case of Sanoma Uitgevers B.V. v. the Netherlands, dealing with tensions between the right to privacy and freedom of expression (*Case of Sanoma Uitgevers B.V. v. The Netherlands*, 2010). The ruling had implications for accessing journalist's documents, which consequently could only be justified, and therefore a lawful intervention, if there is an overriding requirement in the public interest, and, if no less intrusive measure might have sufficed to serve the overriding public interest (Alexander & Krishna, 2022).

It is mentionable that there is strikingly little research conducted from a PA perspective, regarding judicial responses to the usage of technology. This, however, is relevant, since judicial review can have direct implications for administrative processes and decision-making (Donelly, 2017).

3. Methodology

In the following section, the methodology of this research will be explained.

3.1 Description of the Approach

The research is designed as a qualitative single-case study approach as it focuses on detecting challenges and responses concerning the Pegasus spyware (Flick, 2019) The case of the Pegasus Spyware and the global regulatory challenges this case poses, are subject to this research. It follows an interpretive research question, aiming to describe the responses of technology regulatory bodies to challenges posed by surveillance technology. It furthermore aims to interpret those responses in the context of national constitutions, regional agreements, and international rights and freedoms. In the chosen case study approach, a special focus lies on the issues and challenges Pegasus Spyware has brought up while identifying relevant regulatory stakeholders, which gives detailed insights into the specific case (Gerring, 2004). It includes a Stakeholder Analysis, as well as an interpretative review of existing court cases. A more detailed description regarding the case background of the Pegasus Spyware can be found in section 2.1.2.

3.2 Method of Data Collection

The data collection for this research can be categorized as desk research following a qualitative approach. It consists of purposively selected documents. This purposive sampling selection follows the sampling strategy of the “convenience criteria”, implying a selection of samples that are available and accessible to the public (Flick, 2019). Due to resource, as well as time restraints, purposive convenience sampling is the only applicable strategy in this research. Within a single-case study methodology, it is crucial to have diversity within empirical sources, since qualitative approaches depend on multiple perspectives, which is the reason for the variety of sources (Vennesson, 2008).

To gain insights into the ongoing and already judged legal investigations concerning the Pegasus Spyware, governmental legal archives have been accessed. Hence, publicly accessible information has been used to complete the analysis. This means that stakeholder information, public documents, including governmental publications, court documents, policy statements, outputs, EU reports, and draft recommendations, as well as legal framework, has been used. This data is accessible in different governmental and international organizations'

databases. Furthermore, private documents, meaning documents from civil society organizations and NGOs, such as reports by Citizen Lab or Forbidden Stories are part of the data collection (Raum et al., 2021). These can be found in detail in table A1, Appendix A.

3.3 Methods of Data Analysis

Data will be analyzed by making use of the single-case study approach. The extensive literature and legal framework review in the first part of the thesis demonstrates significant issues regarding the regulation of surveillance technology and the protection of individuals and vulnerable groups.

The conducted case study is an instrumental case, which aims to gain a better understanding of the problem, rather than just describing it (Johnson & Stake, 1996). It will be based on a qualitative approach that considers multiple sources for in-depth analysis (Willis, 2014). It will not follow the hypothesis-deductive model but rather try to answer the research question by conducting a thorough literature review to narrow down relevant aspects, key concepts, and already conducted research (Vennesson, 2008). The literature review, however, helps to investigate legal concepts that are crucial to understanding the research topic from an analytical perspective. It serves the purpose of answering an interpretative research question, while identifying gaps in the current legal framework, especially considering universal rights and freedoms.

Due to its positioning within the field of PA, this analysis will be limited to a single-case study approach, while within other fields of study, these approaches can be recognized as legal anthropological approaches or even as an investigation of the political economy of the Pegasus Spyware (Falk Moore, 2000; Milonakis & Fine, 2009).

Therefore, the selected case can be seen an attempt to gain a better understanding of the issue of regulating surveillance technology in a global context (Vennesson, 2008).

3.3.1 Stakeholder Analysis

To identify relevant regulatory bodies and their role in regulating surveillance technologies, such as Pegasus, a stakeholder analysis has been conducted. Stakeholders are therefore defined as those who are affected by the issue in question, meaning by the challenges surveillance technologies pose (Kelanti et al., 2015). The objective of this methodological approach is to understand which interests and roles different stakeholders have in regulating

surveillance technology. Therefore, understanding the issue from multiple stakeholder perspectives is crucial to understand the global scope of the issue (Raum et al., 2021). To achieve this, the analysis will take the following steps:

i) identifying stakeholders,
ii) differentiating and categorizing stakeholders; and
iii) investigating relationships between stakeholders, in their function as regulatory bodies,

from a deductive top-down approach, building on the institutional regulatory categories, introduced in the literature review by Ball et al., and redefined to a certain extent for the purpose of this research (2012; Wang et al., 2012).

The categories are as follows:

Civil Society: Forbidden Stories, Amnesty International Security Lab, Citizen Lab
International and Regional Organizations: United Nations, European Union
Governments: India, Spain, Mexico, UK, India, USA, Israel, Greece, Saudi Arabia
Private Entities: NSO Group.

3.3.2 Court Case Review

Judicial regulatory responses, in the form of publicly available court cases, have been reviewed. The review is categorized into jurisdictions, plaintiffs, and respondents, as well as their assigned interest group, a small case description, the demands issued by plaintiffs, grounds for accusations, the extent to which human rights have been discussed, and, if available, the outcome of the case.

This can be found in detail in table B1, Appendix B.

Building on Ball et al., who define the judiciary as the "first line of defence, dealing with cases involving uses of more innovative surveillance technologies before national laws have caught up to them and in this way charting the course for appropriate legislative approaches." (2012, p. 399), it is relevant for the purpose of this research to gain insights into court cases. Hence, an evaluation of the available legal responses is crucial to investigate regulatory responses to the challenges posed by this surveillance technology.

4. Analysis: Case Study of the Pegasus Spyware

In the following section sub-questions 1-4 will be answered by presenting findings regarding regulatory bodies and the implication these have on universal rights and freedoms.

4.1. Stakeholder Analysis

When looking at how surveillance is regulated as well as who has an interest in regulating surveillance technology, it becomes visible that this task is divided by different interest groups and stakeholders (Ball et al., 2012). By looking at the case of Pegasus, it is possible to identify four main groups, **civil society**, **international and regional organizations**, **national governments**, and **self-regulatory arrangements** in the form of **private entities** that are involved in selling spyware and regulating these technologies. Each of these interest groups consists of stakeholders, that are clustered within these main groups. In the following their role within surveillance technology regulation is presented, while the relationship between different stakeholders is shown.

4.1.1 Civil Society

Civil society takes on a crucial role in regulating surveillance technologies. When considering the Pegasus case, the way the public was informed about the governmental misuse of spyware is especially striking. Non-Governmental Organizations (NGOs), such as Citizen Lab, Amnesty International´s Security Lab, and Forbidden Stories, have played highly relevant roles in the revelations around Pegasus, making the amount of intrusive spyware used against civil society public and therefore a topic of public interest. In other words, they have adopted the role of a so-called “watchdog” function, while at the same time being victims of the spyware.

