Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Provisional version

Committee on Legal Affairs and Human Rights

Pegasus and similar spyware and secret state surveillance

Report*

Rapporteur: Mr Pieter OMTZIGT, Netherlands, Group of the European People's Party

A. Draft resolution

1. In July 2021, an international coalition of investigative journalists coordinated by Forbidden Stories, with the technical support of Amnesty International's Security Lab ("the Pegasus Project"), published information about a leaked list of over 50,000 phone numbers identified as potential targets by clients of NSO Group, an Israeli company that developed and markets around the world a spyware called Pegasus. This list included human rights defenders, political opponents, lawyers, diplomats, heads of state and nearly 200 journalists from 24 countries. 11 countries around the world were identified as potential NSO clients, including two Council of Europe member States, Azerbaijan and Hungary.

2. Subsequent investigative reports, including by CitizenLab of the University of Toronto, have revealed that governments of several Council of Europe member States have acquired and used Pegasus for targeted surveillance of their own citizens. It is known that Pegasus was sold to at least 14 European Union countries, including Poland, Hungary, Spain, the Netherlands, Germany (in a modified version), Belgium and Luxembourg. There is strong evidence that Azerbaijan has also used it, including during its conflict with Armenia. Other member States have acquired or used similar spyware tools, such as Candiru and Predator. These tools have not only been used within the jurisdiction of member States but they have also been exported to third countries with authoritarian regimes and a high risk of human rights violations, including Libya (under the Gaddafi regime), Egypt, Madagascar and Sudan. These exports have potentially breached EU export rules.

3. The Parliamentary Assembly notes that Pegasus is a highly intrusive surveillance spyware, which grants the user complete and unrestricted access to all sensors and information of the targeted mobile phone. It turns the smartphone into a 24-hour surveillance device, accessing the camera and microphone, geolocation data, e-mails, messages, photos, videos, passwords, and applications. While some spyware tools require some action on the part of the victim, such as clicking on a link (for instance, Predator) or opening an attachment, Pegasus is installed through a so-called "zero click attack". Given its unprecedented level of intrusiveness into the private life of the targeted individual and all the target's contacts, the Council of Europe Commissioner for Human Rights and the European Data Protection Supervisor have expressed serious doubts as to whether its use could ever meet the proportionality requirement and therefore be human-rights compliant.

4. The Parliamentary Assembly shares these concerns and believes that the use of Pegasus-type spyware should be limited to exceptional situations as a measure of last resort, to prevent or investigate a specific act amounting to a genuine and serious threat to national security or a specific and precisely defined serious crime, and only targeting the person suspected of committing or planning to commit those acts. In order to limit such a high level of intrusiveness, States should take into account the proportionality of new spyware tools before

* Draft resolution adopted, and the draft recommendation unanimously adopted, by the committee on 8 September 2023..

acquiring and using them; they should also consider using spyware without some of the most invasive features of Pegasus or a version that is programmed in such a way that it limits access to what is strictly necessary.

5. The Assembly is deeply worried about mounting evidence that Pegasus and similar spyware have been used illegally or for illegitimate purposes by several member States, including against journalists, political opponents, human rights defenders and lawyers. Pegasus and other spyware has also been exported from member States to authoritarian regimes outside Europe, potentially in breach of EU export rules. The Assembly welcomes the thorough investigation carried out by the European Parliament's Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (PEGA Committee) leading to the adoption by the European Parliament (EP), on 15 June 2023, of a recommendation. It notes in this respect that the PEGA Committee and the EP have found that:

5.1. in Poland and Hungary, the Pegasus surveillance spyware has been illegally deployed for political purposes to spy on journalists, opposition politicians, lawyers, prosecutors and civil society actors, apparently as part of a system or an integrated strategy;

5.2. in Greece, it has been confirmed that an MEP and a journalist have been wiretapped by the intelligence agency and targeted with Predator spyware, and media reports revealed further possible targets of Predator, including other high-profile politicians. Spyware appears to have been used on an ad hoc basis for political and financial gains;

5.3. in Spain, the Prime Minister and other Ministers' phones were infected with Pegasus, allegedly by a third country (Morocco). 65 persons related to the Catalan pro-independence movement were allegedly targeted with Pegasus and/or Candiru, 18 of whom have been confirmed as lawful targets by the Spanish authorities;

5.4. Cyprus and Bulgaria serve as an export hub for spyware;

5.5. spyware companies are or were present in several member States, including Austria, Bulgaria, Cyprus, France, Germany, Greece, Italy, Luxembourg, Ireland, Romania and Switzerland.

6. The Assembly further notes that according to the "Pegasus Project" revelations, Azerbaijan has also used Pegasus, including against journalists, independent media owners and civil society activists. Recent reports have disclosed its use in connection with the Armenia-Azerbaijan conflict against 12 persons working in Armenia, including an Armenian government official, in what appears to be an example of transnational targeted surveillance.

7. The Assembly unequivocally condemns the use of spyware by state authorities for political purposes. Secretly surveilling political opponents, public officials, journalists, human rights defenders and civil society actors for purposes other than those exhaustively enumerated in Article 8.2 of the European Convention on Human Rights (ETS No. 5) (among which the prevention of disorder or crime and the protection of national security and public safety) amounts to a clear violation of the right to respect for private life (Article 8).

8. If the authorities invoke national security grounds as a justification for using spyware but their real purpose is to target and discredit an opposition politician or to intimidate and silence a human rights defender, the surveillance will give rise to a violation of Article 8 in conjunction with Article 18 of the Convention, which prohibits States from restricting rights for purposes not prescribed by the Convention itself. Such a misuse of power has a chilling effect on the exercise of other human rights and fundamental freedoms, including freedom of expression (Article 10), freedom of association and freedom of assembly (Article 11) and the right to participate in free elections (Article 3 of Protocol No. 1). It may also undermine the integrity of electoral processes and free public debate, and therefore, the foundations of our democratic societies.

9. The targeting of journalists has an impact on the confidentiality of their sources and in turn on their freedom to impart information. The targeting of lawyer-client communications impairs the exercise of defence rights and the right to a fair trial guaranteed by Article 6 of the Convention, which is a fundamental principle of the rule of law.

10. The Assembly underlines that member States have both negative and positive obligations under the Convention. Positive obligations in this area should include the protection of individuals within their jurisdiction from unlawful targeted surveillance by non-State actors and third States (transnational surveillance). This should trigger at the same time a procedural obligation to effectively investigate all cases of alleged unlawful digital surveillance by third actors targeting persons living in the territory of a member State. The Assembly refers in this context to Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on

human rights and business adopted on 2 March 2016, which recalls that member States have a duty to protect individuals against human rights abuses by third parties, including business enterprises.

11. The Assembly considers that the national investigative authorities and courts of the member States accused of spyware abuses must fully investigate and determine whether the use of Pegasus and similar spyware was lawful under domestic law and compliant with the Convention and other international standards. This implies assessing in each individual case whether the interference pursued a legitimate aim under Article 8.2 of the Convention and whether it was strictly necessary in a democratic society and proportionate to that aim. It also means ensuring that all victims of spyware-related abuses have access to effective remedies and redress. In this context, the Assembly urges:

11.1. Poland, to:

11.1.1. inform the Assembly and the Venice Commission about the use of Pegasus and similar spyware, within three months;

11.1.2. conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

11.1.3. refrain from using blanket secrecy rules to deny access to information on the use of spyware to oversight mechanisms and targeted persons;

11.1.4. apply adequate sanctions, either criminal or administrative, in cases of abuse;

11.1.5. comply with the opinion of the Venice Commission on the 2016 Police Act;

11.2. Hungary, to:

11.2.1. inform the Assembly and the Venice Commission about the use of Pegasus and similar spyware, within three months;

11.2.2. conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

11.2.3. refrain from using blanket secrecy rules to deny access to information on the use of spyware to oversight mechanisms and targeted persons;

11.2.4. apply adequate sanctions, either criminal or administrative, in cases of abuse;

11.2.5. implement without delay the judgments of *Szabó and Vissy* and *Hüttl*, as required by the Committee of Ministers in the exercise of its powers under Article 46.2 of the Convention;

11.3. Greece, to:

11.3.1. inform the Assembly and the Venice Commission about the use of Predator and similar spyware, within three months;

11.3.2. conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

11.3.3. refrain from using blanket secrecy rules to deny access to information on the use of spyware to oversight mechanisms and targeted persons;

11.3.4. apply adequate sanctions, either criminal or administrative, in cases of abuse;

11.4. Spain, to:

11.4.1. inform the Assembly and the Venice Commission about the use of Pegasus, Candiru and similar spyware, within three months;

11.4.2. conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

11.4.3. refrain from using blanket secrecy rules to deny access to information on the use of spyware to oversight mechanisms and targeted persons;

11.4.4. apply adequate sanctions, either criminal or administrative, in cases of abuse;

11.5. Azerbaijan, to:

11.5.1. inform the Assembly and the Venice Commission about the use of Pegasus and similar spyware, within three months;

11.5.2. conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

11.5.3. refrain from using blanket secrecy rules to deny access to information on the use of spyware to oversight mechanisms and targeted persons;

11.5.4. apply adequate sanctions, either criminal or administrative, in cases of abuse;

12. The Assembly considers that the Polish parliamentary election of 2019 was not fair as Pegasus was used against political opponents during the electoral campaign.

13. The Assembly calls on member States which seem to have acquired or used Pegasus, including Germany, Belgium, Luxembourg and the Netherlands, to clarify the framework of its use and applicable oversight mechanisms. It invites them to send this information, as well as any statistics on the use of Pegasus, to the Assembly and the Venice Commission within three months.

14. In order to prevent future abuses of spyware and human rights violations in Europe and beyond, the Assembly calls on all member States to:

14.1. ensure that their national laws on secret surveillance are in full conformity with the requirements of the European Court of Human Rights and the Venice Commission, with regard to quality of the law, authorisation procedures, supervision and oversight mechanisms, notification mechanisms and remedies, and review them if necessary;

14.2. ensure that the implementation of their legislative framework is effectively in line with the case-law of the European Court of Human Rights on targeted surveillance, with respect to legality, legitimacy, necessity and proportionality of any surveillance measure;

14.3. pending the assessment of their legislative framework and practice by the Venice Commission, refrain from using tools like Pegasus, Candiru, Predator or similar spyware;

14.4. in the mid-term, regulate specifically the acquisition and use of spyware by law enforcement and intelligence agencies, limiting the use of Pegasus-type spyware to exceptional situations as a measure of last resort, to prevent or investigate a specific act amounting to a genuine and serious threat to national security or a specific and precisely defined serious crime, and only targeting the person suspected of committing or planning to commit those acts. States should also establish oversight mechanisms, including parliamentary oversight, on the acquisition and use of spyware technologies, and incorporate an obligation to take into account proportionality considerations before acquiring and using new spyware tools;

14.5. criminalise the sale to and use of spyware by non-State actors;

14.6. ratify, if they have not yet done so, the Protocol amending Convention 108 for the protection of individuals with regard to the automatic processing of personal data, CETS No. 223, known as “Convention 108+”, which will apply to the processing of data for national security purposes, and already start implementing its standards in national law;

14.7. ratify, if they have not yet done so, the Budapest Convention on Cybercrime (ETS No. 185) and its Additional Protocols;

14.8. refrain from granting export licenses in respect of spyware technologies to countries where there is a substantial risk that those technologies could be used for internal or transnational repression and/or to commit human rights violations and revoke those granted in such cases;

14.9. join the Wassenaar Arrangement if they have not yet done so, and for States already participating in this arrangement, develop a human rights-based framework for the transfer of spyware technologies, according to which export licenses would require a human rights impact assessment of the recipient State and the companies' compliance with the UN Guiding Principles on Business and Human Rights;

14.10. require that all spyware companies domiciled or conducting substantial activities within their jurisdiction apply human rights due diligence throughout their operations or in respect of such activities, in line with the CM/Rec(2016)3 of Committee of Ministers, and implement standards restricting public procurement contracts to only those companies which demonstrate that they apply human rights due diligence.

