Europe's PegasusGate

Countering spyware abuse
As civil society and media organisations expose EU Member States for using the Pegasus commercial spyware, one of the most high-profile spying scandals of recent years is coming to light in Europe. Member States’ intelligence agencies have been accused of abusing highly sophisticated spyware to surveil opposition figures, journalists, lawyers, and high-ranking state officials. ‘Having regard to the European Union’s attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law’, the European Parliament has set up a committee of inquiry. This study (i) introduces the Pegasus product’s features and trading practices, (ii) surveys Pegasus operations and reactions, (iii) identifies transversal and country-specific legal concerns, and (iv) sketches possible ways forward in the public and private sectors.
As civil society and media organisations expose EU Member States' use of the Pegasus commercial spyware, one of the most high-profile spying scandals of recent years is coming to light in Europe. Member States' intelligence agencies have been accused of abusing highly sophisticated spyware to surveil opposition figures, journalists, lawyers, and high-ranking state officials. 'Having regard to the European Union's attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law', the European Parliament has set up a committee of inquiry. This study (i) introduces the Pegasus product's features and trading practices, (ii) surveys Pegasus operations and reactions, (iii) identifies transversal and country-specific legal concerns, and (iv) sketches some possible ways forward.

AUTHOR
Hendrik Mildebrath, Members' Research Service, EPRS.

This paper has been drawn up by the Members' Research Service, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please email: eprs@ep.europa.eu

The author would like to thank Norbert Lorenz, Director of the European Parliament's Legal Service, for reading and commenting on the draft of this paper.

LINGUISTIC VERSIONS
Original: EN

Manuscript completed in June 2022.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.


Photo credits: © Marcos Silva / Adobe Stock.

eprs@ep.europa.eu
http://www.eprs.eu (intranet)
http://epthinktank.eu (blog)
Executive summary

As Pegasus revelations gain momentum and the first EU Member States become implicated, one of the most high-profile spying scandals of recent years is coming to light in Europe. The Canadian interdisciplinary laboratory Citizen Lab first discovered traces of Pegasus spyware in 2015, but it was only in 2021 that the scandal broke on a global level through a joint effort by Citizen Lab, Amnesty International, Forbidden Stories and 17 media organisations. Reports revealed that authoritarian and democratic governments around the world were using Pegasus to spy on journalists, lawyers, activists, politicians, and high-ranking state officials. Investigators link the spyware to human rights harms including intimidation, harassment, detention, and murder. Pegasus was developed by the NSO Group and is designed to breach mobile phones and extract vast amounts of data stored or processed by the target system, including text messages, call interceptions, passwords, locations, microphone and camera recordings, and information from apps.

In the European Union, the Hungarian and Polish governments were the first to be caught in the eye of the storm, after media organisations uncovered extensive use of Pegasus spyware by public authorities against opposition figures and government critics. Meanwhile, Spain finds itself in the throes of the Pegasus ‘cyclone’ after Citizen Lab revealed extensive Pegasus spyware operations against Catalans (‘CatalanGate’). Reportedly, Germany, Belgium and the Netherlands also have Pegasus at their disposal, while Cyprus and Bulgaria may have served as countries of export, raising questions about export destinations and authorisations. These revelations raise concerns on various levels of the European legal order with respect to data protection and privacy, freedom of expression, freedom of the press, freedom of association, redress mechanisms, and democratic processes and institutions. In response to abusive surveillance practices, individuals and authorities are sounding out redress and enforcement options, such as individual litigation, formal complaints, infringement procedures and sanctions mechanisms for qualified rule of law deficiencies. The European Parliament has set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

As the Pegasus revelations shed light on the adverse effects of trade in and abuse of cyber-surveillance technologies, policymakers are seeking adequate responses. While the EU has made substantial progress in the areas of cybersecurity, civil liability, and privacy, improving the effectiveness of EU rules in these areas may help rein in the abuse of spyware. To curb internal spyware abuse, the EU could promote public and private enforcement of data and privacy rights and further clarify the preconditions and parameters for cyber-surveillance and public-private surveillance cooperation. In a more determined approach, the EU may introduce human rights controls in procurement directives, ensure that unlawfully obtained evidence is inadmissible (misconduct defeats its purpose), and stimulate discussions on the legal limits of intelligence outsourcing as well as on enhanced accountability mechanisms. Additionally, the EU or its Member States could promote responsible behaviour of cyber-espionage professionals, if necessary, by reasonably regulating the spyware industry without driving it away or underground (path of legality). To curb external (third-country) abuse, the EU may consider further promoting the adequate and uniform application of export controls and pursuing coherent foreign policies that limit the proliferation and abuse of spyware. To achieve greater impact, the EU may simultaneously pursue a multilateral approach, partnering with like-minded countries to steer the global spyware market and ostracise malicious actors. In all domains, civil society and regulators call for adequate, coherent and uniform implementation of existing and future policies, as well as practical guidance. To ensure a future-proof iteration of the next policy cycle, it appears beneficial to broaden research to include the design, trade and use of cyber-weapons in general.
Table of contents

1. Introduction .................................................................................................................. 1
2. Pegasus technology and trade ....................................................................................... 3
3. Pegasus operations in the EU ........................................................................................ 9
4. Legal concerns ............................................................................................................. 17
   4.1. Transversal concerns ............................................................................................... 17
   4.2. Country-specific concerns ...................................................................................... 20
      4.2.1. Hungary ........................................................................................................... 20
      4.2.2. Poland .............................................................................................................. 21
      4.2.3. Spain ................................................................................................................. 23
      4.2.4. Germany .......................................................................................................... 24
      4.2.5. Bulgaria and Cyprus ......................................................................................... 25
5. Individual and Member State actions .......................................................................... 28
6. EU actions ................................................................................................................... 34
7. Ways forward ............................................................................................................... 37
   7.1. For the public sector ............................................................................................... 37
      7.1.1. Map the spyware market and surveillance practices ........................................ 37
      7.1.2. Promote cyber resilience ............................................................................... 38
      7.1.3. Prevent internal spyware abuse ...................................................................... 41
      7.1.4. Prevent external spyware abuse ..................................................................... 62
   7.2. For the private sector ............................................................................................ 67
   7.3. For civil society .................................................................................................... 69
8. Synthesis and conclusions .......................................................................................... 70
9. Annex I: Preliminary remarks on responsibilities for national security .................... 74
10. Annex II: Preliminary remarks on the applicability of EU data and privacy protection .. 82
11. Annex III: EU framework for public procurement of security capabilities .............. 89
Table of figures

Figure 1: Digital Violence’s documentation of NSO conduct______________________________ 2
Figure 2: Data collected by Pegasus spyware_________________________________________ 3
Figure 3: Pegasus’ data transmission process__________________________________________ 4
Figure 4: Pegasus’ data presentation: Call log and call interception ______________________ 4
Figure 5: Impact of Citizen Lab’s report of 2016 on NSO servers ________________________ 8
Figure 6: Impact of Amnesty International and Citizen Lab reports on NSO domains _________ 8
Figure 7: Timeline of Pegasus operations in Hungary __________________________________ 9
Figure 8: Pegasus targets in Poland _________________________________________________ 12

Table of tables

Table 1: Summary table of EU-related Pegasus operations by Member States _____________ 16
Table 2: Atlantic Council’s partner-and-steer governance approach_______________________ 67
Table 3: Summary table of policy options __________________________________________ 72
1. Introduction

As the Pegasus revelations begin to unfold and the first Member States become implicated, one of the most high-profile spying scandals of recent years is coming to Europe. Primarily in 2021, Citizen Lab, Forbidden Stories, Amnesty International and 17 media organisations revealed that authoritarian and democratic governments used Pegasus software, developed by the Israeli NSO Group, to spy on journalists, lawyers, activists, opposition leaders, and former and present high-ranking state officials. Citizen Lab first detected the existence of the software in 2015 and began reporting on it in 2016. From a leaked list containing 50,000 phone numbers of potential spyware targets, the Pegasus Project found those of at least ten prime ministers, three presidents and one king. The list has not been released, but researchers and journalists are compiling datasets of individuals targeted with Pegasus. Researchers link the technology to the murder of the Saudi journalist Jamal Khashoggi and various human rights harms ranging from intimidation, to harassment, to detention.

Civil society and media organisations submitted plausible explanations for numbers appearing on the list, uncovered circumstantial evidence of Pegasus operations, and detected forensic traces of Pegasus on phones associated with the numbers on the list. In cooperation with Forbidden Stories – an NGO with a mission to protect, pursue and publish the work of other journalists facing threats, prison, or murder – Amnesty International analysed 67 devices, of which 37 showed clear traces of a Pegasus spyware infection, with 80% of the iPhones checked showing traces of Pegasus. Amnesty International's forensic methodology focuses on Apple iOS devices, since they contain significantly more forensic traces ('logs') accessible to investigators than stock Android.

---

1 For the sake of brevity, third-hand accounts are not always designated as such in the text. The manuscript was completed prior to the PEGA committee hearing on 'Stock-taking of EU spyware providers'.

2 The Pegasus Project, Forbidden Stories website.


4 Journalists contemplate that private actors may have gained access through corrupt officials. Others report that private companies used Pegasus malware and that an NSO employee abused the technology to target a love interest.

5 Landing page, NSO Group website; on the evolution of NSO Group's corporate structure, see Amnesty International et al., Operating from the shadows, briefing, 31 May 2021, p. 29 et seq.


8 Benjakob O., The NSO File, Haaretz, 5 April 2022; Sandvik R., Pegasus Project – Individuals listed, targeted or compromised, last updated 7 February 2022; Digital Violence platform, Forensic Architecture website, accessed 7 April 2022; Who's on the List, Organized Crime and Corruption Reporting Project website, accessed 7 April 2022.


11 About us, Forbidden Stories website, accessed 7 April 2022.

devices. New discoveries are made on a rolling basis. After receiving and cross-checking at least 37 mobile phone numbers, NSO's co-founder and CEO, Shalev Hulio, initially claimed neither the list nor the numbers received had anything to do with NSO. He cast serious doubt on the validity of the list, stating that ‘the average for our clients is 100 targets a year. If you take NSO’s entire history, you won’t reach 50,000 Pegasus targets since the company was founded. Pegasus has 45 clients, with around 100 targets per client a year.’ NSO contemplated that the list may simply comprise publicly accessible information, such as from HLR lookup services. Home location registers (HLR) are central databases kept by mobile phone companies that allow real-time queries of subscriber information, including their address, service entitlements and call-routing information. HLR lookup services query these databases to see if a specific mobile number is registered and what its rough location is. The services can be used as a step toward spying on targets. Telecommunication security expert Karsten Nohl, ex-chief scientist for Security Research Labs in Berlin, who prefaced his remarks by saying he had no direct knowledge of the NSO system, noted that HLR lookups and other SS7 queries (Signal System No. 7) are widely and inexpensively used by the surveillance industry – often for just tens of thousands of dollars a year.

As evidence of Pegasus surveillance in the EU mounts, Member States are coming under pressure to explain evidence of unjustified surveillance against EU citizens. While certain forms of cyber espionage may be justified in the event of serious threats to national or public security, its arbitrary deployment against EU citizens for personal and political gains is a clear violation of human rights.

Figure 1: Digital Violence's documentation of NSO conduct

Source: How the NSO Group Enables State Terror, Digital Violence website.

---

2. Pegasus technology and trade

Technology: Pegasus is a software capable of breaching mobile phones and collecting vast amounts of data stored or processed by the target system. Its manufacturer, the NSO Group, advertised it as a tool for ‘cyber warfare’ and the New York Times ornately termed it as ‘the world's most powerful cyber weapon’. According to NSO co-founder Shalev Hulio, such technologies became necessary with the emergence of encrypted mass communication and electronic communication providers that deny governments access to private communications (‘going dark’ problem). In comparison to bulk interception, which aims to indiscriminately collect and analyse vast amounts of data from access points in electronic communication infrastructure, Pegasus exploits vulnerabilities in mobile phones of pre-identified individuals, does not require the involvement of providers of electronic communications services, and combines a variety of electronic surveillance tools. It enables operators to read text messages, track calls, collect passwords, track locations, access and record microphone and camera devices, and harvest information from apps without the target noticing and across countries (‘extraterritorial reach’).

The spyware automatically downloads and installs to the target device after its operator either (i) misleads the target into clicking on an inconspicuous exploit link (‘SMS phishing link’), or (ii) spoofs the target device into connecting to a fake mobile network known as an IMSI catcher (‘network injection’), or (iii) exploits an unknown vulnerability (‘zero-click exploit’), i.e. without action by the target (‘self-executing’).

---

Figure 2: Data collected by Pegasus spyware

Source: NSO Group (purportedly), Pegasus – Product Description, Hacking Team leaks, ~ 2014, p. 16.

---


20 Bulk interception usually involves public authorities obliging telecommunications providers to intercept and share or provide access to transmitted communications content or related metadata for purposes of national security. On the distinction, see European Commission for Democracy through Law (Venice Commission), Report on the democratic oversight of signals intelligence agencies, CDL-AD(2015)011, Council of Europe, 15 December 2015, pp. 8-10; European Union Agency for Fundamental Rights (FRA), Surveillance by intelligence services, Vol. 1: Member States’ legal frameworks, Publications Office of the EU, 2017, pp. 17-18.

21 NSO Group (purportedly), Pegasus – Product Description, Hacking Team leaks, ~ 2014.

Google’s Project Zero considers that NSO has created ‘one of the most technically sophisticated exploits [they have] ever seen’.23 Once the software has infiltrated the system, it disables protection mechanisms and security updates.24 The infected device then transmits the collected data back to a Pegasus Data Server at the client’s premises, via the ‘Pegasus Anonymising Transmission Network’ – likely a proprietary NSO system intended to obfuscate the identity of the government client (see infographic below).25

Figure 3: Pegasus’ data transmission process

![Figure 3: Pegasus’ data transmission process](source)

According to the Society for Civil Rights,26 the NSO Group reserves full control over the technical infrastructure and decides on the modalities of infiltration, reconfiguration and data exfiltration.27 The attack vectors and infrastructure have evolved over time.28

According to a former NSO employee, Pegasus’ (client-facing) user interface is easy to use, sometimes only requiring the input of a target phone number.29 Reportedly, NSO introduced biometric checks to ensure only authorised persons could access the system after an NSO employee abused it.30

According to reports, the German Federal Criminal

![Figure 4: Pegasus' data presentation: Call log and call interception](source)

According to the Society for Civil Rights,26 the NSO Group reserves full control over the technical infrastructure and decides on the modalities of infiltration, reconfiguration and data exfiltration.27 The attack vectors and infrastructure have evolved over time.28

According to a former NSO employee, Pegasus’ (client-facing) user interface is easy to use, sometimes only requiring the input of a target phone number.29 Reportedly, NSO introduced biometric checks to ensure only authorised persons could access the system after an NSO employee abused it.30

According to reports, the German Federal Criminal

---

23 Beer I. and Groß S., A deep dive into an NSO zero-click iMessage exploit, Google’s Project Zero, 15 December 2021. An exploit is software, data, or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behaviour on software, hardware, or an electronic device.


26 A Berlin-based non-profit NGO that filed a formal complaint with the German Federal Commissioner for Data Protection and Freedom of Information against the use of Pegasus by the German Federal Criminal Police Office.

27 Moini B., Beschwerde gegen den Einsatz der Pegasus-Software durch das Bundeskriminalamt, Society for Civil Rights, 22 September 2021, p. 6. It should be noted that this is argued in the context of challenging the outsourcing of inherently governmental functions.


29 Cox J., NSO Employee Abused Phone Hacking Tech to Target a Love Interest, Vice’s Motherboard, 28 April 2020.

30 Cox J., NSO Employee Abused Phone Hacking Tech to Target a Love Interest, Vice’s Motherboard, 28 April 2020.
Police Office (BKA) transmitted target phone numbers to NSO in a hashed\textsuperscript{31} format, thereby preventing NSO from identifying the target person.\textsuperscript{32} Since German authorities allegedly bought a custom version of the software, this procedure may not be characteristic for all instances of Pegasus.

NSO contends that it only provides the software and does not ‘operate’ it. Reportedly, NSO products and services are compartmentalised in a way that no one person ever has full access to a working system and that in-house misuse would likely raise numerous red flags across the organisation.\textsuperscript{33} However, as early as 2018 a former employee, who later pleaded guilty and was sentenced to five years in prison, was able to steal the code from NSO.\textsuperscript{34}

Allegedly, NSO has no visibility into the spyware’s usage,\textsuperscript{35} but security experts call this into question.\textsuperscript{36} In an interview, Shalev Hulio explained that NSO can only access the system and conduct forensic investigation of possible abuses on request or with the permission of the client governments.\textsuperscript{37} NSO may, however, remotely shut down the Pegasus system where it suspects abuse (‘kill switch’).

The NSO also provides maintenance and technical support.\textsuperscript{38} Media sources stated that in at least one country an intermediary company, whose service technicians were certified to process classified information, provided technical support to the client government agency, presumably after receiving appropriate training from the NSO.\textsuperscript{39} Further unofficial and possibly outdated details may be found in the document named ‘Pegasus – Product Description’ that was discovered in the 2015 leaks concerning the competing Italian spyware vendor, Hacking Team.\textsuperscript{40}

**Trade:** NSO disclosed that it only licenses its software to vetted governments and exports through corporate entities based in Israel, Bulgaria, and Cyprus.\textsuperscript{41} According to media sources, in at least one country the software is licensed based on ‘surveillance objects and their context’.\textsuperscript{42} With one licence, governments can retrieve data not only from the designated target device, but also from a limited number of associated devices. Licences are limited to a certain number of targets and are geographically constrained (‘geofencing’).\textsuperscript{43}

Under the **Israel** 2007 Defence Export Controls Act, cybersecurity products, such as Pegasus, must receive export licences from Israel’s Defence Export Controls Agency.\textsuperscript{44} Reportedly, Israel’s Defence Minister Benny Gantz claimed that ‘as a matter of policy, the State of Israel authorizes the export of
cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism.\textsuperscript{45} Israel’s export control lists incorporate items from the Wassenaar Arrangement, an agreement between 42 states aimed at promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, and ‘additional factors’.\textsuperscript{46} Reportedly, Israel instrumentalised its ability to approve or deny access to NSO’s cyber weapons for diplomatic purposes.\textsuperscript{47} Recently, it was reported that ‘Israel blocked Ukraine from buying Pegasus spyware, fearing Russia’s anger’.\textsuperscript{48}

Already in March 2019, the NSO investor Novalpina Capital disclosed that ‘some of NSO’s products are exported from the EU (either Bulgaria or Cyprus), where the relevant authorities apply the EU control list (which is based on the Wassenaar control list)’.\textsuperscript{49} Both Cyprus and Bulgaria denied these allegations in response to an inquiry by Access Now.\textsuperscript{50} In the same vein, Cypriot authorities denied these allegations to the European Commission.\textsuperscript{51} Possibly, NSO did not export Pegasus from these countries, or authorities did not find reference to NSO Group in their database due to its complex corporate structure.\textsuperscript{52} According to an Amnesty International briefing, although ‘NSO Group Technologies Ltd. is a limited company incorporated and registered in Israel, ‘NSO Group’ is also an umbrella term used by the company and the media to refer to […] various related companies’\textsuperscript{53} (italics added for emphasis). NSO’s transparency report of 2021 confirmed that it is closely regulated by Bulgarian and Cypriot export control authorities.\textsuperscript{54} Following the 2021 revelations, the Commission stated that it would ‘raise the matter with competent national export control authorities’.\textsuperscript{55} Reportedly, the NSO Group closed an affiliated Cypriot exploitation company called Circles in 2020.\textsuperscript{56}

**Business ethics:** In a recent opinion piece, Shalev Hulio contends that ‘NSO was the first cyber intelligence company founded in Israel. Many other successful companies followed. It was the first regulated cyber intelligence company and the first to adopt the United Nations Guiding Principles for maintaining human rights. It was the first company to terminate contracts once suspicion of misuse of its technologies arose, even when it meant losing tens of millions of dollars. Pegasus is sold only to vetted agencies of governments allied with the U.S. and Israel, and NSO has refused to sell its product to some 90 countries owing to human-rights concerns.’\textsuperscript{57}

\textsuperscript{45} Spiro A., After NSO bombshell, Gantz asserts that Israel complies with international law, Times of Israel, 20 July 2021. The NSO Group corroborated this, see Washington Post Staff, Response from NSO Group to the Pegasus Project, The Washington Post, 19 July 2021.

\textsuperscript{46} Hindin D., Can Export Controls Tame Cyber Technology?: An Israeli Approach, Lawfare blog, 12 February 2016; What is the Wassenaar Arrangement?, Wassenaar Arrangement website.


\textsuperscript{48} Kirchgaessner S., Israel blocked Ukraine from buying Pegasus spyware, fearing Russia’s anger, The Guardian, 23 March 2022.


\textsuperscript{50} Krahulcova L., Is NSO Group’s infamous Pegasus spyware being traded through the EU?, Access Now, 12 September 2019.

\textsuperscript{51} Executive Vice-President Dombrovskis, Answer to question E-005505/2020, E-005505/2020(ASW), 8 January 2021.

\textsuperscript{52} Amnesty International et al., Operating from the shadows, briefing, 31 May 2021, pp. 29-58.

\textsuperscript{53} Amnesty International et al., Operating from the shadows, briefing, 31 May 2021, p. 31.

\textsuperscript{54} NSO Group, Transparency and responsibility report 2021, 30 June 2021, p. 29.

\textsuperscript{55} Vice-President Jourova, Answer to question P-003661/2021, P-003661/2021(ASW), 4 November 2021.

\textsuperscript{56} Cox J., NSO Group Closes Cyprus Office of Spy Firm, Vice’s Motherboard, 21 August 2020.

NSO changed its human rights policy in 2020 and aligned it with the UN Guiding Principles on Business and Human Rights, i.e. before the 2021 revelations broke, but after researchers had begun investigating and notifying NSO and investors of possible human rights violations.\(^{58}\)

Correspondence from 2019 between the (at the time prospective) NSO investor Novalpina Capital and Amnesty International indicates that Novalpina Capital conducted a due diligence assessment of NSO’s legal compliance, conscious of human rights concerns and prior to investing.\(^{59}\) It concluded that ‘NSO already operates under an ethical governance framework that is significantly more robust than any of its peers’ and that it intends to ‘ensure NSO operates in accordance with the UN Guiding Principles on Business and Human Rights’. In its latest transparency report, NSO emphasises its commitment to human rights and outlined its human rights risk assessment framework and customer oversight mechanism.\(^{60}\)

Amnesty International considers the transparency report ‘another missed opportunity’\(^{61}\) as it fails to address the issue of remediation for victims and fails to disclose pending lawsuits.\(^{62}\) In May 2021, Amnesty International released a report, indicating ‘how the lack of transparency about the company’s operations posed a serious obstacle for victims of unlawful surveillance to seek accountability and the right to remedy’\(^{63}\).

While NSO and associates apparently cooperated with civil society organisations, investigators themselves became targets of Pegasus hacks and (physical) undercover operations, presumably as part of a coordinated effort to collect information and discredit them.\(^{64}\) With a view to the EU context, two Palestinian lawyers and one Cypriot lawyer involved in suing NSO in Cyprus were targeted. A man who presented himself as a partner at Hong Kong-based ENE Investments approached the Cypriot lawyer via e-mail\(^{65}\) and flew her to London, ostensibly to discuss a potential lecture, but later the conversation turned to the prospects and funding of her NSO lawsuit.

---


\(^{60}\) [NSO Group, Transparency and responsibility report 2021](https://www.nso.com/), 30 June 2021.


\(^{64}\) Satter R., [AP Exclusive: Undercover spy exposed in NYC was 1 of many](https://apnews.com/article/b806f424148f34b62a1f671101dc6f32), Associated Press, 11 February 2019; Forensic Architecture, [Pegasus: Targeting the Investigators](https://digitalviolence.net/projects/pegasus), Digital Violence platform, 10 June 2021.

\(^{65}\) Satter R., [An Invitation to a Lecture](https://digitalviolence.net/projects/pegasus), email exchange, 10 February 2019.
Figure 5: Impact of CitizenLab’s report of 2016 on NSO servers


Figure 6: Impact of Amnesty International and Citizen Lab reports on NSO domains

3. Pegasus operations in the EU

In the EU, the Hungarian and Polish governments were the first to be caught in the eye of the storm, after media organisations uncovered extensive use of Pegasus spyware for political gains. Hungarian Fidesz MP Lajos Kósa and Polish Deputy Prime Minister Jarosław Kaczyński, as well as Polish Justice Minister Zbigniew Ziobro, first confirmed the acquisition of Pegasus by public authorities. Meanwhile, Spain finds itself in the throes of the Pegasus ‘cyclone’. The Spanish government initially denied knowledge of hacks against the then President of the Catalan Parliament Roger Torrent, but recently admitted to having intervened, with judicial authorisation, on 18 phones linked to the Catalan independence movement. In Hungary, Poland, and Spain, opposition figures draw comparisons to the US Watergate scandal, which led to President Richard Nixon’s resignation in 1974.

From over 300 leaked Hungarian telephone numbers, the investigative and whistle-blower platform Direkt36 identified (at the time of writing) 39 of the potential Pegasus targets. These include politicians, journalists, lawyers, former senior officials, (former) media magnates and their confidants, as well as one student. Many of the potential targets are critical towards the government or had privileged access to potentially

---

66 Tag Archives: Megfigyelések, Direkt36 website; Pegasus, telex website; Pegasus, tvn24.pl; Pegasus, wyborcza.pl.
67 After admitting that the Ministry of Interior had purchased Pegasus, Lajos Kósa was charged with misuse of classified information shared within the National Security Committee. However, the Prosecutor’s Office closed the investigation, because it found that Kósa’s statement was false and therefore did not qualify as a misuse offence. While the Hungarian government continued to deflect questions and obfuscate events, chairman of the National Security Committee and Jobbik MP János Stummer corroborated Kósa’s claims and re-confirmed them after the Prosecutor’s Office dropped the charges. Finally, Hungary’s data protection authority established that (at least) the Special Service for National Security, Nemzetbiztonsági Szakszolgálat (NBSZ), used the tool. For details, see Cseke B., Ügyészség: Nem a Belügyminisztérium vásárolta meg a Pegasust, így Kósa Lajos nem követett el bűncselekményt, telex, 25 November 2021; Panyi S., Ilyen foszlott szét a kormányzati közödéstis a Pegasus-ügyben, Direkt36, 6 November 2021; Világi M., Stummer szerint Kósa akár 3 év letöltendőt is kaphat, amígért beszélt a Pegasusról, de ő is látta a szerződést, telex, 4 November 2021; Cseke B., Ügyészség: Nem a Belügyminisztérium vásárolta meg a Pegasust, így Kósa Lajos nem követettei bűncselekményt, telex, 25 November 2021; Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Findings of the investigation of the NAIH launched ex officio concerning the application of the ‘Pegasus’ spyware in Hungary, NAIH-423-2/2022, 16 February 2022.
68 Premier Jarosław Kaczyński dla ‘Sieci’: opowieści opozycji o użyciu Pegasusa w celach politycznych to całkowite bzdury, wPolityce.pl, 7 January 2022; pp, akw/kab, Ziobro mówiąc o Pegasusie, odwołał się do wyroku TK. Adwokat: władza nie tylko zlekceważyła ten wyrok, ale poszła o niebo dalej, tvn24, 7 January 2022.
70 Gil J., El ataque a los móviles de Torrent y Maragall con un programa espía israelí desata una tormenta política, El País, 15 July 2020.
71 Casqueiro J. and Hermida X., Los silencios y respuestas que deja Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022; Hermida X., Una comisión de secretos sin secreto, El País, 9 May 2022; González M., La directora del CNI confirma el espionaje legal y autorizado a 18 independentistas, incluido Pere Aragonés, El País, 5 May 2022.
73 Tag Archives: Megfigyelések, Direkt36 website.
74 Panyi S. and Pethő A., President of the Hungarian Bar Association and several other lawyers have been targeted by Pegasus, Direkt36, 20 July 2021.
compromising or otherwise politically sensitive information.

Forensic analysis proved attempted and successful hacking of phones belonging to the opposition publisher Zoltán Páva and various journalists, including Szabolcs Panyi and András Szabó as well as Brigitta Csikász and Dániel Németh. Many other identified individuals had changed phones in the meantime, declined analysis, or refused to comment. Nevertheless, Direkt36 established that the timeline of suspected hacking correlates with conspicuous events that would provide for plausible explanations, including political rifts and the consolidation of power by potential and actual rivals. Examples include former State Secretary Attila Ászódi, who disagreed with a Hungarian cabinet member over plans to expand a nuclear power plant, former and current protective details of the Hungarian President, János Áder, and lawyer László Vértesy, who oversees elections and worked for opposition party Jobbik. While the government did not comment on specific cases, Minister of the Prime Minister’s Office Gergely Gulyás stated that some of the press reports on Pegasus surveillance had a factual basis.

Reportedly, the speaker of the Hungarian Parliament, László Kövér, told Hungarian intelligence services that the opposition is the greatest national security threat. In turn, the opposition called for his resignation.

In Poland, the Pegasus scandal is unravelling on a case-by-case basis.\textsuperscript{80} It appears that Pegasus was taken up in ongoing – possibly politically motivated – investigations of corruption and deployed in a similar fashion as in Hungary. Reportedly, the Pegasus system was acquired by the Central Anti-Corruption Bureau (\textit{Centralne Biuro Antykorupcyjne}, CBA) and first used in Poland in 2017 to surveil former spokesman of the Ministry of National Defence Bartłomiej Misiewicz and former PiS MP Mariusz Antoni K., now accused of influence peddling and exposing the Polish Armaments Group to a loss of 1.2 million złotys.\textsuperscript{81} Other potential Pegasus targets formerly associated with the ruling party PiS include Adam Hofman and Dawid Jackiewicz, who were involved in the ‘Wrocław Collusion’ corruption affair.\textsuperscript{82} According to sources, Katarzyna Kaczmarek, the wife of former CBA agent and former PiS MP Tomasz Kaczmarek (‘agent Tomek’), was surveilled with Pegasus due to her...
knowledge of potentially damaging information about the internal affairs of Mariusz Kamiński, Minister of the Interior and Administration and Coordinator of Special Services.83

Most prominently, targets include opposition figures and their associates, such as: lawyer (and former politician) Roman Giertych, representing opposition leaders including Donald Tusk, who, according to his lawyer, was the real target;84 prosecutor Ewa Wrzosek, who launched an investigation into the organisation of the (eventually called-off) May 2020 presidential elections by postal voting; opposition Senator Krzysztof Breza, as well as his father and former assistant; founder of the ‘Agrounia’ farmers’ movement Michał Kołodziejczak; journalist Tomasz Szwiegier, co-author of a book about Kamiński’s activities as CBA chief; and possibly former (under the Civic Platform government) head of the Central Anti-Corruption Bureau Paweł Wojtunik, as well as former Minister of Transport Sławomir Nowak, who was arrested three days before the second round of the presidential election on suspicion of corruption, management of an organised criminal group, and money laundering.85 Concerning the latter, Mariusz Kamiński formally rejected allegations that Sławomir Nowak was under surveillance in the run-up to elections.86 Roman Giertych assumes that messages obtained through Pegasus were modified and disseminated as part of smear campaigns to discredit him.87 Recently, it was revealed that the President of Employers of Poland, Andrzej Malinowski, had been surveilled with Pegasus.88 He suspects that this could have been related to, among other things, his activities in the Social Dialogue Council, his contacts in Poland and abroad, and his columns critical of PiS, published in Rzeczpospolita.

Additionally, relatives of potential and confirmed Pegasus targets have fallen victim to spoofing attacks.89

---

84 EPP Group, Public Hearing – Pegasus spyware scandal and its impact on democracy in the EU, 10 February 2022, 00:37:00-00:38:24.
86 Minister of the Interior and Administration Mariusz Kamiński, Oświadczenie ws. śledztwa przeciwko Sławomirowi N., Rada Ministrów w Polsce, 23 July 2020.
87 EPP Group, Public Hearing – Pegasus spyware scandal and its impact on democracy in the EU, 10 February 2022.
88 Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 29 April 2022.
According to unofficial information, over 6000 Pegasus attacks were carried out on mobile devices used by employees of the Supreme Audit Office (NIK), and 500 devices were compromised. The Supreme Audit Office, headed by Marian Banaś, who has broken ranks with the PiS, heavily nuanced these allegations in a press conference, clarifying that investigations are still ongoing, but that over 700 attempted cyberattacks had been detected and that it could not rule out that Pegasus was used. In the meantime, spokesperson of the Minister-Special Services Coordinator Stanislaw Żaryn formally rejected the allegations.

In the Spanish context, researchers working with WhatsApp first alerted in 2020 former President of the Catalan Parliament and now Minister of Business and Labour in the Catalan Government Roger Torrent, and another prominent member of the Catalan independence movement, regional deputy Ernest Maragall, that their phones had been targeted with the Pegasus spyware. A Citizen Lab report from 18 April 2022, revealed that at least 65 Catalans had been targeted with spyware, including Members of the European Parliament, Catalan Presidents, including current Catalan

---

92 Rzecznik Ministra Koordynatora Służb Specjalnych, Oświadczenie, Rada Ministrów w Polsce, 4 February 2022.
President Pere Aragonès, legislators, jurists, and members of civil society organisations. Sixty-three Catalans were targeted with Pegasus and four others with Candiru (at least two were targeted with both). Of the 63 Pegasus targets, forensics confirmed 51 successful intrusions, and circumstantial evidence suggests a nexus with Spanish authorities. The Director of Citizen Lab, Ron Deibert, responded to a number of concerns regarding Citizen Lab’s research and independence in a letter to a group of Spanish MEPs.