The ***Forbidden Stories*** collaboration uncovered the scope of the Pegasus misuse and collaboratively published it by coordinating more than 80 journalists from 17 media organizations in ten countries, to identify as many victims of misconduct as possible under the umbrella of the so-called “Pegasus Project” (Richard, 2022). This form of collaborative journalism made Forbidden Stories a global stakeholder and therefore emerging “regulatory body” in regulating surveillance technology. Even though Forbidden Stories' focus as a non-profit organization is not the advocation of surveillance technology regulation and does not fall directly in the category of a watchdog or an ombudsperson, as Ball et al. introduces them, their reporting directly influenced policy decisions made in the following (2012; Richard,

2022). Forbidden Stories is supporting governance regulation by reporting about the abuse of Pegasus on a global scale, since the goal of this reporting is, among other things, the achievement of stakeholder accountability (Hess, 2007). Since the stakeholders being held accountable in this case are governments and the NSO Group, the press takes on the role of an independent oversight mechanism, demanding public as well as corporate accountability and regulatory measures to protect civil society. Additionally, the press has a dual role in this case, since it is not only the "watchdog", but also a victim of the systematic abuses of spyware (Richard, 2022).

To identify said abuses, the identification of spyware on mobile devices is crucial. This technical support has been provided by ***Amnesty International´s Security Lab***, which has the technical and monetary resources to investigate in this scope. The forensic tests provided by the Security Lab have been able to empirically prove the claims of Pegasus abuses and therefore corroborated to demanding accountability for these.

Citizen Lab, an interdisciplinary, laboratory providing technical support and extensive forensic research on identifying Pegasus infections on mobile devices, can be categorized as a civil society stakeholder since their work provides independent proof of alleged abuses (Marczak, 2021). By peer-reviewing the work of the Amnesty International Security Lab, Citizen Lab has not only been able to corroborate the work of the Security Lab and Forbidden Stories but also has become a civil society stakeholder, uncovering potential misuses of Pegasus (Marczak, 2021).

To conclude it is possible to establish that civil society in the form of NGOs, the press, and non-profit organizations are emerging "regulatory bodies" regarding surveillance technology regulation since they have taken on the role of a "watchdog".

4.1.2 International and Regional Organizations

International and regional organizations, such as the ***UN*** and the ***EU***, remain key stakeholders in regulating surveillance technology, since the agreements on these levels directly influence national regulations to meet international or regional standards (Ball et al., 2012). As a reaction to the "Pegasus Project" revelations, the UN High Commissioner for Human Rights Michelle Bachelet explicitly called for better regulation of the use, sale, and transfer of surveillance technologies, since they have been linked to several human rights violations

(Richard, 2022). Additionally, UN experts requested all states to impose a global moratorium on the sale and transfer of surveillance technology until guaranteed compliance with human rights could be achieved through regulatory measures (Richard, 2022). The UN issued a report, stating that surveillance software has been linked to intimidation of journalists and human rights defenders, triggering fear with the consequence of possible self-censorship (Yang, 2021). Furthermore, it has been issued that states have the duty to protect individuals from privacy rights abuses by private companies, like the NSO Group, and advised to legally require businesses to meet human rights responsibilities by establishing effective accountability measures and more transparency (Yang, 2021). FollowPing these actions, it is possible to establish that the UN, as a regulatory body, takes on the role of an advisor for national regulation. By acknowledging and addressing the governmental misuse of surveillance technology, they support claims made by civil society and reinforce the demand for a better regulation key. Thus, regarding the nature of the UN, as an international organization without legal lever, it hands over responsibilities to strengthen protection mechanisms against surveillance to the national governments and their enforcement mechanisms.

The ***EU***, as a regional regulatory body, has responded to the demands for accountability and regulatory action by civil society and the UN, by establishing a committee of inquiry investigating the use of Pegasus and similar spyware, named PEGA Committee (in ´t Veld, 2023). Since the EU, contrary to the UN, has enforcement mechanisms and legal lever, with the European Court of Justice as a judiciary branch, resolutions have direct legal binding in member states national legislations. The PEGA has issued a detailed and final report, including recommendations to prevent future misuse of Pegasus in May 2023 (2022/2077(INI)). This independent report has confirmed that spyware was used to monitor, intimidate, and discredit civil society. Furthermore, it states that the EU governance structures have substantial deficits when effectively dealing with spyware abuses and need reforms (2022/2077(INI)). Additionally, the report gives concrete regulation recommendations regarding the use of spyware, which are presented in the following:

- Spyware should only be used in member states where spyware abuse allegations have been thoroughly investigated,

- where the national legislations are in line with the recommendations of the Venice Commission, the European Court of Human Rights case law, and the EU Court of Justice,
- where Europol is involved in investigations and export licenses, not in compliance with export control regulations have been revoked.

Whether these conditions have been fulfilled shall be assessed by December 2023 within the scope of a public report (2022/2077(INI)). Additional requests were made for the regulation of spyware use in law enforcement, which are summarized in the following:

- surveillance shall only be authorized in exceptional cases with a predefined purpose and limited time,
- data shall be protected regarding lawyer-client privilege, politicians, doctors, and media should be shielded from surveillance unless criminal activity is evident,
- there shall be mandatory notifications for targeted individuals and non-targeted individuals whose data was accessed during surveillance,
- there must be an independent oversight mechanism for surveillance investigations,
- targets of surveillance must be able to access meaningful legal remedies,
- there must be standards for the admissibility of evidence collected while using spyware (2022/2077(INI)).

In general, the committee calls for a common legal definition of the use of national security and “lawful interceptions” as grounds for surveillance to prevent the justification of surveillance technology abuses (2022/2077(INI)).

Furthermore, the report recommends the installation of an EU Tech Lab, an independent research institute to investigate surveillance, and provide legal and technological support as well as an increase in vulnerability research (in ´t Veld, 2023).

Regarding the foreign policy dimension, the report recommends the following steps for regulating surveillance technology:

- in-depth investigation of spyware export licenses,
- strong enforcement of EU´s export control rules,
- joint EU-US spyware strategies,

- dialogue with Israel, and other third countries for the establishment of rules on spyware marketing and exportation,
- ensuring that EU development aid funds do not support the acquisition and usage of surveillance technologies (2022/2077(INI)).

This report and the established resolutions have been adopted by the European Parliament on the 15th of June 2023 and are therefore key implications for future regulations regarding surveillance technology for member states (2022/2077(INI)). This resolution makes the EU a key regulatory stakeholder since it takes concrete steps to ensure a more regulated handling of surveillance technology.

4.1.3 Governments

The most evident institutional regulatory mechanism introduced by Ball et al. is regulation by **national governments** (2012).

Initial responses by national governments to revelations by civil society and challenges, especially regarding human rights violations, raised by the Pegasus spyware have differed greatly.

The ***US government*** has responded by blacklisting the NSO Group since it has acted contrary to the national security and foreign security interests of the USA (Richard, 2022). Hence, the NSO Group will be barred from buying parts from US Companies without obtaining a special license (Richard, 2022). By doing this, the USA is attempting to put human rights at the center of US foreign policy. However, there have been no further steps taken regarding the improvement of regulating overall surveillance technologies (Marczak et al., 2023).

The ***Indian government*** has been forced to respond as a result of petitions filed by different members of civil society, requesting an answer if Pegasus was used to spy on journalists and other members of civil society, and if so, if the process was followed (Case 1, Table B1: Appendix B) Before making this information public, the Indian government claimed that the revelations regarding Pegasus have been an exaggeration to malign Indian institutions and democracy (Case 1, Table B1: Appendix B). Due to pressure from the Indian Supreme Court as well as civil society, the Indian Supreme Court has established a technical committee to evaluate the lawful usage of Pegasus and the legal framework of India (Case 2, Table B1: Appendix B).

The ***Israeli government***, more specifically the Foreign Affairs and Defence Committee, has responded by initiating a commission investigating allegations of Pegasus misuse (Richard, 2022). Since the government can block the export of Pegasus to other countries, which can be used for geopolitical advantages, it has made use of this right and has shortened the export list extensively (Burton, 2023). However, it is not possible to access the exact list, since Israel is not part of the Wassenaar Agreement, and Pegasus Spyware does arguably not fall under the agreement.