15. The Assembly asks the Venice Commission to assess the legislative framework and practice on targeted surveillance of all member States (in priority Poland, Hungary, Greece, Spain and Azerbaijan; and then Germany, Belgium, Luxembourg, the Netherlands and all the other member States), in order to assess if such framework contains adequate and effective guarantees against any possible abuse of spyware, having regard to the Convention and other Council of Europe standards. Given the level of intrusiveness of Pegasus and similar spyware, clear and precise legislation, robust oversight mechanisms, procedural guarantees and effective remedies must be in place before member States can continue using those tools.

16. The Assembly trusts that the evaluation and review mechanism foreseen in amending Protocol CETS No. 223 will ensure the monitoring of the implementation of the relevant provisions of Convention 108+ in the area of targeted surveillance for national security and law enforcement purposes, including the use of spyware tools.

17. The Assembly calls on:

17.1. Israel, which enjoys observer status with the Assembly, to:

17.1.1. strengthen its export control mechanisms to ensure that export licenses are denied or revoked with respect to spyware technologies where there is a substantial risk that those technologies could be used for internal or transnational repression and/or the commission of human rights violations;

17.1.2. fully cooperate with investigations conducted by Council of Europe member States regarding the use of Pegasus and other spyware exported from Israel or sold by Israeli-based companies;

17.1.3. publish its framework on export control and inform the Assembly about it within six months;

17.2. Morocco, which enjoys partner for democracy status with the Assembly, to:

17.2.1. inform the Assembly within three months on whether it has used Pegasus or similar spyware at home and abroad;

17.2.2. launch within three months a fully independent investigation into the alleged use of Pegasus by state authorities against targets in Morocco and targets within the jurisdiction of Council of Europe member States;

18. The Assembly also calls on spyware and surveillance companies domiciled in Council of Europe member States or conducting substantial activities within their jurisdiction to apply human rights due diligence throughout their operations or in respect of such activities and improve transparency, in line with the CM/Rec(2016)3 of Committee of Ministers and the UN Guiding Principles on Business and Human Rights;

19. The Assembly invites the European Union to sign and ratify Convention 108+, make use of the Council of Europe's expertise in this field, and engage with the relevant Council of Europe bodies in areas such as

data protection, targeted surveillance and spyware, for the purposes of standard-setting, monitoring and cooperation.

B. Draft recommendation

1. The Parliamentary Assembly refers to its Resolution … (2023) on Pegasus and similar spyware and secret state surveillance and recommends that the Committee of Ministers:

1.1. adopt a recommendation to member States of the Council of Europe on secret surveillance and human rights, particularly in the light of the threats posed by new surveillance technologies and spyware, taking due account of the highest international standards, the case-law of the European Court of Human Rights and Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data). The recommendation should focus on:

1.1.1. the conditions for the acquisition of spyware by member States' government bodies and agencies;

1.1.2. the conditions for the use of spyware technology for law enforcement and national security purposes;

1.1.3. the conditions for the sale and export of spyware technology to third countries;

1.1.4. authorisation procedures, supervision and oversight mechanisms, notification mechanisms and remedies applicable to the use of spyware by state authorities;

1.1.5. accountability mechanisms in cases of unlawful use of spyware;

1.1.6. human rights due diligence standards for spyware companies;

1.1.7. the transnational aspect of digital surveillance and the use of spyware;

1.2. examine the feasibility of a Council of Europe Convention on the acquisition, use, sale and export of spyware;

1.3. coordinate its efforts with other international organisations, including the European Union and the United Nations, in the areas of data protection, targeted surveillance and spyware, for the purposes of standard-setting and cooperation.

C. Explanatory memorandum by Mr Pieter Omtzigt, Rapporteur

1. Introduction

1. The present report is based on a motion for a recommendation tabled on 21 September 2021 and which the Bureau referred to our Committee for report on 24 September 2021.[1] On 27 September 2021, the Committee appointed me rapporteur.

2. The motion for a recommendation recalled that in mid-July 2021, the Forbidden Stories consortium and its international partners reported on a leaked list of 50 000 phone numbers that had been proposed by clients of the NSO Group as potential targets for NSO's spyware product, Pegasus. Many of the phones in question belonged to journalists, human rights defenders, opposition politicians, and foreign politicians. Whilst the existence of Pegasus had already been known, the apparent scale and manner of its use by governments from around the world were shocking. Its potential impact on media freedom and democratic institutions is of profound concern. The Pegasus revelations show that stricter safeguards against misuse of such technology by public authorities, especially those of oppressive and authoritarian regimes, are needed. The motion called on the Assembly to prepare a report on the Pegasus revelations, with a view to making policy proposals to Council of Europe member States and other relevant actors.

3. In George Orwell's dystopic novel, 1984, all citizens houses and apartments are equipped with telescreens so that they may be watched or listened to at any time. Each person knew they were being observed and it was a stark warning. The present spyware is far more intrusive: the citizen does not know if and when it is used and who uses it. Not only information in the present is transferred, but all data on the phone can be transferred. It is so intrusive that even Orwell did not go this far. Yet this is the reality of our modern world and is part of the tools used against political opponents today.

4. During the preparation of this report, the Committee held two hearings. The first one in September 2022 in Bern, with the participation of Tim Engelhardt, human rights officer of the Office of the United Nations High Commissioner for Human Rights, and Lars Patrick Berg, MEP and member of the European Parliament's PEGA Committee. The second one was held in December 2022, when we had the opportunity to hear the testimony of three victims targeted with Pegasus or similar spyware: Krzysztof Brejza, member of the Polish Sejm for the opposition Civic Platform party, Diana Riba, a Spanish MEP from Catalonia's *Esquerra Republicana de Catalunya* party and Vice-Chair of the EP's PEGA Committee, and Thanasis Koukakis, an investigative journalist from Greece. I have also met with other victims in my capacity as rapporteur. I have also taken into account the motion "*Investigation into the illegal surveillance of foreign leaders, political opponents and activists in Poland"* of 26 April 2023.[2]

5. In this report, I will start by setting out the factual background concerning the reported allegations of misuse of Pegasus and similar spyware by Council of Europe member States, on the basis of different sources, including the findings of the EP's PEGA Committee. I will then refer to the Council of Europe and other international legal standards that may have been breached by States as a consequence of the use of commercial spyware like Pegasus. I will finally present the proposals made by different international actors to further prevent the abuse of Pegasus-type spyware and better address its impact on human rights.

2. The use of Pegasus and similar spyware by Council of Europe member States

2.1. The Pegasus spyware

6. Pegasus is a spyware developed and marketed by the Israeli company NSO Group than can be covertly installed on mobile phones running most versions of iOS and Android. The earliest version of Pegasus, which was discovered by researchers in 2016, infected phones through what is called spear-phishing, text messages or emails that trick a target into clicking on a malicious link.[3] Since then, Pegasus infections can be achieved through so-called "zero-click" attacks, which do not require any interaction from the phone's owner in order to succeed. For instance, in 2019, WhatsApp revealed that Pegasus had employed a vulnerability in its app to

[1] Doc. 15373, Reference No. 4608. On 14 September 2021, our committee held an exchange of views on "Pegasus spyware and secret state surveillance", with the participation of Michelle Bachelet, United Nations High Commissioner for Human Rights, Laurent Richard, Founder and Executive Director of Forbidden Stories, and Tamar Kaldani, Vice-chairperson of the Consultative Committee of the Council of Europe Convention for the Protection of individuals with regard to Automatic Processing of Personal Data (Convention 108).
[2] Doc. 15751.
[3] See: What is Pegasus spyware and how does it hack phones? | Surveillance | The Guardian, 18 July 2021.

launch zero-click attacks; the spyware would be installed onto a target's phone by calling the target phone, and the spyware would be installed even if the call was not answered. More recently NSO has begun exploiting vulnerabilities in Apple's IMessage software. Where neither spear-phishing nor zero-attacks succeed, Pegasus can also be installed over a wireless transceiver located near a target device, or by gaining physical access to the device.[4]

7. Once installed on a phone, Pegasus has been reported to be able to run arbitrary code, extract contacts, call logs, messages, photos, web browsing history, settings,[5] as well as gather information from apps including but not limited to communications apps iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram and Skype.[6] It can secretly turn a mobile phone into a 24-hour surveillance device, as it gains complete access to all sensors and information on the phone. It can read, send or receive messages that are supposed to be end-to-end encrypted, download stored photos, and hear and record voice/video calls. It has full access to the phone's camera, microphone and geolocation module.[7] In a way, the eavesdropping party can know more than the owner of the phone.

8. According to the European Data Protection Supervisor, Pegasus belongs to a new category of spyware tools that differ from "traditional" interception tools used by law enforcement authorities, in three aspects: it grants complete, unrestricted access to the targeted device; it is able to carry out a "zero-click" attack, not requiring any action by the user to be triggered; and it is very difficult to detect.[8] Contrary to conventional wiretapping, which only allows for real-time monitoring of communications, this type of spyware can provide full, retroactive access to files and messages created in the past, passwords, and metadata about past communications.

9. NSO Group claims that Pegasus only collects data from the mobile devices of specific pre-identified individuals, suspected to be involved in serious crime and terror. In this respect, it is (according to NSO) similar in concept to a traditional wiretap and has helped to prevent terrorist attacks, break up paedophilia, sex- and drug-trafficking rings, or find and rescue kidnapped children. NSO licenses Pegasus to law enforcement and intelligence agencies of sovereign states and has no visibility into its usage and its customers' targets.[9] According to NSO, Pegasus is not able to delete or alter data on a mobile device. The company states that it requires human rights compliance clauses in all customer agreements, and that customers must commit to use NSO's systems exclusively for legitimate and lawful prevention and investigation of serious crimes and terrorism. Once the company has completed its internal human rights due diligence procedure for the approval of customer engagements, the applications for export licenses must be approved by the Defence Export Controls Agency of the Israeli Ministry of Defence, who strictly limits the licensing of Pegasus, conducting its own analysis of potential customers from a human rights perspective.[10] Moreover, NSO claims that it tailors the configuration of the Pegasus system with specific settings for each end user. These customized specifications reflect the limitations of use as outlined in the company's internal human rights policies, and as determined by the terms of the export license issued by the Israeli Ministry of Defence. Any allegation that Pegasus has been misused by a state triggers a thorough review process and investigation into the reported claims. It can lead to the termination of the contract with a customer, when necessary. In fact, NSO claims that it launched investigations following the 2021 "Pegasus Project" allegations, including by reviewing domestic legal frameworks, interviewing end-users and verifying facts from objective sources.[11]

10. On 3 November 2021, the United States government (Commerce Department's Bureau of Industry and Security) added NSO Group to the Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the US. This was done on the basis of evidence that this company developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers, even outside their borders. U.S. Secretary of Commerce Gina M. Raimondo stated: "The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and

[4] Ibid.
[5] See: https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html, 25 August 2016.
[6] See: https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/, 25 August 2016.
[7] See European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 February 2022; p. 3: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en
[8] Ibid. pp. 3-4. Security researchers suspect that recent versions of Pegasus inhabit only the phone's temporary memory, rather than its hard drive, meaning that once the phone is powered down virtually, all trace of the software vanishes.
[9] NSO Group, Transparency and Responsibility Report, 30 June 2021, pp 6-7: https://www.nsogroup.com/governance/transparency/
[10] Ibid. pp. 29-30.
[11] Letter and position paper received from NSO Group, 15 August 2022.

organizations here and abroad".[12] The export of technology to the NSO Group and its subsidiaries is therefore prohibited.

11. Companies such as Meta and Apple have filed lawsuits against NSO Group for using the Pegasus spyware against their users.[13] A US appeals court has rejected the Israeli company's claim that it should be protected under sovereign immunity laws.