Despite early suspicions, the Spanish government initially denied or deflected knowledge of hacks. However, the Spanish press reported that, in a recent appearance before the Official Secrets Committee of the Spanish Congress, the Director of the National Intelligence Centre (CNI) admitted to having intervened, with judicial authorisation, on 18 phones linked to the Catalan independence movement. At least partially, these surveillance operations are grounded in containing threats posed by separatists to the ‘territorial integrity, the supremacy of the Constitution, and the rule of law’. Sources alleged that the CNI had bought the Pegasus software for about six million euro to spy abroad. The Spanish Prime Minister further clarified that neither the Police nor the Civil Guard had Pegasus at their disposal.

A fortnight after CatalanGate broke, Minister of the Presidency Félix Bolaños announced that the phones of Prime Minister Pedro Sánchez and Defence Minister Margarita Robles had been hacked in May and June 2021. Later, the government confirmed that the phone of the Minister of the Interior Fernando Grande-Marlaska had also been hacked and that an attempt on the phone of the Minister of Agriculture Luis Planas had failed. The dates of intrusions coincide with Spain’s entanglement in the Ceuta migratory crisis, during which (according to estimates) at least 8,000 immigrants entered into Ceuta in the face of passive Moroccan gendarmerie. Additionally, Spain was in the process of granting pardons to nine Catalan separatists who were convicted over a failed independence bid in 2017. Commentators appear to suspect Morocco of intelligence operations against the Spanish government, but the Spanish government refuses to

---

94 Scott-Railton J. et al., ‘CatalanGate’, Citizen Lab, 18 April 2022; Landing page, CatalanGate website.
96 González M., Spain’s intelligence service has spyware program that targeted Catalan politicians, El País, 16 July 2020; Franceschi-Bicchierai L. and Cox J., Source: Spain is Customer of NSO Group, Vice’s Motherboard, 14 July 2020.
97 Gil J., El ataque a los móviles de Torrent y Maragall con un programa espía israelí desata una tormenta política, El País, 15 July 2020.
98 Casqueiro J. and Hermida X., Los silencios y respuestas que deja Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022; Hermida X., Una comisión de secretos sin secreto, El País, 9 May 2022; González M., La directora del CNI confirma el espionaje legal y autorizado a 18 independentistas, incluido Pere Aragonés, El País, 5 May 2022.
99 Casqueiro J. and Hermida X., Los silencios y respuestas que deja Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022; Hermida X., Sánchez asegura que desconocía el espionaje a los independentistas, pero lo justifica, El País, 26 May 2022.
100 González M., El CNI compró el sistema Pegasus para espiar en el extranjero, El País, 20 April 2022.
102 González M., El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus, El País, 2 May 2022; For more information on the National Cryptological Centre (Centro Criptológico Nacional), which detected the intrusion, see El País, ¿Qué es el Centro Criptológico Nacional que ha detectado el espionaje a Sánchez y Robles?, El País, 2 May 2022.
103 Rodríguez J., El ministro Luis Planas sufrió un ataque fallido de Pegasus en plena crisis con Marruecos, El País, 10 May 2022; González M., El CNI halla rastros de Pegasus en el móvil de Grande-Marlaska, El País, 5 May 2022.
The Guardian reported that the leaked list of possible Pegasus targets contains 200 Spanish mobile phone numbers. Reportedly, the German Federal Criminal Police Office (Bundeskriminalamt, BKA) admitted to buying a modified version of the software and to deploying it in a 'mid-single-digit' number of cases. According to research by several news outlets, the German Federal Intelligence Service (Bundesnachrichtendienst, BND) also uses this software, but little is publicly known about the specific intelligence operations.

Both the Belgian Federal Police (Federale Politie) and Dutch General Intelligence and Security Service (Algemene Inlichtingen-en Veiligheidsdienst, AIVD) have the Pegasus software at their disposal. According to four sources, the Dutch intelligence service used Pegasus to surveil Ridouan T. in 2019, who was a fugitive at the time and hiding abroad. In security circles, it was unofficially confirmed that Belgium is using Pegasus in the fight against serious crime, such as drug trafficking, child abuse, and terrorism.

In France, high-ranking state officials, including the French President, Emmanuel Macron, and five French ministers, as well as journalists, were hacked. After conducting their own investigations, NSO co-founder and CEO Shalev Hulio repeatedly and firmly rejected allegations that President Macron and members of the French Parliament had been hacked. French authorities denied contracting with the NSO Group; French cases are suspected to be part of Moroccan intelligence operations.

Finnish diplomats stationed abroad were also targeted. It is also suspected that former Belgian Prime Minister Charles Michel, US-Belgian citizen Carine Kanimba, Belgian human rights activist El Mahjoub Maliha, and possibly Belgian journalist Peter Verlinden and his wife were subject to surveillance.

---

105 Kirchgaessner S. and Jones S., Over 200 Spanish mobile numbers ‘possible targets of Pegasus spyware’, The Guardian, 3 May 2022; On Moroccan spying in Spain, see López-Fonseca O., Una década de espías marroquíes en España, El País, 6 May 2022.
107 Flade F. et al., BKA bekam maßgeschneiderten Trojaner, Tagesschau, 8 October 2021.
113 Pollet M., France denies talks to buy Israeli Pegasus spyware, Euractiv, 24 November 2021.
114 La rédaction de Mediapart, Pegasus: French judicial probe confirms technical proof of espionage against Mediapart journalists, Mediapart, 30 July 2021.
According to the most recent reports, Commissioner Didier Reynders and senior EU officials were targeted by NSO’s software ‘ForcedEntry’, which serves foreign spy agencies to remotely and invisibly take control of iPhones. The Bulgarian Prime Minister Kiril Petkov stated that there are no indications that Bulgarian services used Pegasus.117 Recently, reports revealed that a Greek journalist was spied on with a similar spyware called ‘Predator’, which is developed by a company called Cytrox with possible customers in Greece.118

Reportedly, most of the NSO Group’s clients ‘are within the European Union’, but governments declined to comment;119 NSO’s CEO Shalev Hulio is reported to have stated that ‘almost all governments in Europe are using [NSO’s] tools’.120 Besides targeting of EU citizens protected by EU law, Pegasus cases feature a variety of European dimensions, including (i) spying on one’s own nationals who are visiting other Member States (Polish lawyer Roman Giertych and possibly members of the Catalan independence movement), (ii) domestic spying on residents from other Member States (Belgian-Canadian student activist Adrien Beauduin), (iii) spying on the confidant of then President of the European Council Donald Tusk, after Tusk changed his mobile phone number (Polish lawyer Roman Giertych), (iv) surveillance attacks in the run-up to the European elections in 2019 (Polish Senator Krzysztof Brejza), (v) the direct or indirect (relational targeting) spying on Catalan MEPs, and (vi) the targeting of Commissioner Didier Reynders and senior EU officials (by means of NSO’s software ‘ForcedEntry’).121

---


118 Triantafyllou E. and Telloglou T., Who was tracking the mobile phone of journalist Thanasis Koukakis?, Inside Story, 11 April 2022; CitizenLab and Meta (formerly Facebook) identified Cytrox’s Predator customers in Greece, see Marczak B. et al., Pegasus vs. Predator, CitizenLab, 16 December 2021 and Dvilyanski M. et al., Threat Report on the Surveillance-for-Hire Industry, Meta, December 2021, p. 10; According to an unnamed Greek prosecutor, investigations have been launched, see Georgiopoulos G., Greek prosecutor to probe alleged bugging of journalist’s phone, Reuters, 21 April 2022; The government spokesperson appeared convinced that the monitoring had been carried out by a private person, see Government Spokesman Mr. I. Economou, Η ενημέρωση των πολιτικών συντακτών, MediaGovGR, 11 April 2022.

119 EPP Group, Public Hearing – Pegasus spyware scandal and its impact on democracy in the EU, 10 February 2022.

120 Farrow R., How Democracies Spy on Their Citizens, The New Yorker, 18 April 2022.

121 EPP Group, Public Hearing – Pegasus spyware scandal and its impact on democracy in the EU, 10 February 2022, [EN version] 00:33:50-00:34:31 and 00:36:32-00:38:30; 00:38:30-00:39:10 and 00:41:15-00:42:42; 00:53:14-00:53:18 and 00:53:45-00:54:05; and 01:10:32-01:11:12; Scott-Railton J. et al., CatalanGate, Citizen Lab, 18 April 2022; Satter R. and Bing C., Exclusive: Senior EU officials were targeted with Israeli spyware, Reuters, 11 April 2022.
Table 1: Summary table of EU-related Pegasus operations by Member States

<table>
<thead>
<tr>
<th>EU countries</th>
<th>Public authorities used Pegasus</th>
<th>Public authorities authorised the export of Pegasus</th>
<th>Citizens or residents were targeted (including by third countries)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hungary</td>
<td>Officially confirmed</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>Poland</td>
<td>Officially confirmed</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>Germany</td>
<td>Reportedly confirmed to oversight committee</td>
<td>No indications</td>
<td>Presumably, since use confirmed and within remit</td>
</tr>
<tr>
<td>Spain</td>
<td>Reportedly confirmed to oversight committee</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>France</td>
<td>Officially denied and suspicion deflected</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>Finland</td>
<td>No indications</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>Belgium</td>
<td>Reportedly confirmed by confidential sources</td>
<td>No indications</td>
<td>Forensically confirmed</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Reportedly confirmed by confidential sources</td>
<td>No indications</td>
<td>Possibly</td>
</tr>
<tr>
<td>Italy</td>
<td>No indications</td>
<td>No indications</td>
<td>Visiting Polish lawyer Giertych was targeted cross-border</td>
</tr>
<tr>
<td>Cyprus</td>
<td>No indications</td>
<td>Possibly</td>
<td>No indications</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>No indications</td>
<td>Possibly</td>
<td>No indications</td>
</tr>
</tbody>
</table>

Source: Author’s own illustration. In a similar case, see the customer list of the Italian spyware vendor Hacking Team.
4. Legal concerns

4.1. Transversal concerns

Pegasus surveillance in Europe raises a variety of legal concerns at different levels of the European legal order. Since the legality of intelligence operations depends on the – not yet established – facts of the particular case as well as the applicable legal framework, a universally valid assessment is hardly possible. Intelligence services used Pegasus in modified configurations and for different purposes within different legal orders. Concerns arise regarding Pegasus' presumed non-compliant default configuration and its deployment in cases where apparently no serious and genuine threat to national or public security was present or foreseeable, as well as in legal orders where deployment conditions appear permissive and redress mechanisms ineffective. Such cases put data protection and privacy rights, freedom of expression, freedom of the press, freedom of association, redress mechanisms, democratic processes and institutions, and possibly rules of evidence (admissibility) to the test.

Cases of spyware abuse raise concerns over the procedural and substantive lawfulness of surveillance practices and the level of protection granted by European and national law, i.e. necessary safeguards on government hacking. In his preliminary remarks, the European Data Protection Supervisor (EDPS) indicates that Pegasus surveillance as described in the media would likely interfere with the essence of the right to privacy and be prohibited irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state. Nevertheless, certain configurations of the software may pass the necessity and proportionality test in the event of serious threats, such as an imminent terrorist attack. Most prominently, victims may invoke their human and constitutional rights to data protection and privacy before the European Court of Human Rights (ECtHR) and national courts. It should be noted that the ECtHR may draw on the Council of Europe Convention 108+ to interpret the ECHR, but cannot directly enforce it.

---

123 Pegasus: the new global weapon for silencing journalists, Forbidden Stories website; ECtHR, Guide on Article 10 of the European Convention on Human Rights, 30 April 2021, p.60 and p. 112.
129 ECtHR, Practical Guide on Admissibility Criteria, 1 February 2022.
130 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
131 Bygrave L., Data Privacy Law: An International Perspective, Oxford University Press, 2014, pp. 35-36: 'While the Convention requires contracting states to incorporate its principles into their domestic legislation (Article 4(1)), it is not intended to be self-executing.' According to its Explanatory Report, 'individual rights cannot be derived from it'. All EU countries involved in the Pegasus scandal ratified Convention 108, though Belgium did not ratify the amending protocol. Notwithstanding, any party may denounce the treaty at any time, though not retroactively. Convention 108+ will enter into force once all parties to ETS 108 ratify the treaty, or on 11 October 2023 if there are 38 Parties to the Protocol at this date. To date, Poland, Bulgaria, Cyprus, Germany, Poland and Spain have ratified Convention 108+, while Belgium, France and Hungary have only signed it.
Prospects for successful litigation are rising, as researchers have identified a trend in ECtHR case law towards assessing the quality of Member States’ laws.\(^{132}\) According to the ECtHR’s research division: ‘States are recognised to have a certain – even large – measure of discretion when evaluating threats to national security and when deciding how to combat these. Nevertheless, the Court now tends to require national bodies to verify that any threat has a reasonable basis in fact.’\(^{133}\) The utility of resorting to the *international* human rights framework is challenged by inherent enforcement constraints.\(^{134}\)

**EU law** provides for various preventive and non-preventive enforcement mechanisms, ranging from infringement procedures,\(^{135}\) to formal complaints, to dedicated sanctioning mechanisms for qualified rule of law deficiencies.\(^{136}\) While implicated Member States may attempt to challenge the applicability of EU law with respect to their perceived exclusive competence for national security, the CJEU recently underlined that ‘the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable’.\(^{137}\) Assuming EU competence and that Member States acted within the scope of Union law such as the EU data protection *acquis*,\(^{138}\) aggrieved individuals may also rely on the EU Charter of Fundamental Rights when seeking redress. In a cross-border case, the Hungarian Civil Liberties Union (HCLU) suggests the right to free movement of persons and workers has been violated.\(^{139}\) Against the backdrop of the Snowden revelations and challenges to data retention directives, the ECtHR and CJEU have developed fairly extensive case law for bulk and targeted data retention involving electronic communications services.\(^{140}\) (For more information, see Section ‘7.1.3. Prevent internal spyware abuse’, as well as Annex I and II).

---


\(^{133}\) National security and European case law, case law research report, ECtHR’s Research Division, 2013; For recent rulings on surveillance operations, see Judgment in *Case with application nos. 58359/12 and 2 others*, Haščák v. Slovakia, ECtHR, 23 June 2022 and Judgment in *Case with applications nos. 58361/12 and 2 others*, Zoltán Varga v. Slovakia, ECtHR, 20 July 2021.


\(^{135}\) Infringement procedure, European Commission website.


\(^{137}\) Judgment in *Joined Cases C-511/18, C-512/18 and C-520/18*, La Quadrature du Net, CJEU, 6 October 2020, para. 99.

\(^{138}\) Additionally, national intelligence operators may have acted well within the scope of EU secondary data protection law, rendering the EU Charter of Fundamental Rights applicable (Article 51(1) EU CFR). For details, see section ‘7.1.3. Prevent internal spyware abuse’ and Annex I.


MEPs Robert Biedroń (S&D, Poland) and István Ujhelyi (S&D, Hungary) requested that the European Commission pay particular attention to the Pegasus scandal in its rule of law reports on Hungary and Poland, planned for July this year. If violations are found in these reports, preventative and sanctioning mechanisms may be initiated. So far, the preventative arm of Article 7 of the Treaty on European Union (TEU) has been triggered twice; firstly by the European Commission against Poland, and secondly by the European Parliament against Hungary. Alongside corruption, the independence of the judiciary and limitations on various freedoms, in September 2018 the European Parliament raised serious privacy and data protection issues as regards Hungary, including the failure to execute the intelligence-related ECtHR judgment Szabó and Vissy v. Hungary. At the time of writing, EU institutions have never operationalised the sanctions arm of Article 7 TEU and could only effectively do so in the most extraordinary circumstances (‘serious and persistent breach’ of EU values). Although the CJEU recently upheld the rule of law conditionality as a viable sanctioning instrument, in the Pegasus context it may prove difficult to establish ‘breaches of the principles of the rule of law in a Member State [that] affect or seriously risk affecting the sound financial management of the Union budget or the protection of the financial interests of the Union in a sufficiently direct way’ (italics added for emphasis). Nevertheless, surveillance abuses may well feed into the rule of law report and arguably bolster enforcement measures. On 5 April 2022, Commission President Ursula von der Leyen announced that the Commission will send the Hungarian government the letter of formal notification to start the conditionality mechanism, mainly over corruption concerns.

The proliferation of cyber capabilities in the international arms markets and the risk of technology winding up in the wrong hands draws policymakers’ attention to the governance of cyber weapons markets. New business models providing governments with offensive – as opposed to defensive – cyber capabilities in return for remuneration, known as ‘access-as-a-service’ or ‘pay-to-play’, are promoting the spread of cyber capabilities. Principally, the dissemination of cyber weapons is regulated by international, supranational and national export control mechanisms. The EU has just recast its dual-use export controls (Regulation (EU) 2021/821) and included an authorisation requirement for the export of cyber surveillance items likely to be used for internal repression or
serious violations of human rights and international humanitarian law (‘catch-all controls’).\textsuperscript{149} Save for exceptional authorisation requirements for intra-Union transfers, the Regulation principally applies to exports from the EU to third countries. On an international level, 42 states committed to the (non-binding) Wassenaar Arrangement. Its effectiveness in curbing the proliferation of cyber surveillance technologies such as Pegasus is constrained by its limited and voluntary membership, its specific list of cyber weapons qualifying as dual-use items, and uneven implementation.\textsuperscript{150}

4.2. Country-specific concerns

Besides these general considerations, country-specific legal concerns have emerged. In the vast majority of Member States, intelligence services are regulated by laws. The legal frameworks typically consist of provisions on the organisation and functioning of these services as well as their mandates and powers, including their means of action and conditions for using them. To avoid abuse of power, to legitimise the exercise of intrusive powers, and to continuously improve intelligence outputs, states have introduced oversight mechanisms. In line with the Venice Commission reports on oversight of security services and signals intelligence agencies, as well as other studies, the general consensus is that oversight should be an effective combination of executive control, parliamentary oversight, expert bodies, and judicial review.\textsuperscript{151} In light of different democratic legal orders, there is no one-size-fits-all solution. A number of concerns have been raised regarding Hungary and Poland’s permissive intelligence frameworks, ineffective checks and lax oversight practices. In Spain, parliamentary control has been absent for the past three years and experts criticise vague and outdated judicial control. In Germany, Bulgaria and Cyprus, issues largely mirror debates surrounding data protection and export controls at EU level.

4.2.1. Hungary

In Hungary, the Minister of Justice is responsible for authorising the Special Services for National Security (\textit{Nemzetbiztonsági Szakszolgálat, SNSS}) to conduct intelligence operations by means of Pegasus (‘external authorisation’).\textsuperscript{152} In response to a written question, Secretary of State Róbert Répássy confirmed that ‘the secret collection of information is authorised by the Minister for Justice, [...] in the event of his impediment, he shall be replaced by the Parliamentary Secretary of State’.\textsuperscript{153} Minister of Justice Judith Varga routinely delegated her power to authorise secret surveillance requests to Répássy’s predecessor, former Secretary of State Pál Völner, who recently resigned after

\textsuperscript{149} EU Dual-Use Regulation (EU) 2021/821 (recast); Immenkamp B., \textit{Review of dual-use export controls}, Briefing, EPRS, European Parliament, July 2021; van Daalen O. et al., \textit{The new rules for export control of cyber-surveillance items in the EU}, Institute for Information Law, June 2021; For more information, see section ‘7.1.4. Prevent external spyware abuse’.


\textsuperscript{152} Hungarian Helsinki Committee, \textit{National intelligence authorities and surveillance in Hungary}, FRA, 26 September 2014, p. 2 and p. 4.

being accused of corruption.154 Democratic Coalition MP Ágnes Vadai considers that Judith Varga illegally delegated her power and the opposition has called for Varga's resignation.155 Conversely, Hungarian Minister of the Prime Minister's Office Gergely Gulyá sees no problem with this approach.156 According to Varga, Interior Minister Sándor Pintér is responsible for operational aspects of the surveillance activities.157 If the ordering took place exclusively in the realm of the executive and without meaningful external control, human rights concerns about oversight arise.158 According to a communication of the HCLU to the Council of Europe Directorate General of Human Rights and Rule of Law, the insufficient oversight and protection mechanisms detected in the Szabó and Vissy v. Hungary ruling of January 2016 remain unresolved.159

4.2.2. Poland

Contrary to a statement by Stanisław Żaryn, the Spokesperson of the Minister Coordinator of Special Services, judge Beata Morawiec, prosecutor Ewa Wrzosek, General Piotr Pytel and Professor Andrzej Zoll do not believe that the Polish authorities could deploy Pegasus legally against their own citizens, and former CBA chief Paweł Wojtunik considers the collected data as inadmissible.160 Żaryn stated that surveillance in Poland is carried out after obtaining the consent of the Prosecutor General's Office and obtaining court approval where necessary.161 Former deputy head of the Internal Security Agency Paweł Białek indicates that, if intelligence services share this position, the authorisation procedures should be examined in view of the wide circle of potential targets.162 Reportedly, judges have to process up to 70 surveillance applications per day after completing their adjudication duties, which results in the approval of most of them.163 Other media sources suggest...
that Pegasus surveillance likely took place outside the designated procedures.\(^{164}\) Prosecutor Ewa Wrzosek considers that the use of the programme is absolutely contrary to the law and conflicts with the CBA Act, \textit{Ustawa o Centralnym Biurze Antykorupcyjnym}.\(^{165}\) Former President of the Supreme Court Professor Adam Strzembosz considers that, if the use of Pegasus had been known about in 2019, the elections ought to have been invalidated,\(^{166}\) and Professor Marcin Rojszczak has traced the dismantling of key safeguards in Poland.\(^{167}\)

As early as 2019, former Commissioner for Human Rights Professor Adam Bodnar and a group of experts proposed to establish an independent institution to supervise the special services, taking into account ECtHR caselaw (see also the Article 8 guide) and the opinion of the Venice Commission of 2016 on amending the Police Act and certain other acts.\(^{168}\) The current Commissioner for Human Rights, Professor Marcin Wiącek, called on the Prime Minister to adapt the rules of surveillance to constitutional and European standards.\(^{169}\) Former director of the Government Centre for Security and former Deputy Minister of the Interior Antoni Podolski criticised the approach, as the PiS-controlled lower house would elect the members of the proposed supervisory body, and suggested a Parliament-centric approach guaranteeing parity to establish democratic control.\(^{170}\)

According to investigations by a Polish news outlet, the Central Anti-Corruption Bureau (\textit{Centralne Biuro Antykorupcyjne}, CBA) may have illegally bought the software with funds from the Polish Justice Ministry dedicated to victims of crime.\(^{171}\) In a Senate Special Committee hearing, former head of the CBA Paweł Wojtunik pointed out that such a purchase would have adverse effects on the institution’s independence.\(^{172}\) As stated elsewhere, the CBA would hardly control the Minister of Justice after accepting illegal funding and risking implication or even self-incrimination.\(^{173}\) The President of the Supreme Audit Office (NIK), Marian Banaś, confirmed the illegality of the co-financing and stated that the current regulations did not provide for effective supervision and did not guarantee the detection of irregularities.\(^{174}\) Allegedly, the Polish spyware trading company Matic, which is said to serve as a cover and avoid suspicion of Polish intelligence secrets passing

\(^{164}\) Czuchnowski W., \textit{Krag podejrzanych w sprawie Pegasusa. Kto odpowiada za inwigilację Brejzy i Giertycha}, wyborcza.pl, 28 December 2021.


\(^{172}\) Polish Senate, \textit{Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała byłego szefa CBA i byłego wiceministra MSWiA}, 15 February 2022.


\(^{174}\) Polish Senate, \textit{Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała prezesów NIK}, 18 January 2022.
through the hands of foreigners (NSO Group servers), earned a margin of 8.4 million zlotys, and another 8.4 million zlotys for testing and training (together almost 3.95 million euro, based on the average exchange rate in 2017). Wojtunik noted that a direct purchase from the NSO Group would be cheaper and more transparent, but that adversaries could more easily discern which tools the CBA has at its disposal.

4.2.3. Spain

In Spain, notably Members of the Catalan independence movement and other critics frame state espionage as a violation of fundamental rights and a threat to democracy. Conversely, CNI Director Paz Esteban repeatedly emphasised that the 18 state surveillance operations were judicially authorised by the Supreme Court and submitted the court orders to the Official Secrets Committee of the Spanish Congress. Reportedly, the judge justified several of these authorisations on the grounds of 'attacking and putting the most precious assets of the Spanish State, territorial integrity, the supremacy of the Constitution, and the rule of law at stake' (unofficial translation). Although surveillance was initially granted only for three months, some were later extended successively, in some cases more than a dozen times. Allegedly, they were nominal, reasoned, and limited in time, as required by the applicable legal framework. Prime Minister Pedro Sánchez stated that he did not know about the espionage on the separatists, but justified the operations by claiming that the unrest in Catalonia in the autumn of 2019, following the judicial conviction of the pro-Catalonia leaders, posed a threat to national security.

Some academics and commentators criticise the Spanish oversight mechanisms as being insufficient and superficial. Organic Law 2/2002 prescribes a special procedure to request judicial authorisation for CNI-related surveillance activities, and Law 11/2002 of 6 May establishes parliamentary control by the Official Secrets Committee of the Spanish Congress.


176 Democracy at risk, CatalanGate website; Pallín J., Pegasus: un caballo desbocado, El País, 9 May 2022.

177 Casqueiro J. and Hermida X., Los silencios y respuestas que dejó Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022.

178 Rincón R., El permiso judicial para espionar a independentistas: nominal, motivado y limitado en el tiempo, El País, 10 May 2022; Casqueiro J. and Hermida X., Los silencios y respuestas que dejó Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022.

179 Hermida X., Sánchez asegura que desconocía el espionaje a los independentistas, pero lo justifica, El País, 26 May 2022; Noguer M. and Baquero C., Las protestas se radicalizan en Cataluña con el apoyo de Torra, El País, 16 October 2019.

180 e.g. Revenga Sánchez M., El control del Centro Nacional de Inteligencia: una perspectiva comparada, Revista Española de Derecho Constitucional, No. 116, 2019, pp. 13-44; Díaz Fernández A.M., ‘Halfway down the road to supervision of the Spanish intelligence services’, Intelligence and National Security, Vol. 21(3), 2006; Ridao J., Cómo se controla el CNI, El País, 30 April 2022; however, practice shows that the problem is not the secrecy of its meetings – something that is chimerial today – but the fact that they are ritual sessions in which nothing relevant is reported, and even less of any secrecy; Hermida X., Una comisión de secretos sin secreto, El País, 9 May 2022: committees of this kind exist in the US Senate, the British Parliament, and the French Assembly, and they must all deal with the same contradiction – how to manage state secrets in a place like Parliament, whose function demands transparency.

182 For more on Spanish intelligence accountability, see Ridao J., Cómo se controla el CNI, El País, 30 April 2022; Jiménez-Pérez D., Legitimidad y control del Centro Nacional de Inteligencia, Grupo de Estudios en Seguridad Internacional
Diego López Garrido, professor of constitutional law and member of the Official Secrets Commission during his time as Socialist spokesperson, argues: ‘The CNI can ask a judge for authorisation to intercept communications on the grounds of a threat to the territorial integrity of Spain or the stability of the rule of law. It is not like the Criminal Procedure Act, which obliges the police to present the judge with evidence of a crime. Here it refers to much less precise concepts, in which almost anything can fit. What the CNI has done is therefore perfectly legal. We need to better define the circumstances under which communications can be tapped’ (unofficial translation). Lecturer Dolors Canals Ametller considers that technical reinforcement of judicial control, as well as an increase in the number of magistrates involved, would give greater legitimacy to judicial decisions authorising institutional surveillance in the digital era. Although some of the Catalan separatists were convicted of crimes against the integrity of the State and others were apparently suspected, former Supreme Court Judge José Antonio Martín Pallín considers the application of the doctrine of national security to Catalan pro-independence politicians and their associates to be *politically* serious, irresponsible, and thoughtless.

The Ombudsman Ángel Gabilondo concluded his *ex officio* review and confirmed that the investigated CNI actions were compliant with the Spanish Constitution and laws. He recommended to further reflect on the adequacy of parliamentary and judicial controls, since the Official Secrets Commission had not convened for the past three years and technological progress may challenge traditional judicial control. There is concern that a law designed to control the interception of conventional telephone conversations serves to authorise the infection of mobiles with spyware that allows for the extraction of all stored information and the manipulation of the target system. The government subsequently announced plans to reform the legal framework; for more information, see Section ‘5. Individual and Member State actions’.

### 4.2.4. Germany

Reportedly, the German Federal Criminal Police Office (BKA) confirmed to the Parliamentary Committee on Internal Affairs that it had acquired and deployed a modified version of the Pegasus software, after concluding that the standard version would violate German law. The default version did not make the necessary distinctions between source telecommunication surveillance and online search and did not sufficiently log its activities on the target phone. The BKA drew up a report, which remains undisclosed. In response to a parliamentary question, the Federal Government indicated that the use of Pegasus is only permitted in individual cases and in respect of strict legal conditions laid down in the German Code of Criminal Procedure (StPO), the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act), and the Federal...
Criminal Police Office Act (BKAG). One commentator expressed concerns about involving private companies in intrusive investigation procedures, while fundamental rights primarily bind the state and not necessarily spyware providers. If private parties could see collected data, it would exacerbate interference with the fundamental right to confidentiality and integrity of IT systems. In the same vein, the Society for Civil Rights (Gesellschaft für Freiheitsrechte) lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI). Additionally, it raises issues of unlawful outsourcing of sovereign powers, insufficient safeguards against unauthorised access and deletion, unlawful commissioning of data processing, insufficient functional limitations, unlawful modifications of the target system, and the illegal exploitation of security vulnerabilities. The Left submitted a draft resolution to the German federal parliament (Bundestag) against the purchase and use of spyware by federal authorities. MP Manuel Höferlin of the Free Democratic Party drew a comparison to hiring a bounty hunter and relying on him to act lawfully and in a technically precise way when invading the homes of suspects. The discussion on Pegasus integrates with the ongoing debate on the constitutionality of ‘source telecommunication surveillance’ (Quellen-Telekommunikationsüberwachung) and the use of remote forensic software (Staatstrojaner).

4.2.5. Bulgaria and Cyprus

Assuming the NSO Group exported Pegasus or similar software from Bulgaria and Cyprus, any authorisation applications for the export of Pegasus made before 9 September 2021 would have been subject to Council Regulation (EC) No 428/2009 and subsequently to its recast, Regulation (EU) 2021/821. In the aftermath of the Arab Spring, it became clear that repressive regimes had used cyber surveillance technology provided by EU-based companies for repressive purposes. Consequently, IP network surveillance systems and items related to intrusion software were placed on the Wassenaar export control list in 2013 and subsequently incorporated in EU export controls in October 2014. Under the EU regime, products such as Pegasus would require an export licence.
from Bulgarian or Cypriot authorities.\textsuperscript{201} Since 2000, the EU Dual-Use Regulation provided that Member States may prohibit or impose an authorisation requirement on the export of non-listed dual-use items for human rights considerations.\textsuperscript{202} As of 2009, it stipulates that a Member State shall take into account their obligations under the so-called 'Common Position regarding the export control of military technology and equipment' when deciding on an expert authorisation.\textsuperscript{203} Consequently, Member State authorities shall take into account 'respect for human rights in the country of final destination as well as respect by that country of international humanitarian law and shall refuse export authorisation in cases where there is a 'clear risk' of 'internal repression'.\textsuperscript{204} As demonstrated by repeated human rights violations,\textsuperscript{205} Member States' export authorities applied these rules poorly. Arguably, this was the result of a lack of capacity to assess (non-specified) human rights standards, of prioritising national economic and security interests, or of insufficient control over the actual usage of software after granting export authorisation.

Against this backdrop, the EU agreed on a recast of its Dual-Use Regulation in November 2020.\textsuperscript{206} The Regulation now subjects non-listed cyber-surveillance to an authorisation framework, which complements pre-existing rules for the export of dual-use items ('catch-all provision'). Additionally, it is the first time that an export regulation explicitly links the authorisation of exports to human rights considerations. Commentators submit that Member States cannot rely on former interpretations of the term 'cyber-surveillance items', but must now interpret them through a human rights lens, notably in consideration of the EU Charter of Fundamental Rights.\textsuperscript{207} It also enhances the European Commission's annual reporting obligation by prescribing that it shall include 'dedicated information on authorisations, in particular on the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications'. If implemented adequately, this may 'lift the veil on the potential sale of spyware tools by commercial actors based in EU member states to authoritarian regimes around the world'.\textsuperscript{208} It remains to be seen whether the recast export rules will curb the spread of EU-supplied surveillance technologies. Civil society organisations are sceptical.