Since three security agencies under the ***Mexican government*** are known to have operated the Pegasus spyware, over the past decade, the current president López Obrador has announced to make all Pegasus-related information public (Richard, 2022). Despite this announcement, the Mexican government continues to spy on civil society, as recent reports show (Marczak et al., 2023).

The ***Saudi Arabian government*** has denied every allegation brought up by civil society that agencies in the Kingdom of Saudi Arabia have used Pegasus spyware to monitor members of civil society. Their response to regulatory challenges brought up by Forbidden Stories was that national policies do not condone such practices (Bergman & Mazzetti, 2021).

The ***government of the United Kingdom*** has issued concerns regarding the misuse of Pegasus spyware but has also failed to take concrete action in furthering regulatory mechanisms that might prevent the misuse of surveillance technology in the future (Pfenniger, 2022).

The ***Spanish government*** has dismissed Paz Esteban López, the former director of the National Intelligence Centre (CNI) of Spain as a response to the Pegasus Project (Richard, 2022). Since the CNI confirmed that 18 members of the Catalan independence movement have been spied on with judicial approval, which has been seen as a direct attack on democracy, a change of staff was seen as necessary (Jones, 2022).

Observing reactions to the Pegasus scandal, while looking at the ***Greek government***, one must consider that the Greek government has allegedly not purchased the Pegasus Spyware, but a similar surveillance technology called the Predator Spyware (Arapi, 2023). As a national stakeholder regulating surveillance technology, the Greek government has continued the conversation around Pegasus and Predator, by introducing new laws. However, a law adopted

in December 2022, banning the sale of spyware for everyone except the Greek authorities, legalizes the identical abuses of spyware, brought to attention by civil society (Arapi, 2023).

Additionally, the EU resolutions, adopted in June 2023, are valid for Greece and Spain since these are both member states of the EU (in ´t Veld, 2023).

4.1.4 Private entities

Finally considering self-regulation arrangements by the industry, introduced by Ball et al., this research evaluates the NSO Group as an emerging stakeholder in regulating surveillance technologies (2012). Even though the NSO Group is not entirely self-regulated, since the Israelian government is able to block the sale of Pegasus, making it a semi-regulated space (Burton, 2023). However, the NSO Group has established an approach towards good governance within their company, claiming to act in line with the United Nations Guiding Principles on Business and Human Rights, with commitment to promoting transparency "wherever possible" (NSO Group, 2023). Despite this claim, the company has an untransparent screening mechanism regarding the sale of Pegasus, claiming that it is only sold to governmental entities that act under human rights principles (NSO Group, 2023). This intention is an indication of self-regulatory measures since the NSO Group limits itself regarding its client selection. As established earlier, the Pegasus Spyware does not fall under the Wassenaar Agreement, due to the way it is sold (Burton, 2023). Meaning that the NSO Group has found a way to avoid the consequences of having to obey the Agreement.

4.2 Court Cases

Since regulatory bodies have, as shown in 5.1, not yet regulated extensive parts of the usage of surveillance technology, it is of value to investigate how abuses of such technologies have been handled. After investigating the existing legal framework and how it regulates abuses of surveillance technologies, an overview of documented and publicly available court cases regarding the Pegasus Spyware and the NSO Group has been conducted and is analyzed in the following. It is crucial to add that this is not an exhaustive overview of all the current court cases involving the abuse of Pegasus Spyware and the NSO Group. According to Amnesty International, open investigations and cases are pending against the NSO Group in France, Mexico, Poland, and Spain (Ingleton, 2022). However, it is not possible to access relevant documents for these cases and investigations. Including the pending investigations which are not publicly accessible, the number of judicial cases is strikingly low regarding the number of

misuses of Pegasus spyware. Seven publicly accessible cases have been subject to this analysis. The following infographic shows the demands made by plaintiffs, categorized into groups of Civil Society, Corporations, and Private Persons.

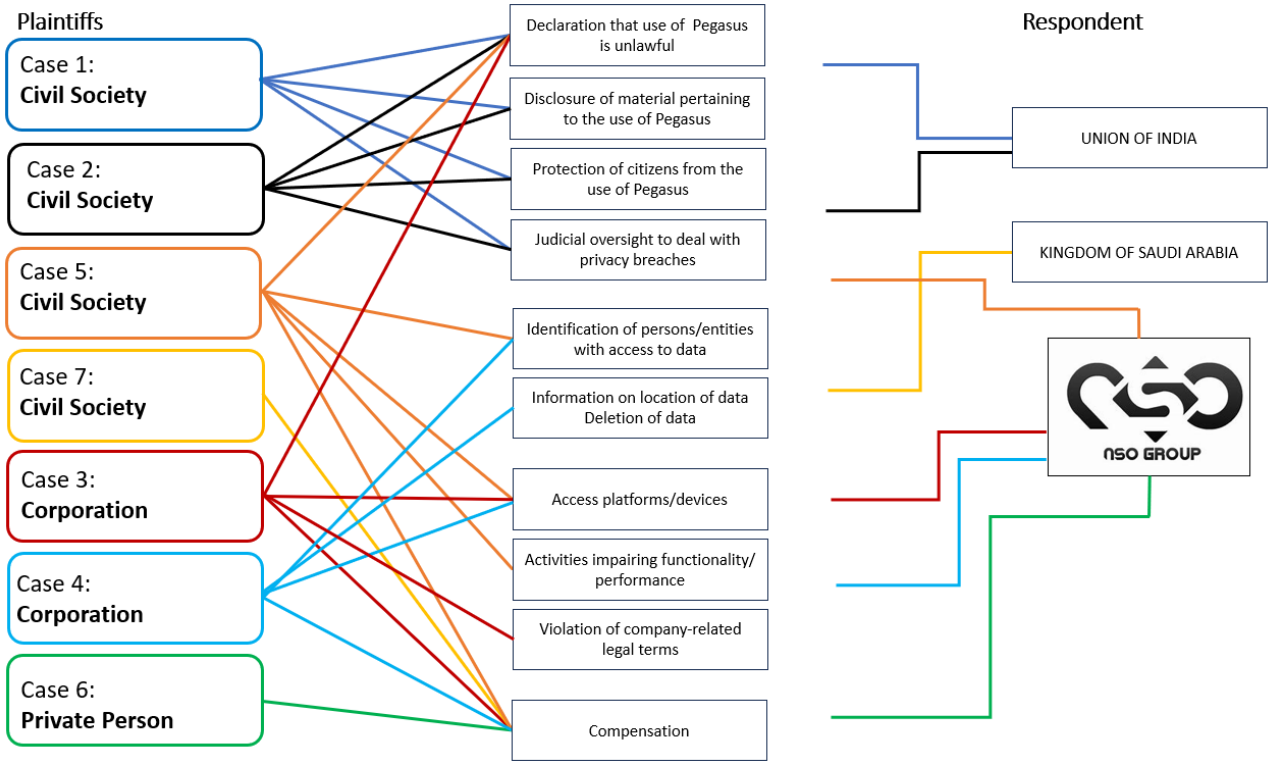

Figure 3: *Demands by plaintiffs, infographic based on Table B1: Appendix B* (source: own presentation)

The infographic shows that more than half of the cases are issued by members of civil society, which aligns with the findings from 5.1.1. The infographic is clustered into four categories, according to their content, for better oversight. Meaning, that if civil society is categorized as a stakeholder regarding surveillance technology regulations, it is making use of independent oversight mechanisms in the form of the judiciary branch. This is done by demanding public (in Cases 1,2, and 7) as well as corporate (in Case 5) accountability and regulatory measures to protect civil society from the judicative entity.