12. Following the "Pegasus Project" revelations and the blacklisting of NSO in the United States, it appears that the list of eligible export countries has been reduced by the Israeli Ministry of Defence from 102 to 37.[14]

2.2. Early allegations concerning the misuse of Pegasus

13. Pegasus' iOS exploitation was identified in August 2016. Arab human rights defender Ahmed Mansoor received a text message promising "secrets" about torture happening in prisons in the United Arab Emirates by following a link. Mansoor sent the link to Citizen Lab of the University of Toronto, which investigated, finding that if Mansoor had followed the link it would have jailbroken his phone and implanted the spyware into it.[15] Pegasus had previously come to light in a leak of records from Hacking Team, which indicated that the software had been supplied to the government of Panama in 2015. Some media have also reported that the United Arab Emirates was using this spyware as early as 2013.[16]

14. Two months after the murder of the Saudi journalist Jamal Khashoggi in Istanbul, Saudi dissident Omar Abdulaziz filed a lawsuit in Israel against NSO Group, accusing the firm of providing the Saudi government with the surveillance software to spy on him and his friends, including Khashoggi.[17] This is disputed by NSO.

15. Allegations concerning the use of Pegasus against targeted individuals in certain Council of Europe member States were also reported before 2021. For instance, according to the *The Guardian* and *El País,* Pegasus software was used to compromise the phones of several politicians in Spain, including the former President of the Parliament of Catalonia, Roger Torrent.[18]

2.3. "The Pegasus Project" revelations in 2021

16. In 2020, a list of over 50,000 phone numbers believed to belong to individuals as "people of interest" by clients of the NSO Group was leaked to Amnesty International and Forbidden Stories, a media non-profit organisation based in Paris. This information was shared with 17 news media organisations in 11 countries in what has been called "The Pegasus Project". Over several months, more than 80 journalists from these media organisations, including *The Guardian*, *Le Monde* and *Radio France*, *Die Zeit, The Washington Post, Le Soir* and *Direkt36*, carried out a joint investigation into the possible misuse of Pegasus against targeted individuals. Amnesty International's Security Lab carried out forensic analyses of mobile phones of some of the potential targets.[19]

17. On 18 July 2021, reports started to be published, revealing that Pegasus had been potentially used against human rights defenders, political opponents, lawyers, diplomats, heads of state and nearly 200

---

[12] https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/; https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[13] See: https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/, 23 November 2021; https://www.theguardian.com/us-news/2021/nov/08/nso-israeli-spyware-company-whatsapp-lawsuit-ruling, 8 November 2021; https://news.bloomberglaw.com/privacy-and-data-security/nso-loses-latest-challenge-to-meta-lawsuit-over-whatsapp-spyware, 6 January 2022.

[14] European Parliament, PEGA Committee, Report on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22 May 2023, par. 463.

[15] See: https://www.bbc.com/news/technology-37192670, 26 August 2016.

[16] See:https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html, 2 September 2016.

[17] See: https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/, 5 December 2018. It has also been reported that phones of other people close to him were targeted before and after his assassination.

[18] See: Phone of top Catalan politician 'targeted by government-grade spyware' | Catalonia | The Guardian, 13 July 2020.

[19] Mr Richard explained during the exchange of views held by the Committee on 14 September 2021 that the owners of some of the phones had been contacted and in a large proportion of cases, traces of Pegasus had been found following analysis by experts at Amnesty International's Security Lab. See minutes (link). See also: Forensic Methodology Report: How to catch NSO Group's Pegasus - Amnesty International, 18 July 2021.

journalists from 24 countries.[20] Forbidden Stories and its partners identified potential NSO clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE). According to *The Washington Post,* 14 former or current heads of state and government, including French President Macron and former Prime Minister of Belgium Charles Michel (current President of the European Council), appeared on the list of potential targets.[21]

2.4. Findings on the use of Pegasus and similar spyware by Council of Europe member States

18. Subsequent investigative media reports and other sources have demonstrated that Pegasus and similar spyware has been bought and used by Council of Europe member States against their own citizens. From information provided by the NSO Group, it is known that Pegasus was sold in at least 14 EU countries until the contracts with two countries were terminated. It is not known which countries these are, but there is a general assumption that they are Poland and Hungary.[22] There is also evidence that Council of Europe member States have exported Pegasus or similar spyware to third countries with authoritarian regimes and a high risk of human rights violations. The following paragraphs summarise some of the findings and conclusions by the European Parliament's PEGA Committee and other sources country by country.

2.4.1 Poland

19. In December 2021, Citizen Lab at the University of Toronto announced that Pegasus had been used in Poland against Roman Giertych, a lawyer representing top opposition politicians including Donald Tusk, and Ewa Wrzosek, a prosecutor involved in a case against the ruling government.[23] Senator Krzystof Brejza's phone had also been compromised numerous times when he was running the Civic Platform electoral campaign in 2019.[24] Other reported victims include Michal Kolodziejczak, leader of the agrarian movement Agrounia; Tomasz Swejgiert, journalist and alleged former associate of the Central Anticorruption Bureau[25]; Andrzej Malinowski, former President of the Employers of Poland; as well as former Law and Justice (PiS) politicians.[26] On 7 February 2022, the Supreme Audit Office revealed that between 2020-2021, 544 of its employees' devices were under surveillance in over 7,300 attacks, and that three could have been infected with Pegasus.[27] The Supreme Audit Office had been at the time investigating the cancellation of the presidential elections in 2020.

20. The case of Senator Brejza is illustrative of the alleged links between the surveillance and the electoral process. He was serving as the head of the election campaign of the Civic Platform during the European and national elections when he was targeted. There were 33 attacks on Brejza's phone from April to October 2019, just days after the end of the electoral cycle. As a result of these infections, text messages and correspondence from his phone were stolen and aired on the state-controlled television network in an alleged orchestrated smear campaign against him. No charges were ever brought against Brejza, but his surveillance was allegedly linked to the criminal investigation against his father (mayor of Inowroclaw) started five years before, where Mr Brejza had not even been questioned as a witness. Mr Brejza Sr himself received 10 text messages in 2019 which Amnesty International's security lab deemed suspicious and which matched the hallmarks of Pegasus. In addition, according to Mr Brejza, the court which authorised the surveillance against him during the electoral campaign was not informed about the use of Pegasus.[28]

---

[20] See: https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/, 18 July 2021.
[21] See: Heads of state found on list of numbers examined by Pegasus Project - The Washington Post, 20 July 2021.
[22] European Parliament, PEGA Committee, Report on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22 May 2023, par. 11.
[23] See: https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.
[24] See: https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 December 2021.
[25] See: https://apnews.com/article/technology-europe-poland-hacking-spyware-4a410bda35df566632703e3578e5a99d, 25 January 2022.
[26] See:https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true,
18 January 2022. Other victims include Deputy Magdalena Łośko, Paweł Tamborski, Deputy Minister of the Treasury from 2012 to 2014, Andrzej Długosz, co-owner of Cross Media PR Sp. z o.o., Deputy Grzegorz Napieralski and Jacek Karnowski, Mayor of Sopot (all heard by the Polish Senate Extraordinary Committee).
[27] See: https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true, 7 February 2022.
[28] PEGA Committee Report, pars. 63-68; hearing of Mr Brejza before our Committee on 12 December 2022 (see the video recording of the hearing: Politicians and journalists targeted by spyware testify at PACE hearing in Paris (coe.int)).

21. While the Polish government had initially denied the acquisition of the spyware, it confirmed in early 2022 that it was in possession of Pegasus. Jarosław Kaczyński, the chairperson of the ruling PiS party, admitted that Poland had acquired the Pegasus spyware but dismissed any allegations about its misuse for political purposes, for instance against opposition politicians in the 2019 parliamentary election campaign. The Minister of Justice, Mr Ziobro stated that any use of Pegasus was done "according to the law".[29] In this connection, a committee set up by the Polish Senate to investigate the use of Pegasus (Senate Extraordinary Committee on Investigation of Cases of Illegal Surveillance, their Impact on the Electoral Process in the Republic of Poland and the Reform of the Special Services) heard different witnesses and experts, among them cybersecurity experts (from Citizen Lab) and the former president of the Supreme Audit Office and subsequently independent Senator Krzysztof Kwiatkowski. In January 2022, he presented two invoices to the committee confirming the purchase of spyware for the Central Anti-Corruption Bureau with PLN 25 million from a Ministry of Justice fund earmarked for victims of crime. Since according to Polish law the operations of the CBA can only be financed from the state budget (the above-mentioned Justice fund not being part of it), it appears that the purchase of Pegasus breached Polish law. As regards the use of Pegasus, it has not been made explicitly clear whether any, let alone all of the persons targeted by Pegasus to date were spied on with judicial authorisation, as required by law. It seems that only the case of prosecutor Ewa Wrzosek and Krzysztof Brejza have been taken up by the courts following their complaints and appeals.[30]

22. In February 2022, I wrote to the Polish authorities, through the chairperson of the Polish Assembly delegation, asking them to provide me with some explanations. On 22 April 2022, Stanislaw Zaryn, Director of the National Security Department, replied that there was no evidence of illegal surveillance against anyone and that every case of operational control by the Polish special services had obtained judicial authorisation.

23. During my fact-finding visit to Warsaw (13-15 March 2023) in the context of the monitoring procedure in respect of Poland (Monitoring Committee), I met with members of the Senate Committee to clarify cases of illegal surveillance and other relevant authorities. I was informed that the number of secret services and law enforcement agencies that are legally allowed to conduct surveillance has proliferated in Poland. As a result, judicial and parliamentary oversight is fragmented and clearly no longer adequate. I regret that besides the Senate Extraordinary Committee, no attempts have been made by the Sejm to investigate the allegations of illegal surveillance, including of prominent political personalities.[31] It must be noted that the Senate committee lacks the investigative powers of the Sejm.

24. The EP's PEGA Committee concluded that "the use of Pegasus [in Poland] is an integral and vital component of a system for the surveillance of the opposition and critics of the government for political gain (…). The scope for surveillance in Poland has been expanded vastly over the past few years, weakening or removing safeguards and oversight provisions. In the course of systematic and targeted legislative changes brought about by the ruling majority, the rights of victims have been minimised and legal remedy and redress have been rendered meaningless in practice. Effective *ex ante* and *ex post* scrutiny, as well as independent oversight, have been *de facto* eliminated."[32] The European Parliament, in its Recommendation of 15 June 2023 on the Investigation of the use of Pegasus and equivalent surveillance spyware, noted that "Pegasus surveillance spyware has been illegally deployed for political purposes to spy on journalists, opposition politicians, lawyers, prosecutors and civil society actors".

2.4.2. Hungary

25. In 2021, it was revealed by the Pegasus Project and confirmed by Amnesty International that over 300 Hungarians had potentially been targeted with Pegasus. The phone numbers of at least 10 lawyers and 5 journalists, an opposition politician, as well as activists and high-profile entrepreneurs were included in the leaked list of potential Pegasus targets.[33] Since then, a number of targets have been confirmed as having been successfully hacked. The phone of Szabolcs Pany, an investigative journalist for Direkt36, was successfully infected with the spyware, according to the forensic analysis by Amnesty International. Mr Pany's phone had been repeatedly compromised by Pegasus during a seven-month period in 2019, with the infection coming

[29] See: https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 January 2022.
[30] PEGA Committee Report, pars. 20, 23, 37 and 46. With regard to the existing legislative framework, there is a pending case before the ECtHR, where the applicants complained that the secret systems for monitoring telecommunications, postal and digital communications and gathering metadata, interfere with their right to respect for private life, and that there is no effective remedy with regard to this interference (*Pietrzak v. Poland* and *Bychawska-Siniarska and others v. Poland: https://hudoc.echr.coe.int/eng-press?i=003-7444850-10197670*).
[31] https://rm.coe.int/draft-information-note-poland-march-2023-information-note-by-the-co-ra/1680ab699f
[32] PEGA Committee Report, pars. 79-80.
[33] See: https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.

soon after he requested comments from government officials (including on an article he had written concerning the move of a Russian bank to Budapest). Other persons identified as targets include journalist Dávid Dercsény; Central Media Group owner Zoltán Varga; professor Attila Chikán (former minister in Viktor Orbán's first government and currently a critic); the son and lawyer of one of Viktor Orbán's former friends (now opponent), Lajos Simicska; János Bánáti, president of the Hungarian Bar Association; Adrien Beauduin, a Belgian-Canadian PhD student of the Central European University who was arrested after attending a protest in Budapest; lawyer Ilona Patócs; the mayor of Gödöllö György Gémesi; Brigitta Csikász, one of Hungary's most experienced crime reporters; as well as persons inside the Fidesz inner circle.[34]

26. In early 2022 a group of six journalists and activists initiated legal actions before the Hungarian authorities and the European Commission. The Hungarian Civil Liberties Union (HCLU) is representing them.[35] At the time of writing, both the Supreme Court and the Constitutional Court had rejected the HCLU's requests.