\textsuperscript{201} Art. 3(1) juncto category 4A005 (Systems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of 'intrusion software.'), 4D004 ('Software' specially designed or modified for the generation, command and control, or delivery of 'intrusion software') and 4E001(c) ('Technology' for the 'development' of 'intrusion software') of Annex I Regulation (EC) No 428/2009 (consolidated version); Amnesty International et al., Operating from the shadows, briefing, 31 May 2021, p. 20; Anderson C., Considerations on Wassenaar Arrangement Proposals for Surveillance Technologies, white paper, Access Now, 13 March 2015; van Daalen O. et al., The new rules for export control of cyber-surveillance items in the EU, Institute for Information Law, June 2021, pp. 48-50.

\textsuperscript{202} Article 8 EU Dual-Use Regulation 2009 and 2020; Article 5 EU Dual-Use Regulation 2000.

\textsuperscript{203} Article 12 EU Dual-Use Regulation 2009.


\textsuperscript{207} van Daalen O. et al., The new rules for export control of cyber-surveillance items in the EU, Institute for Information Law, June 2021, p. 14.

\textsuperscript{208} Article 19 et al., EU: Action needed to tackle spyware abuses after Pegasus revelations, 15 September 2021.
about the text's ability to tackle human rights concerns\(^{209}\) and suggest that Member States should adhere to a set of best practices and that the Commission should promote the convergence of interpretation.\(^{210}\) Depending on export destinations, export licences from Bulgarian and Cypriot authorities would 'raise serious doubts about the [...] respect for human rights'.\(^{211}\)

**Israel's export framework**

NSO’s products qualify as dual-use exports under Israel’s defence export control regime, which is administered by the Defence Export Control Agency (DECA).\(^{212}\) While Israel does not participate in the Wassenaar Arrangement, it does incorporate items from the Wassenaar control list in its national Defence Export Control Law 5766, 2007.\(^{213}\) Its designated objective is to ‘regulate state control of the export of defence equipment, the transfer of defence know-how and the provision of defence services, for reasons of national security considerations, foreign relations considerations, international obligations and other vital interests of the State’. The licensing authority is authorised to condition or refuse authorisations on account of ‘consideration regarding the end-user or the end-use’, but it is not instructed to assess human rights practices or refuse a licence for exports to countries with problematic human rights records. Reportedly, Israel’s Defence Minister Benny Gantz claimed that ‘as a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism’.\(^{214}\) In light of the Pegasus revelations, Israel slashed its cyber export list from 102 countries to 37 countries and clarified eligible use-cases of cyber and intelligence products in its ‘End Use/User Certificate’, which buyers need to sign.\(^{215}\) A Tel Aviv District Court rejected an attempt, by 30 members and supporters of Amnesty International Israel, which sought to force Israel’s Ministry of Defence (MOD) to revoke the security export licence(s) of the NSO Group.\(^{216}\) In view of their classification as confidential, details of NSO licences as well as general information, such as numbers of licences and names of customer countries, are not publicly available.\(^{217}\) Amnesty International deplores the fact that transparency around defence in Israel is significantly curtailed.\(^{218}\)

----


\(^{211}\) Access Now et al., *Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states’ role in Pegasus affair*, Reporters Without Borders, 10 September 2021.


5. Individual and Member State actions

In Hungary, the intelligence services and control authorities\(^{219}\) answer to the Parliamentary Committee of National Security (nemzetbiztonsági bizottság), but hearings take place in camera. The Hungarian data protection authority (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH) published its findings on the Pegasus scandal, while the detailed summary of the investigation remain classified until 2050 (inclusive).\(^{220}\) After establishing the facts,\(^{221}\) the president of the NAIH concluded that all the examined intelligence operations met the requirements of Hungarian intelligence laws; he confirmed that some of the people mentioned in the press had been subject to intelligence gathering. In an interview, he specified that the classification period might be extended and that some information would remain permanently inaccessible to the public.\(^{222}\)

According to a mission report by members of the Committee on Civil Liberties, Justice and Home Affairs, the Hungarian Government has classified all relevant information concerning Pegasus for a duration of 30 years.\(^{223}\) Two human rights lawyers, Beatrix Vissy and Máté Szabó, contend that the DPA ignored a European Court of Human Rights (ECtHR) judgment of 12 January 2016, which rules that the Hungarian legislation on secret surveillance measures is systemically unlawful and still has not been appropriately executed.\(^{224}\) They deplore the fact that the DPA initiated criminal proceedings against those who exposed the Pegasus scandal in Hungary. On behalf of six clients, the human rights NGO Hungarian Civil Liberties Union (HCLU) announced that it would file lawsuits and formal complaints with the Hungarian authorities, the European Commission, the European Court of Human Rights and the Israeli Attorney General.\(^{225}\) Investigations by the Budapest regional office of the Hungarian prosecution service (Budapesti Regionális Nyomozó Ügyészség) are still ongoing.\(^{226}\) Secretary of State Zoltán Kovács rejects the notion that Hungarian laws regulating the use of surveillance are permissive.\(^{227}\)

In Poland, the revelations caused an uproar and the opposition-controlled Senate, the upper chamber of Poland’s parliament, set up a Senate Special Committee on Surveillance (Komisja Nadzwyczajna ds. inwigilacji) on 12 January this year.\(^{228}\) The Committee is tasked with clarifying cases and legal implications as well as launching a legislative initiative to reform the activities of the

\(^{219}\) Hungarian Helsinki Committee, National intelligence authorities and surveillance in Hungary, FRA, 26 September 2014.

\(^{220}\) NAIH, Findings of the investigation of the NAIH launched ex officio concerning the application of the 'Pegasus' spyware in Hungary, NAIH-423-2/2022, 16 February 2022.

\(^{221}\) I.a. based on information from the Parliamentary Committee of National Security and the Specialised National Security Service.

\(^{222}\) Lengyel T., Péterfalvi a Pegasus-vizsgálatról: A megfigyelések indokai nem tüntek kamunak, HVG, 11 February 2022.

\(^{223}\) Mission report following the ad hoc delegation to Budapest, Hungary, 29 September-1 October 2021, P699.096v01-00, Committee on Civil Liberties, Justice and Home Affairs (LIBE), 16 November 2021.

\(^{224}\) EPP Group, Public Hearing – Pegasus spyware scandal and its impact on democracy in the EU, 10 February 2022; Hungarian Civil Liberties Union, Communication on the execution of Case Szabó and Vissy v. Hungary, 26 January 2022; Judgment in Case with Application no. 37138/14, Szabó and Vissy v. Hungary, ECtHR, 12 January 2016, para. 82-84.

\(^{225}\) Pegasus case: foreign procedures, Hungarian Civil Liberties Union website.


\(^{227}\) Kovács Z., Surveillance in Hungary: What you need to know, About Hungary blog, 21 July 2021.

\(^{228}\) Polish Senate, W Senacie powstała Komisja Nadzwyczajna ds. inwigilacji, 12 January 2022.
Europe's PegasusGate

special services; it does not wield investigatory powers. On a number of occasions, it heard from technical, strategic and legal experts as well as surveillance targets. It heard from members of Citizen Lab, Amnesty International and Poland’s Supreme Audit Office (NIK), as well as from the former head of CBA, Paweł Wojtunik, together with the former Deputy Minister of Internal Affairs and Administration, Adam Rapacki; former head of the Military Counterintelligence Service (SKW) General Piotr Pytel, together with former judge and president of the Polish Constitutional Tribunal and former president of the State Electoral Commission, Professor Andrzej Zoll. The Committee also heard from targets, including prosecutor Ewa Wrzosek, Senator Krzysztof Brejza and his father and former assistant, founder of the Agrounia socio-political movement Michał Kołodziejczak, former politician and Donald Tusk’s lawyer Roman Giertych, and the President of Employers of Poland, Andrzej Malinowski.

So far, the ruling PiS party has blocked opposition efforts to set up a committee of inquiry in the lower house, the Sejm. The District Prosecutor’s Office in Ostrów Wielkopolski launched investigations into the Pegasus surveillance of Krzysztof Brejza. Likewise, investigations were launched into alleged spoofing attacks on his wife and daughter. Conversely, the District Prosecutor’s Office in Warsaw refused to initiate proceedings in the case of prosecutor Ewa Wrzosek. In turn, she lodged a complaint, which she hopes will overturn the ‘unjustified and premature refusal to open an investigation’.

In Spain, various Pegasus targets initiated legal actions. Roger Torrent and Ernest Maragall broke ground as the first known targets and filed a complaint against the former director of the National Intelligence Centre (Centro Nacional de Inteligencia, CNI), Félix Roldán, and NSO Group for alleged computer espionage. A judge from Barcelona opened investigations, but ordered their


230 Polish Senate, Komisja nadzwyczajna ds. nielegalnej inwigilacji wysłuchała ekspertów z Kanady, 17 January 2022; Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała prezesów NIK, 18 January 2022; Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała senatora Krzysztofa Brejzy, 19 January 2022; Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 26 January 2022; Polish Senate, Komisja Nadzwyczajna ds. inwigilacji wysłuchała prokuratora Wrzosek i przedstawicieli Amnesty International, 27 January 2022; Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 3 February 2022; Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała prezydenta Inowrocławia Ryszarda Brejzy i posłanki Magdaleny Lośko, 22 February 2022; Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała b. szefa SKW Piotra Pytli i prof. Andrzeja Zolla, 23 February 2022; Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 29 April 2022. For a timeline from 17 January 2022 to 15 February 2022, see Szolucha S. and Korzeniowska A., Komisja ds. Pegasusa w Sejmie coraz bliżej. A co do tej pory ustalono w Senacie?, wyborcza.pl, 17 February 2022.


233 Figaj B., Prokuratura wszczęła śledztwo w sprawie fałszywych alarmów m.in. z telefonu żony senatora Brejzy, Polska Agencja Prasowa, 25 January 2022.

234 Gf, Prosecutor’s office refuses inquiry into prosecutor Ewa Wrzosek’s phone hacking, tvn24, 29 December 2021.


236 Gil J. and Baquero C., Torrent y Maragall presentan una querella porque ‘la Fiscalía no mueve un dedo’ en el caso del espionaje, El País, 30 July 2020.

provisional closure of the inquiry after neither Torrent nor Maragall were able to submit their allegedly infected mobile phones and the court did not receive a response from Israeli authorities for more than one and a half years. Members of various Catalan organisations and political parties initiated further legal proceedings and announced their intention to take action in Member States such as Belgium, France, Switzerland, Luxembourg and Germany. Following a complaint from the State Attorney's Office, the National Court (Audiencia Nacional) opened an investigation regarding the espionage of the Prime Minister and various ministers. Conversely, the National Court rejected the request of the Generalitat of Catalonia to become a party in that procedure due to a lack of standing.

The Spanish Government offered the Catalan party most affected by Pegasus operations, Esquerra Republicana de Cataluña (ERC), four mechanisms to clarify CatalanGate: an internal control investigation by the National Intelligence Centre itself; another independent investigation opened ex officio by the Ombudsman; another investigation in the Official Secrets Committee of the Spanish Congress, where the director of the CNI would appear, and the promise that the Executive is willing to declassify secret documents to clarify the situation.

The Official Secrets Commission (Comisión de Secretos Oficiales or Comisión de Control de los Créditos Destinados a Gastos Reservados), which serves to exercise parliamentary oversight over the CNI, convened, for the first time since February 2019, on 5 May 2022 for a hearing of the Director of the CNI. Despite disclosures by the Director of the CNI, various parties such as the ERC, the CUP, PNV and EH tabled a proposal to set up a commission of inquiry. So far, notably the Spanish Socialist Workers’ Party (Partido Socialista Obrero Español) and the People’s Party (Partido Popular) have blocked these efforts. The ombudsman Ángel Gabilondo concluded his ex officio review and...
confirmed that the investigated CNI actions were compliant with the Spanish Constitution and laws.247 He recommended to further reflect on the adequacy of parliamentary and judicial controls, since the Official Secrets Commission had not convened for the past three years and technological progress may challenge traditional judicial control.248 Authorities disclosed to the Official Secrets Commission the Supreme Court orders authorising the intrusions,249 but only agreed to declassify CNI documents relating to CatalanGate upon request from a judge.250 In a controversial251 reaction to the hacking of Prime Minister Sánchez’s phone, the Spanish government dismissed the CNI’s Director Paz Esteban.252

The Spanish government announced the reform of the Official Secrets Law and the legal framework of the CNI.253 The Spanish law on official secrets, dating back to 1968 and amended only to grant Parliament access to classified information in 1978, does not contain a time limit after which documents declared secret are automatically declassified.254 After discarding a proposal by the PNV, blocked in Congress since 2019, the Government already decided last year to launch its own reform.255 After the Pegasus scandal, Prime Minister Pedro Sánchez stated that ‘it is imperative that the norm is adapted to democratic and constitutional principles’ (unofficial translation) and promised that he would submit to Congress a new and renamed Law on Classified Information after the summer.256 The executive also intends to reform the organic law 2/2002 regulating the prior judicial control of the CNI. Sánchez indicated that the objective is to reinforce the guarantees of this control, and to ensure maximum respect for the fundamental rights of individuals,257 both the recommendations of the Obudsman and the European Parliament would be taken into account. Additionally, Sánchez announced the approval of a new Intelligence Directive, the document in which the government sets the CNI's intelligence objectives and which has not been renewed since

---

247 Ombudsman Ángel Gabilondo, El Defensor del Pueblo verifica que la actuación del cni se ha realizado conforme a la Constitución y la ley en los casos examinados, 18 May 2022, p. 4.
248 Ombudsman Ángel Gabilondo, El Defensor del Pueblo verifica que la actuación del cni se ha realizado conforme a la Constitución y la ley en los casos examinados, 18 May 2022, pp. 7-8.
249 Casqueiro J. and Hermida X., Los silencios y respuestas que deja Pegasus – La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022.
250 Marcos J. and González M., El Gobierno solo desclasificará los papeles del espionaje si lo pide un juez, El País, 11 May 2022; Piñol À., Pere Aragonès exige al Gobierno que aclare quién pidió al juez la autorización para espiarle, El País, 5 May 2022.
251 González M., El CNI se siente cabeza de turco, El País, 4 May 2022; Cué C. and González M., Defensa y La Moncloa chocan por quién asume el fallo de seguridad por el ataque al móvil de Sánchez, El País, 5 May 2022; González M., El error de la directora del servicio secreto, El País, 11 May 2022; El País, El Gobierno dijo en 2020 que las comunicaciones de Sánchez dependen de Moncloa y que el CNI no tiene nada que ver, El País, 12 May 2022; González M., ¿Es posible que Pedro Sánchez no supiera que Pere Aragonès estaba siendo espiado?, El País, 8 May 2022.
252 Cué C., El Gobierno destituye a Paz Esteban como directora del CNI por la crisis de Pegasus, El País, 10 May 2022.
253 Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías, Actividad del presidente, La Moncloa, 26 May 2022; González M., El Gobierno inicia la reforma de la ley franquista de secretos oficiales, El País, 5 April 2022.
255 González M., El Gobierno inicia la reforma de la ley franquista de secretos oficiales, El País, 5 April 2021; For details on the proposal, see González M., Los ‘altos secretos’ de Estado estarán bajo llave al menos 50 años, El País, 31 October 2021.
256 Merino J., Sánchez anuncia la reforma de la norma que regula el CNI para reforzar su control judicial y una nueva ley de secretos oficiales, La Vanguardia, 26 May 2022; González M., El PSOE quiere consensuar con el PP una nueva ley de Información Clasificada, El País, 27 May 2022.
257 Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías, Actividad del presidente, La Moncloa, 26 May 2022; On oversight and control mechanisms relating to the CNI, see Ridao J., Cómo se controla el CNI, El País, 30 April 2022.
March 2019. Sánchez also confirmed that the Executive will update both its 2021 national security strategy and the cybersecurity plan. With all these measures, the head of the Executive has given an assurance that ‘the necessary changes will be undertaken to prevent these security breaches from occurring again in the future’ (unofficial translation).

Reportedly, the German Federal Criminal Police Office confirmed to the Parliamentary Committee on Internal Affairs that it had acquired and deployed a modified version of the Pegasus software. The Society for Civil Rights (Gesellschaft für Freiheitsrechte) lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information.

In France, investigations were initiated into the hacking of presidential and ministerial phones. Paris Public Prosecutor Rémy Heitz opened an investigation into the spying on two Mediapart journalists and delegated the matter to the French Central Office for Combating ICT Crime (OCLCTIC). In an interview with OCLCTIC, the journalists submitted evidence that Moroccan intelligence services had operated the spyware and technicians of the National Cybersecurity Agency of France (ANSSI) confirmed the infiltration of their phones. Other complaints followed, including by Reporters Without Borders and various journalists. Morocco published an official statement in which it ‘categorically rejects and condemns these false and baseless allegations’, and clarifies that it has never acquired software to infiltrate communication devices. Morocco filed a defamation suit against French NGOs and media outlets that had accused the Kingdom of spying on them, but the lawsuit was declared inadmissible.

On behalf of five human rights defenders in Mexico and one editor from Qatar, two Palestinian lawyers and one Cypriot lawyer filed lawsuits against the NSO affiliates ‘Circles Solutions’ and ‘Circles Technologies’ in Cyprus on 30 August 2018. Drawing on a parallel lawsuit in Israel, the plaintiffs may seek compensation and an injunction to prevent the NSO Group from helping anyone spy on them. Possibly, they also aim to provoke restrictions on the trade in hacking tools. According to

---

258 González M., El PSOE quiere consensuar con el PP una nueva ley de Información Clasificada, El País, 27 May 2022.
259 Merino J., Sánchez anuncia la reforma de la norma que regula el CNI para reforzar su control judicial y una nueva ley de secretos oficiales, La Vanguardia, 26 May 2022.
260 Flade F. et al., BKA bekam maßgeschneiderten Trojaner, Tagesschau, 8 October 2021.
263 Le Monde, «Projet Pegasus» : le parquet de Paris ouvre une enquête sur l'espionnage de journalistes de «Mediapart», Le Monde, 20 July 2021; Rouget A., Tweet, 20 July 2021: Le procureur de la République de Paris ouvre une enquête, confiée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), à la suite de la plainte de @Mediapart concernant l'espionnage par le logiciel #Pegasus. [picture of the press release of the prosecutor's office].
264 La rédaction de Mediapart, Pegasus: French judicial probe confirms technical proof of espionage against Mediapart journalists, Mediapart, 30 July 2021.
270 Satter R., Lawsuit lays bare Israel-made hack tools in Mideast, Mexico, Associated Press, 1 September 2018.
Europe's PegasusGate

Citizen Lab, the lawsuit is still ongoing; Vice reported that NSO had closed the Cypriot office of Circles. A statement by the NSO Group indicates that a Cypriot lawsuit to revoke NSO Group's export licence recently failed. Allegedly, investigators of the Pegasus scandal themselves became targets of hacks and (physical) undercover operations, presumably as part of a coordinated effort to collect information and discredit them. With a view to the EU context, the two Palestinian lawyers and the Cypriot lawyer involved in suing NSO in Cyprus were targeted. A man who presented himself as a partner at Hong Kong-based ENE Investments approached the Cypriot lawyer via e-mail and flew her to London, ostensibly to discuss a potential lecture, but the conversation later turned to the prospects and funding of her NSO lawsuit.

The Sofia City Prosecutor's Office (Sofiyska Gradska Prokuratura) is investigating whether state services have illegally used the Pegasus spyware to wiretap Bulgarian citizens. It requested information from special services and the National Bureau for Control over Special Intelligence Means (Nacionalnoto bjuro za kontrol na specialnite razuznavatelni sredstva, NBKSRS).

---

273 Solomon S., Amnesty, research groups map out global reach of Israeli NSO Group's spyware, Times of Israel, 4 July 2021.
274 Satter R., AP Exclusive: Undercover spy exposed in NYC was 1 of many, Associated Press, 11 February 2019; Forensic Architecture, Pegasus: Targeting the Investigators, Digital Violence platform, 10 June 2021.
275 Satter R., An Invitation to a Lecture, email exchange, 10 February 2019.
276 Sofiyska Gradska Prokuratura, СГП извършва проверка за евентуално неправомерно използване на софтуер Pegasus, 11 February 2022.
6. EU actions

At EU level, the Commission reassured the Parliament that it is aware of the developments at Member State level and would include shortcomings in the rule of law report and launch infringement procedures where necessary.\(^{277}\) Recently it signalled that it ‘is not best placed here to investigate individual cases’ (italics added for emphasis) and that ‘investigation of such issues is the responsibility of each Member State’.\(^{278}\)

Prior to setting up a committee of inquiry, Members of the European Parliament discussed the Pegasus scandal on several different occasions: in plenary on 15 September 2021 and 15 February 2022; in committees on 9 September 2021, 29 November 2021 and 1 February 2022; and during a public hearing of the European People’s Party (EPP) on 10 February 2022.\(^ {279}\) The Parliament adopted a report in March 2022 condemning the use of Pegasus surveillance software by Hungarian and Polish state entities and urging the Commission to draw up a list of illicit surveillance software and to continuously update this list.\(^{280}\) Members of the Committee on Civil Liberties, Justice and Home Affairs concluded in their mission report following a three-day visit to Hungary that ‘the Pegasus case [...] shed light on increased surveillance by the state against activists, journalists and lawyers’.\(^{281}\)

With 635 votes in favour, 36 votes against and 20 abstentions, on 9 March 2022 the Parliament adopted the decision to set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware.\(^{282}\) The committee is looking into existing national laws regulating surveillance, and whether Pegasus spyware was used for political purposes against, for example, journalists, politicians and lawyers.\(^ {283}\) It is composed of 38 members and is scheduled to submit its final report within one year. Reportedly, the Committee plans a fact-finding mission to Spain after concluding missions to Poland, Hungary, and Israel.\(^ {284}\)


\(^{278}\) Commissioner Johannes Hahn, *Use of the Pegasus Software by EU Member States against individuals including MEPs and the violation of fundamental rights*, Topical Debate, European Parliament, 4 May 2022: ‘Member States are competent to guarantee their national security. The investigation of such issues is the responsibility of each Member State. Indeed, the Commission is not best placed here to investigate individual cases. The Commission expects national authorities to thoroughly examine any such allegations and to restore citizens’ trust. I also wish to recall that the EU has a strong legal framework for data protection and privacy.’; Nielsen N., *EU Commission won’t probe ‘Pegasus’ spyware abuse*, euobserver, 19 April 2022.


\(^{280}\) Report on foreign interference in all democratic processes in the European Union, including disinformation, P9_TA(2022)0064, INGE Special Committee, 9 March 2022.

\(^{281}\) Mission report following the ad hoc delegation to Budapest, Hungary, 29 September-1 October 2021, P6_TA(2021)0060-00, LIBE Committee, 16 November 2021.

\(^{282}\) Decision on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee, P9_TA(2022)0071, European Parliament, 10 March 2022. The majority of votes against the committee came from ECR MEPs, joined by one ID MEP, pp. 573-574.


In the Israeli context, a Tel Aviv District Court rejected an attempt, by 30 members and supporters of Amnesty International (AI), to force Israel's Ministry of Defence (MOD) to revoke the security export licence of the NSO Group.286 According to Citizen Lab, two other lawsuits were filed in Israel and are still ongoing, including one by five Mexican journalists and activists and one by a confidant of the murdered Jamal Khashoggi.287 Like the Cypriot lawyer and cybersecurity researchers, lawyers involved in Israeli proceedings were presumably targeted by undercover spies.288 Recently, Israel launched investigations into possible misuse of NSO spyware, slashed its cyber export list and clarified eligible uses of cyber and intelligence products in its End Use/User Certificate that buyers need to sign.289 According to investigations by the Calcalist business news website, the Israeli police have been making widespread use of spyware against Israeli civilians, including people not suspected of crimes, exploiting a legal loophole and keeping the surveillance secret.290 The Israeli police initially denied the allegations, but upon a second investigation stated that 'additional findings were discovered that change the state of affairs in certain aspects'. The now retired Attorney General Avichai Mandelblit opened investigations into the police and appointed an investigation team, whose findings are expected to be published by 1 July 2022.291 Deputy Attorney General Amit Marari's preliminary investigation found no indications that the police illegally hacked citizens' phones and Justice Minister Gideon Sa'ar stated 'that there is no need for the dramatic step of establishing a state commission of inquiry'.292 In an interim report, Marari disclosed that three individuals were subject to a court order allowing such phone hacking.293 The statement specifies that the probe will continue and widen beyond the list of alleged targets. In turn, the NSO Group filed a defamation lawsuit against Calcalist.294 While the Foreign Affairs and Defence Committee of Israel's Assembly (Knesset) formed a commission to review allegations of Pegasus misuse, the Knesset Plenum rejected a number of proposals to form a parliamentary commission of inquiry.295

---

286 Judge Rachel Barkai, verdict, 12 July 2020; Ravet H., Court rejects Amnesty International petition to withdraw NSO’s export license, Calcalist, 13 July 2020; Amnesty International, Israel: Stop NSO Group exporting spyware to human rights abusers, 14 January 2020.
288 Satter R., AP Exclusive: Undercover spy exposed in NYC was 1 of many, Associated Press, 11 February 2019; Forensic Architecture, Pegasus: Targeting the Investigators, Digital Violence platform, 10 June 2021.
289 AFP and Times of Israel (TOI) staff, Israeli panel to review potential misuse of NSO spyware around world, Times of Israel, 22 July 2021; Orbach M., Israel defense ministry slashes cyber export list, drops Saudi Arabia, UAE, Calcalist, 15 November 2021; Israeli Ministry of Foreign Affairs, Israel MoD tightens control of cyber exports, press release, 7 December 2021; Defense Exports Control Agency (DECA), End Use/User Certificate, 6 December 2021.
290 Ganon T., Israel police uses NSO’s Pegasus to spy on citizens, Calcalist, 18 January 2022.
291 TOI staff, Attorney general opens investigation into police use of NSO [,] Times of Israel, 20 January 2022; Spiro A. and TOI staff, In about-face, police admit misuse of NSO phone hacking tech, Times of Israel, 1 February 2022.
292 Spiro A., Deputy AG's probe finds 'no indication' police illegally hacked citizens' phones, Times of Israel, 21 February 2022; TOI staff and Spiro A., Sa'ar: Report on illegal NSO spyware use was incorrect, no need for state inquiry, Times of Israel, 22 February 2022.
293 Findings of the review team, press release, Ministry of Justice, 22 February 2022; Calcalist staff, Calcalist System response, Calcalist, 21 February 2022.
294 TOI staff, NSO files defamation lawsuit against Calcalist over reports [,] Times of Israel, 27 February 2022.
295 AFP and TOI staff, Israeli panel to review potential misuse of NSO spyware, Times of Israel, 22 July 2021; Knesset Plenum rejects proposals to form parliamentary commission of inquiry [,] press release, Knesset, 3 February 2022.

---
In the **US context**, WhatsApp and Facebook (now Meta), as well as Apple, filed lawsuits against the NSO Group (see trackers of WhatsApp/Facebook and Apple lawsuits).\(^{296}\) Microsoft, Google, Cisco, GitHub, LinkedIn and VMWare jointly submitted arguments and recommendations in support of the joint WhatsApp-Facebook legal action (‘amicus brief’).\(^{297}\) The US Court of Appeals for the Ninth Circuit allowed WhatsApp’s lawsuit to advance, and rejected the NSO Group’s attempt to block briefs filed by civil society organisations.\(^{298}\) In response, NSO Group’s lawyers petitioned for intervention by the US Supreme Court (‘writ of certiorari’),\(^{299}\) which has yet to decide and invited the Solicitor General of the US Justice Department to file a brief in this case expressing the views of the US.\(^{300}\) The US Commerce Department’s Bureau of Industry and Security (BIS) released a final rule adding the NSO Group to the Entity List, effectively banning trade with the firm (save with exceptional permission).\(^{301}\) During a House Intelligence Committee hearing, Director of the FBI Christopher Wray confirmed that the FBI ‘bought a limited license for testing and evaluation’, but that it was ‘not used in any investigation of anyone’.\(^{302}\)

---


7. Ways forward

As the Pegasus revelations shed light on the adverse effects of trade in and abuse of cyber surveillance technologies, policymakers are seeking adequate responses.\(^{303}\) The following sections outline a selection of preliminary and non-exhaustive avenues to explore for both the public and private sectors, and may serve as food for thought. The aim of this study is to discuss viable avenues to foster ethical surveillance and spyware trade, without denying validity to surveillance in general.\(^{304}\) Depending on political agendas and security situations, these options may be graduated or nuanced.

7.1. For the public sector

7.1.1. Map the spyware market and surveillance practices

The debate on spyware stands to benefit from in-depth legal and factual investigations of public-private surveillance partnerships.\(^{305}\) Reliable and structured information on legal arrangements, market dynamics, commercial ties, and techno-operational details would help to determine whether the current EU governance framework meets policy objectives. Even the most basic roles, arrangements and practices remain unclear: Do technology providers typically act as providers or operators? Are vendors left with the power to take certain (techno-operational) decisions on their own? What specific data processing operations are involved?

Additionally, research into upstream and downstream markets may uncover further governance angles. For instance, if commercial surveillance technologies were frequently built on the basis of purchased information concerning cybersecurity vulnerabilities (‘weaponisation’), it may prove useful to tackle the upstream trade in unknown exploits (‘zero-day exploit markets’)\(^{306}\) as well as unethical disclosure practices.\(^{307}\) Allegedly, intelligence agencies also buy zero-day exploits themselves.\(^{308}\) In the future, exploit brokers may rent out zero-day exploits as a service (‘exploits-as-

---

\(^{303}\) Parliament set up a committee of inquiry and decided that the committee shall ‘make any recommendations that it deems necessary in this matter’. Commission Vice-President Věra Jourová stated that she is looking for legal options at EU level, see Wettach S., EU will gegen Spionage-Software Pegasus vorgehen, WirtschaftsWoche, 2 April 2022.

\(^{304}\) Similarly, Gill P., Intelligence Reform: the never-ending story, Panel 21, International Association for Intelligence Education Conference, June 2016, p. 19.


\(^{308}\) Perliroth N., This Is How They Tell Me the World Ends, Bloomsbury, 2021.
This would make it even easier for both ethical and malicious actors to access exploits and develop 'cyber weapons'.

In order to exploit synergies and ensure a future-proof revision, it appears expedient to broaden the investigation to the design, trade, and use of cyber weapons (espionage and sabotage) and to take into account forthcoming legislation (see next sections). Taking stock of the design, trade, and use of cyber weapons may also prompt discussions on a cyber weapons framework similar to that for arms control and gun control.

### 7.1.2. Promote cyber resilience

**Incentivise cyber resilience**

According to many commentators, governments should incentivise enhanced cybersecurity risk management and, where necessary, mandate it.

As part of the EU cybersecurity strategy, the European Commission tabled a proposal for the NIS 2 Directive, which aims to enhance all-hazards information and communication technology (ICT) resilience on the part of 'essential entities' and 'important entities' meeting specific thresholds in a large number of sectors. The draft directive proposes to substantially extend the scope of the currently applicable NIS Directive, to cover digital infrastructure such as cloud computing and publicly available electronic communication services (e.g. chat services), digital providers such as social networking services platforms, and manufacturers of computer and electronic products, including ICT equipment. It would provide that Member States shall lay down (a) a national cybersecurity strategy, including a policy for coordinated vulnerability disclosure, and reporting obligations for entities referred to as essential entities.

---


312 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

313 On jurisdiction, see Article 24 NIS-2-COM. Cloud computing was already covered by the NIS Directive, but was moved to a higher level of protection.

314 If these entities are designated as critical, further obligations principally concerning non-cyber, i.e. physical, risks are envisioned by the proposal for a directive on the resilience of critical entities, COM(2020) 829 final.

315 On the definition, see Statistical Classification of Economic Activities in the EC, Rev. 2, 2008 (NACE Rev. 2).


317 According to Article 18(2) NIS-2-COM, Member State measures would include at least the following: (a) risk analysis and information system security policies; (b) incident handling (prevention, detection, and response to incidents); (c) business continuity and crisis management; (d) supply chain security, including security-related aspects concerning the relationships between each entity and its suppliers or service providers, such as providers of data storage and processing services or managed security services; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures; (g) the use of cryptography and encryption.

318 Article 20 NIS-2-COM: reporting of ‘any incident having a significant impact on the provision of their services’.
and important entities, and (c) obligations on cybersecurity information-sharing, as well as designating competent national authorities, single points of contact and CSIRTs.

It is uncertain whether the NIS2 Directive, as proposed by the Commission, would contribute to hampering spyware attacks such as Pegasus. As it stands, the proposal primarily aims to enhance the resilience of network and information systems used by essential and important entities to provide services (facilitating nis). Underpinned by dissuasive sanctions, such as fines amounting to 2% of the total worldwide annual turnover, companies would be subject to risk management and reporting obligations. According to the wording, these obligations do not cover consumer products or services themselves, but only facilitating nis used to provide services. Arguably, there may be spillover effects benefiting the resilience of end-user devices and services, where (i) mitigating risks in facilitating nis incidentally close attack-vectors against end-user devices, (ii) mitigating vulnerabilities in end-user products and services is a prerequisite to ensure sufficient cybersecurity of facilitating nis, and (iii) own-brand devices and services are used to provide the service, and risk management insights are re-used for the commercial version.