The infographic further shows that the main demands include a declaration of the courts that the use of Pegasus is unlawful, in four cases, which is next to compensation, in five cases, the demand which is issued most. With three demands, the permanent banning of NSO Group to access either platform or devices of plaintiffs is common.

Visible in table Table B1: Appendix B, issues regarding human rights are mentioned in six out of 7 cases, either as part of an argument, grounds for accusations, or as challenges caused by Pegasus which led to human rights issues. Most mentioned human rights were thereby the right to privacy and the freedom of expression. The only case which does not mention human rights-related issues is WhatsApp v NSO, which has been filed before the Pegasus Project has been published by Forbidden Stories, connecting surveillance technology abuse and human rights-related matters directly (Case 3, Table B1: Appendix B).

Additionally, the only case issuing human rights violations against the NSO Group in the USA, where four cases are handled, is the private person Francesco Corallo, a businessperson in the gambling industry, with allegedly strong ties to the Italian Mafia (Civillini, 2016). He has been charged in 2016 with conspiracy to commit crimes including money laundering and embezzlement (Civillini, 2016). Regarding his complaint against NSO Group and Apple, accusing the companies to conspire with Corallo's native countries Italy and the Netherlands, he claims to be a victim of a years-long persecution campaign that led to his unjust prosecution for tax fraud, bribery, and money laundering (Case 6, Table B1: Appendix B). He has filed a complaint regarding human rights violations on the grounds of systematic targeting, harassment, persecution, intentional infliction of emotional distress, invasion of privacy, and data hacking (Case 6, Table B1: Appendix B).

An outcome of the cases is available for the cases in India (Case 1,2) and to a certain extent for the case in the UK (Case 7). The cases in the USA are still pending.

The cases issued by civil society in India have led to the court requesting a detailed counter-affidavit regarding the issued demands. The Union of India has then submitted a 'limited affidavit', stating complete denial of all allegations made against the Union, claiming that petitions were only based on unsubstantiated media reports which cannot be made a basis for invoking writ jurisdiction (Case 1, Table B1: Appendix B). As a response to this, the Union has formed a committee of experts to investigate issues regarding surveillance technology abuses to prevent any wrong narrative from being spread and to confirm that sufficient checks and balances on government surveillance powers are in place. This reaction has been assessed as insufficient and lacking, to which the Solicitor General stated that a certain disclosure of facts will hamper the national security. The court has responded with an expression of displeasure towards the Union of India and has issued a creation of a Technical

Committee to investigate the truth or falsity of the allegations. The Committee has completed the investigation into the alleged misuse of Pegasus but is still contemplating suggestions on proposed amendments to strengthen privacy rights in India (Case 1 & 2, Table B1: Appendix B).

Regarding the case in the UK, handled by the King's Bench Division of the high court, which has permitted an individual to file a lawsuit against the Kingdom of Saudi Arabia, opening the way for other hacking victims to bring cases against foreign governments in the UK (Case 7, Table B1: Appendix B). The court functions as a regulatory body since it allows victims of abuse to seek justice, even against governmental entities.

5. Discussion of the Findings

This research aims to interpret and map responses to challenges posed by Pegasus spyware. It has been found that none of the mapped responses and findings would have taken place to this extent, if stakeholders within the group of civil society had not published and conducted their investigations regarding the scale of Pegasus misuses. This makes civil society arguably a controlling mechanism by uncovering and publishing abuses and seeking public and corporate accountability. Civil society has been able to detect a high number of Pegasus uses that have happened under the coat of "lawful interceptions" but had arguably no legal grounds. It has adopted the role of a so-called watchdog. However, reports of surveillance of civil society can trigger fear, especially with spyware as intrusive as Pegasus. Since it does not only access an individual's unique data but also targets core identity data, fear and worry as a societal response are expected (Marx, 2021). Surveillance of the press has led to self-censoring in the past (Jamil, 2020). Since the press, as part of civil society, is a key "regulatory body", while must simultaneously fear abuses by the means of surveillance technology, there is a certain danger of limiting its watchdog functions. If this was the case, chilling effects on universal rights and freedoms, for both members of civil society, and society at large could be a reality. Self-censored reporting infringes the right to information, due to the fear of an infringement of the right to privacy and freedom of expression, caused by surveillance technology abuses. Fear might additionally be a reason for the strikingly small number of court cases in which Pegasus is involved, since, as Lyon establishes, cyber surveillance serves the purpose of surveilling groups of people to impose a certain influence over them (2014).

This also becomes visible when looking at often-issued demands in available court cases. The demand, in three cases, is a permanent ban against NSO Group to access the plaintiffs' platforms or mobile devices, which shows a fear of being surveilled by this intrusive spyware in the future. McAllister emphasizes that the independence of regulation mechanisms and institutions is crucial to regulate surveillance technologies, which is only possible if civil society and judicial branches can do their work without fearing surveillance (2012). Another explanation for the small number of cases can be that the public has issues trusting judicial review mechanisms since their trust in democratic institutions has been fractured severely (Popelier et al., 2021). However, to further analyze whether fear, issues with judicial review

as an independent control mechanism, or other factors are the reason for the small number of court cases, further research must be conducted.

The evaluation of national governmental responses is essential when it comes to reviewing regulation mechanisms. Starting with Mexico, which has issued a statement, but has not taken additional actions to improve their surveillance technology regulations and continues to spy on members of civil society. This indicates that government entities feel secure in infringing human rights since there is no institutional control in place, able to hold them accountable. Since Mexico is additionally the deadliest country in the world for journalists, it is unlikely to encounter opposition in the form of lawsuits, since fear, as established earlier, can lead to self-censorship and obedience (Linares, 2021).

The UK has stated its concerns regarding the Pegasus spyware, while not taking further actions to prevent misuse of surveillance technology. Including Saudi Arabia in this evaluation, which has reacted with denial of using Pegasus, it is compelling to examine the implications of the case of Al-Masarir, a critical satirist and therefore member of civil society, against the Kingdom of Saudi Arabia, which is tried in the UK (Case 7, Table B1: Appendix B). While the UK government has not acted further, the judiciary branch has opened ways for individuals to seek justice against foreign governments if certain violations of universal rights have occurred in combination with surveillance technology abuses. This is, in Al-Masarirs case, physical harm caused by agents of Saudi Arabia as a consequence of using the Pegasus spyware. By admitting this case, the UK judiciary opens the way for individuals to obtain governmental accountability for the misuse of surveillance technology. At the same time, a member of civil society is making use of its function as a watchdog by filing a lawsuit against a national government and demanding public accountability.

Regarding India, the judiciary and members of civil society were able to make use of their role as watchdogs and hold the Union of India accountable for the misuse of Pegasus. Since the judiciary has decided in favor of the plaintiffs, it has prioritized universal rights and freedoms and was able to reach public accountability, by establishing a new and independent committee to investigate the government's wrongdoings.

Considering challenges caused by Pegasus in the USA, which has blacklisted the NSO Group, stating that by this they are prioritizing human rights (Richard, 2022). However, as Moses

establishes the regulation of new technologies requires responses adaptable to change, rather than singular and very specific policy responses (2015). So, even though the Pegasus spyware might be blacklisted in the USA, surveillance technology, in general, is not regulated more effectively and leaves further room for abuse of such.