27. Hungarian authorities initially neither commented nor denied the use of Pegasus. In November 2021, Lajos Kósa, Chair of the Parliamentary Defence and Law Enforcement Committee, admitted that the Ministry of Interior had purchased Pegasus but said that it had never been used against Hungarian citizens.[36] The Ministry of the Interior bought Pegasus for EUR 6 million indirectly through Communication Technologies Ltd from NSO Group's company registered in Luxembourg in 2017. On 31 January 2022, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) presented the conclusions of an investigation launched ex officio into the use of Pegasus by the Hungarian authorities. NAIH concluded that Pegasus was used by the National Security Service on several persons whose names had appeared in the press, but always in compliance with the legal framework (with a Ministry of Justice or court authorisation) and on grounds of national security. Not all the 300 Hungarian citizens whose phones appeared on the leaked list were investigated by NAIH, since according to its president, Amnesty International did not provide them with such a list.[37] The investigation's reasoning will remain classified until 2050.

28. In February 2022, I wrote to the Hungarian authorities, through the chairperson of the Hungarian Assembly delegation, to provide me with some explanations. Unfortunately, I received no reply.

29. Other spyware companies such as Black Cube and Cytrox also appear to have connections with Hungary. Black Cube became involved in Hungary during the 2018 elections, when they spied on various NGOs and persons who had connection to George Soros.[38] In 2015, files leaked from the Hacking Team revealed that the Hungarian government was a client.

30. The EP's PEGA Committee concluded that "the use of Pegasus in Hungary appears to be a part of a calculated and strategic campaign to destroy media freedom and freedom of expression by the government. The government has utilised this spyware in order to usher in a regime of harassment, blackmail, threats and pressure against independent journalists, media, political opponents and civil society organisations with ease and without fear of recourse."[39] The EP, in its Recommendation, reached the same conclusion as with Poland, namely that "the Pegasus surveillance spyware has been illegally deployed for political purposes to spy on journalists, opposition politicians, lawyers, prosecutors and civil society actors''.

2.4.3. Greece

31. In March 2022, Citizen Lab revealed that investigative journalist Thanasis Koukakis'phone had been infected with the Predator spyware in 2021.[40] Predator is a one-click exploit that requires the target to click on a link in order for the spyware to infect the phone, unlike Pegasus. Predator was developed by Cytrox, a firm based at the time in North Macedonia. Cytrox was subsequently acquired by Tal Dilian (former member of the Israeli Defence Force with Maltese citizenship) and became part of the Intellexa alliance, a consortium of spyware vendors with representations in Cyprus, Greece, Ireland and France. In July 2022, the Member of the European Parliament and leader of the Greek opposition PASOK party Nikos Androulakis announced that he was filing a complaint against attempts to infect his phone with Predator. The attempted infection with spyware

[34] See: https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/, 19 July 2021. See also: https://telex.hu/direkt36/2021/07/20/pegasus-nso-surveillance-hungary-lawyers-bar-association-janos-banati, 20 July 2021. In some of these cases, the phones showed traces of potential Pegasus hacks, but it was not possible to confirm whether there had been a successful infection.
[35] See: https://hclu.hu/en/pegasus-case-foreign-procedures.
[36] See: https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217, 4 November 2021.
[37] See: https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/, 31 January 2022.
[38] PEGA Committee Report, pars. 129-131.
[39] Committee Report, par. 132.
[40] Mr Koukakis participated in a hearing before our Committee on 12 December 2022 (video recording at: Politicians and journalists targeted by spyware testify at PACE hearing in Paris (coe.int)).

was discovered during a check of the phone by the European Parliament's IT service. These attempts took place when Mr Androulakis was a candidate for the leadership of PASOK. In November 2022, the Greek media revealed a list of 33 targets of Predator, all of whom were high-profile personalities, including members of the government, former Prime Minister Samaras and former EU Commissioner Avramopoulos. In February 2023, the President of the Hellenic Data Protection Authority (HDPA) confirmed that 300 text messages related to Predator spyware had been sent to approximately 100 devices.[41] Some confirmed targets of Predator are Christos Spiritzis, former Minister of Infrastructure and member of parliament for the Syriza party, and Artemis Seaford, a Greek-American former employee at Meta who had written about a case of sexual harassment by a politician.

32. Both Mr Koukakis and Mr Androulakis tried to obtain information or redress from the competent national authorities, including through the Hellenic Authority for Communication Security and Privacy (ADAE) and by lodging criminal complaints. They have also lodged applications with the ECtHR.

33. In August 2022, the Greek Government admitted that the National Intelligence Service (EYP)[42] had been monitoring (through conventional wiretapping) Mr Koukakis and Mr Androulakis, but it denied that it had ever purchased Predator or used it against them. On 8 August, Prime Minister Mitsotakis stated that the surveillance of Mr Androulakis had been 'legal' but 'politically unacceptable'. He made no reference to the case of Mr Koukakis or other alleged cases. After the initial revelations, the Director of the EYP and Grigoris Dimitriadis, the government's Secretary-General, resigned. The former Director of the EYP stated that the wiretapping of Mr Androulakis had been launched at the request of the intelligence agencies of Armenia and Ukraine, in the light of his participation in the EP's Committee on International Trade, which deals with trade relations between the EU and China. It is possible that Predator was not directly purchased by the State, but through other channels.[43]

34. It has also been confirmed that the Greek Government has granted export licences to Intellexa for the sale of the Predator spyware to governments such as Madagascar and Sudan. This could have been a violation of the EU Dual Use Regulation. [44]

35. The EP's PEGA Committee concluded that "there are patterns suggesting that the Greek government enables the use of spyware against journalists, politicians and businesspersons. It also allows the export of spyware to countries with poor human rights records (…) Although the use of spyware is illegal in Greece, the investigation into origins of the spyware attacks only gained momentum in Summer 2022 (…) The highest political leadership in the country use spyware as a tool for political power and control, in some cases in parallel or after legal interception (…) Unlike other cases, such as Poland, the abuse of spyware does not seem to be part of an integrated authoritarian strategy, but rather as a tool used on an ad hoc basis for political and financial gain." The EP, in its Recommendation, added that "it is highly probable that Predator has been used by or on behalf of persons very close to the Prime Minister's office."

2.4.4. Spain

36. In April 2022, Citizen Lab published a report (CatalanGate Report) according to which 65 persons had been targeted or infected with Pegasus or similar spyware between 2017 and 2020: 63 with Pegasus, four with Candiru (another spyware sold by the Israeli-registered firm Candiru) and at least two persons with both. At leas 51 individuals' devices were successfully infected. All these were members of the Catalan pro-independence movement (Members of the European Parliament, Catalan Presidents, legislators, lawyers and members of civil society) or family and staff linked to them. Citizen Lab did not attribute the attacks to a specific entity but suggested that evidence pointed to "a strong nexus with one or more entities within the Spanish government". In May 2022, the Spanish authorities admitted having targeted, with the authorisation of a Supreme Court's judge 18 individuals out of the 65 alleged cases. The former director of the Spanish National Intelligence Centre (CNI) Paz Esteban appeared before the Official Secrets Committee of the Congress of Deputies at a meeting held in camera to provide justification for the surveillance of these 18 persons, but the judicial warrants have never been made public. Among the confirmed targets are the current President of Catalonia Pere Aragonès, former President and current MEP Carles Puigdemont (relational targeting), former Presidents of the ANC (Catalan civil society organisation supporting independence) Jordi Sanchez and Elisenda Paluzie, and former Vice-President of the NGO Omnium Cultural Marcel Mauri. Some of the

[41] PEGA Committee Report, par. 136.
[42] Under the direct control of Prime Minister after a change in the law following the victory of Néa Dimokratia in 2019.
[43] One possibility would be through Keytak, the Centre for Technological Support, Development and Innovation set up by former Director of the EYP. See PEGA Committee Report, pars. 141-142, also with regard to the links between Intellexa, the company that owns Predator, and the Greek State.
[44] PEGA Committee Report, pars. 153-155.

confirmed targets have faced criminal charges related to the 2017 independence referendum and follow-up events. Others were allegedly targeted at the time of the public protests and blockages organised by the Committees for the defence of Republic (*CDR*) as a reaction to the criminal conviction of the Catalan leaders involved in the illegal referendum. The authorities have invoked reasons of secrecy and national security for not expanding on the reasons for the surveillance. The government has not commented on the 47 remaining persons and it remains unclear whether these individuals were indeed legally targeted with a court order. Some of the targets were outside Spain when the infection took place, among other places in Belgium and Switzerland.[45] According to some sources, the Spanish government purchased Pegasus in the first half of the 2010s for an estimated EUR 6 million.[46]

37. One of the targeted groups are the pro-independence Catalan Members of the European Parliament. We heard about the case of Diana Riba at our Committee hearing of 12 December 2022. She is MEP of *Esquerra Republicana de Catalunya* (ERC). According to her, her phone was infected with Pegasus on two occasions. The first one was in June 2019, after she had just taken her seat as an MEP and during political discussions on the vacant seat of Oriol Junqueras, who could not take up his position as an MEP while in pre-trial detention for his involvement in the 2017 illegal Catalan referendum. The second infection was in October 2019, after the Supreme Court's judgment against pro-independence leaders, including her own partner and former Catalan Minister Raül Romeva. The majority of her phone calls related to that case, including conversations with his lawyers.[47]

38. Other persons among the 65 alleged targets include Marta Rovira, Secretary General of the ERC party living in Switzerland; Elena Jiménez, International Representative of Omnium Cultural serving on the legal team of Jordi Cuixart (former President of Omnium Cultural); and lawyers representing some of the then imprisoned pro-independence Catalan politicians.

39. At the same time, in May 2022, shortly after the CatalanGate revelations, the Spanish government disclosed that the phones of Prime Minister Pedro Sánchez, Minister of Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska had been infected with Pegasus spyware in 2020-2021. Minister for Agriculture Luis Planas, who had previously served as a diplomat in Morocco, was also targeted but no successful infection was achieved. While no confirmation of the source of these attacks has been given, there are suspicions that the Moroccan authorities (also suspected of having used Pegasus against targets in France) are behind them, given the diplomatic crisis between the two countries at the time.