Apart from that, relevant cybersecurity obligations are laid down in Articles 40 and 41 EECC, Articles 5(1)(f) and 32 GDPR, Article 4 ePrivacy Directive, the Delegated Regulation (EU) 2022/30 supplementing the Radio Equipment Directive and various other EU and national measures. Regulation (EU) 2019/881 on information and communications technology cybersecurity certification (EU Cybersecurity Act) sets up a voluntary EU cybersecurity framework scheme for ICT products and thus does not guarantee an increase of cybersecurity for ICT products. The Proposal for a Regulation on general product safety (GPSD), ‘only cover[s] the risks related to health and safety (e.g. a physical incident) created by, for example, a lack of sufficient cybersecurity features’ (i.e. not ‘risks for privacy or data protection’).

A recent study commissioned by the European Commission found that the current and prospective legal framework does not ensure sufficient cybersecurity of ICT products, notably of consumer Internet of Things (IoT) devices. Similarly, a non-paper from the Dutch Government, states ‘an

---

319 These would be repealed pursuant Article 40 NIS-2-COM, since relevant services would become subject to the NIS 2; BEREC raises serious concerns about this approach, see Opinion on the proposed NIS 2 Directive and its effect on Electronic Communications, BoR(21)60, 19 May 2021. For technical guidance on the application of Articles 40 and 41 EECC, see ENISA, Guideline on Security Measures under the EECC, 7 July 2021.

320 Commission Delegated Regulation (EU) 2022/30 with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU. For an introduction, see Questions and Answers: Strengthening cybersecurity of wireless devices and products, European Commission, 29 October 2021.

321 For an overview, see Study on the need of cybersecurity requirements for ICT products No. 2020-0715, SMART 2019/0024, European Commission, December 2021, pp. 42-45 and 49-51; Regulation (EU) 2019/881 on information and communications technology cybersecurity certification (The Cybersecurity Act) sets up a voluntary EU cybersecurity framework scheme for ICT products and thus does not guarantee an increase of cybersecurity for ICT products. The Proposal for a Regulation on general product safety (GPSD), COM(2021)346 final, 30 June 2021, ‘only cover[s] the risks related to health and safety (e.g. physical incident) created by e.g. lack of sufficient cybersecurity features’, i.e. not ‘risks for privacy or data protection’ (see the accompanying impact assessment, p. 28).


324 Study on the need of cybersecurity requirements for ICT products No. 2020-0715, SMART 2019/0024, European Commission, December 2021, p. 55 and p. 254: ‘Particularly, the analysis drew the attention on the following issues: (i) the current EU legislative framework does not cover all the security objectives set out in Art. 51 of the Cybersecurity Act; (ii) the legislation related to the NLF does not address fully the cybersecurity requirements for ICT products; (iii) the granularity of some of the requirements identified in the legislation does not guarantee the fulfilment of the security objectives and; (iv) some cybersecurity requirements addressed to service operators apply indirectly to ICT products used to operate the service.’
important piece of the puzzle for a holistic and comprehensive approach to cybersecurity is still missing with regard to the cybersecurity of digital products, processes and services, since many initiatives take a sectoral approach or do not cover the entire digital domain.\footnote{The Netherlands, \textit{Non-paper on the principles of a Cyber Resilience Act}, 12 January 2022.} Building on the contractors' study, the Commission is now preparing a \textbf{Cyber Resilience Act} and has recently opened a call for evidence.\footnote{Cyber Resilience Act, European Commission website. For an overview, see Breton T., \textit{How a European Cyber Resilience Act will help protect Europe}, European Commission, 16 September 2021; On the envisioned interplay with the Radio Equipment Directive, see \textit{Questions and Answers: Strengthening cybersecurity of wireless devices and products}, European Commission, 29 October 2021.} As announced by the EU's cybersecurity strategy for the digital decade, the act would likely contain 'new horizontal rules' for connected products and associated services. It will likely follow a standards-based approach and aim to take into account any progress made on developing standards under the Radio Equipment Directive and the Cybersecurity Act. This legislation might reinforce contractual duties and impose an obligation on providers to notify users in case the provider becomes aware of a security breach. Considering the complex\footnote{European Court of Auditors, \textit{Challenges to effective EU cybersecurity policy}, Briefing Paper, March 2019.} cybersecurity policy landscape, it could be conducive if the Commission provided \textbf{comprehensive guidelines} on the interplay and application of current and forthcoming EU regulations.

In the same vein, it may be helpful to clarify under which circumstances sellers and manufacturers become \textbf{liable for failing to provide security updates}. In principle, the national acts transposing the Sales of Goods Directive\footnote{Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods.} oblige sellers to provide mobile phones with updates for at least two years (note: reversal of the burden of proof after one year!). However, this does not cover (i) the liability of manufacturers, (ii) the liability of sellers for the period that consumers were unaware of the security vulnerability and did not yet inform the seller of the lack of conformity, (iii) what quality of security vulnerability would present a lack of conformity, (iv) damages that would arise from government surveillance which exploit unpatched security vulnerabilities, and (v) whether the seller's liability extends beyond two years in accordance with the consumer's reasonable expectations. Similar considerations apply to digital content providers, such as WhatsApp (data as a counter-performance), under the \textbf{Digital Content Directive}.\footnote{Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services.} The forthcoming revision of the \textbf{Product Liability Directive} (PLD) – the EU's regime of strict liability for defective products – provides an opportunity to discuss the issue of manufacturers' liability for cyber vulnerabilities. As the Commission indicates in its inception impact assessment, one of the core issues driving the revision is whether the notion of 'defect' covers cyber vulnerabilities.\footnote{Inception impact assessment on the PLD, \textit{Ares}(2021)4266516, European Commission 30 June 2021.} Furthermore, the Commission raises\footnote{Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, \textit{COM(2020) 64 final}, European Commission 19 February 2020.} concerns that, under the existing PLD, manufacturers may attempt to escape liability for cybersecurity weakness with the 'later defect defence'\footnote{‘The defect developed after the product was put into circulation.’} and the
'development risk defence'. Drawing inspiration from a ruling of the German Federal Constitutional Court, another option is for Member States to put in place legal frameworks that determine how intelligence agencies (and possibly the surveillance industry) shall handle knowledge of security vulnerabilities, ranging from disclosure to exploitation. According to the ruling, the State's duty to protect IT systems against unauthorised third-party access 'necessitates' a legal framework that governs how authorities shall balance the competing aims of protecting IT systems and keeping vulnerabilities secret in order to leverage them for purposes of public security.

7.1.3. Prevent internal spyware abuse

Promote and support the public and private enforcement of data protection and privacy rights

The human rights-consistent design and deployment of spyware by Member States is most notably mandated by the European Convention on Human Rights, the EU Charter of Fundamental Rights (CFR), and secondary EU data protection and privacy laws.

While Member States may challenge the applicability of EU law and the jurisdiction of the CJEU on the grounds of their responsibility for safeguarding national security (Article 4(2) TEU and Article 1(3) ePrivacy Directive (ePD)), the CJEU may well take a substantive approach and circumscribe the term as indicated in its ruling in La Quadrature du Net (LQDN) and Privacy International. Undoubtedly, there is much controversy about the legal conditions and legal effect of Article 4(2) TEU. According to the LQDN and Privacy International rulings, Member States' responsibility for

---

333 ‘Even in possession of state of the art knowledge available at the time the product was put into circulation, the manufacturer could not have detected the defect.’


335 German Federal Constitutional Court, Constitutional complaint regarding the police’s handling of security vulnerabilities in IT systems is inadmissible, Press Release No. 62/2021, 21 July 2021; Decision in Case 1 BvR 2771/18, German Federal Constitutional Court, 8 June 2021.


national security ‘corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities’.

Although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law (italics added for emphasis).

This clarifies that Member States' declarations or intentions do not take precedent over other (so far largely indeterminate) criteria of national security and that national security threats are characterised by their particular seriousness and exceed serious public security threats. Case law and the rationale of Article 346 TFEU indicate that (evidently) false national security pretences would not exempt or justify Member State activities (see Annex I). Where Member States repeatedly and evidently invoke 'national security' as a pretext for economically, or even politically, motivated spying, the national security exemption/justification may not apply (for indicators of abuse, see Annex I). Based on the rationale of Article 348(2) TFEU, or even the provision itself, qualified parties may attempt to initiate an in camera abuse control.

Besides challenging the nature of the threat, qualified parties may also attempt to leverage CJEU case law, establishing that the involvement of certain actors in safeguarding national security renders EU law applicable (notwithstanding if they pass the abuse control). Legislative measures requiring providers of electronic communications services to retain and share traffic and location data for the purposes of protecting national security are subject to EU law (‘to the extent that they regulate the activities of those actors’).

It is not yet settled whether public-private spyware operations for the purpose of protecting national security and their corresponding legal basis would systematically be subject to EU law. A strict interpretation may argue that the involvement of private entities ‘dictates inclusion within an area (namely the protection of privacy required of those private operators)’.
Europe's PegasusGate

governed by EU law'. In contrast, Member States could argue that in such cases the State dimension outweighs the private dimension. Unlike electronic communications providers, spyware providers rely on state instructions to provide their services lawfully. Additionally, public-private spyware operations do not rest on upstream commercial data processing and largely resemble State activities that intelligence agencies would otherwise perform in-house. Spyware providers appear to be ‘directly and specifically involved in the exercise of official authority’. Lastly, it may well lie within the scope of ‘safeguarding national security’ to take unfettered advantage of intelligence outsourcing and Member States have been reluctant to confer on the EU competence for (sensitive) security policies. Nevertheless, absent settled case law, the outcome is uncertain and further research appears necessary. For more information, see Annex II.

Even if Pegasus cases pass the 'national security' test, Member States may attempt to interpret the scope of secondary data protection and privacy laws in a way that excludes Pegasus cases. As a knock-on effect, this could render the EU Charter of Fundamental Rights inapplicable (Article 51 CFR). While this is conceivable, applicants can make a solid case for the applicability of the EU data protection and privacy acquis (see Annex II). Finally, ‘it is important to emphasise that the use of digital surveillance tools by EU Member State authorities for national security purposes, even when it falls outside the scope of Union law, is nevertheless subject to national constitutional law as well as the relevant legal framework of the Council of Europe, in particular the European Convention on Human Rights’. As discussed in the section on legal concerns, these rights and laws may be enforced through legal proceedings, formal complaints, infringement procedures, and dedicated sanctioning mechanisms for qualified rule of law deficiencies.

The substantive legal assessment depends on the facts of the particular case ('contextuality'). The EDPS considers that Pegasus surveillance as described by the media would clearly interfere with the fundamental rights to privacy and data protection, but that modified versions of the product may – in certain circumstances – qualify as necessary and proportionate to combat imminent threats. The Society of Civil Rights makes a similar case on the basis of German national law. Further inspiration may be drawn from legal assessments concerning other state-procured spyware such as

---

345 Opinion in Joined Cases C-511/18 and C-512/18, La Quadrature du Net, AG Campos Sánchez-Bordona, 15 January 2020, para 85.
349 Certain arguments made in Annex II regarding the e-Privacy Directive may apply mutatis mutandis in the primary law context. Cameron I., 'Metadata retention and national security: Privacy International and La Quadrature du Net', Common Market Law Review, Vol. 58(5), 2021, pp. 1457-1458; 'The referring courts take a constitutional (hierarchy of norms) approach: the adoption of secondary EU law should not be used to expand the scope of EU competences under the Treaties, in the face of an express exclusion clause written into primary EU law. The Court seems to proceed from another, and opposite, constitutional logic: that in the case of framework Treaties, as the TEU and TFEU undoubtedly are, a decision by the Member States to adopt secondary legislation in fact shows their intentions as to what does, and what does not, fall within the scope of an exclusion clause.';
HackingTeam, FinSpy/FinFisher, and DigiTask.\textsuperscript{353} The general trend in CJEU case law towards recognising the concept of ‘chilling effects’\textsuperscript{354} further bolsters the protective effect of fundamental rights. Additionally, a number of country-specific issues have been raised (see Section ‘4.2. Country-specific concerns’).

The EU may promote and support public and private enforcement of these rights. It could support private enforcement by funding civil society projects aiming to facilitate exchange of information between aggrieved parties (as well as their legal counsels)\textsuperscript{355} or to confirm forensically the infection of targeted mobile phones.\textsuperscript{356} A special need for EU public enforcement arises where effective and timely enforcement is obstructed on a national level and private enforcement is blocked at a higher level – for instance, because aggrieved parties do not qualify as applicants (EU procedures) or must first exhaust domestic remedies (ECtHR procedure). In the case at hand, the need for action would be exacerbated, since implementation records attest to limited and protracted ‘general execution’ of ECtHR judgments in countries using Pegasus.\textsuperscript{357} Most notably, the Commission (or Member States) may launch infringement proceedings where national administrative practices consistently and generally depart from EU law (Article 17 TEU and Articles 258 and 259 TFEU).\textsuperscript{358} While the Commission initially announced it would investigate alleged abuses and, if necessary, launch infringement procedures, it recently signalled that ‘the Commission is not best placed here to investigate individual cases’ (italics added for emphasis) and that ‘investigation of such issues is the responsibility of each Member State’.\textsuperscript{359} If Parliament considers that the Commission takes insufficient action, it may exercise its powers of scrutiny.\textsuperscript{360} Additionally, it may raise the reputational and political cost of non-action for both Member States and the Commission by collecting further evidence, tracking the (in)adequacy of Member States’ responses, and


\textsuperscript{354} Pech L., The concept of chilling effect, Open Society European Policy Institute, 2021.

\textsuperscript{355} Perhaps a trusted party could screen, anonymise and aggregate relevant information and suggest mutually beneficial cooperation between aggrieved parties.

\textsuperscript{356} For an example of a tool funded by the EU to assist victims of fundamental rights violations under the ‘Fundamental Rights and Citizenship’ Programme (JUST/2013/FRC/AG), see CharterClick.


\textsuperscript{358} Judgment in Case C-156/04, Commission v Greece, CJEU, 7 June 2007; On the Commission priorities, see EU law: Better results through better application, 2017/C 18/02, European Commission, 19 January 2017, pp. 14-16; As stated in Section ‘4.1. Transversal concerns’, operationalising the rule of law mechanisms would be challenging, but surveillance abuses may well feed into the rule of law report and arguably bolster enforcement measures.

\textsuperscript{359} Commissioner Didier Reynders, The surveillance of politicians, prosecutors, lawyers and journalists, and other persons and entities in EU Member States using cyber surveillance software, Debate, European Parliament, 15 February 2022: ‘S’il le faut, nous introduisons des procédures d’infraction’; Commissioner Johannes Hahn, Use of the Pegasus Software by EU Member States against individuals including MEPs and the violation of fundamental rights, Topical Debate, European Parliament, 4 May 2022: ‘Member States are competent to guarantee their national security. The investigation of such issues is the responsibility of each Member State. Indeed, the Commission is not best placed here to investigate individual cases. The Commission expects national authorities to thoroughly examine any such allegations and to restore citizens’ trust. I also wish to recall that the EU has a strong legal framework for data protection and privacy.’; Nielsen N., EU Commission won’t probe ‘Pegasus’ spyware abuse, euobserver, 19 April 2022.

campaigning for action. Parliament may also advocate a more dissuasive, seamless, and clear legal framework (see Section 7.1.2.-7.1.4.) to fix unambiguous standards of conduct, thereby facilitating proactive compliance as well as enforcement measures.

Ensure continuous data and privacy protection and enforceable individual rights

Against the backdrop of the Pegasus revelations, the Commission and MEPs have called for the swift adoption of the e-privacy regulation. In general, this could increase the level of EU privacy protection, but it appears necessary to clarify aspects of the proposal to increase the chances of effective protection against public(-private) spying. For an increase in protection through the proposed e-privacy regulation, the prospective rules would need to apply to state surveillance facilitated by private spyware and bind Member States through mandatory rules and/or conditional derogation clauses.

As mentioned under the first point in this section and in Annex I, there would be good reasons for the CJEU to insist on the applicability of the EU data protection and privacy acquis where Member States attempt to bypass EU law by invoking their exclusive competence for national security as a mere pretext for politically motivated surveillance. In comparison with the current ePrivacy Directive, the proposed e-privacy regulation would ensure that not all 'activities of the State in areas of criminal law' fall outside its scope, but only those law enforcement activities which fall within the corollary scope of the Law Enforcement Directive (LED) (Article 2(2)(d) e-privacy regulation). The exact boundaries would be blurry, but EU secondary legislation would prima facie grant data subjects and end-users largely continuous protection (see second part of Annex II). Where intelligence operations are evidently taken under false national security and law enforcement pretence, the ePD and the GDPR may apply. To reinforce such a conclusion, it would be conducive to add a recital to this effect and, possibly, to specify the limits of EU control (for more information, see Annex I).

Drawing on the La Quadrature Du Net and Privacy International rulings, some might argue that the involvement of private spyware providers systematically renders EU law applicable (see above). While the CJEU repeatedly applied the ePD to legislative measures empowering security authorities to involve electronic communications providers in data retention, it is doubtful whether the

362 Article 4(2) TEU and Article 2(2)(a) e-privacy regulation proposal.
363 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 99: ‘Indeed, according to the Court’s settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.’
364 Article 1(3) ePrivacy Directive states ‘activities of the State in areas of criminal law’; The CJEU also noted this distinction when comparing Article 1(3) ePrivacy Directive and Article 2(2)(d) GDPR (which is equivalent to Article 2(2)(d) e-privacy regulation), see Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 102 (‘Although...’).
366 Section 1.3, para. 3, explanatory memorandum of the e-privacy regulation explains that the proposal ‘maintains the substance of Article 15 ePrivacy Directive’ and that ‘Member States are free to keep or create national data retention frameworks [...], taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights;’ Judgment in Joined Cases C-203/15 and C-698/15, Tele2 Sverige, CJEU, 21 December 2016; Judgment in Case C-207/16, Ministerio Fiscal, CJEU, 2 October 2018.
367 Article 2(2)(d) e-privacy regulation would exclude ‘activities which fall outside the scope of Union law’ and ‘activities of competent [i.e. law enforcement] authorities for the purposes of the prevention, investigation, [...] of criminal
CJEU would extend this rationale to measures legitimising cooperation with other private sector actors for intelligence purposes or even purely state-implemented operations. If the systematic application of e-privacy rules is desired, it appears conducive to clarify that state surveillance involving (qualified?) commercial spyware remains subject to the e-privacy regulation despite its Article 2(2)(d). Additionally, it may be clarified that the involvement of extraterritorial spyware providers does not exempt the state from e-privacy rules and that the rules apply to private controllers or processors not established in the Union, such as certain spyware providers. To ensure a future-proof review, it appears conducive to look beyond the Pegasus cases and draw up a taxonomy of public-private surveillance cooperation, to identify key legal factors determining the applicability of e-privacy rules and to configure the regulation in a way that covers the desired cases. There is mounting evidence that negotiating these aspects with Council would be tough, if not futile.

An Austrian preliminary reference lodged on 6 September 2021 suggests that Article 15(1) (possibly read in combination with Article 5) of the ePrivacy Directive is applicable to national rules that allow ‘security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation’, see Summary of the request for a preliminary ruling, Case C-548/21, Landesverwaltungsgericht Tirol, 6 September 2021; Conversely, see Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 103: ‘By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, […] with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR’; For details, see Annex II.

Relevant decision nodes include: Do spying parties declare that their surveillance activities concern exempt domains, while they objectively do not qualify as such? (Article 1(3) ePD); Is a private party involved in surveillance operations? (LQDN, para. 103); Is the private party subject to the territorial scope of the ePD transposition acts? Does the private party qualify as an electronic communications service provider or another party, against which the potentially infringed provision protects? (Articles 3 and 5(3) ePD; LQDN, para. 103); How is decision-making power distributed among the public and private parties and does this imply that another regime overrides the ePD? (interplay ePD and LED, see Articles 3(8), 3(7)(b) and 21 LED as well as Articles 3(9) and 22 LED); Does the private party conduct qualify as interference or as part of collective interference with a provision under Articles 5 and 6 ePD?

The Council is advocating broad exemptions from the e-privacy regulation, Member States disapprove of the CJEU’s data retention case law and the affordance of a broad protection of privacy, the Pegasus scandal spans an increasing number of Member States, and the use of (and possibly trade in) spyware technologies are relevant to national
If the e-privacy regulation were applicable, its Article 11(1) would likely empower Member States to derogate from rights and obligations laid down in the regulation by adopting legislative measures authorising surveillance through private spyware. Such a restriction would need to respect the essence of fundamental rights and freedoms and constitute a necessary, appropriate and proportionate measure in a democratic society to safeguard certain general public interests. To ensure that this derogation clause applies to the case at hand, Recital 26 could be formulated more openly or complemented with examples illustrating situations in which the protection of information stored in and related to end-users’ terminal equipment needs to be restricted in the public interest. Further safeguards may be included in the text.

Where Member States implement Union law, the EU Charter of Fundamental Rights applies (Article 51 of the Charter). This is the case when Member States transpose directives or act within the scope of EU secondary law, including data protection and privacy law. The potentially interlocking and overlapping scope of existing and prospective EU data protection and privacy legislation would ensure broad applicability of the Charter. National derogations from the EU data protection and privacy framework would be measured against relevant derogation clauses, read in light of the EU Charter of Fundamental Rights. Even where surveillance measures are not subject to EU rules, national constitutional law and the Council of Europe framework, in particular the European Convention on Human Rights, apply.

Provide practical guidance and facilitate dialogue about best surveillance practices

In consultation with intelligence agencies, oversight bodies and export control authorities, the EDPB may draft guidelines on the lawful design, trade and use of spyware – or of cyber weapons in general. Against the backdrop of Member State competences, the board could assess which edge cases still fall within the purview of the LED, GDPR, ePrivacy Directive and the Charter, and clarify the applicability of derogation provisions (see above and Annex I and II). Additionally, it could clarify which circumstances manufacturers, traders and operators should take into account and how to weigh them when taking decisions with fundamental rights implications. Special attention might be paid to public-private surveillance partnerships and the implications of exporting products to third-country clients. Spyware exports beg the question whether products dedicated to third-country clients are subject to more permissive design conditions or whether the risk of EU data processing necessitates a precautionary design. The guidance could possibly clarify technical, organisational and legal safeguards that providers should put in place to mitigate the risks of clients violating human rights and data protection rules. Additionally, it could detail how EU and Member State authorities may ensure that no intelligence stemming from undemocratic and abusive surveillance by third

---

security interests; The adoption of the Council’s position on the ePrivacy Directive’s national security exemption may undo CJEU rulings such as Privacy International and La Quadrature du Net, see Article 2(2)(a) e-privacy regulation; Kayali L, Tension mounts ahead of key ruling on French data retention, Politico, 14 April 2022; Kayali L, France seeks to bypass EU top court on data retention, Politico, 3 March 2021.

Currently, it emphasises ‘providers of electronic communications services’ and ‘interception of electronic communications’.

Explanations relating to the Charter of Fundamental Rights, Notice No. 2007/C 303/02, Praesidium of the European Convention, 14 December 2007, p. 32.

Article 11(1) e-privacy regulation, Article 23 GDPR, and Articles 13(3), 15, and 16(4) LED.

See, for instance, Judgment in Joined Cases C-203/15 and C-698/15, Tele2 Sverige, CJEU, 21 December 2016; Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020.


countries reaches EU and Member State databases.\textsuperscript{379} Finally, more frequent and possibly formalised dialogue between DPAs,\textsuperscript{380} the judiciary and security authorities may further promote best practices.

To dissuade disproportionate data collection, to instil a sense of responsibility and prudence, and to ensure effective redress, policymakers may consider enhancing liability rules. The EDPS suggests that: ‘Criminal procedural laws should outlaw the use of highly intrusive hacking tools like Pegasus. Based on Article 82 of the Treaty on the Functioning of the European Union (TFEU), the EU has the competence to adopt minimal standards on the rights of individuals in criminal procedures. This includes restricting the admissibility of evidence collected with the help of highly intrusive hacking tools like Pegasus or even outlawing it. The EU could also, based on Article 83 TFEU, define criminal offences such as illegal use of spyware technologies.’\textsuperscript{381} EU Commissioner Didier Reynders recently indicated that Pegasus operations are ‘a crime throughout the Union thanks to the Directive on attacks against information systems’ (unofficial translation from French).\textsuperscript{382} From a civil law perspective, illegal interference with such an IT system would likely trigger tort liability of the operator and possibly the provider.\textsuperscript{383}

Cases crossing international borders, like those suspected in France, add another layer of complexity since they are subject to private international law and governments benefit from state immunity. In a lawsuit, NSO is also attempting to derive immunity for itself from the immunity of the foreign state it was supporting.\textsuperscript{384} The US Supreme Court recently invited the Solicitor General of the US Justice Department to file a brief in this case expressing the views of the US.\textsuperscript{385} According to then UN Special Rapporteur David Kaye, individuals should be able to hold both private and public actors accountable. This may require a re-interpretation of the norms of sovereign immunity.\textsuperscript{386}

The utility of resorting to the international human rights framework is challenged by inherent enforcement constraints.\textsuperscript{387} Nevertheless, its considerable positive impact and its profound

---


\textsuperscript{382} The Pegasus spyware scandal, Debate, European Parliament, 15 September 2021.


\textsuperscript{385} Invitation of the Solicitor General to file a brief expressing the views of the US in case no. 21-1338, Order list: 596 U.S., 6 June 2022, p. 1.


moral/political significance should not be underestimated.\textsuperscript{388} UN Special Rapporteur Joseph A. Cannataci put up for discussion in 2018 a draft legal instrument establishing global surveillance standards.\textsuperscript{389} Legal redress based on the (regionally applicable) \textit{European Convention on Human Rights} appears more promising, but extends only to its 46 signatory states, primarily applies to public actors, requires prior exhaustion of domestic remedies, and implementation of judgments is unsatisfactory – not least in countries using Pegasus.\textsuperscript{390} Researchers are exploring new mechanisms capable of holding corporations accountable for human rights violations,\textsuperscript{391} which could cover spyware providers complicit in abusive surveillance operations. In another context, one researcher proposes to establish 'shared' corporate-state responsibility through codes of conduct, which countries would make a prerequisite for exports.\textsuperscript{392}

\textbf{Stimulate a discussion on legal limits of intelligence outsourcing}

The involvement of private actors in intelligence operations raises concerns regarding the legal limits on the privatisation of public functions. In its complaint to the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), the Society for Civil Rights considers that the bugging of mobile phones to bypass encryption of communications and extract data qualifies as an inherently governmental function, which must be performed in-house by officials. Consequently, the involvement of the NSO Group would violate this exclusive attribution of functions.\textsuperscript{393}

Journalists, academics and policymakers discussed widely the outsourcing of US intelligence activities after a series of scandals involving private intelligence contractors in the early twenty-first century.\textsuperscript{394} The privatisation of intelligence activities raises concerns familiar to debates over the outsourcing of the state control of force to private military and security companies (PMSCs, 'privatisation of security').\textsuperscript{395} In the US, functions are inherently governmental and may not be

\begin{itemize}
  \item E.g. Shorrock T., \textit{Spies for Hire}, Simon & Shuster, 2008; Chesterman S., \textit{We Can't Spy ... If We Can't Buy!}: \textit{The Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions}, European Journal of International Law, Vol. 19(5); Puyvelde D., \textit{Outsourcing US Intelligence: Private Contractors and Government Accountability}, Edinburgh University Press, 2019, p. 142: 'The involvement of contractors in [interrogation] scandals [notably Abu Ghraib] was a turning point in the public debate on outsourcing.'
  \item Chesterman S., \textit{We Can't Spy ... If We Can't Buy!}: \textit{The Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions}, European Journal of International Law, Vol. 19(5), p. 1057: 'It frequently
\end{itemize}
outsourced if they 'require either the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government' ('key decisions'/‘steering’).396 Inherently governmental functions involve, among other things, ‘the interpretation and execution of the laws of the U.S. so as to significantly affect the life, liberty, or property of private persons'. Nevertheless, ‘public-private boundaries remain susceptible to a variety of interpretations' and the practical application will depend on the interpretation of individual agencies.397 'There is little dissent from the view that key decisions regarding paramilitary actions, including targeted killings, should always remain in the hands of elected officials or their political appointees.'398 A similar case can be made for the interrogation of detainees.399

Opinions differ on whether the collection400 and analysis401 of intelligence – both of which are features of Pegasus – present inherently governmental functions. Since top-level analysis of intelligence is intimately linked with the 'direction and control of intelligence operations' and may shape strategic policy, it may be perceived as influencing key decisions and thus an inherently governmental function.402 Conversely, intelligence analysis may be perceived as 'developing options', the choice of which remains with the government. One academic concludes that 'as long as appropriate review procedures ensure the integrity of intelligence products, outsourcing analysis does not pose major problems'.403 According to another academic, contracting out hard- or software for the collection of data, largely appears to support the implementation of policy and does not

---


399 Chesterman S., We Can't Spy ... If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing ‘Inherently Governmental Functions’, European Journal of International Law, Vol. 19(5), pp. 1072-1073; Trybus M., A Response to Simon Chesterman We Can't Spy ... If We Can't Buy!, EJIL’Talk!, 26 January 2009; Shorrock T., Spies for Hire, Simon & Shuster, 2008, p. 379; In opposition is Puyvelde D., Outsourcing US Intelligence, Edinburgh University Press, 2019, pp. 198-199, who for reasons of necessity argues against a ban and instead advocates stringent accountability mechanisms such as keeping government officials in the field to directly control the work of contractors.

400 Chesterman S., We Can't Spy ... If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing ‘Inherently Governmental Functions’, European Journal of International Law, Vol. 19(5), pp. 1057-1065 and pp. 1072-1073.


402 Shorrock T., Spies for Hire, Simon & Shuster, 2008; Puyvelde D., Outsourcing US Intelligence, Edinburgh University Press, 2019, p. 202; In an interview with D. Puyvelde, ‘[i]nvestigative journalist Tim Shorrock has argued that ‘the entire analysis operation’ should be brought ‘back into government so that Congress can have full oversight over what goes into intelligence reports.’

usually delegate 'control' over intelligence operations, i.e. the discretionary exercise of government authority.404

In the EU, limits on the privatisation of public functions are largely determined by national law. Academics are only beginning to explore whether international law prohibits state actors from devolving inherently governmental functions to private actors.405 The notion of 'inherently governmental' varies across countries; for instance, in the UK the privatisation of prison services and military installation is a common occurrence, while many countries in mainland Europe consider these services to be inherently governmental.406 Depending on the jurisdiction, one could argue that the development of spyware is not per se an inherently governmental task that must be performed by officials.407 However, ensuring the development of compliant software may be considered an inherently governmental function, which must be performed by the government.

In certain jurisdictions, fundamental rights may further particularise a public duty to put in place procedural and organisational measures, such as selection criteria, control mechanisms, and a right of instruction (see section on accountability).408 A breach of these duties, which does not extend to outsourcing compliance checks,409 would likely interfere with fundamental rights, rather than the exclusive attribution of inherently governmental functions.

Where contractors are involved in law enforcement and intelligence operations and left with decisional discretion, one might argue there is an interference with the exclusive attribution of inherently governmental functions.410 Allegedly, NSO was left with control over the technical infrastructure and power of decision on the modalities of device infiltration, system reconfiguration and data exfiltration.411 Consequently, the Society for Civil Rights asserts that the involvement of NSO in intelligence operations violates the German constitutional provision attributing exclusive competence of governmental functions.

Even where governments do not leave contractors with discretion, but contractors by design retain technical means of substantial, possibly even real-time, influence on particularly sensitive operations, one might say there is an interference with inherently governmental functions. While a right of instruction or closer integration with the governmental apparatus may legally tie the contractor to the mast, the practical risk of non-compliance may comprehensively prevent outsourcing in sensitive areas. After all, ‘who is really in control when the private sector develops, constructs, ships, arms, flies the drones remotely, and a government official just presses the button?’412 Conversely,


406 Trybus M., A Response to Simon Chesterman ‘We Can’t Spy ... If We Can’t Buy!’, EJIL-Talk!, 26 January 2009.


409 See last sentence of previous paragraph.


one may argue that the functional maintenance of spyware during operations does not qualify as an inherently governmental function, since the key decisions rest with government officials.

At least, such activities may qualify as a ‘closely associated’ or ‘critical’ functions, which require particular oversight (see section on accountability).

Include human rights controls and transparency obligations in public procurement rules and strengthen Parliament’s power of the purse

Privacy International recommends increasing public participation in public authorities’ procurement decisions. Such models have been introduced on a local level, but allegedly never in federal intelligence agencies, which often have a greater need for more sophisticated technology and secrecy. Similarly, former UN Special Rapporteur David Kaye called for meaningful public oversight concerning the purchase of surveillance technologies.

EU procurement rules possibly provide avenues for the review of non-transparent procurement procedures resulting in the purchase of non-compliant surveillance technologies by intelligence agencies. Typically, EU procurement rules do not apply to Member States’ intelligence agencies making sensitive purchases for security purposes (see Annex III).