The USA is handling most lawsuits filed against the NSO Group. Prioritization of human rights can be observed in the case of the El Faro journalists against the NSO Group, in which members of civil society demand corporate accountability from NSO Group for accessing their devices with Pegasus spyware (Case 5, Table B1: Appendix B). Nevertheless, the instrumentalization of human rights can be observed as well, regarding the case of Corallo v. NSO Group and Apple. Corallo has filed a complaint in which he issues, as the ground for accusation, several human rights violations. Corallo, a businessperson with allegedly strong ties to the Italian Mafia, being charged with several crimes, might be arguably an individual who falls under the coat of “lawful interception”. Since “lawful interception” is not a defined term, which increases the risk of misuse and can lead to cases like Corallos, the unclear meaning of this term offers grounds for the exploitation of judicial review (Case 6, Table B1: Appendix B). It is visible in his case, that the danger of instrumentalizing human rights under unregulated circumstances, is elevated.

Regarding the responses of Spain and Greece, which have undertaken staff changes and issued national laws that do not reduce the risk of governmental misuse of surveillance technology. This can be seen as an indication of non-transparency regarding governmental accountability. It becomes even more evident when attempting to access legal documents regarding Pegasus spyware abuses in Spain. As already criticized by the EU, Spain does not make ongoing trial documents available regarding issues related to Pegasus abuses (in ´t Veld, 2023).

Israel is the state from which Pegasus is distributed and the place of business for the NSO Group. As established earlier, Israel is not part of the Wassenaar Agreement, and, since the Pegasus spyware does arguably not fall under the agreement, NSO clients are not required to inform about the acquisition of Pegasus (Burton, 2023). It can be stated that there is a gap in the distribution of interceptive surveillance technology within the agreement, which enables members of this international agreement to make use of such technologies without proof of acquisition and consequently have a smaller risk to be held publicly accountable for misuses.

This enables the NSO Group to follow its business interests and sell surveillance technology in a relatively unregulated environment. This is in line with the client's interests since, as McAllister states, the governmental interest in surveillance technology is high (2012). Therefore, the interest in keeping the private sector distributing surveillance technology relatively unregulated can be described as relatively equal between national governments and the NSO Group. This additionally becomes evident with the attempt of the NSO Group to dismiss lawsuits in the USA, in which corporate accountability is demanded. However, to thoroughly investigate the relationship between public and private entities in the surveillance context, and the implications this might have on regulatory measures, further research is needed.

The UN has called for a global moratorium on the sale, transfer, and use of surveillance technology until there can be guaranteed compliance with human rights through regulatory measures (Yang, 2021). This statement shows that there are known, and to this point tolerated, global regulation gaps regarding surveillance technology, which frequently lead to human rights violations. These include the limited ways in which individuals can take legal action against governments if they have experienced a violation of human rights. Visible in Al-Masarir v Kingdom of Saudi Arabia, the admissibility could only be achieved because Al-Masarir has experienced physical harm by the Kingdom of Saudi Arabia, meaning that there are limited possibilities to hold states accountable for their actions in court. The other option for seeking justice, is, as shown in the Indian court cases, a strong independent judiciary branch, able to issue a certain kind of control regarding governmental misuse of surveillance technology.

These issues and regulatory shortcomings are reflected in the EU report, issued by the PEGA Committee, which has evaluated the existing legal framework, law enforcement action, and the dealing with third states regarding surveillance technology in the EU (2022/2077(INI)). Thereby it has identified severe gaps and proposed crucial regulatory reforms regarding the handling of surveillance technology. It has been noted that there is a gap when it comes to the common legal definition of "lawful interception", which has widely enabled justifications for surveillance technology abuses. The identification and potential filling of this legal gap could help victims of Pegasus abuses to obtain corporate or public accountability. Another aspect PEGA proposes is the establishment of an independent research institute, the EU Tech

Lab, to investigate issues in this area. This is in line with McAllisters emphasis on independent regulation institutions to effectively regulate surveillance technology (2012). However, it is possible to critically engage with the proposed regulations by the PEGA Committee. Firstly, the recommendations are vague regarding targets being able to access meaningful legal remedies, while not considering external influences, which might complicate the accessibility of such remedies, for example, as established earlier, the aspect of fear or distrust in institutions. Additionally, there is a certain lack of efforts to find a global solution regarding the distribution control of surveillance technology, since the focus lies more on direct dialogues with third countries, rather than strengthening existing agreements and filling gaps in international legal frameworks. This is additionally visible in the foreign policy intention to cooperate in creating a joint EU-US spyware strategy, which displays a Western-centric approach, disregarding the global sphere of the issue of surveillance technology regulation.

However, it is valid to point out that most global solutions are difficult to achieve since national contexts are crucial in how notions of privacy, data protection, or civil liberties are being handled (Ball et al., 2012). A possible solution for regulatory issues on the national level might be a multiple-stakeholder approach, including members of civil society, the private sector, experts, as well as government officials in policy recommendations to gain a more comprehensive picture of existing issues (Chan, 2019; Fenwick et al., 2017). Until there is no secure regulatory framework and guaranteed compliance with universal rights and freedoms cannot be achieved, it is reasonable to follow the UN recommendation to proclaim a global moratorium on the sale, transfer, and usage of surveillance technologies.

6. Conclusion

After conducting a thorough literature and legal review, a stakeholder analysis including relevant regulatory bodies connected to the case of Pegasus and evaluating judiciary reviews of cases including the use of Pegasus, an answer to the posed research question can be formulated. The question: *To what extent are technology regulatory bodies responding to challenges posed by surveillance technologies, regarding the Pegasus Spyware, considering the national constitutions, regional agreements, and universal rights and freedoms?*, will be answered in the following.

Regulatory bodies are responding to posed challenges, namely the prevention of further misuse of Pegasus and similar spyware, and the detection of severe gaps in regulatory frameworks in different manners. This research has found members of civil society to have a crucial impact on uncovering and publishing misuse of surveillance technology, and therefore being emerging stakeholders in the regulation of surveillance technology. Due to the work of members of civil society issues regarding surveillance regulation have been put on the global agenda, and forced international, regional, national, and private stakeholders to respond to uncovered issues. This has made them take on the role of a controlling mechanism, or in other words, a watchdog function. As established earlier, public, and private stakeholders have responded in different ways. While regional stakeholders like the EU, have conducted investigations, attempting to fill gaps in regulatory frameworks, international stakeholders like the UN, have advised proclaiming a global moratorium on the sale, transfer, and use of surveillance technology until there can be guaranteed compliance with universal rights and freedoms through regulatory measures. Both responses highlight the fragmented legal framework regarding surveillance technology and the need to fill existing gaps to prevent further human rights violations.

National regulatory bodies have responded within their national contexts. Severe differences have been noted, especially including, and connecting available court cases with governmental responses. In this context, prioritization of universal rights and freedoms by courts has been observed, while simultaneously the instrumentalization of human rights was detectable in a certain case.

Regarding private regulatory bodies, namely the NSO Group, tension between business interests and the upholding of human rights has been observed, especially regarding court

cases in the USA. To a certain extent, self-regulation has been observed, could, however, not be proven either wrong or right, since client lists of the NSO Group are confidential and cannot be accessed.

This research has shown the close interconnectedness between the regulation of surveillance technology and the chilling effects these intrusive technologies can have on human rights. Bell et al., have introduced different bodies to institutionally regulate surveillance technology. These have shown to be important regarding control and regulatory measures. However, as an additional emerging "regulatory body", this research has identified members of civil society, acting as watchdogs, overseeing, and uncovering misuse of surveillance technology and demanding corporate as well as governmental accountability. This has been achieved to a certain extent since regulatory bodies have taken steps to improve the regulation of surveillance technology on national, regional, and international levels.