40. As a result of the CatalanGate revelations, the Spanish Ombudsman carried out an ex officio investigation. On 18 May 2022, he concluded that the 18 confirmed targets had been surveilled in accordance with the law as the interceptions had been approved by a Supreme Court judge and the authorisation was accompanied by the required justification. He had had access to the classified documents but did not comment on the substance of the justification contained in the judicial warrants or the proportionality of the surveillance.[48] Although the Spanish Congress voted against a proposal to establish of committee of inquiry on the use of Pegasus in 2022, the recent elections held in July 2023 have led to a change of position of the ruling Socialist party (PSOE), which has ultimately agreed to create a committee of inquiry on Pegasus in exchange of the support of the Catalan pro-independence parties to the newly elected Speaker of the Congress.[49] The Catalan Parliament had already established a committee of inquiry in 2022.[50]

41. Different criminal complaints have been filed with investigative courts in Barcelona by some of the individuals concerned, civil society organisations and even the Catalan Parliament.[51] However, investigations are not advancing as quickly as expected, and there are difficulties in proving the infections. It appears that investigating judges do not always accept the expert evidence presented by the plaintiffs and the public prosecutors ask for the infected mobile phones to be checked by the police. Complaints by some of the confirmed targeted individuals seeking access to the judicial warrants and documents related to their

[45] PEGA Committee Report, pars. 329-331; 338-346. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.
[46] El CNI compró el sistema Pegasus para espiar en el extranjero | España | EL PAÍS (elpais.com).
[47] Video recording of the hearing at: Politicians and journalists targeted by spyware testify at PACE hearing in Paris (coe.int).
[48] El Defensor del Pueblo concluye que el CNI espió "conforme a la Constitución" (elnacional.cat).
[49] Spain: Pedro Sánchez's socialist candidate wins crucial vote for control of parliament | Euronews.
[50] Constituïda la comissió d'investigació sobre l'espionatge amb els programes Pegasus i Candiru - Parlament de Catalunya.
[51] El Parlament presenta la denúncia pels fets relacionals amb el programa d'espionatge Pegasus - Parlament de Catalunya.

surveillance have been rejected by the Supreme Court. [52] Under Spanish law, information related to intelligence services and their activities is classified.[53] The case of the surveillance of Prime Minister Pedro Sánchez and other Ministers also reached the *Audiencia Nacional* in Madrid. The investigating judge of this court set a formal request for international judicial assistance (letter rogatory) to the Israeli Government asking for information on different aspects of the Pegasus software. However, the judge has recently decided to provisionally close this case "due to the complete lack of cooperation from Israel".[54]

42. The EP's PEGA Committee concluded that the 47 targeted persons mentioned in the CatalanGate report should have access to justice and an investigation should be launched. With regard to the 18 cases with judicial authorisation, their proportionality and necessity remain to be checked by a court, given that the Ombudsman only verified their (formal) legality. The EP in its Recommendation called on Spain to invite Europol, which could contribute with technical expertise, to join the investigations.

2.4.5. Azerbaijan

43. According to the 2021 "Pegasus Project" revelations, Azerbaijan is among the countries that uses Pegasus. At least 48 journalists were potentially selected for Pegasus targeting.[55] These included Sevinc Vaqifqizi, a freelance journalist for the independent media outlet Meydan TV, whose phone was successfully infected over a two-year period (2019-2020) and Khadija Ismayilova, an investigative journalist at the Organized Crime and Corruption Reporting Project, whose phone was regularly infected for nearly three years (2018-2021).[56] Reports also referred to civil society activists, such as Fatima Movlamli, a female activist whose intimate photographs had been leaked on Facebook in 2019.[57] In this connection, the publication of private and intimate photos and conversations of women raises particular concerns and illustrates the specific gender-related dangers of targeted surveillance of female journalists and human rights defenders.

44. The investigation conducted by the Organized Crime and Corruption Reporting Project (OCCRP) revealed that there were more than 1,000 Azerbaijani numbers in the Pegasus Project list. 245 phone numbers were identified. Out of this list, a fifth belonged to reporters, editors, or media company owners.[58] Around 62 individuals brought complaints before the Prosecutor General's Office, claiming that their phones had been illegally infiltrated by Pegasus spyware and that this amounted to a violation of their right to private life guaranteed by the ECHR. The Prosecutor General's Office replied that their complaints had to be sent to the Investigative Directorate of the State Security Service (SSS). The SSS refused to give an official written answer and officials orally informed the lawyers of the individual applicants that they had not used such spyware against them. The applicants have filed lawsuits against the General Prosecutor's Office and the SSS for inaction and refusal to launch a criminal investigation. While some complaints are still pending before domestic courts at different instances, some have already reached the ECtHR.[59]

45. Recent reports have revealed that Pegasus has been used during the Armenia-Azerbaijan conflict. The phones of 12 people working in Armenia, including the spokesperson of the Armenian Foreign Ministry, a UN official and several Armenian civil society activists and journalists (most of whom had reported on the conflict), were allegedly infected with Pegasus between October 2020 and December 2022.[60] There is no evidence suggesting that Armenia has ever been a Pegasus user (see below, concerning the possible purchase of Cytrox's Predator). CitizenLab has identified a suspected Pegasus operator in Azerbaijan that could have reached targets in Armenia.

---

[52] Information I have received from Omnium Cultural. Particularly, the case of its former Vice-President Marcel Mauri, who has lodged a complaint with the Constitutional Court asking it to order the Supreme Court to grant him access to these documents.

[53] El govern espanyol nega espiar dos diputats d'ERC, però no desclassifica informació de Pegasus (elnacional.cat). The Government has however positively replied to the investigating judge's request to take oral evidence from the current President of the CNI. The Government had announced in 2022 that it would reform the legal framework of the CNI to strengthen its guarantees and submitted a new preliminary draft law on classified information (the current Law on official secrets dates from 1968).

[54] Spain closes Pegasus investigation over 'lack of cooperation' from Israel | Spain | The Guardian.

[55] See: Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 July 2021.

[56] https://forbiddenstories.org/journaliste/sevinc-vaqifqizi/.

[57] Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 July 2021.

[58] https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything. During our Committee hearing on "Threats to life and safety of journalists and human rights defenders in Azerbaijan" (April 2023), Ulvi Hasanli, founder and executive director of AbzasMedia, stated that he himself and current editor-in-chief had been tracked with Pegasus (declassified minutes).

[59] Information received in June 2023.

[60] https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

2.4.6. Cyprus

46. According to the EP, "Cyprus is an important European export hub for the surveillance industry and an attractive location for companies selling surveillance technologies". Tal Dilian, former member of the Israeli Defence Force, started a career as intelligence expert in Cyprus, where he launched Aveledo Ltd., later to be known as WS WiSpear Systems Ltd. He also launched Intellexa Alliance, a consortium of vendors of surveillance equipment. In 2019, Tal Dilian reportedly entered into a non-contractual arrangement with Hermes Airports to use his WiSpear equipment for the purpose of enhancing the Wi-Fi signal for passengers at Larnaca Airtport. It appears that the true reason for the agreement was to test WiSpear's interception technology. WiSpear was fined EUR 76 000 by the Assize Court on 22 February 2022 for illegal surveillance of private communications and data protection violations. The criminal charges against Tal Dilian and other WiSpear employees were dropped. Following this case, Mr Dilian moved Intellexa's operations to Greece, although he never left Cyprus.[61]

47. Although the Cypriot Government denies the export of Pegasus and the register of any NSO Group entity in Cyprus, NSO Group reports indicated that Cyprus had granted export licenses for its technology.[62] According to a document shared by with the European Parliament by the opposition party AKEL, the NSO Group has reportedly exported Pegasus through one if its subsidiaries in Cyprus to a company in the United Arab Emirates. In 2017, a meeting with NSO officials and Saudi Arabian customers took place in the Four Seasons Hotel in Limassol to present them with the latest capabilities of Pegasus. The Saudi Arabian clients immediately purchased it, one year before the killing of Jamal Khashoggi in the Saudi consulate in Istanbul and the alleged surveillance of persons close to him with Pegasus.[63]

48. According to the EP's PEGA Committee, "in practice it would seem that rules are easy to circumvent and there are close ties between politicians, the security agencies and the surveillance industry. It seems to be the lax application of the rules that makes Cyprus such an attractive place for trade in spyware."[64]

2.4.7. Other member States[65]

49. The Austrian Government stated that **Austria** has not been a client of NSO. However, its former Chancellor Sebastien Kurz has close ties to the founder of NSO Group, Shalev Hulio. In October 2022, they launched a cybersecurity firm called Dream Security. Moreover, a spyware company, Decision Supporting Information Research and Forensic (DSIRF) is based in Austria. In July 2022, Microsoft found that a software tool from DSIRF (called 'Subzero') was used to attack law firms, banks and strategic consultancies in Austria, the United Kingdom and Panama. Given the absence of an export licence for DSIRF, the Vienna Public Prosecutor's Office initiated a preliminary investigation. The software could have been used by a foreign actor, which would mean that export restrictions would have been violated by DSIRF. [66]

50. **Belgium** appears to be one of the 14 EU States which purchased Pegasus. A former Israeli intelligence official revealed that the Belgian police uses Pegasus in its operations. In September 2021, the Minister of Justice mentioned that Pegasus could be used in a legal way, bud did not confirm whether the Belgian services were a client of NSO. Persons targeted by Pegasus on Belgian territory (most likely by third countries) include former Prime Minister and current President of the European Council Charles Michel as well as his father Louis Michel; El Mahjoub Maliha, human rights defender from the Western Sahara; Carine Kanimba, daughter of a Rwandan political activist; current EU Commissioner for Justice Didier Reynders as well as EU Commission staff members.[67]

51. In **Bulgaria**, national authorities deny having granted export licenses to the NSO Group or its subsidiaries. However, NSO Group reports indicate that NSO products are or have been exported from both Cyprus and Bulgaria.[68] According to media reports, some of the servers of the network structure over which Pegasus attacks are conducted are located in a Bulgarian data centre owned by a Bulgarian company in turn

[61] PEGA Committee Report, pars. 268-280.
[62] NSO Group, Transparency and Responsibility Report, 30 June 2021, p. 4: https://www.nsogroup.com/governance/transparency/, p. 4.
[63] PEGA Committee Report, pars. 285-286. This is disputed by NSO.
[64] PEGA Committee Report, par. 302.
[65] Only member States in respect of which there have been allegations concerning the use of Pegasus or similar spyware by state authorities or third countries, the effective purchase or export of such spyware, or the register of spyware companies. I have excluded those which showed interest in purchasing or using spyware, but were ultimately refused to do so (see: Israel Blocked Sale of Pegasus Spyware to Ukraine and Estonia - The New York Times (nytimes.com)).
[66] PEGA Committee Report, pars. 403-405, 509-512.
[67] PEGA Committee Report, pars. 360-361 and 411.
[68] NSO Group, Transparency and Responsibility Report, 30 June 2021, p. 4, cited above.

owned by the NSO Group, Circle Bulgaria. From Bulgaria, this company provides the Cypriot subsidiaries with research and development services and exports products to governments. The Sofia City Prosecutor's Office is investigating whether state services have illegally used Pegasus against Bulgarian citizens.[69]

52. In **France,** the Pegasus Project revealed several cases of attempted hacks by Pegasus, including of President Macron. Traces of Pegasus infections were confirmed on the phones of five ministers and one member of Parliament, the director of Parisian radio station TSF Jazz Bruno Delport, investigative journalists Edwy Plenel and Lénaïg Bredoux, as well as lawyers and relatives of Saharawi activists. In most cases, Morocco seemed to be behind the attacks.

53. At the same time, France is home to different spyware companies, such as Nexa Technologies (part of Tal Dilian's Intellexa Alliance) and Amesys. In July 2021, following several complaints by human rights organisations, four executives of Amesys and Nexa Technologies were indicted over the sale of surveillance technology to the governments of Libya (under the Gaddafi regime) and Egypt. It is unknown if export licences were granted for the export of spyware to these countries.[70]

54. In **Germany**, media reported that the German Federal Criminal Police Office (BKA) had acquired a modified version of Pegasus (with access only to live communications, for it to be compliant with German law) in late 2020. According to media, the Vice-President of the BKA confirmed the purchase during an *in camera* meeting of the Interior Committee of the Bundestag and that it had been used since March 2021. The German foreign intelligence service also bought a modified version of Pegasus. The information regarding these operations remains classified. Before the Pegasus revelations, both the BKA and Berlin Police LKA purchased FinSpy from FinFisher (based in Munich) in 2012 and 2013, also in a modified version with access only to live communications. Former FinFisher executives have been charged by the public prosecutor's office in Munich for exporting surveillance technology to Türkiye without an export licence. FinFisher has declared insolvency and its operations have now ceased. More recently, it has been reported that the Government (through the Central Office for Information Technology in the Security Sector: ZITiS) had been in contact with other spyware companies (Italian RCS Lab, Austrian DSIRF, Candiru, Intellexa or Cytrox), although it has not been confirmed whether any additional spyware was actually acquired.