Arguably, where intelligence agencies (evidently) invoke national security purposes as a pretext for covertly purchasing surveillance technologies to spy on the political opposition, EU procurement rules, notably Public Procurement Directive 2014/24/EU, would apply (see first point in this section and Annex I and III). Where contracting parties are awarded such a contract without conducting the necessary procurement procedures, the Commission may consider launching an abuse control procedure under Article 348(2) TFEU or an infringement procedure and aggrieved bidders could initiate review proceedings against contracting entities. In line with the rationale of Article 348(2) TFEU, procedures could be held in camera. Even where national authorities have conducted the necessary procurement procedures, the acquisition of software that is non-compliant by design (relative to the envisioned uses) and therefore not legally operational raises questions about selection criteria and the evaluation of tenders (especially about the selection of the economically

---


417 Similarly, Gill P., Of intelligence oversight and the challenge of surveillance corporatism, Intelligence and National Security, Vol. 35(7), 2020, p. 982: ‘Companies themselves may play a role as an “accountability-holder”, for example, by keeping government officials in their conduct of procurement processes, yet corporate self-regulation cannot be the whole answer and the rules must still be defined by government officials with their responsibility to protect the public interest.’ In the same vein is Puyvelde D., Outsourcing US Intelligence, Edinburgh University Press, 2019, p. 130.
most advantageous tender). Critics arguing that Pegasus is non-compliant by design may also consider its public procurement a violation of constitutional principles of efficiency and economy. However, establishing that these authorities evidently intended to purchase software for politically motivated spying would be very difficult.

Despite limited applicability of the EU procurement acquis to procurements of surveillance technologies by certain public authorities (see above), the EU could further strengthen the protection of human rights in its procurement acquis and hope for spillover effects. The EU may consider disqualifying from procurement procedures (certain) security capabilities providers, who remain under the purview of the EU procurement acquis, but intentionally or negligently supplied human rights abusers with technology. In the same vein, legislators may prescribe that contracting authorities must take into account the supply of human rights abusers by bidders when evaluating the tender. Additionally, procurement rules may also include contracting preferences for security capabilities vendors with self-regulatory human rights schemes, such as ethics committees.

To enable contracting authorities to vet bidders (human rights assessment), procurement rules may mandate that a bidder must disclose its customers and suppliers (‘know your vendor’ provisions). If such disclosure excessively interferes with the confidential nature of the spyware trade and therefore risks driving vendors away or underground, co-legislators may instead impose vendor background screening on contracting authorities. To enhance the effectiveness of such screening obligations, legislators may complement them with notice procedures that would allow for input from NGOs and an information exchange mechanism or ‘enforcement coordination mechanism’ that would ensure information sharing among contracting authorities. Finally, the need for fundamental rights-compliant technology may be emphasised as an award criteria.

Such modifications would imply that procurement departments build proficiency in assessing privacy, data protection and human rights implications. In practice, procurement departments may voluntarily apply these practices to sensitive purchases of cyber-surveillance technologies. Furthermore, these rules may serve as a blueprint for national legislators or oversight bodies in modernising rules on sensitive contracts exempt from EU law (‘gold plating’). On a Member State

---

418 Audit Office for violating the constitutional principle of efficiency and economy by acquiring non-compliant spyware, see ‘PIRATEN zeigen BKA wegen Spähoware an’, Zeitschrift für Datenschutz-Aktuell, Vol. 3(6), 2016, no. 03512; Trybus M., A Response to Simon Chesterman ‘We Can’t Spy ... If We Can’t Buy’, EJILTalk!, 26 January 2009: ‘In any national context the procurement of defence and intelligence supplies and services has to operate within a triangle of three objectives: (1) national security, (2) value for money, and (3) democracy and the rule of law. [...] There is a connection between national security and value for money since the earlier is affected when the security budget is depleted through inefficient procurement and necessary services cannot be provided as a result. Democracy and the rule of law form the basis of a country such as the United States. Not even the national security objective can be allowed to compromise these most basic principles on which any democracy is built. A balance needs to be struck between the three corners of this triangle.’

419 For a discussion of this approach in an international context, see DeSombre W. et al., Countering cyber proliferation: Zeroing in on Access-as-a-Service, Report, Atlantic Council, 1 March 2021. Concerning corporate due diligence, Parliament had called for ‘the prohibition of the importation of products related to severe human rights violations such as forced labour or child labour’ (italics added for emphasis).

420 Or even the confidentiality of export licences.

421 On the negative implications of driving spyware providers away or underground, see Section ‘7.1.4. Prevent external spyware abuse’, point four.

422 Inspiration may be drawn from EU dual-use export control rules (see sections 4’2.4. Bulgaria and Cyprus’ and ‘7.1.4. Prevent external spyware abuse’, point 2) and possibly even the Proposal for a Directive on corporate sustainability due diligence and the German Supply Chain Due Diligence Act (notion of ‘substantiated knowledge’).
level, the principles of the rule of law and sound financial management (budget law), would likely counteract the procurement of non-compliant software.423

**Financial oversight** of intelligence agencies may present avenues to prevent the procurement of non-compliant spyware as well as doing business with unvirtuous spyware vendors. In Europe, the executive formulates intelligence budgets and audit offices and specialised parliamentary committees scrutinise budgets and expenditure in approval and review procedures.424 The applicable rules balance budgetary transparency with the need to maintain operational secrecy.425 While the principle of sound financial management may warrant that budgetary controllers block purchases of surveillance technologies that are non-compliant by design (in relation to their prospective use-cases426), a number of factors may prevent such an intervention. Low budget granularity, misleading descriptions or classifications, time constraints, lack of sufficient technical know-how to scrutinise highly complex surveillance technologies, and politicisation of oversight committees may hamper regular and detailed oversight.427

Consequently, Member States may consider enhancing scrutiny of surveillance technology purchases. Where this is not already the case, budget committees may consider instructing intelligence agencies to detail or separately submit purchases of cyber surveillance technologies with particular implications for fundamental rights (or above a certain value threshold) for prior approval. In the US, the Director of National Intelligence must ‘submit a list of all contractors that have been the subject of audits by an inspector general, or have been investigated for criminal violations, fraud, financial waste, and other actions that could affect their ability to deliver services’.428 An overview of providers whose technology facilitated human rights violations and guidance on how to recognise non-compliant technologies may also prove useful. Parliament adopted a report condemning the use of Pegasus surveillance software by Hungarian and Polish state entities and urging the Commission to draw up a list of illicit surveillance software and to keep this list updated.429

---


426 In practice, it would be challenging to determine conclusively that a specific surveillance technology is generally non-compliant by design. Sophisticated systems such as Pegasus contain technical safeguards as well as configuration options, and severe threats to national and public security may justify operations beyond conventional democratic constraints. The EDPS contends that ‘one cannot exclude the possibility that the application of certain features of Pegasus may pass the necessity and proportionality test in specific situations of very serious threat, such as imminent terrorist attack’.427


According to civil society organisations and former UN Special Rapporteur David Kaye, national legislators should pro-actively review and, if necessary, amend **law enforcement and intelligence laws** to meet human rights standards, by including safeguards such as legality, legitimate objective, necessity, proportionality, and meaningful and effective oversight, as well as effective remedies and legal recourse. Various commentators call for an update of traditional oversight and control mechanisms to better contain novel surveillance technologies (including through oversight tech). For a discussion on country-specific oversight lacunae, see Section 4.2. Country-specific concerns, and on accountability issues relating to public-private surveillance cooperation, see subsequent point.

**Stimulate a discussion on governance and accountability of public-private surveillance cooperation**

While the oversight of state surveillance has been analysed extensively and oversight standards have been developed in case law, stakeholders and researchers have not yet fully explored the accountability and oversight implications of EU intelligence outsourcing.

**Accountability** is understood here as being liable to give account or explain actions and, where appropriate, to suffer consequences for errors. Means of accountability include control, authorisation, review, oversight, and sanctioning by executive authorities, the judiciary, parliament, expert bodies, and independent bodies. One may also classify monitoring by civil society and the media as a form of accountability.

---

430 Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International website; UN Special Rapporteur David Kaye, Report on surveillance and human rights, A/HRC/41/35, 28 May 2019, pp. 15-17; See also the case law digests, cited under the previous point.

431 Vieth K. and Wetzling T., Data-driven Intelligence Oversight, Stiftung Neue Verantwortung, November 2019; Wetzling T. and Vieth K., Upping the Ante on Bulk Surveillance, Stiftung Neue Verantwortung, November 2018; Ombudsman Angel Gabilondo, El Defensor del Pueblo verifica que la actuación del cni se ha realizado conforme a la Constitución y la ley en los casos examinados, 18 May 2022, pp. 7-8; Canals Ametller D., Secreto de las comunicaciones y vigilancia digital, El País, 4 May 2022.


433 For a case law digest, see Guild E. et al., Data Retention and the Future of Large-Scale Surveillance, Queen Mary Law Research Paper No. 372/2021, 29 November 2021, pp. 24-29; Malgieri G. and de Hert P., European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‘Good Enough’ Oversight, Preferably But Not Necessarily by Judges’, in Gray D. and Henderson S., The Cambridge Handbook of Surveillance Law, Cambridge University Press, 2017; Recently an Austrian Court requested a preliminary ruling (inter alia) on whether EU data protection and privacy law precludes national provisions which allow security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation without the authorisation of a court or independent administrative body, see Summary of the request for a preliminary ruling, Case C-548/21, Landesverwaltungsgericht Tirol, 6 September 2021, p. 2 and pp. 5-7.


In the area of bulk surveillance, which relies on public-private cooperation, several academics have concluded that the oversight frameworks of 10 Member States do not meet the requirements handed down in the CJEU ruling *La Quadrature du Net and Others*.[437] These oversight requirements mainly aim to enhance scrutiny of intelligence activities, but do not explicitly address the risks of private-public cooperation. In the Pegasus context, the Hungarian Civil Liberties Union (HCLU) criticises oversight deficits in the Hungarian legal framework, but likewise does not explicitly address particularities intrinsic to spyware outsourcing. Conversely, one expert indicates in her UN input paper that the involvement of the private sector in state espionage ‘creates a multitude of risks, including insufficient oversight of and accountability mechanisms for activities tied to the use of force’.438 ‘Since the logic of necessity is likely to dictate the government’s reliance on contractors, adequate accountability mechanisms need to be in place to control the involvement of contractors’.439 Since the CJEU at best implicitly treats possible risks associated with involving electronic communications service providers,440 policymakers may consider investigating these risks and, where necessary, enhancing accountability as a means to bolster public law values and safeguard fundamental rights. Without intending to be exhaustive, the subsequent paragraphs briefly review features of public-private spyware cooperation, the risks associated with intelligence outsourcing, and possible interventions.

Unlike the one-off supply of certain security equipment, intrusion and surveillance software may be supplied continuously and adapted over time – for instance, with regard to attack vector and data analysis functionalities. It remains uncertain whether its execution presents a largely foreseeable, or even deterministic, process, without involving discretionary decisions from the provider. Providers offer both off-the-shelf and build-to-order versions. Presumably, contractors retain the technical means to interfere with intelligence operations, but exercise (contractually mandated and commercially motivated) self-restraint. Frequently, intrusion software providers are headquartered in foreign jurisdictions, store data abroad, pursue business objectives,441 answer to shareholders,442 and employ former intelligence officers. They contract on a global scale, where actors mainly pursue their interests through ‘bargaining and persuasion’.443 When security and intelligence services

---

contract out sensitive activities, ‘information about public-private collaboration is protected both by government and private sector policies’.444

Drawing on the experience of US intelligence outsourcing, private sector involvement (arguably) bears the risk of corruption and abuse, as well as undermining intelligence accountability mechanisms (see Annex IV). In the Pegasus context, Polish politicians and media outlets raised concerns about illegal funding of Pegasus 445 and possible profiteering446. Former NSO employees abused the spyware to target a love interest447 and stole Pegasus source code to sell it for personal gains448. Other risks associated with intelligence outsourcing include (i) strategic mistakes based on biased private intelligence analysis, (ii) sidestepping the illegality of conduct through regulatory arbitrage, (iii) public actors skirting responsibilities and checks through a combination of informal/secret outsourcing and deliberate ignorance, (iv) private actors interfering with operations, and (v) private actors sharing confidential data with adversaries or other parties (for details, see Annex IV). Academics identify several problem drivers, including the emergence of a profit motive in intelligence activities, a culture of loyalty and common patriotism among private-public partners, insufficient contract and contractor management, a lack of control and (dissuasive) sanctioning mechanisms against private actors, a culture of informality and secrecy, and the reactive (as opposed to proactive) posture of (parliamentary) oversight holders. Academics also noted a particular lack of systematic control and oversight in times of crises, notably where the influx of contractors triggered by the post-9/11 surge in intelligence demand overwhelmed public structures and processes. Some academics consider that many of these risks are not unique to public-private surveillance partnerships, that government officials may likewise pursue their own views and interests449 at the expense of good practices, and that there is no greater proportion of mismanagement and abuse in public-private partnerships than within government agencies.450

Contemporary spyware outsourcing exacerbates challenges. It is characterised by international transactions and operations, a tendency for arms-length cooperation, network dynamics, and high-tech solutions.451 Spyware providers act on a global scale where individual states do not ‘monopolise the levers of influence’. States are not exclusive customers and must pursue their interests through ‘bargaining and persuasion’. Power asymmetries may persist in both directions, but governments increasingly rely on key/unique private sector technologies.452 '[T]he more dominant is the

445 Zieliński R., Pieniądze z funduszu na wsparcie ofiar przestępców poszły na system do inwigilacji, tvn24, 21 September 2018.
446 P., Pośrednik w zakupie Pegasssa z milionowymi kontraktami od rządowych instytucji. Wyniki kontroli poselskiej, tvn24, 19 January 2022: ‘The question arises as to what connects the leadership of the Law and Justice party with former SB agents’, Joński asked. ‘Who recommended this [intermediary] company [Matic] in all these institutions, from NCBR to all government institutions?’ added Joński. As he pointed out, this must be explained.
447 Cox J., NSO Employee Abused Phone Hacking Tech to Target a Love Interest, Vice’s Motherboard, 28 April 2020.
448 The Office of the State Attorney, 5 years in prison for NSO employee, Israel’s Ministry of Justice, 16 January 2019; Cox J., NSO Group Employee Allegedly Stole Company’s Powerful Spyware for Personal Profit, Vice’s Motherboard, 5 July 2018.
449 E.g. monetary, personal or organisational.
452 Chesterman S., One Nation Under Surveillance, Oxford University Press, March 2011, pp. 129; Shorrock T., Spies for Hire, Simon & Shuster, 2008, p. 379: ‘We saw it at the NSA, where the cooperation of the private sector – including telecom
corporate sector in identifying problems and devising solutions, the more they will set the agenda and limit the state’s options. Unlike national security and intelligence services, spyware providers are not part of the government and can (to a certain extent) jurisdictionally evade hierarchical government action. Unlike telecommunication providers who are involved in bulk data collection, spyware providers have an innate interest in satisfying government intelligence demands, while restricting government insights into proprietary methods, intellectual property, and (adversary) government customers. A UN working group and researchers term spyware providers as ‘cyber mercenaries’ – signifying a lack of national allegiance, a disregard for national security, and a principal interest in remuneration. Paradigmatically, NSO is suspected of hacking high-ranking government officials of a customer government (Spain) on behalf of other customers. Finally, the hiring of former intelligence officers, as well as possible legal and coercive influence of host countries on corporate headquarters, raise concerns about data confidentiality and espionage.

Mainly in response to the US outsourcing experience, critics proposed a number of interventions aimed at mitigating the aforementioned risks. Besides reinforcing the control and oversight of government actors, standards and processes may be developed to ensure accountability of spyware contractors and public-private surveillance partnerships. Experts recommend to:

- develop procurement criteria, standard contractual clauses and clear management procedures (including monitoring procedures) that safeguard integrity, independence, manageability, instructability, sanctionability and justiciability of private actors as well as ensures alignment with public law values,
- facilitate effective redress by investigating and, where appropriate, disclosing affiliated incorporations of private partners,
- ensure lawful intrusion, the integrity of collected data and the accuracy of data analysis/presentation through (code) review procedures,
- tighten the requirements for approval and warranting of surveillance measures,

providers and IT companies – is so critical that, according to Dick Cheney, a failure by Congress to grant immunity to those companies that assisted the government in the warrantless surveillance program would put the nation in grave danger. When a Vice President of the United States has to stoop to fear-mongering to protection corporations that may have ‘broken the law, it’s time to pull the plug on privatization.’


454 Wetzling T. and Vieth K., *Upping the Ante on Bulk Surveillance*, Stiftung Neue Verantwortung, November 2018, p. 51: ‘Intermediaries that are compelled to cooperate have an incentive to closely measure each government request against the relevant legal requirements. Internet companies have reputational costs associated with enabling far-ranging access to their customers data and, therefore, may only allow what is strictly necessary’; Telecommunication providers have been known to both comply with and challenge data access orders.


459 From the bulk surveillance context, see Wetzling T. and Vieth K., *Upping the Ante on Bulk Surveillance*, Stiftung Neue Verantwortung, November 2018, p. 33; For a discussion on the prior approval and review requirements for EU bulk surveillance, see Guild E. et al., *Data Retention and the Future of Large-Scale Surveillance*, Queen Mary Law Research Paper No. 372/2021, 29 November 2021, pp. 24-29; Michaels J., *All the President’s Spies*, California Law Review, Vol. 96(4), 2008, p. 943, fn. 189 and p. 944, notes ‘With the imposition of greater legal requirements, there is also the problem that some potentially useful intelligence-sharing partnership will simply not come together’.
promote transparency and public scrutiny – for instance, through authorised public disclosure of intelligence information such as standard contractual terms,\textsuperscript{460}

empower oversight bodies to perform proactive or real-time oversight – for instance, through enhanced and regular reporting\textsuperscript{461} and enhancing oversight through periodic re-authorisation requirements,\textsuperscript{462}

promote direct and independent dialogues between oversight bodies and private actors, to contravene opaque agency interactions with private intermediaries,\textsuperscript{463}

procure software with integrated audit tools for oversight bodies and immutable audit logs (‘oversight-by-design’),\textsuperscript{464}

develop standard contractual terms and management protocols that are impervious to a surge in intelligence outsourcing and pass stress tests,

make procurement conditional on contractors’ submission to codes of conduct with a dedicated oversight committee and grievance mechanisms,\textsuperscript{465} or rely on peer-pressure and competition among contractors as an incentive to submit to codes of conduct,\textsuperscript{466}

broader whistleblower protection so that sousveillance\textsuperscript{467} (undersight) may complement oversight,

incentivise a critical and responsible surveillance industry that would hold public actors to account – for instance, by (i) mandating corporate legal assessments of governmental instructions, task orders, and warrants, (ii) sanctioning actions lacking appropriate warrants [or legal basis], including by holding executives criminally and civilly liable, (iii) imposing obligations on private partners to directly report to

\textsuperscript{460} Puyvelde D., \textit{Outsourcing US Intelligence}, Edinburgh University Press, 2019, pp. 230-231; van Buuren J., ‘From Oversight to Undersight: the Internationalization of Intelligence’, \textit{Security and Human Rights}, Vol. 24(3-4), 2013 holds that ‘scholars should acknowledge that almost every intelligence scandal has been revealed by investigative journalists and/or whistle-blowers’; Note, however, that the ‘public reputational mechanism’ (naming and shaming) is not always effective, see Gill P., \textit{Intelligence Reform: the never-ending story}, Panel 21, International Association for Intelligence Education Conference, June 2016, p. 15.


\textsuperscript{463} Vieth K. and Wetzling T., \textit{Data-driven Intelligence Oversight}, Stiftung Neue Verantwortung, November 2019, pp. 41-43.


oversight bodies, and (iv) restricting immunity to actions clearly defined in contracts and properly reported to oversight bodies.469

- ensure effective contract management, including reporting and contract performance evaluation (metrics).470
- instil a sense of responsibility and prudence and ensure effective redress by tightening state liability rules for contractor behaviour,471
- introduce objective threat measures to prevent a ‘terrorism industry’472 from exaggerating threats and needs for more intelligence workers and capabilities,473
- maintain government control over domains that are mission-critical and, where necessary, deploy officials directly in the field to cooperate with and control contractors,474
- ensure lawfulness and coherence through internal policies475 and ensure sufficient expertise to make strategic decisions and critically review contractors’ advice and behaviour.476

The validity of these risks, the regulatory performance of traditional control and oversight mechanisms, the need for intervention,477 and the effectiveness and suitability of the aforementioned mitigation strategies merit further investigations, which are beyond the scope of this study. When assessing policy problems and formulating policy objectives, security and confidentiality needs must be taken into account. Already in 2015, and again in 2017, the European Union Agency for Fundamental Rights found in its study on ‘surveillance by intelligence agencies’ that the ‘private sector’s role in surveillance requires a separate study’.478 In the same vein, an academic identified the need to study private intelligence in countries other than the US.479 Since the debate is largely influenced by the US experience with intelligence outsourcing, a number of contextual discrepancies, such as the post-9/11 surge in intelligence outsourcing, should be taken

---

469 Michaels J., ‘All the President’s Spies’, California Law Review, Vol. 96(4), 2008, pp. 951-966; Gill P., ‘Of intelligence oversight and the challenge of surveillance corporatism’, Intelligence and National Security, Vol. 35(7), 2020, p. 982: ‘Companies themselves may play a role as an ‘accountability-holder’, for example, by keeping government officials in their conduct of procurement processes, yet corporate self-regulation cannot be the whole answer and the rules must still be defined by government officials with their responsibility to protect the public interest’.


475 These policies could clarify what (not) to outsource (inherently governmental functions) and how to outsource (procurement, oversight measures, etc.). Depending on sensitivity, criticality and intrusiveness of the mission, different procurement and oversight standards may apply. On a methodology for scoring surveillance technologies, see Sorell T. et al., SURVEILLE Deliverable 2.6 Matrix of Surveillance Technologies, SURVEILLE Work Package 2, 31 July 2013; Sorell T. et al., SURVEILLE Deliverable D2.9: Consolidated survey of surveillance technologies, SURVEILLE Work Package 2, 8 April 2015.


477 Including whether traditional accountability mechanisms are fit or purpose.

478 FRA, Surveillance by intelligence services, Vol. 1: Member States’ legal frameworks, Publications Office of the EU, 2017, p. 8; This was reiterated on p. 19 of the legal update of 2017.

into account (see Annex IV). Investigations may also attempt to further distinguish types of outsourcing, such as commodity, personnel, and support outsourcing, as well as public-private cooperation models, including actors’ contractual and operational roles and responsibilities. Best practices may be developed for different outsourcing categories and stages. Even if specific risks do not manifest in the Pegasus context and the EU lacks competence and the CJEU jurisdiction, a critical debate over accountability of public-private surveillance cooperation may help mitigate future risks and inform European and national best practices, legal interpretations, or even reform efforts.

Integrate and strengthen oversight bodies

To ensure that surveillance measures are carried out lawfully, many Member States put in place prior approval and warranting procedures (ex ante scrutiny), continuous oversight and ex post legal recourse. Since the CJEU clarified that more intelligence regulations and operations are subject to EU law than expected, closer cooperation or even a network of intelligence oversight agencies may be considered. Such networks may facilitate the sharing of knowledge, information, practices and experiences with network participants. Participants may specialise in different types of tasks and develop expertise in different areas to benefit the overall network. This could have knock-on effects such as promoting integration, encouraging lawful practices, relieving pressure on the judiciary and (by freeing judicial capacity) supporting effective access to justice. This would also allow for more targeted cooperation with data protection authorities.

The UN Special Rapporteur Joseph A. Cannataci initiated the first (‘very successful’) International Intelligence Oversight Forum in 2016. It brought together nearly 70 participants from some 26 institutions in 20 countries. These included independent oversight authorities, parliamentary committees, some members of civil society and even an oversight tribunal. Participants were invited to start an open and frank debate in a trusted framework on the adequacy of oversight mechanisms; existing and anticipated surveillance measures, which may have a negative impact on privacy; the distinction between targeted surveillance and mass surveillance; the proportionality of such measures in a democratic society; and the cost-effectiveness and overall efficacy of such measures. The Special Rapporteur concluded that the 2016 forum ‘demonstrated that the discussion on how to manage the oversight of intelligence in a way that reinforces privacy safeguards is a complex process requiring much time, resources, occasional culture changes, political will and the generation of trust’ (italics added for emphasis). He recommended that all UN member states ‘should engage in the painstaking discussion of the oversight of intelligence’ and that ‘governments should encourage oversight bodies and intelligence agencies to take part in the Forums and facilitate their participation’ (italics added for emphasis). The annual forum in 2020 was postponed due to the Covid-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to


481 E.g. of the ECHR, constitutional law, as well as national criminal and security law.


484 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020.

work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption.\textsuperscript{486}

### 7.1.4. Prevent external spyware abuse

**Moratorium or global ban**

UN experts and civil society organisations have called prominently for a moratorium or ban on the trade in/sale of surveillance technology, at least until appropriate safeguards are put in place.\textsuperscript{487}

**Ensure the adequate and uniform application of export controls**

The EU and Member States should ensure that licensing authorities adequately and uniformly apply the recast export controls, including their human rights aspects. By law, licensing authorities must perform *adequate human rights compliance assessments*,\textsuperscript{488} possibly even taking into account the European Commission’s adequacy assessment under the GDPR and the LED.\textsuperscript{489} It is a prerequisite that authorities *build the necessary capacity* to assess human rights situations in third countries.

It would be counter-productive if export control authorities undercut each other and thereby favoured 'jurisdiction shopping', i.e. taking advantage of the most permissive control practices within the EU (‘export control havens’\textsuperscript{490}). As indicated in Recital 30 of the recast dual-use export control regulation, Member States should *uniformly implement and interpret export control criteria*, not least in light of fundamental rights ('convergence' and 'coherence'). So far, Member States have varied significantly in how they apply the former catch-all controls and penalties. Under the revised dual-use export controls, the new 'enforcement coordination mechanism' will bring together Member States' licensing authorities and enforcement agencies to exchange information in confidence and on a number of topics, such as 'risk-based audits' and 'the detection and prosecution of unauthorised exports of dual-use items'. A key challenge will be to draft the mandated guidelines for the new catch-all control and determine which human rights concerns should be taken into account.\textsuperscript{491} Commentators submit that Member States cannot rely on former


\textsuperscript{487} UN Special Rapporteurs and experts, Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech, 12 August 2021; Peggy D. and Lewis P., Edward Snowden calls for spyware trade ban amid Pegasus revelations, The Guardian, 19 July 2021; Amnesty International et al., Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, 27 July 2021.

\textsuperscript{488} On human rights controls of cyber-surveillance technologies, see Article 3(1) in conjunction with items 4A005, 4D004, 4E001.c, 5A001.f and 5A001.j and Article 5(1) Recast Dual-Use Regulation, and Article 2(2) Council Common Position 2008/944/CFSP; For details, see User’s Guide to Council Common Position 2008/944/CFSP, 10858/15, Council of the EU, 20 July 2015; Note that the Commission initially proposed to delete the reference to the Council Common Position and clarify in the main text that competent authorities should consider ‘respect for human rights in the country of final destination as well as respect by that country of international humanitarian law’, see Proposal for a dual-use export control regulation, COM(2016)616 final, European Commission, 28 September 2016.

\textsuperscript{489} van Daalen O. et al., The new rules for export control of cyber-surveillance items in the EU, Institute for Information Law, June 2021, pp. 22-36, and notably p. 33 on the relevance of Commission adequacy decisions.


\textsuperscript{491} Articles 5(2), third sentence, and 26(1) of the Recast Dual-Use Regulation instructing the Commission to draw up guidelines; Bromley M. and Brockmann K., Implementing the 2021 Recast of the EU Dual-use Regulation, Non-Proliferation and Disarmament Papers no. 77, EU Non-Proliferation and Disarmament Consortium, September 2021, pp. 9-10.
interpretations of the term 'cyber-surveillance items', but must now interpret them through a human rights lens, notably in reinforced consideration of the EU Charter of Fundamental Rights. One academic suggests mandating **external auditing** of national licensing decisions by institutions with human rights expertise, introducing an **EU export control adequacy mechanism**, and further **strengthening transparency** of export control decisions. Another academic proposes to make export licensing conditional on applicants' submission to and compliance with qualified codes of conduct (on the latter see the next point). The UN Special Rapporteur suggests that governments should solicit public input and conduct multi-stakeholder consultations when processing licences. In view of the fair balance doctrine, such proposals for additional transparency would need to be balanced against the competing (security and business) interests for confidentiality. The Commission had initially proposed to strengthen human rights controls by replacing the reference to the Council Common Position with an explicit obligation to control the respect for human rights in the main text, but this did not find its way into the final text.

**Foster socially responsible behaviour by spyware vendors and professionals**

Since many experts consider export controls ineffective in curbing the proliferation of spyware, an alternative approach might focus on fostering responsible behaviour among spyware professionals. Prima facie, both hard and soft law instruments may contribute to a change in mind-set.

Against the backdrop of increased litigation and mounting public pressure, the risks associated with investing in spyware providers are growing. Responsible business conduct and capital appreciation objectives both warrant the vetting of potential investee companies for human rights compliance, customer profiles, and pending litigation. Consequently, investors might welcome the option of seeking assurance from an authoritative and non-partisan body that exercises independent scrutiny, for instance through voluntary certification schemes or codes of conduct. Overtime, peer-pressure and competition among contractors may elevate this to an industry standard and help to promote practices consistent with human rights. The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2014-2020) suggests that policymakers should take 'a page from the effort to restrict the private mercenary industry' and

---


'work toward a global code of conduct'. Similarly, the Association of Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) could further develop their ethical guidelines for computing professionals. 

However, the uptake and effectiveness of such rules in an industry built on confidentiality and controversial practices appears uncertain. Purportedly, Pegasus is only the ‘tip of the iceberg’; an iceberg which remains to be uncovered and presumably continues to facilitate abusive surveillance. In this case, it may prove more effective to prescribe the responsible design and handling of spyware; regulating the domestic spyware profession and industry may present viable avenues to foster socially responsible behaviour. This may include obligations to vet employees, mandate employment restrictions, restrict access through biometric checks, control permissions, keep records of access, provide training on human rights and intellectual property crime, obtain professional licences, disclose certain exploits, register with a dedicated company register, and


499 ACM Code of Ethics and Professional Conduct, Association for Computing Machinery website; IEEE Code of Ethics, Institute of Electrical and Electronics Engineers website.

500 Gill P., Intelligence Reform: the never-ending story, Panel 21, International Association for Intelligence Education Conference, June 2016, pp. 12-15; Puyvelde D., Outsourcing US Intelligence: Private Contractors and Government Accountability, Edinburgh University Press, 2019, p. 212; From the corporate due diligence context, see Resolution on Corporate due diligence and corporate accountability, P9_TA(2021)0073, European Parliament, 10 March 2021, para. 1: ‘Considers that voluntary due diligence standards have limitations and have not achieved significant progress in preventing human rights and environmental harm and in enabling access to justice.’


502 Benjakob O., Did NSO Go Rogue and Use Pegasus for Private Ops?, Haaretz, 13 February 2022: ‘Zuk Avraham is the founder and CEO of ZecOps, a cybersecurity firm whose platform inspects phones for current infections or traces of historic attacks. He stressed that there is no “technical restriction that prevents a worker with access to [NSO’s] codes from using it for an attack; only legal and ethical restrictions exist.”’

503 The Office of the State Attorney, 5 years in prison for NSO employee, Israel’s Ministry of Justice, 16 January 2019.
assess potential customers' compliance with human rights. Additionally, policymakers could devise special rules for the transnational and collaborative creation of spyware.

This may also present an opportunity to dissuade EU spyware professionals from side-stepping export controls and building or supporting foreign cybersecurity vendors abroad – for instance, by sanctioning or criminalising such action and enforcing this upon re-entry into the EU. Any regulation should maintain consistency with procurement and export rules as well as accountability and oversight mechanisms. In the spirit of compromise and international reach, a code of conduct could be negotiated at an international level and reinforced at a regional or domestic level by conditioning export authorisations on providers' submission to and compliance with the code (on a comprehensive multilateral approach, see the last point in this section).

Since spyware vendors support intelligence agencies, one might argue that it does not seem inappropriate if they shared the same fate of being regulated. However, in contrast to public authorities, private companies are not accustomed to assessing and balancing fundamental rights, which implies a special need for workable and clear frameworks. Considering litigation and the backlash against spyware vendors holding valid export licences, the industry would likely welcome clarity regarding their responsibilities, notably as opposed to those of export control authorities and intelligence services. While economic concerns may not be at the forefront of human rights debates, the stifling effect of excessive regulation and the security implications of driving the spyware industry away or underground should be taken into account. Spyware vendors can easily relocate to jurisdictions with less oversight or offer their services on the black market – neither being in the public interest. Ideally, new entrants would meet market demands, but competition in intelligence markets may well be imperfect and governments dependent on select private sector technologies. Furthermore, the prevalent (but contested) belief is that cyberspace favours the 'offense', implying that honing such capabilities is not insignificant in the event of cyberwar. Perhaps an environment with adequate checks and sufficient respect for confidentiality would present a compromise and appeal to the industry ('path of legality').