The detection of gaps in international agreements and their implications for the global handling of surveillance technology has been achieved through study design and extensive literature as well as legal review. This can be called a strength of this research. The innovative approach of investigating judicial reviews and connecting these with an analysis of stakeholder interests has additionally allowed insights into institutional control mechanisms and which indications these have for the regulation of surveillance technology.

It must be added that this research has limitations. The cross-country investigation of court cases makes it difficult to compare the contents of these cases since the judiciary differs immensely due to the national context. Since national responses must be seen in their historical, societal, and structural context, which would have extended the scope of this research, the validity of this research might be limited. There have, moreover, not been available outcomes for most reviewed cases since most are still in the process of being tried. Judiciary cases that are not publicly accessible have not been considered for this research either, which might distort findings.

A further research opportunity would be a repetition of this research when cases regarding Pegasus spyware have been closed and an outcome can be analyzed and compared. However, since this research has been conducted under the scope of PA research, it is possible to shift this perspective and review surveillance technology regulation from a political economy, or

even a legal anthropology angle. This might convey further insights into the researched topic since a multidisciplinary approach is fitting for this multidisciplinary research. A further opportunity for research is the reviewing of how national governments of member states will adopt PEGA recommendations regarding the regulation of surveillance technology. In this context, social justice implications can furthermore be investigated, especially regarding the imbalance of power between surveilled entities and surveilling entities. The differentiation between implication of mass data collection and targeted spying has been touched upon within this research but can be further elaborated on. The tension between private actors and public officials regarding the distribution and sale of surveillance technology is additionally an aspect of surveillance technology regulation that needs to be further researched. Moreover, determining the influence of the presence and usage of cyber spyware on democratic values is an important research gap that offers opportunity for further research. As this research has shown, unregulated or uncontrolled usage of surveillance technology can lead to huge violations of privacy and potential use of violence and must therefore be researched further.

In conclusion, it is possible to establish that regulatory bodies have responded to surveillance technology regulatory challenges as a reaction to the publications by civil society, to different extents. However, it is advisable to follow the UN's recommendation to proclaim a global moratorium on sale, transfer, and usage of surveillance technology until compliance with universal rights and freedoms can be guaranteed. As this research has shown, the wide misuse of surveillance technology has led to chilling effects on human rights and can only be properly addressed if working regulatory mechanisms are put in place. This must be given before making further use of surveillance technology and thereby risking further misuse as it has occurred with Pegasus spyware.

7. References

Alexander, A., & Krishna, T. (2022). Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism. *Laws 2022, Vol. 11, Page 85*, *11*(6), 85. https://doi.org/10.3390/LAWS11060085

Arapi, G. (2023). Greece's surveillance scandal must shake us out of complacency. *Amnesty International*.

Ball, K., Haggerty, K. D., & Lyon, D. (2012). Regulating surveillance technologies : Institutional arrangements. *Routledge Handbook of Surveillance Studies*, *10204*, 397–404. https://doi.org/10.4324/9780203814949-62

Bergman, R., & Mazzetti, M. (2021). Israeli Companies Aided Saudi Spying Despite Khashoggi Killing - The New York Times. *The New York Times*. https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

Burton, S. (2023). Pegasus and the Failure of Cybersurveillance Regulation. *The SAIS Europe Journal of Global Affairs Spring 2023*.

Chan, A. (2019). The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware. *Brooklyn Journal of International Law*, *44*(2). https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/7

Chawla, A. (2021). Pegasus Spyware – "A Privacy Killer." *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3890657

Civillini, M. (2016). Italy's "King of Slots" Arrested. *Organized Crime And Corruption Reporting Project*. https://www.occrp.org/en/daily/5894-italy-s-king-of-slots-arrested

Convention on Cybercrime, (2001) (testimony of Council of Europe).

Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data, (2018) (testimony of Council of Europe). www.coe.int/dataprotection

Donnelly, C. (2017). Participation and expertise: Judicial attitudes in comparative perspective. *Comparative Administrative Law: Second Edition*, 370–385. https://doi.org/10.4337/9781784718671.00031

Case of Sanoma Uitgevers B.V. v. The Netherlands, (September 14, 2010).

Falk Moore, S. (2000). *Law as Process: An Anthropological Approach*.

Fenton, N., Freedman, D., & Witschge, T. (2010). *Protecting the News: Civil Society and the Media*. *2*(2), 31–72. https://doi.org/10.2307/26804351

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. M. (2017). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2834531

Flick, U. (2019). Gütekriterien qualitativer Sozialforschung. *Handbuch Methoden Der Empirischen Sozialforschung*, 473–488. https://doi.org/10.1007/978-3-658-21308-4_33

Gerring, J. (2004). *What Is a Case Study and What Is It Good for?* The American Political Science Review. https://www.jstor.org/stable/4145316

Hess, D. (2007). Social Reporting and New Governance Regulation: The Prospects of Achieving Corporate Accountability Through Transparency. *Business Ethics Quarterly*, *17*(03), 453–476. https://doi.org/10.5840/beq200717348

in ´t Veld, S. (2023). *European Parliament Draft Recommendation 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*. https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html

Jamil, S. (2020). Red lines of journalism : Digital surveillance, safety risks and journalists' self-censorship in Pakistan. *Journalist Safety and Self-Censorship*, 29–46. https://doi.org/10.4324/9780367810139-3

Johnson, K. E., & Stake, R. E. (1996). The Art of Case Study Research. *The Modern Language Journal*, *80*(4), 556. https://doi.org/10.2307/329758

Jones, S. (2022). Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy.' *The Guardian*.

Kaldani, T., & Prokopets, Z. (2022). *Pegasus Spyware and its impacts on human rights*.

Kaster, S. D., & Ensign, P. C. (2022). Privatized espionage: NSO Group Technologies and its Pegasus spyware. *Thunderbird International Business Review*. https://doi.org/10.1002/tie.22321

Kelanti, M., Hyysalo, J., Lehto, J., & Saukkonen, S. (2015). *Soft System Stakeholder Analysis Methodology*. https://www.researchgate.net/publication/290920320_Soft_System_Stakeholder_Analysis_Methodology

Le Nguyen, C., & Golman, W. (2021). *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: ' Law on the books ' vs ' law in action '*. https://doi.org/10.1016/j.clsr.2020.105521

Linares, A. (2021). *Mexico is deadliest country for journalists, who also face government harassment*. NBC Latino. https://www.nbcnews.com/news/latino/mexico-deadliest-country-journalists-also-face-government-harassment-rcna833

Lyon, D. (2014). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Routledge.

Lyon, D. (2015). The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society*, *13*(2), 139–152. https://doi.org/10.24908/ss.v13i2.5363

Marczak, B. (2021). *Independent Peer Review of Amnesty International's Forensic Methods for Iden-tifying Pegasus Spyware-The Citizen Lab*.

Marczak, B., Scott-Railton, J., Razzak, B. A., & Deibert, R. (2023). Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains. In *The Citizen Lab*. https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

Marx, G. T. (2021). *Windows into the Soul: Surveillance and Society in an Age of High Technology* (Vol. 32, Issue 2). Routledge. https://doi.org/10.1080/10511253.2021.1883696

McAllister, L. K. (2012). Regulation by Third-Party Verification. *Boston College Law Review*, *53*. https://heinonline.org/HOL/Page?handle=hein.journals/bclr53&id=5&div=&collection=

Milonakis, D., & Fine, B. (2009). *From Political Economy to Economics: Method, the Social and the Historical in the Evolution of Economic Theory*.