55. With regard to **Italy,** no reports on the possible purchase or use of spyware by the authorities have been published. However, spyware companies such as Tykelab and RCS Lab are based in Italy. Hacking Team, now called Memento Labs, exported RCS spyware to authoritarian countries.[71]

56. In the **Netherlands**, the media reported in June 2022 that the Dutch intelligence service used Pegasus when it assisted the police in tracking down a high-profile suspect of multiple murders related to organised crime, Ridouan Tagh. The Dutch Government refused to comment. Other media reports have revealed that in 2019 the Dutch Ministry of Defence was about to sign an agreement with WiSpear, the company owned by Tal Dilian. But it has not been confirmed whether the contract was signed or if any spyware was acquired.[72]

57. Relevant connections with the spyware industry exist in **Luxembourg, Ireland, Malta** and the **Czech Republic.** Luxembourg hosts nine entities directly related to NSO Group, although the Foreign Minister confirmed that none of them had been authorised to export surveillance products from Luxembourg. In October 2021, Prime Minister Xavier Bettel confirmed however that Luxembourg bought and used Pegasus 'for reasons of state security'. Ireland hosts some of the spyware companies mentioned (Intellexa and Thalestris Limited, its parent company), allegedly due to its favourable fiscal laws. Several figures from the spyware trade, including Tal Dilian, have acquired Maltese passports. And the home of the annual European fair of the spyware industry, the ISS World "Wiretappers Ball", is in Prague.[73]

58. According to CitizenLab report, likely Predator customers were found in **Armenia**. It appears that Government-backed actors purchased Cytrox products.[74]

59. **Romania** purchased FinFisher spyware, like other EU countries (Belgium, the Czech Republic, Estonia, Germany, Hungary, Italy, the Netherlands, Slovakia, Slovenia and Spain). Black Cube was involved in a hacking scandal: the heads of the company admitted to spying on the former chief prosecutor of Romania's National Anti-Corruption Directorate Laura Kövesi; former Romanian agent Daniel Dragomir was allegedly the

[69] PEGA Committee Report, pars.409-410.
[70] PEGA Committee Report, pars. 376-390.
[71] PEGA Committee Report, pars. 400-402.
[72] PEGA Committee Report, pars. 354-359.
[73] PEGA Committee Report, pars. 370-375, 391-399.
[74] https://carnegieendowment.org/programs/democracy/commercialspyware.

person who commissioned the job. Some other spyware companies (Cognyte, QuaDream) reportedly operate from Romania.[75]

60. According to some reports, **Serbia** has been a client of Circles Technologies (owned by the NSO Group), Predator, Cognyte and FinFisher[76]

61. Subsidiaries of the company Thalestris, parent company of Intellexa Alliance, are located in **Switzerland**. DigiTask (Germany) sold spyware to Swiss authorities, according to information disclosed in 2011.[77]

62. **Türkiye** used FinSpy from FinFisher in 2017. The software was disguised as a downloadable app recommended to participants in anti-government demonstrations.[78] German prosecutors have charged four former company executives with illegally selling software to Türkiye's secret services.

63. According to CitizenLab, phones of **UK** Government officials, including from the Prime Minister's Office and the Foreign and Commonwealth Office, were infected with Pegasus in 2020-2021. The suspected infections relating to the Foreign Office were associated with Pegasus operators linked to third countries, including the United Arab Emirates, India, Cyprus and Jordan.[79]

3. Relevant legal standards

3.1. The European Convention on Human Rights

64. Targeted secret surveillance, including intercepting mobile-telephone communications, is an interference with the right to respect for private life and correspondence enshrined in Article 8.1 of the **European Convention on Human Rights** (ETS No.5, "The Convention").[80] According to the case-law of the European Court of Human Rights ("the Court"), secret surveillance of an individual can only be justified under Article 8.2 if it is "in accordance with the law", pursues one or more of the "legitimate aims" to which this paragraph refers (among which the prevention of disorder or crime and the protection of national security and public safety), and is "necessary in a democratic society" in order to achieve such aims.[81]

65. As to the first requirement, this means that the surveillance must have some basis in domestic law and that the law must be accessible to the person concerned and foreseeable as to its effects. The law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret measures of surveillance. In its case-law on such measures, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of the measure; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.[82] The Court has confirmed that these minimum safeguards apply in cases where the interception was for the purposes of preventing or detecting criminal offences, but also in those where the measure was ordered on national security grounds.[83] It has however admitted that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By their very nature, threats to national security may vary in character and may be unanticipated or difficult to define in advance.

[75] PEGA Committee Report, pars. 473, 487, 495, 513.
[76] PEGA Committee Report, pars. 287 and 483; https://carnegieendowment.org/programs/democracy/commercialspyware.
[77] PEGA Committee Report, par. 487; https://carnegieendowment.org/programs/democracy/commercialspyware.
[78] PEGA Committee Report, par. 514.
[79] https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/.
[80] The interference can also be with the right of a third party whose communications with the targeted individual have been intercepted (see *Lambert v. France,* Application No. 23628/94, judgment of 24 August 1998, paragraph 21). The mere collection and storing of data by security services on particular individuals, including the person's whereabouts and movements in the public sphere, also constitute an interference with private life (see *Shimovolos v. Russia,* Application No. 30194/09, judgment of 21 June 2011, paragraph 65).
[81] European Court of Human Rights, *Roman Zakharov v. Russia,* Application No. 47143/06, judgment of 4 December 2015 (Grand Chamber), paragraph 227. See Case-Law Guide on Article 8 of the Convention, 2022.
[82] Ibid., paragraphs 228-231, with further references therein.
[83] Ibid., paragraphs 231 and 246-248; *Big Brother Watch and Others v. the United Kingdom,* Applications Nos. 58170/13 and Others, judgment of 25 May 2021 (Grand Chamber).

The law must at least indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity.[84]

66. The second condition for an interference to be justified under Article 8.2 is that the measure shall be "necessary in a democratic society" in the interest of one of the stated goals in this paragraph (national security, public safety, the prevention of disorder or crime, etc.). The powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions.[85] Moreover, the measure must be strictly necessary for the obtaining of vital intelligence in an individual operation. In order to ensure that secret surveillance measures are applied only when "necessary in a democratic society", the Court must also be satisfied that there are adequate and effective guarantees against abuse. This implies assessing *inter alia* the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, as well as any notification mechanisms and remedies provided for by national law.[86]

67. As regards authorisation procedures, although prior judicial authorisation may be an important safeguard against indiscriminate surveillance, the Court also scrutinises its scope of review (whether the judge applies a "necessity" or "proportionality" test) and the content of the interception authorisation (i.e. mentioning specific persons or premises). The authorisation authority must indeed be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance, such as, for example, acts endangering national security.[87] As regards review and supervision, it is in principle desirable to entrust supervisory control to a judge, as judicial control offers the best guarantees of independence and impartiality as well as a proper procedure. However, supervision by non-judicial bodies may also be considered Convention-compliant if the supervisory body is independent of the authorities carrying out the operation and is vested with sufficient powers to exercise an effective and continuous control. [88] Applying these principles, the Court found in *Szabó and Vissy v. Hungary*[89] that the authorisation and supervision of secret surveillance measures by the Minister of Justice (without judicial prior authorisation) was inherently incapable of ensuring the requisite assessment of strict necessity. For the Court, supervision by a politically responsible member of the executive did not provide the necessary guarantees. Moreover, where a supervising judge or court adopts a passive attitude and merely endorses, without genuinely checking the facts, the actions of security services, such supervision is not compatible with Article 8.[90]

68. After the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and is able to challenge their legality retrospectively, unless any person who suspects that his communications are being or have been intercepted can apply to courts, so that the court's jurisdiction does not depend on notification to the interception subject. Information should however be provided in principle to the subject after the termination of the surveillance measures "as soon as notification can be carried out without jeopardising the purpose of the restriction".[91]

---

[84] *Roman Zakharov v. Russia,* paragraph 247. In this case, the Court criticised the fact that the law in question left the authorities an almost unlimited degree of discretion in determining which events or acts constituted a threat and whether that threat was serious enough to justify secret surveillance.

[85] *Klass and Others v. Germany,* Application No. 5029/71, judgment of 6 September 1978, paragraph 42.

[86] *Roman Zakharov v. Russia*, paragraphs 235-238.

[87] Ibid., paragraphs 257-267. In this case, the Court criticised a system which allowed the secret services and the police to intercept directly the communications of any citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else (paragraph 270). The Court concluded that the abusive surveillance practices indicated by the applicant appeared to be due to the inadequate safeguards provided by the Russian legislation, which did not meet the requirements of Article 8 (paragraphs 303-304). See also *Ekimdzhiev and Others v. Bulgaria,* Application No. 70078/12, judgment of 11 January 2022, where the Court took issue with the fact that Bulgarian courts issuing surveillance warrants gave no reasons at all or gave blanket and generalised reasons (paragraphs 307-322).

[88] Ibid., paragraphs 233 and 275.

[89] *Szabó and Vissy v. Hungary,* Application No. 37138/14, judgment of 12 January 2016, paragraphs 75-77. The execution of this judgment is still under supervision by the Committee of Ministers (enhanced procedure); the government has recognised that legislative amendments are required (see Interim Resolution by the Committee of Ministers of 9 March 2023: https://hudoc.echr.coe.int/eng?i=001-223725).

[90] See, for instance, *Zoltán Varga v. Slovakia,* Application No. 58361/12 and 2 others, judgment of 20 July 2021, paragraphs 155-163.

[91] *Roman Zakharov v. Russia*, paragraphs 234 and 287. In this case, the absence of a notification requirement or any other possibility of requesting and obtaining information about interceptions undermined the effectiveness of the applicable remedies. By contrast, in *Kennedy v. the United Kingdom,* judgment of 18 May 2010, since the jurisdiction of the courts

69. The Court has found violations of Article 8 in cases concerning secret surveillance of human rights activists,[92] members of non-governmental organisations,[93] lawyers,[94] and journalists,[95] among others.

70. With regard to journalists, targeted surveillance measures with a view to discovering their journalistic sources may also infringe their right to freedom of expression, as guaranteed by Article 10 of the Convention, in the absence of adequate safeguards in the law[96] or any overriding requirement in the public interest justifying such measures in the concrete case.[97] The Court has constantly held that the right of journalists to protect their sources is part of the freedom to "receive and impart information and ideas without interference by public authorities" protected by Article 10 and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest. An interference potentially leading to disclosure of a source cannot therefore be considered "necessary" under Article 10 unless it is justified by an overriding requirement in the public interest.[98]

71. Lawyer-client communication is especially protected under Article 8 of the Convention. In principle, oral communication as well as correspondence between a lawyer and his/her client is privileged and must remain confidential. It is also an important safeguard of the right to defence and the right to a fair trial guaranteed by Article 6.[99] The use of spyware also has adverse consequences on the exercise of other Convention rights, particularly by human rights defenders and political activists, including the right to freedom of assembly and association (Article 11), the right to participate in free elections (Article 3 of Protocol No. 1), and in the most extreme cases, the right to physical and mental integrity and the right to life (Articles 2 and 3).

72. Whether the reported cases of Pegasus infections described in the section above breached the Convention rights and in particular the right to respect for private life will have to be determined by the different national courts seized and ultimately by the European Court of Human Rights. Some individual cases have already been lodged with the Strasbourg Court. Although there has not yet been any decision or case-law on the use of Pegasus, the use of this or similar spyware by state authorities raises new issues in terms of human rights implications. Giving access to all the contents and features of a smartphone (location, phone calls, text and voice messages, emails, photos, videos, passwords, web browsing history, or the possibility to remotely use the camera and microphone in real time) leads to an unprecedented level of intrusiveness. It reveals the most sensitive information (including health, sexual life, political opinions, religious or other beliefs) not only about the targeted individuals but also their family, colleagues, friends, clients, etc. In this connection, the European Data Protection Supervisor, in his preliminary remarks published on 15 February 2022, stated that given the level of interference with the right to privacy and the difficulty in meeting the requirements of proportionality, the regular deployment of Pegasus or similar highly intrusive spyware technology would not be compatible with the EU legal order. He therefore proposed a ban on the development and the deployment of such spyware in the EU and, in the alternative (if such tools are nevertheless applied in exceptional situations), some measures to prevent unlawful use (strengthening the oversight of surveillance measures, full implementation of EU privacy and data protection law, judicial review, no politically-motivated abuse of the national security exception, etc.).[100] The Council of Europe Commissioner for Human Rights also expressed

---

did not depend on the notification to the interception subject, the absence of notification was found to be compatible with the Convention.