504 Additional inspiration may be drawn from: Button M. and Stiernstedt P., ‘Comparing private security regulation in the European Union’, Policing and Society, Vol. 28(4), 2018; International Code of Conduct Association (ICoCA), The International Code of Conduct for Private Security Service Providers, 10 December 2021; Secretary-General, Use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, A/76/151, United Nations, 15 July 2021; UN Working Group on the Use of Mercenaries, Call for inputs: report on the provision of military and security cyber products and services by ‘cyber mercenaries’ and its human rights impact, United Nations, 12 February 2021; Legal, organisational and technical safeguards necessary under data protection law; Security enhancing measures under cybersecurity laws; Possibly, from rules on handling of dangerous and hazardous substances.


506 Reportedly, this was the purpose of the UAE DarkMatter Group. See DeSombre W. et al., Countering cyber proliferation: Zeroing in on Access-as-a-Service, Report, Atlantic Council, 1 March 2021, p. 14.

507 Due to international sales and extraterritorial reach, the technology would continue to affect EU countries and be more likely to fall ‘into the wrong hands’.

508 Puyvelde D., Outsourcing US Intelligence, Edinburgh University Press, 2019, pp. 100-103.


Stakeholders, academics and experts contend that the EU and Member States should pursue coherent foreign policies that dissuade the use of spyware in violation of human rights standards and limit its dissemination. The former UN Special Rapporteur considers that governments should negotiate a global export regime containing clear rights-compliant safeguards. Microsoft contends that ‘countries should be having open discussions about the appropriate metes and bounds for law enforcement and national security agencies’, instead of ‘hiding the national discussion behind back-door conversations about export control guarantees’. Even if global efforts fail, the EU and its Member States have instruments at their disposal to influence the behaviour of third countries. For instance, the EU has integrated cybersecurity in five external policy areas. Additionally, Member States may cut security aid, including equipment and training, for third countries that would use spyware in violation of human rights. Similarly, MEPs raised concerns about EU ‘Horizon’ science funding going towards foreign military and security companies. Moreover, the EU may use trade agreements to incentivise good behaviour.

In view of the limited effectiveness of international regulation and unilateral deterrence, the Atlantic Council think tank proposes a partner-and-steer governance approach. As cyber surveillance vendors span different jurisdictions and clients, ‘virtuous’ governments would need to develop partnerships. In their view, a coalition of like-minded partners could understand, shape, and, in time, restrain spyware vendors. As a first key policy, legislators should adopt ‘Know Your Vendor’ (KYV) laws to enable informed decisions when awarding spyware contracts and to enhance expertise among policymakers. To influence market actors, the coalition might (i) adopt penalties for vendors selling to governments and other entities placed on a list of concern, (ii) standardise risk assessments for cyber surveillance vendors, (iii) incentivise corporate ethics committees through government procurement and contracts, and (iv) limit military sales and foreign assistance to states that purchase from banned cyber surveillance vendors. Finally, the coalition should (i) selectively

---

511 Kaye D. and Schaake M., Global spyware such as Pegasus is a threat to democracy. Here’s how to stop it, opinion piece, The Washington Post, 19 July 2021.


513 Cybersecurity: EU External Action, European Commission website.


disclose vulnerabilities that are being exploited by banned vendors, (ii) establish employment restrictions for former government cybersecurity employees, (iii) impose business costs by litigating against criminal vendors, and (iv) promote technical limitations that would restrict the use of surveillance technologies temporally and regionally. However, this may fracture the market into spheres of influence and contribute to the deepening global rift.

7.2. For the private sector

**Strengthen cybersecurity**

Leaving the complex EU cybersecurity requirements aside, civil society organisations advocate for the use of cybersecurity tools and end-to-end encryption so that content is not even visible to the provider itself.

Table 2: Atlantic Council’s partner-and-steer governance approach

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vulnerability research and exploit development</td>
</tr>
<tr>
<td>2</td>
<td>Malware payload development</td>
</tr>
<tr>
<td>3</td>
<td>Technical command and control</td>
</tr>
<tr>
<td>4</td>
<td>Operational management</td>
</tr>
<tr>
<td>5</td>
<td>Training and support</td>
</tr>
</tbody>
</table>

Source: DeSombre W. et al., Countering cyber proliferation, Atlantic Council, March 2021.

A vulnerability treatment plan, good disclosure practices (see next point), and a swift vulnerability identification and mitigation cycle would further enhance cyber resilience. Maintaining and honouring a bug bounty programme also prevents security researchers from selling zero-day exploits to potentially malicious brokers.

---

519 For an overview, see Study on the need of cybersecurity requirements for ICT products No. 2020-0715, SMART 2019/0024, European Commission, December 2021; European Court of Auditors, Challenges to effective EU cybersecurity policy, Briefing Paper, March 2019.

520 Certain cybersecurity services and tools are available free of charge.


522 Culafi A., Burned by Apple, researchers mull selling zero days to brokers, TechTarget, 15 October 2021.
According to experts, good disclosure practices enable vulnerable companies to investigate and mitigate vulnerabilities, which hampers their weaponisation. Industry alliances such as Cybersecurity Tech Accord provide further avenues for shared commitment and collective action. Additionally, like-minded industry could cooperate with civil society to exchange knowledge and enhance each other’s cyber resilience capabilities. According to Privacy International, standard-setting bodies should prioritise cybersecurity and an open internet as opposed to surveillance.

Industry alliances such as Cybersecurity Tech Accord provide further avenues for shared commitment and collective action.

In line with data protection laws and according to former UN Special Rapporteur David Kaye, spyware vendors should put in place technical, organisational and legal safeguards that ensure compliant design and use of their products. These could include technical limitations that would restrict the use of surveillance technologies temporally and regionally, as well as contractual clauses that prohibit the customisation, targeting, servicing or other use that violates rights. Technical design features could flag, prevent or mitigate any misuse. It should be possible to deactivate the software remotely in case of human rights violations and without having to terminate the contract beforehand ('kill switch').

Companies should also include human rights clauses and restrictions on customisation in their terms (for more details, see the UN Special Rapporteur’s report on surveillance and human rights). Possibly, companies may consider additional trust-enhancing mechanisms such as security deposits that would fall to victim funds or cybersecurity initiatives in case the client government violates human rights.

In respect of human rights, spyware vendors should refrain from participating in transactions that enable human rights abuses.

To this end, companies may introduce a human rights due diligence procedure, comprising a human rights impact assessment, a risk classification, and singling-out mitigation measures, if warranted. Privacy International highlights that employees may launch collective action and

---


524 The Cybersecurity Tech Accord, Cybersecurity Tech Accord website.


pressure companies to refrain from doing business with potentially adverse human rights implications.\textsuperscript{530}

Investors should take into account human rights practices and commitments

In line with responsible business conduct and capital appreciation objectives, company shareholders and investors should perform adequate due diligence and demand from business a clear commitment to human rights, transparency, and accountability.\textsuperscript{531} For instance, several business, including Microsoft, Amazon and IBM, announced that they would not invest in companies that sell facial recognition technology.\textsuperscript{532}

7.3. For civil society

Contribute to cybersecurity efforts

Civil society organisations and software providers recommend that users should vary passwords, install updates, and apply ‘multi-factor’ authentication. While there is no perfect security, users can drive up the costs of attack; it should also be noted that encryption is not a panacea. Digital training may further improve awareness and feature strategies that further protect users. Civil society organisations should continue their work; they have already played a crucial role in uncovering human rights violations, advocating for human rights-consistent legislation (export controls) and providing guidance on due diligence assessments.


\textsuperscript{532} For references, see Leslie D., Understanding bias in facial recognition technologies, Alan Turing Institute, 2020, p. 22.
8. Synthesis and conclusions

After examining Pegasus’ technical functionality, trading practices, and EU-related surveillance operations, this study identifies legal concerns, including possible disregard of fundamental and human rights, and develops options to strengthen common rights and values.

Pegasus is a spyware designed to breach mobile phones and extract vast amounts of data stored or processed by the target system, including text messages, call interceptions, passwords, locations, microphone and camera recordings, and information from apps. It was developed by the Israeli NSO Group, which today has affiliates under different names in Israel, the UK, Luxembourg, the USA, Cyprus and Bulgaria. According to NSO’s 2021 transparency report, it only licenses software to vetted governments, exports through corporate entities based in Israel, Bulgaria, and Cyprus, and obtained all necessary licences from export control authorities. Both NSO’s CEO and its main investor stressed that the Group has significantly more robust human rights controls in place than any of its industry peers. Nevertheless, civil society organisations deplore the fact that Pegasus was used for severe human rights violations, including murder, and argue that safeguards and responses to abuse notifications were insufficient. Allegedly, researchers and investigators themselves became targets of Pegasus hacks and (physical) undercover operations.

Reports have revealed that authoritarian and democratic governments around the world have used Pegasus to spy on journalists, lawyers, activists, politicians (including opposition leaders), and high-ranking state officials. Investigators link the spyware to human rights harms including intimidation, harassment, detention, and murder. In the European Union, the Hungarian and Polish governments were the first to be caught in the eye of the storm, after media organisations uncovered extensive use of Pegasus spyware by public authorities against opposition figures and government critics. Meanwhile, Spain finds itself in the throes of the Pegasus ‘cyclone’. Reportedly, Germany, Belgium and the Netherlands also have Pegasus at their disposal and Cypriot and Bulgarian authorities may have authorised exports to third countries. Member States and third countries have targeted residents and citizens of Hungary, Poland, Spain, France, Finland, Belgium, and possibly Germany. Reportedly, most of the NSO Group’s clients ‘are within the European Union’, but governments declined to comment. Besides targeting of EU citizens protected by EU law, Pegasus cases feature a variety of European dimensions, including (i) spying on own nationals who are visiting other Member States (Polish lawyer Roman Giertych and possibly members of the Catalan independence movement), (ii) domestic spying on residents from other Member States (Belgian-Canadian student activist Adrien Beauduin), (iii) spying on the confidant of then President of the European Council Donald Tusk (Polish lawyer Roman Giertych), (iv) surveillance attacks in the run-up to the European elections in 2019 (Polish Senator Krzysztof Brejza), (v) the direct or indirect (relational targeting) spying on Catalan MEPs, and (vi) the targeting of Commissioner Didier Reynders and senior EU officials (by means of NSO’s software ‘ForcedEntry’).

The revelations raise concerns on various levels of the European legal order with respect to data protection and privacy, freedom of expression, freedom of the press, freedom of association, redress mechanisms, and democratic processes and institutions. Experts and other commentators criticise Hungary and Poland’s permissive intelligence frameworks, ineffective checks and lax oversight practices. Additionally, reports have surfaced that the Polish Central Anti-Corruption Bureau (CBA) illegally bought the software with funds from the Polish Justice Ministry dedicated to victims of crimes. Spain’s National Intelligence Centre (CNI) maintains that it launched only 18 rather than the suspected 65 intelligence operations against members of the Catalan independence movement. The Spanish government maintains that the CNI acted in accordance with the law and on the
Europe’s PegasusGate

grounds of judicial authorisations, but launched legislative and non-legislative measures to update Spain’s surveillance framework. No specificities are known about cases in Germany, except that the German Federal Criminal Police Office procured a custom version of the spyware. Nevertheless, the Society for Civil Rights (Gesellschaft für Freiheitsrechte) lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) raising concerns over excessive outsourcing of sovereign powers and data protection violations, following logically from the spyware’s non-compliant design. The Belgian and Dutch authorities refused to comment on their use of the Pegasus spyware. Assuming the NSO Group exported Pegasus or similar software from Bulgaria and Cyprus, these authorisation applications would have been subject to EU dual-use export controls, which contain human rights controls as of 2009. EU policymakers enhanced these controls in November 2020 for any export applications as of 9 September 2021.

Individuals and authorities are sounding out redress and enforcement options in response to abusive surveillance practices. The most frequently mentioned instruments include individual litigation, formal complaints, infringement procedures and sanctioning mechanisms for qualified rule of law deficiencies. Most prominently, victims may invoke their human and constitutional rights to data protection and privacy, before national courts and, after – in principle – exhausting domestic remedies, the European Court of Human Rights (ECtHR). While implicated Member States may attempt to challenge the applicability of EU law with respect to their exclusive competence for national security, the CJEU recently stated that ‘the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable’. Particularly, where Member States evidently performed intelligence operations under false (national security) pretences, the EU data acquis, including the EU Charter of Fundamental Rights, may be applicable.

In a cross-border case, the Hungarian Civil Liberties Union (HCLU) suggested the right to free movement of persons and workers had been violated.

The European Parliament set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware. It is looking into existing national laws regulating surveillance, and whether Pegasus spyware was used for political purposes against, for example, journalists, politicians and lawyers.

As the Pegasus revelations implicate Member States and attest to a possible disregard for fundamental and human rights, policymakers seek adequate responses. A special need for EU public enforcement arises where effective and timely enforcement is obstructed on a national level, and private enforcement is blocked at a higher level – for instance, because aggrieved parties do not qualify as applicants (relevant EU procedures) or must first exhaust domestic remedies (ECtHR procedure). Where implementation records attest to limited and protracted general execution of judgments – such as in countries using Pegasus – this need is exacerbated.\(^{533}\)

This study has identified a number of policy options to strengthen common rights and values (see Table 3 on the next page).

---

Table 2: Summary table of policy options

<table>
<thead>
<tr>
<th>Governance angle</th>
<th>Policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry suppliers</td>
<td>- Promote/fund research into upstream markets such as the vulnerabilities market to uncover possible further governance approaches.</td>
</tr>
</tbody>
</table>
| Spyware industry | - Promote/fund research on public-private corporation models, including actors’ contractual and operational roles, as well as market dynamics.  
- Foster socially responsible behaviour by spyware developers, providers and professionals through (international) codes of conduct or by reasonably regulating the spyware industry without driving it away or underground (‘path of legality’). |
| Spyware purchasers | - Stimulate discussions on the legal limits of intelligence outsourcing, notably on functions qualifying as inherently governmental.  
- Include human rights controls and transparency obligations in EU public procurement rules, not least to facilitate Member States’ adoption in areas of exclusive national competence through best practices or legislation (‘gold-plating’). |
| Budget overseers | - Raise awareness of national parliaments’ power of the purse as a means to block purchases of non-compliant surveillance technologies and procurement from unethical providers facilitating human rights abuses.  
- Facilitate the work of competent parliamentary committees, by tracking unethical providers and non-compliant software. |
| Export controllers | - Impose a moratorium on the trade in surveillance technologies until appropriate safeguards are put in place.  
- Monitor the adequate and uniform implementation of export controls as well as the implementation of the new ‘enforcement cooperation mechanism’, the direct cooperation and information-sharing mechanism, and Commission guidelines, for instance in implementation reports. |
| Spyware operators | - Provide practical guidance on the lawful design and use of spyware, including on legal preconditions and parameters for surveillance, public-private surveillance cooperation, and on necessary technical, organisational and legal safeguards.  
- Promote more frequent and formalised dialogue between DPAs, the judiciary, oversight bodies, and security authorities at a national level.  
- Strengthen the intra-EU exchange of best practices, for instance, through a network of intelligence actors or the UN International Intelligence Oversight Forum.  
- Ensure that misconduct defeats its purpose, for instance by prohibiting the admission of unlawfully obtained evidence (inadmissibility rules).  
- Ensure that perpetrators including states, companies, and natural persons are liable for unlawful surveillance. |
| Operations overseers | - Stimulate a discussion on the accountability risks associated with public-private surveillance cooperation, the regulatory performance of traditional control and oversight mechanisms, the need for intervention, and the effectiveness and suitability of mitigation strategies (see list of strategies under Section ‘7.1.3. Prevent internal spyware abuse’, point 8). |
| Surveillance targets | - Incentivise cyber resilience of potential target devices, for instance through an effective Cyber Resilience Act.  
- Provide comprehensive guidelines on the interplay and application of current and forthcoming EU cybersecurity regulations as well as the liability of sellers and manufacturers for failing to provide security updates.  
- Stimulate a discussion on vulnerability disclosure policies for security and intelligence agencies that clarifies under which circumstances cybersecurity interests outweigh intelligence interests, thereby warranting the disclosure of vulnerabilities.  
- Support private enforcement of rights and legislation, for instance by funding civil society projects aiming to facilitate exchange of information between aggrieved parties (as well as their legal counsels).  
- Ensure continuous data and privacy protection for individuals by clarifying the applicability of the pending e-privacy regulation and warranting enforceability through comprehensibility. |
| Member States | - Prepare public enforcement, such as infringement procedures, for instance by collecting evidence and tracking Member State responses. |
| Non-EU actors | - Partner with like-minded countries to steer the global spyware market and ostracise malicious actors (multilateral approach). |

Source: Author’s own elaboration based on references in the body text.
If the Parliament considers that the Commission takes insufficient action, it may exercise its powers of scrutiny. 534

Additionally, both the private sector and civil society organisations may further contribute to driving up the costs of spyware attacks by bolstering cybersecurity. Spyware providers may consider technical, organisational and legal safeguards that ensure compliant design and use of their products. To prevent the abuse of spyware products for unethical intelligence operations, providers may put in place human rights due diligence procedures and vet potential customers. Responsible business conduct and capital appreciation objectives may drive spyware investors to include human rights aspects in their due diligence of investee companies and demand from business a clear commitment to human rights, transparency, and accountability.

9. Annex I: Preliminary remarks on responsibilities for national security

While Member States may challenge the applicability of EU law and the jurisdiction of the CJEU on the grounds of their responsibility for safeguarding national security (Article 4(2) TEU and Article 1(3) ePrivacy Directive (ePD)\(^{535}\)), the CJEU may well take a substantive approach and circumscribe the term as indicated in its ruling in *La Quadrature du Net (LQDN)* and *Privacy International (PI)*. Undoubtedly, there is much controversy about the legal conditions and legal effect of Article 4(2) TEU.\(^{536}\) According to the *LQDN* and *PI* rulings, Member States' responsibility for national security ‘corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities’.\(^{537}\) Such threats distinguish themselves ‘by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise’.\(^{538}\) Although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law (italics added for emphasis).\(^{539}\) This clarifies that Member States’ declarations or intentions do not take precedent over other (so far largely indeterminate) criteria of national security and that national security threats are characterised by their particular seriousness and exceed serious public security threats. The treaties, legislative texts, CJEU case law, and academic theories shed light on possible interpretations of the indeterminate criteria and review standards.

### Public security and fundamental interests of society

The Court develops in its case law basic notions of ‘(qualified) public security’, ‘essential security interests’, and ‘fundamental interests of society’ that may shed light on the concept of national security. It determines that public security as a ground for derogating from fundamental freedoms

---


\(^{537}\) Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, CJEU, 6 October 2020, paras. 135-136; Judgment in *Case C-623/17, Privacy International, CJEU, 6 October 2020*, paras. 74-75; In other words, see Judgment in *Case C-817/19, Ligue des droits humains, CJEU, 21 June 2022*, para. 170.

\(^{538}\) Strictly speaking, this interpretation concerns Article 15(1) ePD, read in the ligh of Article 4(2) TEU; For more details, see Judgment in *Case C-140/20, Commissioner of An Garda Síochána, CJEU, 5 April 2022*, para. 62.

\(^{539}\) Judgment in *Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020*, para. 99; Similarly, Judgment in *Case C-300/11, ZZ, CJEU, 4 June 2013*, paras. 35-38; Judgment in *Joined Cases C-715/17, C-718/17 and C-719/17, Commission v Poland (Temporary mechanism (...)), CJEU, 2 April 2020*, paras. 143, 146, and 170; On conceivable interpretations, see Brewczyńska M., ‘A critical reflection on the material scope of the application of the LED and its boundaries with the GDPR’, in Kosta E. et al., *Research Handbook on EU Data Protection Law*, Elgar, 2022, pp. 101-103.
and rights of third country nationals must be interpreted strictly and that Member States cannot unilaterally determine its scope without any control by the institutions.\(^{540}\) With varying degrees of emphasis, the Court clarifies that EU law does not impose a ‘uniform scale of values’ and that ‘Member States remain free to determine, in accordance with their national needs, which can vary from one Member State to another and from one time to another, the requirements of public policy and public security’.\(^{541}\) Nevertheless, the CJEU determined that measures in the name of ‘(qualified) public security’ remain subject to EU control and must be based exclusively on the personal conduct of the individual concerned and that that conduct must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.\(^{542}\) The Court specified that public security covers both internal and external security.\(^{543}\) Consequently, ‘a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security’. Additionally, the fight against crime in connection with drug trafficking as part of an organised group or against terrorism may be included within the concept of public security.\(^{544}\) The CJEU also referred to the definition of public security when reviewing ‘national security and public order’ as grounds for the detention of an applicant for international protection (Article 8(3)(e) of the Directive 2013/33).

The Court further develops its notion of threats affecting fundamental interests of society in connection with measures taken in the name of ‘public order’, ‘public policy’ and ‘(imperative grounds of) public security’. It clarifies that the persistent hostility to the fundamental values enshrined in Articles 2 and 3 TEU after committing war crimes over 10 years prior, is capable of constituting a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.\(^{545}\) Conversely, the Court ruled that that a traffic offence, punishable by mere administrative fines, does not present a sufficiently serious threat affecting one of the fundamental interests of society or a threat to public security.\(^{546}\) In the context of ‘public policy’-grounds, the Court develops that conduct may not be considered as being of a sufficiently serious nature to justify restrictions concerning intra-EU mobility, where the host Member State does not adopt, with respect to the same conduct on the part of its own nationals genuine and effective measures


\(^{541}\) Judgment in Case C-33/07, Lipa, CJEU, 10 July 2008, para. 23; Judgment in Case C-54/99, Église de scientologie, CJEU, 14 March 2000, para. 17; Judgment in Case C-348/09, I, CJEU, 22 May 2012, paras. 21-23 and para. 29; Judgment in Case C-137/17, Van Gennip and Others, CJEU, 26 September 2018, paras. 56-57; Judgment in Case C-18/19, Stadt Frankfurt am Main, CJEU, 2 July 2020, para. 42.

\(^{542}\) Judgment in Case C-54/99, Église de scientologie, CJEU, 14 March 2000, para. 17; Judgment in Case C-339/19, Romenergo and Aris Capital, CJEU 16 September 2020, para. 40; Judgment in Case C-39/11, VBV - Vorsorgekasse, CJEU, 7 June 2012, para. 29; Judgment in Case C-78/18, Commission v Hungary (Transparency of associations), CJEU, 18 June 2020, paras. 91-95; Judgment in Case C-371/08, Ziebell, CJEU, 8 December 2011, para. 82.

\(^{543}\) Judgment in Case C-145/09, Tsakouridis, CJEU, 23 November 2010, para. 44.

\(^{544}\) Judgment in Case C-601/15 PPU, N, CJEU, 15 February 2016, paras. 64-67; See also Judgment in Case C-373/13, T, CJEU, 24 June 2015, paras. 78-80.

\(^{545}\) Judgment in Joined Cases C-331/16 and C-366/16, K. (Right of residence and alleged war crimes), CJEU, 2 May 2018, p. 66.

\(^{546}\) Judgment in Case C-118/20, Wiener Landesregierung (Révocation d’une assurance de naturalisation), CJEU, 18 January 2022, para. 68-71.
intended to combat such conduct. In the context of assessing an expulsion decision restricting an EU national’s freedom of movement based on ‘imperative grounds of public security’, the Court considers that it is open to the Member States to regard criminal offences such as those referred to in the second subparagraph of Article 83(1) TFEU as constituting a particularly serious threat to one of the fundamental interests of society, [...] as long as the manner in which such offences were committed discloses particularly serious characteristics (italics added for emphasis). In the various contexts, the Court refrains from giving a generic definition of fundamental interests of society and indicates discretion of Member States, but consistently reviews the threat level.

It follows from CJEU case law that Member States retain substantial power of definition or margin of appreciation in determining security notions, but that the EU may (at least) control the prevalence and seriousness of a threat where Member States intend to derogate from EU fundamental freedoms and rights. It appears that the CJEU’s control inter alia builds on (in)consistencies in Member States’ security measures, the (lack of) case-specific threat assessments, the (un)reasonableness of Member States’ argumentation in light of known facts (e.g. market conditions), the disqualification of measures designed predominantly to attain economic objectives, and the degree of substantiation by Member States. While the case law on public security measures reveals the possible extent and methods of EU control, the CJEU held that national security threats exceed general serious public security threats. Specifically, it clarified that a national security threat, by its nature, its seriousness, and prevalence, is able to justify particularly intrusive measures; closed to other justifications such as combating general threats of public security disturbances and serious crime.

**Essential security interests**

Besides the public security derogations in Articles 36, 45(3), 51(1), 62, and 65(1)(b) TFEU, the TFEU also contains a essential security interests derogation, which prima facie provides Member States with a wide margin of appreciation. Article 346(1)(a) TFEU expressly stipulates that Member States can refuse to disclose information ‘which it considers contrary to the essential interests of its security’. Article 346(1)(b) TFEU enables any Member State to take measures derogating from EU law that it ‘considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms’. Despite language indicating ‘self-judgment’ or a wide margin of appreciation (‘as considers necessary’), both the Commission and the Court have demonstrated willingness to review essential security interests within the meaning of Article 346 of the TFEU. The Court considers that it is for the Member States to define their essential security interests.

---


548 Judgment in Case C-348/09, I., CJEU, 22 May 2012, paras. 28 and 33; As stated in para. 20, ‘The concept of ‘imperative grounds of public security’ presupposes not only the existence of a threat to public security, but also that such a threat is of a particularly high degree of seriousness, as is reflected by the use of the words ‘imperative grounds’.


550 Nevertheless, even measures with economic advantages, may be necessary for national security reasons.

551 Judgment in Case C-140/20, Commissioner of An Garda Síochána, CJEU, 5 April 2022, para. 62: ‘[...] a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a [...] particularly intrusive measures.

552 Judgment in Case C-140/20, Commissioner of An Garda Síochána, CJEU, 5 April 2022, para. 57 and 62.

interests within the meaning of Article 346 of the TFEU, but interprets the derogation strictly. It also allocated the burden of proof with the Member States by stating, for instance, that ‘a Member State which wishes to avail itself of those derogations must establish that the protection of such interests could not have been attained within a competitive tendering procedure as provided for by Directives’.554

After reviewing relevant case law, one academic concludes: ‘An attempt to describe the appropriate standard of review could [...] be made, being that scrutiny of security exceptions goes beyond mere control of outright abuses. However, this does not amount to a full scale proportionality review regarding the soft elements of the exception, i.e., the essential security interests and necessity. The case law indicates that in obvious cases in which security is not at stake (but, for example, economic interests), or in which a measure is clearly not suited to reach the acclaimed goal, or in which the harm caused by the measure is excessively greater in relation to the intended security aim, can the Court declare a measure to be in violation of the ‘as considers necessary’-exceptions. It can thus assess the reasonableness of the Member States arguments with regard to its security concerns. Under no circumstances can it impose its own assessment of a situation and the adequate reaction to a security over the diverging but reasonable assessment of the relevant Member State.’555 Other scholars have argued in favour of limiting the standard of review to an abuse control.556 Measures relying on ‘essential security interests’ within the meaning of Article 346 TFEU may become subject to an abuse control pursuant Article 348(2) TFEU. One expert argues that a Member State evidently exceeds its margin of appreciation and thus acts abusive, where (i) it pursues purely economic or protectionist motives, (ii) the measures evidently do not serve national security purposes (and e.g. instead fuel conflicts), (iii) measures exceed what is necessary for security interests, or (iv) measures derogate from fundamental EU values (see Article 2 TEU in conjunction with Article 7 of the TEU).557 Ultimately, there is no agreement on the precise standard of review. To the very least, the Court can perform an abuse control, but, in view of case law, it likely exercises a more wide-ranging control.558 Consequently, even the essential security interests derogations relating to core military and intelligence concerns and prima facie providing Member States with a wide margin of appreciation, remain subject to firm EU control.

Threats to fundamental structures and direct threats

While CJEU case law on security measures reveals the possible scope of EU control, the CJEU held that national security threats exceed general serious public security threats. In the second half of the
national security definition, the CJEU gives an indication for the nature and severity of national security threats. The Court specifies that Member States’ responsibility for national security encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. The former element closely resembles one of the aims qualifying certain serious crimes as terrorist offences within the meaning of EU law (and national transposition acts). Lawyers, judges and prosecutors across six Member States expressed concern at the breadth and lack of legal certainty in national definitions of the offence of terrorism; even where transposition acts more narrowly defined terrorist offences. Some academics criticised that this phrase (prima facie) resembles a political rather than a legal provision. Depending on legal order, fundamental constitutional and political structures may comprise key features of democracy and rule of law principles, for instance the right to vote freely, the independence of the judiciary, and the exclusion of all forms of tyranny and arbitrary rule. Fundamental economic and social structures may comprise the principle of a (social) market economy and the welfare state principle. Activities that threaten to completely or very substantially impair their functioning are likely capable of seriously destabilising these structures. The latter element of the national security definition (directly threatening society, the population or the State itself), reminds of the alternative aims qualifying serious crime as a terrorist offence and may therefore comprise activities directly threatening to intimidate a population or unduly compelling a government to perform or abstain from performing an act. Even if this is not the case, one may derive from threat scenarios affecting society, the population, or the state that a large-scale impact is required. Requiring a high degree of severity is also consistent with the ‘primary interest in protecting the essential functions of the State’, as this presupposes that only absolutely necessary or extremely important functions such as preserving the territorial integrity of the state are covered (Article 4(2) TEU).

Standard of review in national security cases

Assessing the transplantability of review standards on a case-by-case basis goes beyond the scope of these preliminary remarks. Nevertheless, the CJEU demonstrated in data retention cases that it

---

559 Article 3(2)(c) Directive (EU) 2017/541; See also Article 1(2), third indent, of the Council Framework Decision of 13 June 2002 on combating terrorism.
562 Section 92(2) of the German Criminal Code and Section 120(2)(3b) German Courts Constitution Act.
564 Article 3(2)(a) and (b) of Directive (EU) 2017/541
565 Despite their distinct enumeration in Article 4(2), second sentence, of the TEU, the concepts of ‘maintaining law and order’ and ‘national security’ may overlap. One may argue that the Member States’ responsibility for national security ‘corresponds to the primary interest’ of maintaining law and order where threats to law and order affect a ‘fundamental interests of society’. Further limitations may apply: For more information, see Blanke H.-J., ‘Article 4’, in Blanke H.-J., The Treaty on European Union (TEU): A Commentary, Springer, 2013, para. 72-80.
does not systematically refrain from reviewing national security measures, which restrict fundamental rights to privacy, data protection, and freedom of expression. In its statements on national security, the Court clearly alluded to essential and public security derogations. By way of reference, it draws on the rationale developed in the context of essential and public security to establish the justiciability of certain measures taken for the purpose of protecting national security. While national security may be considered the most fundamental prerogative of a state, comprehensively exempting any measures subjectively taken on behalf of national security from EU law ‘might impair the binding nature of Union law and its uniform application’. Leaving aside theories on the legal nature of the national security derogation, one could argue that this rationale applies even more, where a derogation would comprehensively exempt the subject matter from EU law as a whole. Additionally, it appears doubtful whether it was the intention of the Intergovernmental Conference to systematically provide Member States departing from EU law in the name of national security, including in situations of flagrant abuse, with impunity. Some scholars derive from security case law that ‘scrutiny [of certain national security measures] by the ECJ shall […] be expected’. Besides this, experts have argued for a substantial approach to national security and some explicitly in favour of firm judicial reviewability. Other researchers argue that the applicability of EU law should depend on the subject matter of a measure, rather than on its effect, but (drawing on the rationale of Article 348 (2) TFEU) concede that purely economic scenarios should remain within the purview of EU law.

Against this backdrop, it is not inconceivable that the CJEU maintains a certain control over which threats qualify as matters of national security and that it would at least review cases of flagrant abuse. Even if Member States’ intelligence agencies benefitted from an extended margin of appreciation or a legal presumption that they act in the interest of national security, it appears questionable whether this should cover, for instance, evident and repeated interference with

---


567 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 99 and Judgment in Case C-623/17, Privacy International, CJEU, 6 October 2020, para. 44 with reference to: Judgment in Case C-300/11, ZZ, CJEU, 4 June 2013, para. 38; Judgment in Case C-187/16, Commission v Austria (State printing office), CJEU, 20 March 2018, paras. 75 and 76; Judgment in Joined Cases C-715/17, C-718/17 and C-719/17, Commission v Poland (Temporary mechanism [...]), CJEU, 2 April 2020, paras. 143 and 170.

568 Similarly, Judgment in Joined Cases C-715/17, C-718/17 and C-719/17, Commission v Poland (Temporary mechanism [...]), CJEU, 2 April 2020, para. 143 (referenced in La Quadrature du Net and Privacy International rulings) and Judgment in Case C-273/97, Sirdar, CJEU, 26 October 1999, para. 16.

569 Note the wording of the declaration of the Intergovernmental Conference’s on Article 16 of the TFEU annexed to the Treaty of Lisbon: ‘The Conference declares that, whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter’ (italics added for emphasis).