Moses, L. B. (2015). How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target. *Law, Innovation and Technology*, *5*(1), 1–20. https://doi.org/10.5235/17579961.5.1.1

NSO Group. (2023, May 15). *Transparency - NSO Group*. https://www.nsogroup.com/governance/transparency/

Pfenniger, K. (2022). Pegasus Project: what has happened since the revelations? *Forbidden Stories*. https://forbiddenstories.org/pegasus-project-impacts-map/

Popelier, P., Kleizen, B., De Clerck, C., Glavina, M., Van, W., & Uantwerp, D. (. (2021). *The Role of Courts in Times of Crisis: A Matter of Trust, Legitimacy and Expertise*. https://libertescheries.blogspot.com/2020/04/covid-19-le-

Raum, S., Rawlings-Sanaei, F., & Potter, C. (2021). A web content-based method of stakeholder analysis: The case of forestry in the context of natural resource management. *Journal of Environmental Management*, *300*, 113733. https://doi.org/10.1016/j.jenvman.2021.113733

Richard, L. (2022). *Forbidden Stories: Impact Report 2021*.

Rueckert, P. (2021). Pegasus: The new global weapon for silencing journalists. *Forbidden Stories*.

Scott-Railton, J., Marczak, B., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2017). *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*. https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

Srivastava, M., & Bradshaw, T. (2019). Israeli group's spyware "offers keys to Big Tech's cloud." *Financial Times*.

International Covenant on Civil and Political Rights, (1967) (testimony of United Nations).

Vennesson, P. (2008). Case studies and process tracing: Theories and practices. In *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective* (pp. 223–239). Cambridge University Press. https://doi.org/10.1017/CBO9780511801938.013

Wang, J., Ge, J., & Lu, Q. (2012). *A Review of Stakeholder Analysis*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6340802

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, (1995) (testimony of Wassenaar Arrangement Secretariat).

Willis, B. (2014). The Advantages and Limitations of Single Case Study Analysis. *Www.E-Ir.Info*, 1–9. https://www.e-ir.info/2014/07/05/the-advantages-and-limitations-of-single-case-study-analysis/

Yang, C. (2021). Pegasus: Human rights-compliant laws needed to regulate spyware | UN News. *UN News: Human Rights*. https://news.un.org/en/story/2021/07/1096142

Appendix A

List of reviewed Documents

Table A1:

(Own presentation)

Year	Issued by	Title	Accessed through
2023	European Parliament	2022/2077(INI): European Parliament Draft recommendation 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. **Cited as**: 2022/2077(INI)	Legislative Observatory of the European Parliament
2022	Forbidden Stories: Laurent Richard	2021 Forbidden Stories Impact Report. **Cited as**: Richard, 2022	Forbidden Stories Archive
2023	The Citizen Lab: Marczak et a.	Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains. **Cited as**: Marczak et al., 2023	The Citizen Lab Pegasus Archives
2021	Government of West Bengal Home and Hill Affairs Department.	Notification on West Bengal setting up Inquiry Commission.	Supreme Court of India Archives
2021	Supreme Court of India: Civil original jurisdiction	Writ Petition (CIVIL) No. 826 of 2021 (Under Article 32 of the Constitution of India) Singh and Shatakshi v Union of India and Ministry of Home Affairs.	Supreme Court of India Archives
2021	Supreme Court of India: Civil original jurisdiction	Writ Petition (CIVIL) No. 314 of 2021 (Under Article 32 of the Constitution of India) Manohar Lal Sharma v Union of India.	Supreme Court of India Archives
2021	Union of India	Limited Affidavit on behalf of Union of India, dated 16.08.2021.	Supreme Court of India Archives
2022	Royal Court of Justice, London	Judgment Approved by the High Court of Justice: Neutral Citation Number: [2022] EWHC 2199 (QB): Ghanem Al-Masarir v Kingdom of Saudi Arabia.	Royal Courts of Justice of the United Kingdom Archives
2021	United States District Court: Northern District of California, San Jose Division	Complaint – Demand for jury trial, Case 5:21-cv-9078: Apple Inc. v NSO Group Technologies limited, and Q Cyber Technologies limited.	California Court Archives

2022	United States District Court: Northern District of California, San Jose Division	Complaint – Demand for jury trial, Case 5:22-cv-07513: Carlos Dada, Sergio Arauz, Gabriela Caceres Gutierrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz, Lazo Escobar, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Nelson Rauda Zablah, Mauricio Sandoval Soriano, Jose Luis Sanz v NSO Group Technologies limited, and Q Cyber Technologies limited.	California Court Archives
2019	United States District Court: Northern District of California	Complaint – Demand for jury trial, Case 3:19-cv-07123 WHATSAPP INC., a Delaware corporation, and FFACEBOOK, INC., a Delaware corporation v NSO Group Technologies limited, and Q Cyber Technologies limited.	California Court Archives
2022	United States District Court: Northern District of California, San Jose Division	Complaint – Demand for jury trial, Case 5:22-cv-05229 Francesco Corallo v NSO Group Technologies limited, and Q Cyber Technologies limited and Apple Inc.	California Court Archives

Appendix B

Court Case Review

Table B1:

(Own presentation based on judicial documents Table A1: Appendix A)

The table lists and reviews seven court cases regarding Pegasus Spyware and the NSO Group. It is categorized into jurisdictions, plaintiffs, and respondents, as well as their assigned interest group, a small case description, the demands issued by plaintiffs, grounds for accusations, the extent to which human rights have been discussed, and, if available, the outcome of the case.

Jurisdiction	Plaintiff and Respondent	Case Description	Demand	Grounds for Accusation	Extent of Human Rights Discussion	Outcome
Case 1: India: Supreme Court of India	**Civil Society**: Jagdeep Chhokar (founder of Association for Democratic Reforms), Paranjoy Guha Thakurta (Journalist), N. Ram (Journalist and Editor of The Hindu), John Brittas (Rajya Sabha MP) V Union of India and Prime Minister and Ministry of Home Affairs	**Petition** Plaintiffs targeted by Pegasus Spyware: Petition of a judicial probe to investigate if Indian government used Pegasus to spy on journalists/other citizens, if so if process was followed	1. A declaration from the Supreme Court that the use of Pegasus or similar malware is unconstitutional. 2. A direction for the Union to disclose material such as documentation of investigations, authorizations, and orders, pertaining to the use of Pegasus. 3. A direction for the Union to take steps to protect citizens from the use of surveillance software's such as Pegasus. 4. A direction for the Union to install a judicial oversight mechanism to deal with breaches of privacy and to punish officials responsible for such breaches.	Violation of Information Technology Act (IT Act), 2000: Section 66B punishment of 'dishonest receiving of stolen computer resources' Section 69 and the Telegraph Act, 1885: Section 5 use of Pegasus 'goes much beyond' the interception, monitoring and decrypting of messages, no refusion by the Government to use spyware, since NSO only sells to Governments, makes this an issue of State Law	Clearly discussed and specific human rights mentioned: Privacy, freedom of speech, free press, free access to information, right to work freely (as a journalist)	1. Court requests detailed counter-affidavit → Submission of 'limited affidavit': complete denial of all allegations made against the Union, petitions were only based on unsubstantiated media reports which cannot be made a basis for invoking writ jurisdiction, Union will form a committee of experts to investigate the issue to prevent any wrong narrative from being spread & sufficient checks and balances on government surveillance powers that Pegasus reports have no factual basis 2. Limited affidavit insufficient and lacking → Solicitor General stated that a certain disclosure of facts will hamper the national security 3. expression of displeasure towards the Union of India and creation of Technical Committee to investigate the truth or falsity of the allegations 4. Committee has completed the investigation into the alleged misuse of Pegasus, still contemplating suggestions on proposed Amendments to strengthen privacy rights in India