[92] *Shimovolos v. Russia,* Application No. 30194/09, judgment of 21 June 2011.

[93] *Case of Association "21 December 1989" and Others v. Romania,* Application No. 33810/07, judgment of 24 May 2011.

[94] *Vasil Vasilev v. Bulgaria,* Application No. 7610/15, judgment of 16 November 2021. The Court has constantly held that Article 8 affords strengthened protection to lawyer-client communications, the interception of which may also have implications for the Article 6 (fair trial) rights of the lawyer's client.

[95] *Azer Ahmadov v. Azerbaijan,* Application No. 3409/10, judgment of 22 July 2021.

[96] *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands,* Application No. 39315/06, judgment of 22 November 2012, paragraphs 84-102: no prior review by an independent body with the power to prevent or terminate the measure. The Court has recently identified criteria concerning the protection of journalistic material under Article 10 when it comes to bulk interception regimes, distinguishing between intentional access and unintentional access to such material (*Big Brother Watch and Others v. the United Kingdom*, paragraphs 447-450; as regards the difference between targeted interception and bulk interception, see paragraphs 343-347).

[97] *Sedletska v. Ukraine,* Application No. 42634/18, judgment of 1 April 2021, paragraphs 64-73, concerning access to a journalist's communications data stored by her mobile telephone operator. In this case, the Court interestingly indicated to the Government, under Rule 39 of the Rules of the Court and during the Strasbourg proceedings, that they should ensure that the public authorities abstain from accessing any of the data specified in the order issued by the investigating judge concerning the applicant.

[98] *Sanoma Uitgevers B.V. v. the Netherlands,* Application No. 38224/03, judgment of 14 September 2010 (Grand Chamber), paragraphs 50-51.

[99] *Altay v. Turkey (no. 2),* Application No. 11236/09, judgment of 9 April 2019, paragraphs 49-50.

[100] See European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 February 2022, https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.

serious doubts as to the compatibility of the use of Pegasus or similar spyware with the case-law of the Court, given its level of intrusiveness.[101] In any event, and irrespective of the proportionality assessment on the use of such spyware in each individual case, the Court will first have to examine the quality of the legislative framework concerned, as it often does in surveillance cases under Article 8. According to different studies, the legislative framework of some of the countries that have used Pegasus is weak or inefficient, particularly with regard to *ex ante* and *ex post* oversight mechanisms, as well as remedies.[102] In some cases, the shortcomings have already been identified by the Court in previous cases of surveillance unrelated to Pegasus (Hungary, e.g. lack of notification requirement after the termination of the surveillance[103] and limited oversight powers of the Data Protection Authority[104]). In others (Poland, Greece), these studies have led the PEGA Committee and the European Parliament to identify gaps that appear to raise concerns with regard to Convention standards. For instance, in Greece, a legislative amendment in 2021 abolished the ability of the ADAE to notify citizens of the lifting of the confidentiality of communications. As for Poland, the Venice Commission found that the 2016 Police Act regulating the surveillance of citizens (still in force) did not contain sufficient safeguards to prevent abuse.[105]

3.2. Other Council of Europe standards

73. The 1981 **Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (ETS No. 108), the only legally binding international instrument in the data protection field with global relevance (ratified by 55 Parties, including 9 non-Council of Europe members), grants additional protection for any data processing carried out by the private and public sector, including data processing by judicial and other enforcement authorities. However, States may make declarations aimed at excluding from the scope of the Convention certain types of data processing (e.g. national security and defence purposes).[106] As recalled by Ms Kaldani, Vice-chairperson of the Consultative Committee of the Convention, during the hearing of 14 September 2021, the **modernised Convention 108+** (Protocol CETS No. 223, opened for signature on 10 October 2018 and not yet into force[107]) removes this possibility. The modernised Convention also establishes stronger requirements regarding the lawfulness of the processing, proportionality, and data minimisation, recalling that data processed should be adequate, relevant and not excessive in relation to the purposes for which they are processed.[108] It provides individuals with stronger rights and imposes greater transparency requirements,[109] which may however be restricted when this is prescribed by law, respects the essence of the fundamental rights and freedoms, and constitutes a necessary and proportionate measure in a democratic society for "essential objectives of general public interest", including the protection of national security, defence, public safety or the prevention, investigation and prosecution of criminal offences.[110] Convention 108+ also reinforces investigative and corrective powers and the independence of data protection authorities. It does however allow for a limited number of exceptions in the area of national security and defence, as long as they are provided by law and are necessary in a democratic society.[111] In any event, the processing activities for national security and defence purposes must be subject to independent and effective review and supervision under domestic law.[112]

---

[101] Human Rights Comment, "Highly intrusive spyware threatens the essence of human rights", 27 January 2023.
[102] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, February 2023, "The use of Pegasus and equivalent surveillance spyware": https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf. For a detailed overview of recent legislative reforms in the area of intelligence services, particularly with regard to oversight mechanisms and remedies, see European Union Agency for Fundamental Rights (FRA), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – 2023 update.
[103] *Szabó and Vissy v. Hungary,* Application No. 37138/14, judgment of 12 January 2016.
[104] *Hüttl v. Hungary,* Application No. 58032/16, committee judgment of 29 September 2022.
[105] https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e.
[106] See Article 3.2. For example, the declaration by Andorra which excludes among others personal data relating to State security and to the investigation and prevention of criminal offences.
[107] To date, 27 States have ratified it. It is expected that the required number of ratifications for the entry into force (38) will be reached some time in 2024. See also Council of Europe, Information Society Department DGI(2022)04, Pegasus spyware and its impacts on human rights, June 2022.
[108] Article 5.
[109] Articles 8 and 9.
[110] Article 11.1.
[111] Articles 11.3 and 15.2, notably regarding the powers of investigation and intervention or the power to issue decisions with respect to violations of the Convention.
[112] Article 11.3. Ms Kaldani stated that there is a reflection within their committee to provide a document on the practical use of the data protection principles in the context of surveillance. It has also been argued that Convention 108+ does not fully and explicitly address some of the challenges posed in our digital era by unprecedented surveillance capacities and that stronger safeguards at international level (e.g. a comprehensive international human rights law instrument framing the operations of intelligence services) are needed. See in this regard the Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, "Better

74. The **Budapest Convention on Cybercrime** (ETS No. 185, also known as ″Budapest Convention″ or ″Cybercrime Convention″) was opened for signature in 2001 and has since then attracted membership from all regions of the world. It contains provisions on substantive criminal law and procedural law, as well as on international co-operation, in relation to computer-related crime. The notion of "computer system" defined in Article 1.a covers modern mobile telephones, smart phones, tablets or similar devices, which have the capacity to produce, process and transmit "computer data".[113] Among the abuses that the Convention requires States Parties to criminalise, those relevant for the present topic are "illegal access" (Article 2), "illegal interception" (Article 3) and "misuse of devices" (article 6). "Illegal interception" applies to all forms of electronic data transfer (e.g. by telephone), but the interception must be committed "intentionally" and "without a right". In this respect, the interception is justified if it is "lawfully authorised in the interests of national security or the detection of offences by investigating authorities".[114] The "misuse of devices" refers to the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the other offences; or of a computer password, access code or similar data by which the computer system is capable of being accessed. The Cybercrime Convention Committee (T-CY) has clarified that all forms of malware are covered by these provisions, depending on what the malware actually does.[115] The Budapest Convention could come to play in those cases where the interception using spyware was clearly not lawful under domestic law, in which case it could amount to "illegal interception" and should be criminalised.[116] Furthermore, the Budapest Convention contains specific provisions on interception of content data of communications ("in relation to a range of serious offences to be determined by domestic law") and related mutual assistance between States (Articles 21 and 34). The interception should in any case be subject to human rights safeguards, including those arising under the Convention and other international treaties, and in particular to the principle of proportionality, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such measure/power (Article 15).

75. The **Assembly's previous work** on this topic shows that it has always been in favour of maintaining the highest possible level of protection for privacy rights, both against targeted and mass surveillance. In this context, reference must be made to Resolution 1843 (paragraph 18) and Recommendation 1984 (2011) on the protection of privacy and personal data on the Internet and online media; Resolution 1986 (paragraph 6.1) and Recommendation 2041 (2014) ″Improving user protection and security in cyberspace" (paragraphs 2.1 and 2.9),[117] and Resolution 2256 (2019) "Internet governance and human rights" (paragraph 7).

76. In Resolution 2045 (2015) "Mass surveillance", adopted following the disclosures by Mr Edward Snowden about mass surveillance practices by the United States and certain Council of Europe member States, the Assembly urged member and observer States to: "ensure that national law allows the collection and analysis of personal data (…) only with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and treatment should be penalized in the same way as the violation of the traditional mail secret (…)"; "ensure, in order to enforce such a legal framework, that their intelligence services are subject to adequate judicial and/or parliamentary control mechanisms (…)"; "agree on a multilateral 'intelligence codex" for their intelligence services, which lays down rules governing co-operation for the purposes of the fight against terrorism and organised crime (…); and "refrain from exporting advanced surveillance technology to authoritarian regimes" (paragraph 17). In its Recommendation 2067 (2015) "Mass surveillance", the Assembly invited the Committee of Ministers to consider addressing a recommendation to member States on ensuring

protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services", 7 September 2020, at: https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb.

[113] T-CY Guidance Note #1 On the notion of "computer system", Article 1.a of the Budapest Convention on Cybercrime, December 2012: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6.

[114] Explanatory report to the Convention, § 58.

[115] T-CY Guidance Note #7, New forms of Malware, 5 June 2013: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b4. Malware has been defined by the Organisation for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners".

[116] The PEGA Committee noted, for instance, that infecting a device with spyware was a criminal offence under the Greek Criminal Code, as well as the production, sale, supply, use, importation, possession and distribution of malware, including spyware (PEGA Committee Report, par. 166).

[117] The Assembly invited the Committee of Minsters to consider the feasibility of drafting an additional Protocol to the Cybercrime Convention regarding serious violations of fundamental rights of users of online services. It also invited the CM, on the basis of evidence released by Edward Snowden about mass violations of the right to privacy under Article 8 of the Convention, to set up an action plan to prevent such violations.

the protection of privacy in the digital age and Internet safety in the light of the threats posed by the newly disclosed mass surveillance techniques, and further exploring Internet security issues related to mass surveillance and intrusion practices, with regard to the human rights of Internet users (paragraphs 2.1 and 2.2).

77. The **Committee of Ministers** has also adopted important texts in this field: the 2013 Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies; Recommendation No. R (87) 15 Regulating the use of personal data in the police sector; Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users (Appendix, §§ 65-85), and Recommendation CM/Rec(2016)5 on Internet freedom (Appendix, § 4.2).The CM has recalled that any measures in the interest of national security should rigorously meet the requirements set out in the Convention, in particular regarding Articles 8, 10 and 11. It has also underlined that member States have both negative obligations and positive obligations, which include the protection from arbitrary restrictions by non-State actors.[118]

78. Finally, the **Venice Commission** has established relevant standards with respect to security services. Its main focus has been on accountability, namely parliamentary and judicial accountability.[119]

3.3. Other international standards

79. On 28 May 2019, the **United Nations** Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression published a Report on Surveillance and human rights, which referred to the Pegasus spyware as an example of mobile device hacking used as a targeted surveillance tool in 45 countries. The report gives a general overview of State human rights obligations at the UN level that protect against targeted surveillance, among which Articles 12 (right to privacy) and 19 (freedom of expression) of the Universal Declaration of Human Rights, Articles 17(1) (right to privacy) and 19 (freedom of expression) of the International Covenant on Civil and Political Rights (ICCPR). In addition to the primary obligations not to interfere with these rights, States have positive duties to protect individuals against third-party interference, including with regard to transnational surveillance committed by foreign entities against one's own citizens. The report also refers to the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework adopted by the Human Rights Council in 2011, which are relevant both for States and for the private surveillance industry (human rights due diligence processes, remediation, etc.). In terms of export control, reference is made to the non-binding Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Participating States to this arrangement are expected to apply export controls to all items on the list of dual-use goods and technologies, which includes items related to "intrusion software" and Internet Protocol network communications surveillance systems since 2013. The UN Special Rapporteur regrets however that the arrangement lacks guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools.[120]

80. With respect to **European Union legislation**, apart from the Charter of Fundamental Rights (Articles 7, 8, 11, 41, 42, 47 and 52(1)[121]) the e-Privacy Directive,[122] and the Law Enforcement Directive,[123] it is worth mentioning the EU Dual-Use Regulation (recast), which has introduced new export controls for "cyber-surveillance items", where there is a risk of them being used in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.[124] The EP, in its 15 June 2023 Recommendation on the Pegasus inquiry, concluded for instance that there was evidence of "maladministration in the implementation of the EU Dual-Use Regulation in Cyprus", on the basis of reports that showed that Cyprus had become an export hub for spyware to repressive third countries.