574 Pursuant the non-binding Recital 14 of the Law Enforcement Directive 2016/680, ‘activities of agencies or units dealing with national security issues’ fall outside the scope of EU law. The term ‘dealing’ is ambiguous, but the recital may determine that it must be presumed that activities of ‘agencies or units responsible for national security’ were taken validly in the interest of national security. Some argue that such activities are systematically exempt from the scope of EU law.
fundamental EU values under the pretext of national security. Practically, this would transform the question of EU law applicability into a question of distribution of competences among national authorities. The following circumstances could possibly indicate intelligence operations performed under false (national security) pretences: ● an evidently and drastically exaggerated or even spurious threat assessment; ● the threat is not even remotely capable of seriously destabilising fundamental structures of a country and of directly threatening society, the population, or the state itself; ● the selective reliance on an exceptionally broad notion of national security, for instance, engulfing typical law enforcement activities or presenting an incoherent application of the national legal order; ● atypically and drastically disproportionate security measures, possibly even adversely affecting the security situation; ● the operation strategically integrates with other attacks on democracy, the rule of law, or other EU fundamental values; ● intelligence agencies and their oversight bodies have been purged; ● operations rely on extraordinary powers and lack oversight based on a state of emergency that was declared without any sign of emergency; and ● intelligence operations are clearly linked to dominant ulterior goals of their initiator, for instance, personal gains. The cumulative and repeated manifestation of such indicators could potentially count towards evident abuse. Where Member States repeatedly and evidently invoke ‘national security’ as a pretext for economically, or even politically, motivated spying, the national security derogation may not apply. Based on the rationale of Article 348(2) TFEU, the Commission may attempt to initiate an in camera abuse control. In view of extensive legal uncertainties, further research on the standard of review is necessary.

EU applicability arising from the involvement of qualified actors

Besides threats of a certain nature, the involvement of certain actors may systematically render EU law applicable. Such cases would remain subject to EU law, even if they passed an abuse control. According to CJEU case law, legislative measures requiring providers of electronic communications services to retain and share traffic and location data for the purposes of protecting national security are subject to EU law (‘to the extent that they regulate the activities of those actors’). It is not yet settled, whether public-private spyware operations for the purpose of protecting national security and their corresponding legal basis would systematically be subject to EU law. A strict interpretation, may argue that the involvement of private entities ‘dictates inclusion within an area (namely the protection of privacy required of those private operators) governed by EU law’. In contrast, Member States could argue that in such cases the state dimension outweighs the private dimension. Unlike electronic communications providers, spyware providers rely on state instructions to provide their services lawfully. Additionally, public-private spyware operations do

---

575 Dittert D. in para. 27 specifically mentions that Articles 346 and 347 TFEU may not be used to derogate from fundamental EU values as stipulated in Article 2 TEU in conjunction with Article 7 of the TEU; Judgment in Joined Cases C-402/05 P and C-415/05 P, CJEU, Kadi and Al Barakaat International Foundation v Council and Commission, 3 September 2008, para. 303.

576 For more information on the Article 348 procedure, see Dittert D., ‘Artikel 348 AEUV’, in von der Groeben H. et al., Europäisches Unionsrecht, Nomos, 2015, paras. 27.

577 EU law is applicable to the extent that these extors are concerned.


not rest on prior/upstream commercial data processing and largely resemble state activities that intelligence agencies would otherwise perform in-house. Spyware providers appear to be ‘directly and specifically involved in the exercise of official authority’.581 Lastly, it may well lie within the scope of ‘safeguarding national security’ to take unfettered advantage582 of intelligence outsourcing and Member States have been reluctant to confer on the EU competence for (sensitive) security policies. In the spirit of compromise, one might argue that only where the government apparatus closely controls activities of contractors, the state dimension takes precedent over the commercial or private dimension. Nevertheless, absent settled case law, the outcome is uncertain and further research appears necessary. Undoubtedly, Member States would also raise concerns over EU competence creep. For more information, see Annex II.583

583 Certain arguments made in Annex II regarding the e-Privacy Directive may apply mutatis mutandis in the primary law context. It should be noted that the CJEU frequently avoids developing the notion of national security under Article 4(2) TEU and concentrates on determining the applicability of secondary law, read in light of Article 4(2) TEU. Through this approach, the CJEU avoids discussing notions that are not decisive for the case as well as prematurely defining the division of competences at a primary law level. It is not always easy to discern whether notions of primary or secondary law drive the interpretation and to what extent inferences may be drawn for primary law. Cameron I., ‘Metadata retention and national security: Privacy International and La Quadrature du Net’, Common Market Law Review, Vol. 58(5), 2021, pp. 1457-1458: ‘The referring courts take a constitutional (hierarchy of norms) approach: the adoption of secondary EU law should not be used to expand the scope of EU competences under the Treaties, in the face of an express exclusion clause written into primary EU law. The Court seems to proceed from another, and opposite, constitutional logic: that in the case of framework Treaties, as the TEU and TFEU undoubtedly are, a decision by the Member States to adopt secondary legislation in fact shows their intentions as to what does, and what does not, fall within the scope of an exclusion clause.’; Ibid., 1462: ‘This, then, is what the Court offers the security and intelligence agencies to sweeten the bitter jurisdictional pill it wants them to swallow as regards Article 4(2) TEU. In doing so, it follows a familiar pattern. The Court establishes a controversial principle, but at the same time, States are assured that, in this particular case, their actions are (or relatively simply can be made) compatible with EU law.’
10. Annex II: Preliminary remarks on the applicability of EU data and privacy protection

Member States may advocate an interpretation of secondary data protection and privacy laws that excludes Pegasus cases from their application. Conversely, aggrieved parties may argue firmly in favour of its applicability, notably where Member States invoke national security and law enforcement purposes as a pretext for politically motivated spying. Some notions may even serve to interpret Article 4(2) TEU and to determine the division of responsibilities between Member States and the EU.584

**Intelligence and security authorities** could argue that their activities escape the purview of both the ePrivacy Directive (ePD) and the Law Enforcement Directive (LED). Notably, intelligence agencies may claim that they do not qualify as 'competent authorities' within the meaning of the LED (see Recital 14 LED),585 but that their operations qualify as 'activities of the state'586 concerning public security, defence, State security or 'activities of the state in the area of criminal law' exempting them from the ePD (Article 1(3) ePD). The legacy wording of Article 1(3) ePD relating to the pillar system before the Treaty of Lisbon587 appears to exempt clearly from the ePD (direct) government hacking for law enforcement purposes and intelligence operations involving largely deterministic spyware that does not require for its proper functioning services or other contributions from private entities.

Member States may argue that it also exempts privatised surveillance activities on behalf of public security agencies and other qualified involvement of private entities in surveillance operations. They could insist that the ePD, if at all, only applies to private intermediaries who generally process data on their own account for commercial purposes, rather than to private intermediaries who primarily act on behalf of public authorities and whose business model consists of carrying out intelligence operations or qualified parts thereof according to instructions from security authorities. Unlike electronic communications service providers, spyware providers do not usually retain or share commercially transmitted data, but instead perform targeted interventions as part of dedicated

---

584 Cameron I., ‘Metadata retention and national security: Privacy International and La Quadrature du Net’, Common Market Law Review, Vol. 58(5), 2021, pp. 1457-1458: ‘The referring courts take a constitutional (hierarchy of norms) approach: the adoption of secondary EU law should not be used to expand the scope of EU competences under the Treaties, in the face of an express exclusion clause written into primary EU law. The Court seems to proceed from another, and opposite, constitutional logic: that in the case of framework Treaties, as the TEU and TFEU undoubtedly are, a decision by the Member States to adopt secondary legislation in fact shows their intentions as to what does, and what does not, fall within the scope of an exclusion clause.’


586 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 92.

intelligence operations. Consequently, their surveillance services may be perceived as dissociated from commercial or private data processing. On the contrary, spyware providers, in principle, cannot process data lawfully unless commissioned/instructed by the State and their activities largely resemble State activities that intelligence agencies would otherwise perform in-house. Essentially, their activities may be perceived as a continuum of State activities, which results in the State dimension taking precedence over the commercial or private dimension.\(^{588}\) It would also appear logical that the private agent shares the fate, i.e. being exempt from the ePD, of its dominant State principal. By extension,\(^{589}\) legislation enabling such public-private cooperation would fall outside the scope of the ePD.

It may also be argued that the CJEU explicitly provided for the possibility that private activities satisfy the exemption criteria under Article 1(3), since it explicitly characterises the exempt policy areas as activities ‘of State authorities’ or ‘of the [wider] State’, possibly including private activities.\(^{590}\) Additionally, CJEU case law explicitly states that the direct implementation of (legislative) measures derogating from the confidentiality of communications, without imposing processing obligations on electronic communications service providers, is not subject to the ePD.\(^{591}\) Furthermore, intelligence agencies might argue in favour of an exemption that neither private intermediaries nor they themselves process personal data in connection with the provision of publicly available electronic communications services in public communications networks (Articles 3 and 2(1) as well as Recital 25 ePD, in conjunction with Articles 2(4) and 125 EECC).\(^{592}\) Finally, the coherence of subjecting (non-abusive) intelligence operations involving private parties other than providers of electronic communications services, as well as corresponding legal bases to the ePD or the GDPR, as opposed to the LED or other dedicated laws, would need to be assessed critically.

Conversely, aggrieved parties and applicants could argue that politically motivated surveillance falls under the purview of the ePD. Such activities do not satisfy the exemption criteria under Article 1(3) ePD, since politically motivated surveillance does not qualify as an activity ‘concerning public security’ or ‘in the area of criminal law’. In line with considerations on the national security test, it may not suffice that authorities merely subjectively take or declare measures as ‘concerning’ law enforcement or public security, while this does not correspond with the objective quality required by law. Furthermore, the broad scope of Article 5(3) ePD and the need to preserve the practical effect of Article 15(1) in conjunction with Article 5(3) ePD (‘the legislature does not legislate in vain’), restrict the Article 1(3) exemption and ultimately subject legislation enabling public-private spyware operations and activities of commercial spyware providers to the ePD.

**Article 5(3) ePD** protects information stored on terminal equipment not only against the unjustified processing by electronic communication services providers, but also against spyware, as explicitly

---

588 Opinion in Joined Cases C-511/18 and C-512/18, La Quadrature du Net, AG Campos Sánchez-Bordona, 15 January 2020, paras. 69 and 79.

589 Interplay of Articles 1(3), 15(1) and 5(3) ePD. For additional arguments, see Opinion in Joined Cases C-511/18 and C-512/18, La Quadrature du Net, AG Campos Sánchez-Bordona, 15 January 2020, para. 73.

590 Judgment in Case C-623/17, Privacy International, CJEU, 6 October 2020, para. 35; Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para 92; See, by way of analogy, Judgment in Case C-25/17, Jehovan tīvintītājai, CJEU, 10 July 2018,para. 38; Judgment in Case C-101/01, Lindqvist, CJEU, 6 November 2003, paras. 43 and 44.

591 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 103.

592 For more information on this wording, see ePrivacy Directive: assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, SMART 2013/0071, European Commission, 2015, pp. 8-9 and p. 35; Concerning the German transposition, see Data Protection Conference (DSK), Orientierungshilfe der Aufsichtsbehörden für AnbieterInnen von Telemedien, 20 December 2021, p. 4.
stated in Recital 24. The reformulation of Article 5(3) in 2009 and the underlying rationale indicate that the Article means to protect information stored on terminal equipment against any type of ‘third-party’ spyware irrespective of how the spyware was disseminated (Recitals 65 and 66 Citizen’s Rights Directive 2009/136/EC). Like Article 5(1) ePD, Article 5(3) ePD may a fortiori apply to the measures taken by all persons other than users, whether private persons or bodies or State bodies. Consequently, transposition acts should be interpreted to regulate any third party threat actors, within the territorial scope of the Directive, if not beyond (gold-plating).

**Article 15(1) in conjunction with 5(3) ePD** presupposes that Member States may need to restrict the protective effect of Article 5(3) to safeguard general public interests, not least in spyware scenarios (Recital 24 ePD). In other words, Article 15(1) presupposes scenarios where gaining access to information stored in terminal equipment through spyware is prohibited under Article 5(3) ePD, but may be necessary to ‘safeguard national security’ or ‘prevent [...] criminal offences’. While threat actors violate Article 5(3) ePD when they deploy spyware, they collect information on their own account for private, likely illicit, interests. The collected information would hardly help safeguard national security or prevent criminal offences, and threat actors usually aim to avoid notice by and cooperation with public authorities. If Article 15(1) ePD only empowered Member States to legitimise cooperation with such threat actors, its practical effect would (arguably) be unduly restricted to improbable and ineffective cooperation.

To maintain sufficient practical effect of Article 15(1) ePD in spyware scenarios and prevent the legislature largely having legislated in vain, it would be conducive if Article 15(1) ePD covered realistic scenarios such as public-private spyware cooperation for targeted surveillance. This

---

593 ePrivacy Directive: assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, SMART 2013/0071, European Commission, 2015, pp. 8-9 and Article 29 WP, Opinion 2/2010 on online behavioural advertising, WP 171, 22 June 2010, p. 9: ‘The Working Party has already pointed out in WP 29 Opinion 1/200821 that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used’.

594 EDPS, Second opinion on ePrivacy, OJ C 128, 6 June 2009, p. 31: ‘Article 5(3) of the ePrivacy Directive, [...] is binding not only upon PPECS, but also upon anyone who attempts to store information or gain access to information stored in the terminal equipment of individuals. Moreover, in the current legislative process, the Commission has even proposed a variation of the extension of Article 5(3) when similar technologies (cookies/spyware) are not only delivered through electronic communication systems but through any other possible method (distribution through downloads from the Internet or via external data storage media...); Similarly, Article 29 WP, Opinion 1/2009 on the proposals amending the ePrivacy Directive, WP 159, 10 February 2009, p. 5, fn. 7: gPrivacy Directive: assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, SMART 2013/0071, European Commission, 2015, pp. 51-53; van Hoboken J. and Zuiderveen Borgesius F., Scoping Electronic Communication Privacy Rules, Journal of Intellectual Property, IT and E-Commerce Law, Vol. 6(3), 2015, p. 202; Note also the extended scope in Article 2(1) e-privacy regulation, as opposed to Article 3 ePrivacy Directive.

595 It is commonly recognised that Article 5(3) ePD incorporates an ‘extended material scope’.

596 Judgment in Joined Cases C-203/15 and C-698/15, Tele2 Sverige, CJEU, 21 December 2016, para. 77; Judgment in Case C-207/16, Ministerio Fiscal, CJEU, 2 October 2018, para. 36.

597 EDPS, Internal Document 04/2021 on criteria of territorial competence of supervisory authorities to enforce Article 5(3) of the ePrivacy Directive, 18 June 2021, p. 3: ‘If the data controller/service provider has no establishment in a Member State, the national law of this Member State may provide other criteria than establishment to enforce its national law in respect of this controller/service provider.’; Similarly, EDPS, Internal Document 04/2021 on criteria of territorial competence of supervisory authorities to enforce Article 5(3) of the ePrivacy Directive, 18 June 2021, p. 3: ‘If the data controller/service provider has no establishment in a Member State, the national law of this Member State may provide other criteria than establishment to enforce its national law in respect of this controller/service provider.’; Similarly, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, SMART 2013/0071, European Commission, 2015, pp. 29-30, pp. 32-33, and p. 69.

598 Recital 24 ePD and Recital 65 and 66 Rights Directive 2009/136/EC.

599 Even if Article 15(1) ePD only empowered Member States to legitimise such unlikely cooperation, Article 15(1) in conjunction with Article 5(3) ePD would not be fully deprived of any practical effect. The provision may also cover legislation empowering law enforcement authorities to order providers of services installed on the terminal device, such as operating systems, to extract or grant access to user data for purposes in the general public interest.
interpretation would also ensure consistent application of the ePD, as individuals take up encrypted communication channels and public authorities shift from obliging private entities to perform targeted interceptions, to cooperating with spyware providers in order to extract similar, sometimes identical, data at the source (terminal equipment). Consequently, legislation empowering agencies to use commercial spyware, whose functioning rests on qualified involvement of private entities, would be subject to the ePD.\textsuperscript{601}

In line with this interpretation, it may be argued that the CJEU case law excluding from the ePD derogations, which do not impose processing obligations on \textit{electronic communications service providers}, does not apply in this context.\textsuperscript{602} This outcome is also in line with a warranted strict interpretation of the exemption.\textsuperscript{603} Even if the ePD only covered accessing of information by private agents and not by the state principal, applicants could argue that this outcome simply the consequence of involving private actors.\textsuperscript{604} From a holistic perspective, it may be argued that, despite being integrated in intelligence operations, spyware providers’ services are principally transactional and therefore constitute private processing subject to the EU data acquis. A UN working group and researchers terms spyware providers as ‘cyber mercenaries’—signifying a lack of national allegiance, a disregard for national security, and a principal interest in remuneration.\textsuperscript{605} Paradigmatically, NSO is suspected of hacking high-ranking government officials of customer governments (Spain) on behalf of other customers. Additionally, NSO is suspected of hacking the phones of members of a legal team challenging the Group in court as well as Amnesty International staff. These examples signify unscrupulous pursuit of commercial interests.

\footnotetext[0]{601}{The CJEU clarifies that ‘Such measures, to the extent that they regulate the activities of such providers, cannot be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58’, see Judgment in \textit{Case C-207/16, Ministerio Fiscal, CJEU}, 2 October 2018, para. 37 and Judgment in \textit{Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU}, 6 October 2020, para. 96. It should be noted that this conclusion turns on the fact that private entities fall within the territorial scope of the ePD transposition acts, that Article 5(3) ePD also protects against activities from \textit{private entities that are not electronic communications services}, and that private entities make \textit{qualified} (see footnote above) contributions to intelligence operations. Notwithstanding, where Member States repeatedly and evidently invoke law enforcement and public security purposes as a \textit{pretext} for politically motivated spying, it would be difficult to refute the applicability of the ePD.}

\footnotetext[0]{602}{By way of analogy, see Judgment in \textit{Case C-73/16, Puškár, CJEU}, 27 September 2017, para. 38. In its case law, the CJEU juxtaposes ‘\textit{felds in which individuals are active}’ (e.g. door-to-door preaching/charitable activities) with policy areas mentioned in Article 1(3), arguably indicating that states predominantly perform(ed) the activities under Article 1(3) self-reliantly, see Judgment in \textit{Case C-623/17, Privacy International, CJEU}, 6 October 2020, para. 35; Judgment in \textit{Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU}, 6 October 2020, para 92; See, by way of analogy, Judgment in \textit{Case C-25/17, Jehovan todisajat, CJEU}, 10 July 2018, para. 38; Judgment in \textit{Case C-101/01, Lindqvist, CJEU}, 6 November 2003, paras. 43 and 44.}

\footnotetext[0]{603}{Where the principal is subject to the LED or GDPR and the private entity acts as a processor, it could be argued that ePD rules particularise and complement the provisions applicable to private processors. For more information, see the last paragraph of Annex I.}

Applicability of ePD to 'direct' law enforcement activities:
An Austrian preliminary reference lodged on 6 September 2021 even assumes that Article 15(1) (possibly read in combination with Article 5) of the ePD is applicable to national rules that allow 'security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation'. Law enforcement authorities attempted to access information stored on the applicant's terminal equipment and the referring court appears to assume that the ePD is applicable. Such a conclusion may rest on a modern interpretation of the legacy wording in Article 1(3) ePD, and/or on an extensive interpretation of Articles 5(3) and 15(1) ePD. However, even if Article 1(3) ePD were interpreted progressively and aligned with Article 2(2)(d) GDPR, law enforcement activities by 'competent authorities' would be explicitly exempt from the ePD's scope. Nevertheless, such a contestable interpretation would limit the exemption's breadth and arguably keep intelligence authorities' activities within the material scope of the ePD. Instead, applicants may argue that the broad scope of Article 5(3) ePD and the need to preserve practical effect of Article 15(1) in conjunction with Article 5(3) ePD (the legislature does not legislate in vain), restrict the Article 1(3) scope exemption and ultimately subject such direct law enforcement data processing to the ePD. However, even if Article 15(1) did not cover legislation empowering law enforcement authorities' access to information stored on the terminal equipment, the provision would maintain practical effect and the provision would not be in vain. It could be argued that Article 15(1) merely covers legislative measures empowering law enforcement authorities to cooperate with spyware providers or to impose obligations on private entities (such as operating system providers) to extract or share data from terminal equipment. An extensive interpretation would appear to break with the CJEU's traditional approach.

Additionally, aggrieved parties may argue that, besides the ePD, the LED and/or the GDPR apply to public-private surveillance cooperation. Within the scope of EU law, it is likely that at least one of the two data protection instruments will apply due to their corollary scope (Article 2(2)(d) GDPR and Article 1(1) LED). Aggrieved parties could argue that not only law enforcement agencies, but also intelligence agencies or dedicated departments thereof, which perform law enforcement-related intelligence activities, qualify as 'competent authorities' and are subject to the LED.

---

606 Summary of the request for a preliminary ruling, Case C-548/21, Landesverwaltungsgericht Tirol, 6 September 2021.
607 Mutatis mutandis, Judgment in Case C-817/19, CJEU, 21 June 2022, paras. 66-67.
608 In the course of the data protection and privacy reform, the Commission aimed to modernise the scope of the e-privacy rules (Article 2(2)(d) e-privacy regulation) to match the wording of the GDPR as a corollary to the LED (Article 2(2)(d) GDPR and Article 1(1) LED, see Latvijas Republikas Saeima, para. 69). Unlike the GDPR and the LED, the co-legislators have not yet adopted the e-privacy regulation and so the text remains unchanged. Considering that the Article 1(3) exemption was consistent with that of the Data Protection Directive (Article 3(2), first indent) and its recast was set to mirror that of the GDPR, a GDPR-consistent interpretation of the legacy wording in Article 1(3) ePD may be considered. In its ruling La Quadrature du Net, para. 102, the CJEU remarks on (case-specific) consistency in interpretation between the ePD and the GDPR, but points out the distinct wording ('competent authorities'). It is questionable whether the CJEU would fully align its interpretation of Article 1(3) ePD with that of Article 2(2)(d) GDPR in light of the legislators' disagreement over the e-privacy regulation's scope.
609 Depending on the interpretation of 'competent authorities'.
610 Concerning Article 15(1) ePD in conjunction with Article 5(1) ePD, Gilid E. et al., Data Retention and the Future of Large-Scale Surveillance, Queen Mary Law Research Paper No. 372/2021, 29 November 2021, pp. 6-7.
611 See, notably, Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 103: 'By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, [...] with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR.'
613 Sajfert J. and Quintel T., ‘Data Protection Directive EU 2016/680 for Police and Criminal Justice Authorities’, 1 December 2017, p. 4: 'When national intelligence agencies process data for the purposes of the Directive, they should be viewed as competent authorities under Article 2(1) instead of not being covered by EU law.'
Where **spyware providers** act on behalf of the competent authorities within the scope of the LED, they qualify as **processors**\(^{614}\) under the LED (see Articles 4(8) and 22 and Recital 11, sixth sentence, LED).\(^{615}\) The application of the GDPR remains unaffected for processing of personal data outside the scope of the LED. Conversely, where spyware providers exercise decision-making power over key elements of the processing, they would qualify as **controllers** under the GDPR or the LED.\(^{616}\) Where private entities qualify as GDPR controllers despite cooperating with LED controllers such as law enforcement agencies, legal complexities of mixed LED-GDPR controllership arise. Since it is unlikely that Member States would deputise\(^{617}\) spyware providers, they would fail to qualify as 'competent authorities’ and, by extension, as ‘controllers’ under the LED (Articles 3(8), 3(7)(b) and 26, and Recital 11, second sentence, LED). Consequently, a situation of mixed LED-GDPR controllership can arise. In an expert group meeting, the ‘Commission suggested that national law could lay down the rules on [mixed LED-GDPR] joint controllership and responsibility for the personal data in ... [shared] databases, as well as the rules on the point of contact for data subjects’.\(^{618}\)

Researchers argue that the respective acts may apply selectively to the parties and processing operations.\(^{619}\) An additional layer of complexity is added where GDPR provisions are particularised by the ePD.\(^{620}\) However, the NSO Group likely acted as a (possibly illegitimate) **processor**.\(^{621}\)

Especially where neither the LED nor the ePD apply – **prima facie**, paradoxically, in the context of intelligence operations – the GDPR's applicability must be considered.\(^{622}\) Like under Article 15(1)

---


\(^{620}\) EDPB, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR*, 12 March 2019, pp. 13: ‘To the extent that the information stored in the end-user device constitutes personal data, article 3(5) of the ePrivacy Directive shall take precedence over article 6 of the GDPR with regards to the activity of storing or gaining access to this information. [...] Subsequent processing of personal data [...] must also have a legal basis under article 6 of the GDPR in order to be lawful.’

\(^{621}\) Moini B., *Beschwerde gegen den Einsatz der Pegasus-Software durch das Bundeskriminalamt*, Society for Civil Rights, 22 September 2021, pp. 8-9. However, in the context of discussing the outsourcing of inherently governmental functions on p. 6, the Society for Civil Rights assumes that the NSO Group reserves full control over the indispensable technical infrastructure and decides over the modalities of infiltration, reconfiguration and data exfiltration.

\(^{622}\) Purtova N., *Between the GDPR and the Police Directive*, *International Data Privacy Law*, Vol. 8(1), 2018, p. 63; ‘The GDPR explicitly mentions these purposes in the context of restrictions from some of its provisions; such restrictions
ePD, Member States may derogate from certain rights and obligations under the GDPR (Article 23) and the LED (Articles 13(3), 15 and 16(4)).

are allowed when necessary for 'the prevention, investigation, detection or prosecution of criminal offences' (Article 23 GDPR). There would be no need for such provision in the GDPR if all data processing for the law enforcement purposes was removed from the scope of the Regulation altogether [...] When it comes to processing for the law enforcement purposes, the GDPR forms a safety net that 'catches' all data processing for law enforcement purposes when the Police Directive does not apply, thus eliminating the situations where data processing is not regulated by any one of the two instruments; Similarly, see Judgment in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, CJEU, 6 October 2020, para. 102; Commissioner Johannes Hahn, Use of the Pegasus Software by EU Member States against individuals including MEPs and the violation of fundamental rights, Topical Debate, European Parliament, 4 May 2022: ‘In certain cases, the General Data Protection Regulation may also apply’.

11. Annex III: EU framework for public procurement of security capabilities

EU procurement rules possibly provide avenues for the review of non-transparent procurement procedures resulting in the purchase of non-compliant surveillance technologies by intelligence agencies.

As an instrument of secondary EU law, the EU procurement directives 'do not change the Treaty and must abide by the Treaty.' Their application is therefore also subject to the expectations provided for by the Treaty on the Functioning of the European Union, in particular Articles 36, 51, 52, 62 and 346 TFEU. [...] This means in particular that contracts may be awarded without applying the Directive[s] in cases where this is necessary for the protection of essential security interests of a Member State. Arguably, Article 346 TFEU overrides Article 4(2), third sentence, TFEU, as the more particular provision (lex specialis). Although the Defence and Security Procurement Directive 2009/81/EC (DSPD) accounts for the specific needs and requirements of defence and security procurement, there may be contracts which are so confidential and/or important for national sovereignty that even the specific provisions do not suffice to safeguard Member States’ essential interests. Recourse to Article 346 TFEU should be limited to clearly exceptional cases. Where intelligence agencies (apparently) invoke national security purposes as a pretext for covertly purchasing surveillance technologies to spy on the political opposition or civil society, the implementation of procurement procedures would hardly qualify as a disclosure 'contrary to the essential interests of [a Member State’s] security'. A similar logic may be argued, if Article 4(2), third sentence, TFEU were to apply (see Annex I). However, establishing that national authorities evidently purchased software for politically motivated spying would be very difficult.

Materially, Directive 2009/81/EC applies to military purchases and to sensitive purchases which have a security purpose and involve classified information. Recital 11 specifies that '[i]n the specific field of non-military security, this Directive should apply to procurements which have features similar to those of defence procurements and are equally sensitive. This can be the case [...] where the purpose of the procurement is to protect the security of the Union and/or the Member

---

624 Guidance note on Field of application, Ares(2016)764791, European Commission, 12 February 2016, p. 1; See Article 2 Directive 2009/81/EC: 'Subject to Articles 30, 45, 46, 55 and 296 of the Treaty'.
629 Both may apply to dual-use equipment, see Heuninckx B., 'Article 15', in Caranta R. and Sachez-Graells A., European Public Procurement, Elgar, 2021, para. 15.08, and Institut de Relations Internationales et Stratégiques et al., Study on the industrial implications in Europe on the blurring of dividing lines between Security and Defence, European Commission, 2010, p. 122; Interpretative communication on the application of Article 296 TEC [now Article 346 TFEU] in the field of defence procurement, COM(2006) 779 final, European Commission, 7 December 2006, p. 4 clarifies that Article 296(1)(a) of the TEC [now Article 346 of the TFEU] ‘can [...] cover the procurement of dual-use equipment for both military and non-military security purposes, if the application of Community rules would oblige a Member State to disclose information prejudicial to the essential interests of its security.’
States on their own territory or beyond it, against serious threats from non-military and-or non-governmental actors. This may involve, for example, border protection, police activities and crisis management missions.\textsuperscript{630} The DSPD applies to supply and service contracts which have a value estimated to be at least € 431 000. Consequently, the Directive (arguably) applies to purchases of cyber-surveillance technologies by intelligence agencies and police forces, notably when marked classified.\textsuperscript{631}

However, if public authorities already determined at the time of procurement that they would primarily use the procured surveillance technologies for political gains instead of security interests, the required security purpose under the DSPD\textsuperscript{632} is likely not satisfied and the ordinary public procurement rules apply instead (Article 15(1)(a) Public Procurement Directive 2014/24/EU). Where such a contract was awarded without conducting the necessary procurement procedures, the Commission may consider launching an infringement procedure and aggrieved bidders could initiate review proceedings against contracting entities.\textsuperscript{633} Even where authorities conducted the necessary procedures, the acquisition of software that is non-compliant by design (relative to the envisioned uses) and therefore not legally operational raises questions about selection criteria and the evaluation of tenders (especially about the selection of the economically most advantageous tender).\textsuperscript{634}

Conversely, even where the security purpose is satisfied, particularly sensitive purchases of cyber surveillance technologies for the purposes of intelligence activities would be exempt from the application of secondary EU procurement law. According to Article 13(b) and Recital 27 of the DSPD, the EU defence procurement rules do not apply to 'contracts for the purposes of intelligence activities' including 'procurements provided by intelligence services' (italics added for emphasis).\textsuperscript{635} According to the European Commission guidance note, '[t]his provision is based on the assumption that contracts related to intelligence are by definition too sensitive to be awarded in a transparent and competitive procedure. [...] The definition of the scope of Article 13(b) [...] covers purchases for the purpose of all types of intelligence activities, no matter whether the service or the agency concerned is in charge of a specific intelligence function (military, security, criminal or external intelligence) or specialised in the collection of information from certain sources (e.g. imagery or

\textsuperscript{630} For details, see Guidance note on Field of application, Ares(2016)764791, European Commission, 12 February 2016, pp. 6-7.
\textsuperscript{633} Similarly, Gill P., 'Of intelligence oversight and the challenge of surveillance corporatism', Intelligence and National Security, Vol. 35(7), 2020, p. 982: 'Companies themselves may play a role as an `accountability-holder’, for example, by keeping government officials in their conduct of procurement processes, yet corporate self-regulation cannot be the whole answer and the rules must still be defined by government officials with their responsibility to protect the public interest'.
\textsuperscript{634} The Pirate Party (Germany) went so far as to report the German Federal Criminal Police Office to the German Federal Audit Office for violating the constitutional principle of efficiency and economy by acquiring non-compliant spyware, see PIRATEN zeigen BKA wegen Spähsoftware an, Zeitschrift für Datenschutz -Aktuell, Vol. 3(6), 2016, no. 03512.
\textsuperscript{635} Directive 2009/81/EC; For details, see Trybus M., Buying Defence and Security in Europe, Cambridge University Press, 2014, pp. 281-283.
One expert explicitly argues that this exemption also covers police authorities who are not intelligence agencies per se, but exercise similar activities.637

Similarly, pursuant to Article 13(a), the Directive shall not apply to 'contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security'.638 Recital 27 elucidates that this covers 'contracts [which] are so sensitivethat it would be inappropriate to apply this Directive, despite its specificity'. This is the case for 'particularly sensitive purchases which require an extremely high level of confidentiality, such as, for example, certain purchases intended for border protection or combating terrorism or organised crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces'. According to a European Commission guidance note, these examples 'indicate [...] that Article 13(a) was introduced essentially to allow for the explicit exclusion of highly confidential non-military security contracts'.639 Furthermore, the Commission clarifies that the exclusion of contracts related to intelligence activities (Article 13(b) DSPD) 'provides a tailor-made exclusion for a specific category of highly-sensitive contracts' (Article 13(a) DSPD). Pursuant to Article 15(1)(b) of the Public Procurement Directive 2014/24/EU, the specific exclusions under the DSPD would also prevent the applicability of ordinary EU procurement rules. Essentially, secondary EU procurement law would not apply, unless contracting parties purchase surveillance technologies under false pretenses.