Case 2: India: Supreme Court of India	**Civil Society:** Rupesh Kumar Singh and Ipsa Shatakshi V The Union of India: Ministry of Electronics and Information Technology and Ministry of Home Affairs	**Petition** Plaintiffs targeted by Pegasus Spyware: Petition of a judicial probe to investigate if Indian government used Pegasus to spy on journalists/other citizens	1. Declaration that installation and use of malware/spyware like Pegasus is illegal and unconstitutional. 2. A direction for the Union to disclose material such as documentation of investigations, authorizations, and orders, pertaining to the use of Pegasus. 3. A direction for the Union to take steps to protect citizens from the use of surveillance software's such as Pegasus. 4. A direction for the Union to install a judicial oversight mechanism to deal with breaches of privacy and to punish officials responsible for such breaches.	Violation of their right to privacy under Article 21, rights to freedom of speech, the free press, free access to information, and the Petitioner No.1's right to work freely as journalists under Articles 19(1)(a) and 19(1)(g) of the Constitution. Information Technology Act, 2000 ["IT Act"]: especially Section 69, 66, 72, and 43 Telegraph Act, 1885	Within Grounds for Accusation, clearly discussed and specifically mentioned: Privacy, freedom of speech, free press, free access to information, right to work freely (as a journalist)	Same outcome as Case 1
Case 3: USA: California, District Court	**Corporation:** WhatsApp Inc., a Delaware Corporation and Facebook, Inc., a Delaware Corporation V NSO Group Technologies limited, and Q Cyber Technologies limited	**Complaint** April - May 2019: NSO accessed WhatsApp Servers located in USA to send Malware to ca. 1400 mobile devices, software designed to infect these with purpose of conducting surveillance of specific WhatsApp users	1. Declaration that NSO has violated different laws, 2. Permanent injunction restraining NSO from accessing WhatsApp/Facebook platform and computer systems, creating/maintaining accounts, any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of services, 3. any activities that violate WhatsApp's or Facebook's Terms, 4. Compensation	Violation the Computer Fraud and Abuse Act, 18 U.S.C. §1030. ii. Violated the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502. iii. Trespassed onto Plaintiffs' property in violation of California law. iv. Intruded upon Plaintiffs' seclusion in violation of California law.	none	Ongoing

Case 4: USA: California, District Court	**Corporation:** Apple Inc. V NSO Group Technologies limited, and Q Cyber Technologies limited	**Complaint** NSO accessed Apple software and products, designed to infect these with the purpose of conducting surveillance	1. Permanent injunction restraining NSO from accessing and using any Apple servers, devices, hardware, software, applications, or other Apple products/services, 2. Identify the location of any and all information obtained from any Apple users' device and deleting all obtained data, 3. Identity of everyone whom NSO shared this information, 4. Restraining NSO from developing, distributing, using, and/or causing or enabling others to use any spyware on Apple devices, 5. Compensation	Violations of Computer Fraud and Abuse Act 18 U.S.C. § 1030(a), Violations of California Business and Professions Code § 17200, Breach of Contract, Unjust Enrichment	Broadly discussed as human rights abuses committed through NSO spyware, not specified	Ongoing
Case 5: USA: California, District Court	**Civil Society:** El Faro Journalists: Carlos Dada, Sergio Arauz, Gabriela Caceres Gutiérrez, Julia Gavarrete, Román Gressier, Gabriel Labrador, Ana Beatriz, Lazo Escobar, Efrén Lemus, Carlos Martínez, Oscar Martínez, María Luz Nochez, Víctor Pena, Nelson Rauda Zablah, Mauricio Sandoval Soriano, José Luis Sanz V NSO Group Technologies limited, and Q Cyber Technologies limited	**Complaint** El Faro's journalists were targeted over an eighteen-month period by Pegasus technology, which can surreptitiously provide access to the content's devices and cloud accounts. Attacks often coincided with El Faro's investigations into President Nayib Bukele's administration.	1. Declaration that NSO has violated different laws, 2. Permanent injunction restraining NSO from accessing devices, 3. Enter permanent injunction requiring NSO to catalogue all information obtained because of the Pegasus attacks, 3. Disclose the identities of all persons/entities with whom NSO shared information, delete and return data, 4. Compensation	Violated the Computer Fraud and Abuse Act, 18 U.S.C. §1030. ii. Violated the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502. iii. Trespassed onto Plaintiffs' property in violation of California law. iv. Intruded upon Plaintiffs' seclusion in violation of California law.	Cleary discussed and specifically mentioned: Pegasus as threat to human rights and press freedom, also mentioned are right to privacy, free speech	Ongoing

Case 6: USA: California, District Court	**Private Person:** Francesco Corallo (Italian casino owner with ties to the Italian Mafia, charged with conspiracy to commit crimes) V NSO Group Technologies limited, and Q Cyber Technologies limited and Apple Inc.	**Complaint** for allegedly conspiring with Corallo's native country Italy and the Netherlands, he claims is a years-long persecution campaign that led to his unjust prosecution for tax fraud, bribery, and money laundering	1. Compensation	**NSO**: Article 12 of the UHDR (Universal Declaration of Human Rights), Article 9 and 17 of the ICCPR (International Covenant on Civil and Political Rights), Article 23 of the Guiding Principles on Business and Human Rights, human rights violations by systematic targeting, harassment, persecution, intentional infliction of emotional distress, invasion of privacy, and data hacking, Violation of the Alien tort claims Act 28 U.S.C. § 1350, Violations of the Federal Computer Fraud and Abuse Act 18 U.S.C. § 1030, Invasion of Privacy California State Law, Civil Conspiracy California State Law, Violations of California's comprehensive Computer Data Access and Fraud Act, Cal. Penal § 502, Intentional Inflict of Emotional Distress California State Law **APPLE**: Negligence California State Law, Violations of California's False Advertising Law CAL. BUS. and PROF. CODE, §§ 17500 ET SEQ	Within Grounds for Accusation, clearly discussed and mentioned: systematic abuse of human rights through acts of harassment, persecution, intentional infliction of emotional distress, invasion of privacy, data hacking, as well as other offensive and actionable conduct	Ongoing

Case 7: United Kingdom: High Court of Justice Queen's Bench Division, Media, and Communication List	**Civil Society:** Ghanem Al-Masarir (satirist granted asylum in the UK, who is a frequent critic of the Saudi royal family) V Kingdom of Saudi Arabia	Allegations that Saudi Arabia ordered the hacking of digital device, and that the plaintiff was physically assaulted by agents of the Kingdom of Saudi Arabia in London in 2018	1. Damages for misuse of private information, harassment, trespass to goods, and assault resulting in personal injury	1. Claim is brought in misuse of private information; harassment; trespass to goods; and assault 2. Plaintiff alleges that Defendant is not immune in respect of the claim because the exception to sovereign immunity under s 5 of the SIA 1978 is applicable	To an extent discussed, specifically mentioned: Privacy, Proportionality of Immunity Principle	1. Held that s. 5 SIA could cover both sovereign acts (*jure imperii*) and private law acts (*jure gestionis*). 2. Found that the application of s. 5 SIA did not require that the entirety of the tort (causing personal injury etc) occur in the UK. 3. It was "overwhelmingly likely" that Saudi Arabia had infected Al-Masarir's devices and was using Pegasus to spy on him. 4. Saudi Arabia was likely responsible for the persons committing the assault, 5. There was sufficient evidence to support these points, and such was enough to also proceed with the claim **Outcome** of the lawsuit still ongoing