---

[118] See Reply to Recommendation, Doc. 13911, 14 October 2015.
[119] European Commission for Democracy Through Law (Venice Commission), Report on the Democratic Oversight of the Security Services, adopted in June 2007 and updated in March 2015, at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e.
[120] A/HRC/41/35: Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression | OHCHR
[121] Right to respect for private and family life; protection of personal data; freedom of expression and information; right to good administration; right of access to documents; scope of guaranteed rights/limitations.
[122] OJ L 201, 31/07/2002, p. 37-47.
[123] Directive EU 2016/680 of 27 April 2016, OJ L 119, 04/05/2016, p. 89-131, Article 30.1. This Directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Article 1.1), an area which is excluded from the scope of the General Data Protection Regulation (GDPR).
[124] OJ L 206, 11/06/2021, p. 1-461.

4. The way ahead: proposals to prevent the abuse of spyware and better address its impact on human rights

81. Following the Pegasus revelations, different international actors have made proposals to prevent the abuse of spyware and better address the human rights risks that it poses.

82. On 27 January 2023, on the occasion of European Data Protection Day, the **Council of Europe Commissioner for Human Rights** published a Human Rights Comment entitled "Highly intrusive spyware threatens the essence of human rights". The Commissioner observed that 18 months after the disclosure of the leak of over 50,000 phone numbers that had been identified as potential targets for surveillance through the Pegasus spyware, human rights activists, journalists, and opposition politicians continued to be targeted with powerful zero-click hacking tools that procured complete and unrestricted access to their private lives, putting their personal safety and access to basic human rights at risk. While welcoming the ongoing inquiries into the export, sale, transfer, and use of highly intrusive spyware such as Pegasus, the Commissioner called on member States to take action to prevent further abuse, to impose a strict moratorium on the export, sale, transfer and use of zero-click spyware tools such as Pegasus, and to put in place a comprehensive and human rights compliant legislative framework for the use of modern surveillance technology. This should provide for meaningful procedural guarantees, robust systems of ex-ante and ex-post oversight, and effective redress mechanisms for victims. The Commissioner further reflected on the need for more public awareness of the rampant threat to human rights, including the rights to privacy, freedom of expression and public participation, stemming from an uncontrolled spyware industry and the opaque operations of national security services.

83. The **UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression** proposed (in 2019 a legal and policy framework for regulation, accountability and transparency within the private surveillance industry, in order to improve compliance with international standards and address the gaps in implementation. He called for tighter regulation of exports of surveillance equipment and regulations on their use, as well as for an immediate moratorium on the export, sale, transfer, use or servicing of surveillance tools until the use of those technologies could be technically restricted to lawful purposes that are consistent with human rights, or until it could be ensured that those technologies will only be exported to countries in which their use is subject to authorisation granted in accordance with due process and the standards of legality, necessity and legitimacy by an independent and impartial judicial body. States participating in the Wassenaar Arrangement should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the UN Guiding Principles on Business and Human Rights.[125]

84. The former **United Nations High Commissioner for Human Rights**, Ms Bachelet, expressed the view that until compliance with human rights standards can be guaranteed, governments should implement a moratorium on the sale and transfer of surveillance technology.[126] A recent report prepared by the Office of the UN High Commissioner for Human Rights, apart from reiterating previous calls to implement a moratorium on the (domestic and transnational) sale and use of surveillance systems, recommends that hacking of personal devices be employed only as a measure of last resort, to prevent or investigate a specific act amounting to a serious threat to national security or a specific serious crime, and narrowly targeting the suspect; such measures should also be subject to strict independent oversight and should require prior approval by a judicial body.[127]

85. The **European Parliament**, in its June 2023 Recommendation following its inquiry into the use of Pegasus, has made important recommendations to EU member States, EU institutions and other relevant actors. Apart from addressing specific recommendations to the main EU member States concerned (Poland, Hungary, Greece, Spain and Cyprus), particularly with regard to their legislative framework and investigations, it calls for the "adoption of conditions for the legal use, sale, acquisition and transfer of spyware" and sets a deadline for all member States (end of 2023) to fulfil four conditions in order to be allowed to continue using spyware. These conditions are the following: a) investigation and resolution of spyware abuse cases without delay; b) alignment of the national legal framework with the standards of the Venice Commission, the CJEU

[125] OHCHR | The Special Rapporteur's 2019 report to the United Nations Human Rights Council, 2019; and "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech", 12 August 2021. See also OHCHR, Report: *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, 24 June 2020, §§ 24-40; and Report: *The right to privacy in the digital age*, 30 June 2014. See UN General Assembly resolution 73/179 of 17 December 2018.

[126] Statement during the exchange of views held by the Committee on 14 September 2021. See: OHCHR | Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe
 Hearing on the implications of the Pegasus spyware. See also: OHCHR | Use of spyware to surveil journalists and human rightsdefenders
Statement by UN High Commissioner for Human Rights Michelle Bachelet, 19 July 2021.

[127] A/HRC/51/17 (undocs.org), 4 August 2022.

and the ECtHR; c) explicit commitment to involve Europol in their investigations; and d) repeal of export licenses that are not compliant with the Dual-Use Regulation. The fulfillment of these conditions should be assessed by the EU Commission by 30 November 2023. Regarding long-term action, the EP considered that owing to the EU dimension of the use of spyware (judicial cooperation in criminal matters and internal market), there is a need for common EU standards that should regulate and limit the use of spyware. For instance, the authorisation for the use of spyware should only be granted in exceptional cases with respect to investigations into a "limited and closed list of clearly and precisely defined serous crimes that represent a genuine threat to national security". Other recommendations by the EP include, *inter alia*:

- Ratification by all member States of the Council of Europe Convention 108+ and immediate application of its standards in national law, and accession by the EU itself ;
- Additional European legislation that would require corporate actors producing and/or exporting surveillance technologies to include human rights and due diligence frameworks, in line with the UN Guiding Principles on Business and Human Rights;
- Involvement of Europol in investigations into allegations of spyware abuses, including by proposing to the national authorities to initiate, conduct or coordinate an investigation;
- Better implementation and enforcement of EU export rules to avoid "export regime shopping";
- Better management of EU development aid to prevent potential abuse of surveillance technology by third countries;
- Creation of a EU Tech Lab that would be tasked with discovering and exposing the unlawful use of software for illicit surveillance purposes, and providing technical support to individuals by detecting spyware traces in their devices;
- Integration of EU member States' unlawful use of spyware in the EU Commission's rule of law reports.

86. NGOs and civil society have also made proposals for further regulation in this area, calling for an immediate moratorium on the sale, transfer and use of spyware until such a regulatory framework is put in place.[128] Some have criticised that the EP recommendations did not go far enough. For instance, the fact that there are still doubts as to whether the legal use, sale, acquisition and transfer of spyware will effectively continue while the evaluation of the four conditions is carried out by the EU Commission, that there is no enforcement action foreseen in case of non-compliance of these conditions, or simply that that the EP has not called for a total ban on the use of this intrusive form of spyware.[129]

5. Conclusions

87. The Pegasus revelations and subsequent investigations have provided evidence that Pegasus and similar spyware (e.g. Candiru, Predator) has been used as a hacking and surveillance tool against journalists, lawyers, politicians and human rights activists in several Council of Europe member States and beyond. Given the unprecedented level of intrusion of this software, which grants unauthorised ("zero-click") and unrestricted remote access to the mobile phone and all its personal and private data, its use has serious implications for fundamental human rights of the persons targeted and all their contacts, including their right to privacy and their right to freedom of expression, as well as more generally for media freedom and democratic institutions. It has been argued that its very use could hardly ever meet the requirements of proportionality that any interference with those rights should fulfil, having regard precisely to its level of intrusiveness and stealth. I tend to agree with those who have voiced these concerns, including the Council of Europe Commissioner for Human Rights and the European Data Protection Supervisor. In any event, national investigative authorities and courts of the countries concerned must still shed more light on whether these highly intrusive interferences with the rights of the individuals concerned pursued a legitimate aim (national security, prevention of crime) or were mainly based on political considerations, and on whether they were necessary and proportionate to achieve that aim in the specific case, as required by Convention and other international standards. Spying on politicians, journalists and human rights defenders for purely political purposes clearly does not comply with Council of Europe values, human rights, rule of law and democratic principles. It does not only have a chilling effect on the exercise of fundamental rights by civil society actors, politicians and journalists, but also affects the essence and integrity of electoral processes and public debate. Victims should have access to effective remedies in all cases of unlawful targeted surveillance, which presumes having access to the relevant

[128] Amnesty International, 2021: Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector - Amnesty International ; Geneva Declaration on Targeted Surveillance and Human Rights, September 2022: The Geneva Declaration on Targeted Surveillance & Human Rights (accessnow.org).

[129] EU: 'Greater steps' needed to protect rights after EU Parliament suggests regulating spyware - Amnesty International ; PEGA Committee does not go all the way on spyware regulation - European Digital Rights (EDRi). A previous draft of EP recommendation by the rapporteur Sophie in' t Veld included a call for the immediate adoption of a conditional moratorium, that should be lifted on a country-by-country basis if the four conditions were met.

information once the surveillance measure has been terminated. However, in many of the countries concerned, victims have faced obstacles in proving that their devices were infected or targeted, partly because of the lack of transparency and cooperation from national authorities, which invoke reasons of secrecy and national security. The legislative frameworks and oversight systems on surveillance activities in some member States are weak or inefficient, and there is a clear need for stronger regulation and safeguards and better implementation and monitoring.

88. The Parliamentary Assembly should address specific recommendations to the member States that have acquired and used Pegasus or equivalent spyware, including Poland, Hungary, Greece and Spain. It should also address general recommendations to all member States, many of which have used or still use similar spyware, drawing from standards laid down by the ECtHR in this area. States should refrain from using spyware unless their legislative framework, oversight mechanisms and system of remedies are fully in line with those standards. In this respect, the Assembly should invite all member States to report to the relevant Council of Europe bodies (be it the Committee of Convention 108+ once the amending protocol enters into force, or the Venice Commission) on whether their regulatory frameworks and implementation is in line with the Council of Europe standards and to share their best practices. Until such an assessment is made, member States should apply an immediate moratorium on the acquisition and use of highly intrusive spyware tools such as Pegasus. The Committee of Ministers should also be invited to draft a recommendation to member States on surveillance and human rights, with a specific focus on the acquisition, use, export and transfer of spyware, taking due account of all Council of Europe and international legal standards. All these standards would benefit from being brought together in a consolidated form for clarity purposes. This recommendation would also codify the highest standards in this field, drawing for instance from existing UN and Council of Europe texts on human rights and business (Recommendation CM/Rec(2016)3) and adapting them to the context of the spyware industry. At a later stage, the Committee of Ministers could examine the feasibility of drafting a new Council of Europe Convention on the acquisition, use, export and transfer of spyware, with a monitoring mechanism.