Formally, public procurement rules derived from primary law, notably the TFEU, may still apply.640 However, a contract subject to the secrecy or intelligence services exemption in Article 13(a) or (b) DSPD will normally allow derogation on the basis of Article 346(1)(a)641, 36 or 52(1) TFEU.642 This does not mean that 'derogation from the Treaty is [...] automatic in case one of the categorical exclusions from the Defence Directive applies, since the earlier still depend on proportionality to be assessed on a case-by-case bases'.643 Nevertheless, such proportionality tests may well lead to the same

---

638 According to one expert, Article 13(a) of the DSPD amounts to the same effect as Article 346(1)(a) TFEU and is, legally speaking, superfluous, see Trybus M., Buying Defence and Security in Europe, Cambridge University Press, 2014, pp. 278-280.
640 Heuninckx B., Defence and Security Procurement in Theory and Practice, Seminar, The University of Nottingham, May 2018, slide 27: 'Even if the Directive does not apply, EU Treaties principles applicable to procurement apply: non-discrimination (transparency, sufficient advertising), basic mutual recognition, equal treatment (some form of competition), proportionality, effective judicial protection/as long as procurement has a certain cross-border interest'.
641 Interpretative communication on the application of Article 296 of the TEC [now Article 346 of the TFEU] in the field of defence procurement, COM(2006) 779 final, European Commission, 7 December 2006, p. 4 clarifies that 'Article 296(1)(a) TEC goes beyond defence, aiming in general at protecting information which Member States cannot disclose to anyone without undermining their essential security interests. This can also concern the public procurement of sensitive equipment, in both the defence and the security sector. In general, however, possible confidentiality needs related to the procurement process for military equipment are covered by Article 296(1)(b)TEC [now Article 346(1)(b) TFEU]; Article 346 of the TFEU, together with Articles 347 and 348 TFEU, are said to balance the tension between Member States' responsibility for their national security and the EU's responsibility for the functioning of the internal market, see Karpenstein U., 'Art. 346 AEUV', in Schwarze J. et al., EU-Kommentar, Nomos, 2019, para 1.
outcome, since 'the principle of proportionality applies to the use of both Article 346 TFEU and Article 13(a). This is particularly important because the reasoning for using this exclusion and the Treaty-based exemption may often be very similar.'  

Consequently, particularly sensitive purchases of cyber surveillance technologies for credible(!) essential security interests would likely be exempt from EU procurement acquis and withstand any challenges at EU level, thereby relegating chances of effective review to national fora.


Politicians, journalists, and researchers discussed widely the accountability implications of intelligence outsourcing in the aftermath of a series of US scandals involving private intelligence contractors during the early twenty-first century. While these may serve as inspiration for the EU debate, a number of contextual discrepancies should be taken into account. In the US context, academics emphasise an uncontrolled and ever closer integration of private actors with the US intelligence apparatus as the post-9/11 boom in intelligence contracting gained momentum. While EU Member States did not necessarily reproduce this degree of integration, the US example illustrates the risks posed by a strong enmeshment of public and private actors as well as their differing logic (public welfare vs economic gains). Unlike Pegasus cases, US cases revealed widespread economic misconduct including waste, fraud, and corruption, besides human rights abuses. However, according to reports, the Polish Central Anti-Corruption Bureau (CBA) illegally bought the Pegasus spyware with funds from the Polish Justice Ministry dedicated to victims of crimes, and politicians have called for increased scrutiny of the Polish intelligence-ware broker Matic. Pegasus cases mainly concern commodity contracting, whereas the US experience equally relates to support and personnel contracting. While a range of common themes cut across these different types of outsourcing, problems may appear with differing intensity, and more granular taxonomies and best practices could be developed.

Researchers identified a number of issues and risks associated with US intelligence outsourcing. According to one academic, the problem with involving private intelligence actors is that they are equipped with immunity as well as special powers under circumstances obstructing scrutiny, and that private sector intelligence analysis may shape strategic policy.

Another researcher summarises the situation as follows:

*The trend toward intelligence privatization and outsourcing is a cause for concern for many reasons. First, it breeds corruption and gross inefficiency. Second, it has resulted in massive abuses of civil liberties and human rights. Third, it weakens the quality of intelligence products, as national intelligence becomes dominated by private interests with strong incentives for biased reporting. Fourth, it creates difficulties for the control and oversight of intelligence activities, as it is more difficult for the government to monitor contracted companies and private*

---


647 Cost overruns, mismanagement, bidding back, and cronyism.

648 Black sites detention centres, extraordinary rendition programme, torture, excessive wiretapping and search warrants.


companies have less obligation to turn over information to congressional oversight bodies. Fifth, in the long term, it will cause a loss of core competencies and expertise to the private sector, especially as it concerns technology.652

Conversely,

While defenders concede that a few cases of private intelligence mismanagement and abuse have occurred, these are in no greater proportion than those occurring within government agencies or other corporations. Most defenders also acknowledge the higher cost of private intelligence, as well as that of institutional secrecy, the vagaries of contracting and outsourcing, and the scope and scale of private intelligence make third-party oversight problematic or ineffective.653

The uncontrolled rise of US intelligence outsourcing entrenched structural conditions that facilitated the undermining of democratic values. It introduced a strong profit motive in intelligence activities, promoted material interdependence, fostered a sense of unity, loyalty and common patriotism among private-public partners, and solidified a culture of informality and secrecy.654 Coupled with compartmentalised information and layers of obfuscation and ambiguity, these conditions undermined traditional control and oversight mechanisms, enabled corruption and cronyism as well as cost overruns, and facilitated unethical bidding, deniability and deliberate oversight skirting.655 Factors perceived to challenge administrative control include:656

- companies gaining bargaining power and governments ceasing to ‘monopolise the levers of influence’ (shift in governance mode from unilateral and hierarchical to multilateral and interdependent),
- an extended chain of command and confusion over responsibilities,
- lack of attention and planning behind intelligence outsourcing,
- insufficient and deficient control of contracts by intelligence officials,

Europe’s PegasusGate

- insufficient preparation and structures to manage the surge in outsourcing to meet the demand for intelligence capabilities and workforce in times of crisis,
- regulatory ambiguities and vagaries as well as unclear guidelines on what (not) to and how to outsource,
- interpretive flexibility of task orders, statements of work, and other contracting documents,
- deliberate ignorance to avoid difficulties, maintain deniability, or allow condoned but illegal, behaviour to continue,
- biased reporting by contractors and officials captive to private interests,
- regulatory arbitrage,
- lack of dissuasive sanctioning mechanisms for private contractors.

Factors perceived to challenge oversight include.\(^{657}\)

- the reactive, instead of proactive, posture of parliamentary oversight, committees’ reliance on the executive to be made aware of problems, and its dependence on the executive’s willingness to be overseen (parliament’s ‘outsider role’),
- lack of adequate resources, time and expertise,
- ‘constraints on deliberation arising from the need to maintain secrecy of classified materials’,
- reluctance of legislators to ‘curtail funding for a programme or discuss it publicly because they feel bound by the secrecy that protects intelligence sources and methods’,
- lack of commitment to systematic oversight in times of crisis, as well as when public-private interests merge, and when government is in a weaker negotiating position (‘gray mail’ and government’s dependence on private technologies or cooperation),
- even if committees can ask to see any piece of evidence, practical access to meaningful information (the full picture) is poor, since contractors add organisational layers and information is compartmentalised across organisations and access restricted,
- allegedly, ‘private companies have less obligation to turn over information to congressional oversight bodies’,
- lack of legal clarity can create uncertainty regarding judicial interpretation and discourage prosecution,
- public-private intelligence actors may mislead or obstruct oversight for fear of exposure.

In the same vein, societal scrutiny was impeded by secrecy of private-public dealings and operations, which are protected both by government and private sector policies.\(^{658}\) While commentators have called for the reversal and restriction of certain intelligence outsourcing.\(^{659}\)


there is widespread agreement that there will be no return to the status quo ante and that outsourcing will continue. Even 'critics have acknowledged that private firms provide agencies with technical strengths, managerial expertise, and workforce flexibility'. Commentators recommended a number of *corrective interventions*, including the following:

- empower oversight bodies to perform proactive or real-time oversight – for instance, through enhanced and regular reporting and enhancing oversight through periodic re-authorisation requirements,
- maintain government control over domains that are mission-critical and where necessary deploy officials directly in the field to cooperate with and control contractors,
- extend public law values into the private domain through contractual accountability and constraints,
- broader whistleblower protection so that *sousveillance* (undersight) may complement oversight,
- incentivise a critical and responsible surveillance industry that would hold public actors to account – for instance, by (i) mandating corporate legal assessments of governmental instructions, task orders, and warrants, (ii) sanctioning actions lacking appropriate warrants (or legal basis), including by holding executives criminally and civilly liable, (iii) imposing obligations on private partners to directly report to oversight bodies, and (iv) restricting immunity to actions clearly defined in contracts and properly reported to oversight bodies.


Michaels J., *All the President’s Spies*, California Law Review, Vol. 96(4), 2008, pp. 951-966; Gill P., *Of intelligence oversight and the challenge of surveillance corporatism*, Intelligence and National Security, Vol. 35(7), 2020, p. 982: ‘Companies themselves may play a role as an ‘accountability-holder’, for example, by keeping government officials in their conduct of procurement processes, yet corporate self-regulation cannot be the whole answer and the rules must still be defined by government officials with their responsibility to protect the public interest.’
Europe’s PegasusGate

- make procurement conditional on contractors’ submission to codes of conduct with a dedicated oversight committee and grievance mechanisms,669 or rely on peer-pressure and competition among contractors as an incentive to submit to codes of conduct,670
- dedicate an office in the Department of Justice to strictly enforce criminal liability regimes and impose progress reporting obligations on the office,671
- ensure effective contract management, including reporting and contract performance evaluation (metrics),672
- ensure lawfulness and coherence through internal policies673 and sufficient expertise to make strategic decisions and critically review contractors’ advice and behaviour,674
- instil a sense of responsibility and prudence and ensure effective redress by tightening state liability rules for contractor behaviour,675
- ensure immutable audit logs,676
- introduce objective threat measures to prevent a ‘terrorism industry’677 from exaggerating threats and needs for more intelligence workers and capabilities,678
- develop oversight and management mechanisms that are impervious to a surge in intelligence outsourcing,679
- tighten financial discipline to prevent ‘off-the-books' budgeting.680

673 These policies could clarify what (not) to outsource (inherently governmental functions) and how to outsource (procurement, oversight measures, etc.). Depending on sensitivity, criticality and intrusiveness of the mission, different procurement and oversight standards may apply.
680 Gill P., Intelligence Reform: the never-ending story, Panel 21, International Association for Intelligence Education Conference, June 2016, p. 16.
REFERENCES

Academic sources

Blauberger M. and Weiss M., 'If you can't beat me, join me! How the Commission pushed and pulled member states into legislating defence procurement', Journal of European Public Policy, Vol. 20(8), 2013.
Braun F. and Roggenkamp J., '0Zapftis v2.0', Privacy in Germany, Vol. 7(2), 2019.
Bromley M. and Brockmann K., Implementing the 2021 Recast of the EU Dual-use Regulation, Non-Proliferation and Disarmament Papers no. 77, EU Non-Proliferation and Disarmament Consortium, September 2021.
Chesterman S., We Can't Spy ... If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions', European Journal of International Law, Vol. 19(5), 2008.


Fidler M., Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities, Stanford University, 2014.


Gill P., Intelligence Governance and Democratization, Routledge, 2016.

Gill P., Intelligence Reform: the never-ending story, Panel 21, International Association for Intelligence Education Conference, June 2016.


Hawickhorst K., § 129a StGB - Ein feindstrafrechtlicher Inweg zur Terrorismusbekämpfung, Duncker & Humblot, 2011.


Hindin D., Can Export Controls Tame Cyber Technology?: An Israeli Approach, Lawfare blog, 12 February 2016.


Jiménez-Pérez D., Legitimidad y control del Centro Nacional de Inteligencia, Grupo de Estudios en Seguridad Internacional (GESI), Universidad de Granada, 2019.


Marczak B. et al., *Pegasus vs. Predator*, CitizenLab, 16 December 2021


Perlroth N., *This Is How They Tell Me the World Ends*, Bloomsbury, 2021.


Sandvik R., Pegasus Project – Individuals listed, targeted or compromised, last updated 7 February 2022.


Scott-Railton J. et al., ‘CatalanGate’, Citizen Lab, 18 April 2022.


Trybus M., ‘A Response to Simon Chesterman ‘We Can’t Spy ... If We Can’t Buy!’’, EJIL:Talk!, 26 January 2009.


van Daalen O. et al., The new rules for export control of cyber-surveillance items in the EU, Institute for Information Law, June 2021.


### Public sector sources

60 MEPs, *Cross-party joint letter convey concern about the formalisation of the Horizon Europe agreement with the State of Israel*, European Coordination of Committees and Associations for Palestine, 15 December 2021.


*Call for inputs: report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact*, United Nations, 12 February 2021.


Decision on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee, *P9_TA(2022)0071*, European Parliament, 10 March 2022.


Einsatz von Späh­software durch Bundes­behörden, Deutscher Bundestag website.


Executive Vice-President Dombrovskis, Answer to question E-005505/2020, E-005505/2020 (ASW), 8 January 2021.


Findings of the review team, press release, Israel’s Ministry of Justice, 22 February 2022.


Free Cybersecurity Services and Tools, Cybersecurity and Infrastructure Security Agency Website

German Federal Commissioner for Data Protection and Freedom of Information, Bericht des Bundesdatenschutzbeauftragten zum Staatstrojaner geleakt, Chaos Computer Club, 18 February 2012.

German Federal Constitutional Court, Constitutional complaint regarding the police’s handling of security vulnerabilities in IT systems is inadmissible, Press Release No. 62/2021, 21 July 2021.


Hearing, Committee on Civil Liberties, Justice and Home Affairs (LIBE), 29 November 2021.

Hearing, LIBE Committee, 1 February 2022.

Hearing, Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE), 9 September 2021.


Inquiry into the killing of Mr. Jamal Kashoggi, United National Office of the High Commissioner for Human Rights website.


Invitation of the Solicitor General to file a brief expressing the views of the US in case no. 21-1338, Order list: 596 U.S., 6 June 2022.


MEPs István Ujhelyi and Robert Biedroń, Pegasus affair: request for additions to Polish and Hungarian rule of law reports, 5 January 2022.

Minister of the Interior and Administration Mariusz Kamiński, Oświadczenie ws. śledztwa przeciwko Sławomirowi N., Rada Ministrów w Polsce, 23 July 2020.

Mission report following the ad hoc delegation to Budapest, Hungary, 29 September-1 October 2021, PE699.096v01-00, Committee on Civil Liberties, Justice and Home Affairs (LIBE), 16 November 2021

Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías, Actividad del presidente, La Moncloa, 26 May 2022.

Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała prezesów NIK, 18 January 2022.

Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała senatora Krzysztofa Brejzy, 19 January 2022.

Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała byłego szefa CBA i byłego wiceministra MSWiA, 15 February 2022.

Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała b.s. szefa SKW Piotra Pytla i prof. Andrzeja Zolla, 23 February 2022.

Polish Senate, Komisja Nadzwyczajna ds. nielegalnej inwigilacji wysłuchała byłego szefa CBA i byłego wiceministra MSWiA, 15 February 2022.

Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 26 January 2022.

Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 3 February 2022.

Polish Senate, Posiedzenie Komisji Nadzwyczajnej ds. inwigilacji, 29 April 2022.

Polish Senate, W Senacie powstała Komisja Nadzwyczajna ds. inwigilacji, 12 January 2022.

Public hearing – Pegasus spyware scandal and its impact on democracy in the EU, EPP Group, 10 February 2022.

Question time with Commission President Ursula von der Leyen, Press release 20220401IPR26529, European Parliament, 5 April 2022.

Report on foreign interference in all democratic processes in the European Union, including disinformation, P9_TA(2022)0064, INGE Special Committee, 9 March 2022.


Sofiyska Gradsko Prokuratura, СГП извършва проверка за евентуално неправомерно използване на софтуер 'Pegasus', 11 February 2022.


Sorell T. et al., SURVEILLE Deliverable D2.9: Consolidated survey of surveillance technologies, SURVEILLE Work Package 2, 8 April 2015.

Spokesperson of the Minister Coordinator of Special Services, Oświadczenie, Council of Ministers of Poland, 4 February 2022.


Taylor C., EC Defence Equipment Directives, SN/IA/4640, Library House of Commons, 3 June 2011.


The Bavarian Data Protection Commissioner, Prüfbericht Quellen-TKÜ, 30 July 2012.

The EU’s Rule of Law toolbox, Factsheet, European Commission, April 2019.

The Office of the State Attorney, 5 years in prison for NSO employee, Israel’s Ministry of Justice, 16 January 2019.


The surveillance of politicians, prosecutors, lawyers and journalists, and other persons and entities in EU Member States using cyber surveillance software, Debate, European Parliament, 15 February 2022.


UN Special Rapporteurs and experts, Spyware scandal: UN experts call for moratorium on sale of ‘life threatening’ surveillance tech, 12 August 2021.


Vice-President Jourová, Answer to question P-003661/2021, P-003661/2021(SAW), 4 November 2021.
Europe's PegasusGate

What is the Wassenaar Arrangement?, Wassenaar Arrangement website.

Civil society contributions
Access Now et al., Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states’ role in Pegasus affair, Reporters Without Borders, 10 September 2021.
Access Now et al., New guide: surveillance technology investors face significant risks if human rights are ignored, 9 March 2022.
Access Now et al., Urgent call to Council of the EU: human rights must come first in Dual-Use final draft, November 2020.
Amnesty International et al., Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, 27 July 2021.
Amnesty International et al., Open letter to Novalpina Capital, CC: NSO Group, Francisco Partners, 18 February 2019.
Amnesty International et al., Operating from the shadows: Inside NSO Group’s Corporate Structure, briefing, 31 May 2021.
Coalition Against Unlawful Surveillance Exports (CAUSE), A critical opportunity: bringing surveillance technologies within the EU Dual-User Regulation, June 2015.
Commission’s actions to implement new EU Export Control Regulation, Memo, European Commission, 9 September 2021.
Cybersecurity: EU External Action, European Commission website.
Eichner J., Staatstrojaner: Chronologie des staatlichen Hackings, Digitalcourage, 2 November 2018 (last updated 7 May 2020).
Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International website.
Grabowska-Moroz B., National intelligence authorities and surveillance in Poland (legal update), Helsinki Foundation for Human Rights, 8 July 2016.
Krahulcova L., Is NSO Group’s infamous Pegasus spyware being traded through the EU?, Access Now, 12 September 2019.
Lampert K., Dual-use surveillance tech: How trade agreements can incentivise good behaviour, about: intel, 3 November 2020.
Europe's PegasusGate

Media sources

Abril G., El independentismo catalán anuncia en Bruselas querellas por el ciberespionaje de Pegasus, El País, 19 April 2022.

Abril G., El Parlamento Europeo prevé enviar una misión de investigación a España por el ‘caso Pegasus’, El País, 10 May 2022.

AFP and Times of Israel staff, Israeli panel to review potential misuse of NSO spyware around world, Times of Israel, 22 July 2021.


Article 19 et al., EU: Action needed to tackle spyware abuses after Pegasus revelations, 15 September 2021.

Baars C., Wie 'Pegasus' aufs Handy kommt, Tagesschau, 18 July 2021.


Baquero C. and Piñol À., El independentismo cuestiona el espionaje al presidente del Gobierno con el programa Pegasus, El País, 2 May 2022.

Barnoczk B., Répássy Róbert lesz az igazságügyi államtitkár szombattól, telex, 10 December 2021.


Brewster T., Everything We Know About NSO Group, Forbes, 25 August 2016.

Bueno J. and Gil J., El juez investiga el 'hackeo' de los móviles de Torrent y Maragall, El País, 22 October 2020.

Bueno J., El juez de Barcelona que investiga Pegasus espera la respuesta de Israel desde hace un año y medio, El País, 19 April 2022.

Business & Human Rights Resource Centre, Apple files lawsuit against NSO Group, saying its US users were targets of Pegasus spyware, Tracker, 24 November 2021.

Calcalist staff, Calcalist System response, Calcalist, 21 February 2022.

Casqueiro J. and Hermida X., Los silencios y respuestas que deja Pegasus La exdirectora del CNI mostró a los diputados las resoluciones del Supremo que autorizaron el espionaje al entorno de Puigdemont, El País, 21 May 2022.

Casqueiro J. et al., Los socios del Ejecutivo se quedan ‘intranquilos’ tras la sesión secreta y exigen más información, El País, 5 May 2022.

Casqueiro J., El Congreso constituye la comisión de secretos oficiales con la entrada de ERC, Bildu, Junts y la CUP, El País, 28 April 2022.

Casqueiro J., El PSOE y el PP vetan la comisión de investigación sobre Pegasus, pero Sánchez tendrá que comparecer en el Congreso, El País, 3 May 2022.

Casqueiro J., ERC y Unidos Podemos siquen apuntando a Robles tras la destitución de la directora del CNI, El País, 10 May 2022.

Casqueiro J., Los socios intensifican el control en el Congreso y exigen una comisión de investigación sobre el espionaje de Pegasus, El País, 3 May 2022.

Cebrián J., Cuando el poder vulnera las reglas, El País, 2 May 2022.

Cebrián J., Las cloacas del Estado y otras cloacas, El País, 16 May 2022.


Clerix K., Pegasus-spyware: iPhone van journalist Peter Verlinden gehackt, Knack, 17 September 2021.

Cox J., NSO Employee Abused Phone Hacking Tech to Target a Love Interest, Vice’s Motherboard, 28 April 2020.


Cox J., NSO Group Employee Allegedly Stole Company’s Powerful Spyware for Personal Profit, Vice’s Motherboard, 5 July 2018.


Cue C. and González M., Defensa y La Moncloa chocan por quién asume el fallo de seguridad por el ataque al móvil de Sánchez, El País, 5 May 2022.

Cue C., El Gobierno destituye a Paz Esteban como directora del CNI por la crisis de Pegasus, El País, 10 May 2022.

Culafi A., Burned by Apple, researchers mull selling zero days to brokers, TechTarget, 15 October 2021.

Czuchnowski W. and Piątek T., Kupili Pegasusa dla PiS i wzięli miliony. 'Rodzinna firma' ludzi MO i SB, wyborcza.pl, 17 January 2022.


Czuchnowski W., Krag podejrzanych w sprawie Pegasusa. Kto odpowiada za inwigilację Brejzy i Giertycha, wyborcza.pl, 28 December 2021.

Czuchnowski W., Tak PIS kupował Pegasusa. Prywatna spółka zarobiła miliony, wyborcza.pl, 11 January 2022.

D'Amato R., 'Is EU 'Horizon' science funding going towards Pegasus spyware?', euobserver, 15 December 2021.


El País, El Gobierno dijo en 2020 que las comunicaciones de Sánchez dependen de Moncloa y que el CNI no tiene nada que ver, El País, 12 May 2022.


El País, Qué es el Centro Criptológico Nacional que ha detectado el espionaje a Sánchez y Robles, El País, 2 May 2022.


Figaj B., Prokuratura wszczęła śledztwo w sprawie fałszywych alarmów m.in. z telefonu żony senatora Brejzy, Polska Agencja Prasowa, 25 January 2022.

Flade F. et al., BKA bekam maßgeschneiderten Trojaner, Tagesschau, 8 October 2021.

Franceschi-Bicchierai L. and Cox J., Source: Spain is Customer of NSO Group, Vice's Motherboard, 14 July 2020.


Ft, pp/pm, NIK ujawnia faktury za 'zakup środków techniki specjalnej'. Pieniadze CBA otrzymało z Funduszu Sprawiedliwości, tvn24, 14 January 2022.

Gálvez J., El juez amplía la investigación por los presuntos espionajes a miembros del Gobierno con Pegasus, El País, 11 May 2022.

Gálvez J., El juez del 'caso Pegasus' rechaza la personación de la Generalitat por carecer de legitimación, El País, 18 May 2022.

Gálvez J., El juez ofrece a Pedro Sánchez y a Margarita Robles personarse en la causa sobre el presunto espionaje con Pegasus, El País, 5 May 2022.

Gálvez J., El juez señala que las intrusiones en el móvil de Sánchez se produjeron el 19 y el 31 de mayo de 2021, El País, 2 May 2022.

Gamarra L., Qué es la comisión de secretos oficiales que quiere activar el Gobierno tras el espionaje a políticos catalanes, ABC, 26 April 2022.

Ganon T., Israel police uses NSO’s Pegasus to spy on citizens, Calcalist, 18 January 2022.

Garcia Bueno J., El juez de Barcelona archiva de forma provisional la causa por el espionaje con Pegasus a Torrent y Maragall, El País, 30 May 2022.

García de Blas E., Feijóo invita a Sánchez a adelantar las elecciones por el ‘caos’ del Gobierno en la coalición y con sus aliados, El País, 4 May 2022.

Georgiopoulos G., Greek prosecutor to probe alleged bugging of journalist’s phone, Reuters, 21 April 2022.


Gera V., Two more Poles identified as victims of hacking with spyware, The Associated Press, 23 January 2022.

GF, Prosecutor’s office refuses inquiry into prosecutor Ewa Wrzosek’s phone hacking, tvn24, 29 December 2021.

Gil J. and Baquero C., Torrent y Maragall presentan una querella porque ‘la Fiscalía no mueve un dedo’ en el caso del espionaje, El País, 30 July 2020.
Europe's PegasusGate

Gil J., El ataque a los móviles de Torrent y Maragall con un programa espía israelí desata una tormenta política, El País, 15 July 2020.

Gil J., La empresa israelí sostiene que no puede saber a quién se espía, El País, 4 May 2022.

González G., Un juzgado archiva el espionaje por Pegasus a cargos de ERC en el Govern y el Ayuntamiento de Barcelona, El Mundo, 20 May 2022.

González M. et al., El Gobierno ofrece una investigación interna del CNI y otra del Defensor del Pueblo para aclarar el espionaje a independentistas, El País, 24 April 2022.

González M., ¿Es posible que Pedro Sánchez no supiera que Pere Aragonès estaba siendo espiado?, El País, 8 May 2022.

González M., El CNI compró el sistema Pegasus para espiar en el extranjero, El País, 20 April 2022.

González M., El CNI halla rastros de Pegasus en el móvil de Grande-Marlaska, El País, 5 May 2022.

González M., El CNI se siente cabeza de turco, El País, 4 May 2022.


González M., El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus, El País, 2 May 2022.

González M., El Gobierno inicia la reforma de la ley franquista de secretos oficiales, El País, 5 April 2021.

González M., El PSOE quiere consensuar con el PP una nueva ley de Información Clasificada, El País, 27 May 2022.

González M., La directora del CNI confirma el espionaje legal y autorizado a 18 independentistas, incluido Pere Aragonès, El País, 5 May 2022.


González M., Spain’s intelligence service has spyware program that targeted Catalan politicians, El País, 16 July 2020.

Gross J., Israel: If NSO Group violated export permits, ‘appropriate action’ will be taken, Times of Israel, 19 July 2021.


Hermida X., Sánchez asegura que desconocía el espionaje a los independentistas, pero lo justifica, El País, 26 May 2022.


Hermida X., Una comisión de secretos sin secreto, El País, 9 May 2022.


Hulio S., The man at the center of the storm, Unholy: Two Jews on the news, 11 February 2022.

I. Economou, Η ενημέρωση των πολιτικών συντακτών, MediaGovGR, 11 April 2022.


Ivanova E., Jest zażalenie prok. Wrzosek na odmowę zbadania jej inwigilacji Pegasusem, wyborcza.pl, 5 January 2022.


Kaye D. and Schaake M., Global spyware such as Pegasus is a threat to democracy. Here’s how to stop it, opinion piece, The Washington Post, 19 July 2021.


Kaye D. and Schaake M., Global spyware such as Pegasus is a threat to democracy. Here’s how to stop it, opinion piece, The Washington Post, 19 July 2021.


Kayali L., France seeks to bypass EU top court on data retention, Politico, 3 March 2021.

Kayali L., Tension mounts ahead of key ruling on French data retention, Politico, 14 April 2022.

McLaughlin J., *'Giving intelligence contractors whistleblower protections doesn't have to be "complicated"*, The Intercept, 6 November 2015.
Merino J., *Sánchez anuncia la reforma de la norma que regula el CNI para reforzar su control judicial y una nueva ley de secretos oficiales*, La Vanguardia, 26 May 2022.
Noguer M. and Baquero C., *Las protestas se radicalizan en Cataluña con el apoyo de Torra*, El País, 16 October 2019.
Panyi S. and Pethő A., *He has been uncovering the lavish lifestyle of Viktor Orbán’s circles. This summer, he was surveilled with Pegasus spyware*, Direkt36, 21 September 2021.
Panyi S. and Pethő A., *President of the Hungarian Bar Association and several other lawyers have been targeted by Pegasus*, Direkt36, 20 July 2021.
Europe’s PegasusGate

Panyi S., Hungarian president’s closest bodyguards targeted with Pegasus spyware, Direkt36, 13 December 2021.
Panyi S., Így fozzott szét a kormányzati kóditől a Pegasus-ügyben, Direkt36, 6 November 2021.
Pegasus: the new global weapon for silencing journalists, Forbidden Stories website.
Pethő A., Hungarian opposition publisher was surveilled with Pegasus in spring 2021, Direkt36, 8 September 2021.
Pethő A., Orbán’s ally told Hungarian intelligence services that opposition is the greatest national security threat, leaked recording reveals, Direkt36, 27 November 2021.
Piñol À., Pere Aragonès exige al Gobierno que aclare quién pidió al juez la autorización para espiarle, El País, 5 May 2022.
Pollet M., France denies talks to buy Israeli Pegasus spyware, Euractiv, 24 November 2021.
Premier Jarosław Kaczyński dla 'Sieci': opowieści opozycji o użyciu Pegasusa w celach politycznych to całkowite bzdury, wPolityce.pl, 7 January 2022.
Ravet H., Court rejects Amnesty International petition to withdraw NSO’s export license, Calcalist, 13 July 2020.
Reporters Without Borders, NSO/Pegasus : 17 journalistes de 7 pays se joignent aux plaintes déposées par RSF à l’ONU et devant la justice française, 5 August 2021.
Ridao J., Cómo se controla el CNI, El País, 30 April 2022.
Rincón R., El permiso judicial para espiar a independentistas: nominal, motivado y limitado en el tiempo, El País, 10 May 2022.
Rodríguez J., Sánchez y Robles, espia dos por el Pegasus, las claves del ataque a los teléfonos del Gobierno, El País, 2 May 2022.
Rovira M., El Parlamento catalán mueve ficha para investigar los pinchazos de Pegasus, El País, 3 May 2022.
Satter R. and Bing C., Exclusive: Senior EU officials were targeted with Israeli spyware, Reuters, 11 April 2022.
Satter R., An Invitation to a Lecture, email exchange, 10 February 2019.
Satter R., AP Exclusive: Undercover spy exposed in NYC was 1 of many, Associated Press, 11 February 2019.
Satter R., Lawsuit lays bare Israel-made hack tools in Mideast, Mexico, Associated Press, 1 September 2018.
Solomon S., Amnesty, research groups map out global reach of Israeli NSO Group’s spyware, Times of Israel, 4 July 2021.
Spiro A. and Times of Israel staff, In about-face, police admit misuse of NSO phone hacking tech, Times of Israel, 1 February 2022.
Spiró A., Deputy AG’s probe finds ‘no indication’ police illegally hacked citizens’ phones, Times of Israel, 21 February 2022.
Tenczer G., Ellenzéki párók: Völner után Varga Juditnak is mennie kell!, telex, 7 December 2021.

Times of Israel staff and Spiro A., *Sa’ar: Report on illegal NSO spyware use was incorrect, no need for state inquiry*, Times of Israel, 20 January 2022.

Times of Israel staff, *Attorney general opens investigation into police use of NSO spyware against Israelis*, Times of Israel, 29 January 2022.


Times of Israel staff, *NSO files defamation lawsuit against Calcalist over reports on police use of spyware*, Times of Israel, 27 February 2022.

Triantafyllou E. and Telloglou T., *Who was tracking the mobile phone of journalist Thanasis Koukakis?*, Inside Story, 11 April 2022.


Világi M., *Stummer szerint Kósa akár 3 év letöltendőt is kaphat, amiért beszélt a Pegassusról, de ő is láttá a szerződést*, telex, 4 November 2021.


Wettach S., *EU will gegen Spionage-Software Pegasus vorgehen*, WirtschaftsWoche, 2 April 2022.

WhatsApp Inc. and Facebook Inc., *Complaint*, United States District Court, 29 October 2019.


Ziobro mówiąc o Pegasusie, odwołał się do wyroku TK. Adwokat: władza nie tylko zlekażała ten wyrok, ale poszła o niebo dalej*, tvn24, 7 January 2022.

Петков: Явно сме засегнали големи интереси с разследването на 'Булгаргаз', OFFNews, 11 February 2022.
As civil society and media organisations expose EU Member States for using the Pegasus commercial spyware, one of the most high-profile spying scandals of recent years is coming to light in Europe. Member States’ intelligence agencies have been accused of abusing highly sophisticated spyware to surveil opposition figures, journalists, lawyers, and high-ranking state officials. ‘Having regard to the European Union’s attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law’, the European Parliament has set up a committee of inquiry. This study (i) introduces the Pegasus product’s features and trading practices, (ii) surveys Pegasus operations and reactions, (iii) identifies transversal and country-specific legal concerns, and (iv) sketches possible ways forward in the public and private sectors.