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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Declassified*
AS/Jur (2022) 04
8 April 2022
ajdoc04 2022

Committee on Legal Affairs and Human Rights

Pegasus and similar spyware and secret state surveillance

Introductory memorandum

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

1. Introduction

1. The present introductory memorandum 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 recommendation recalls 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 proposal calls 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 this introductory memorandum, I will set out the factual background of the future report concerning the allegations of misuse of Pegasus and similar spyware, based on information from existing public sources; summarise the reactions; provide an overview of relevant Council of Europe and other international standards; and make proposals for further work on the final report.

2. The Pegasus revelations

2.1. The Pegasus spyware

4. 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

* Document declassified by the Committee on 4 April 2022.

[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): see minutes.

or emails that trick a target into clicking on a malicious link.[2] 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 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.[3]

5. 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,[4] as well as gather information from apps including but not limited to communications apps iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram and Skype.[5] 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.[6] In a way, the eavesdropping party can know more than the owner of the phone.

6. 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.[7]

7. NSO Group claims that Pegasus is not a mass surveillance tool, and 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 in its usage.[8] 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.[9]

8. NSO Group reports suggest that Cyprus and Bulgaria had granted export licenses for its technology.[10] However, both Cypriot and Bulgarian authorities have denied issuing export licenses for NSO.[11]

2.2. Early allegations concerning the misuse of Pegasus

9. 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.[12]

---

[2] See: What is Pegasus spyware and how does it hack phones? | Surveillance | The Guardian, 18 July 2021.
[3] Ibid.
[4] See: https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html, 25 August 2016.
[5] 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.
[6] 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
[7] 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.
[8] NSO Group, Transparency and Responsibility Report, 30 June 2021, pp 6-7: https://www.nsogroup.com/governance/transparency/
[9] Ibid. pp. 29-30.
[10] Ibid. p. 4.
[11] https://www.europarl.europa.eu/doceo/document/E-9-2020-005505-ASW_EN.html; http://altanalyses.org/en/2021/07/27/the-pegasus-scandal-9-questions-and-some-answers/?utm_source=rss&utm_medium=rss&utm_campaign=the-pegasus-scandal-9-questions-and-some-answers. It appears that the company Circles operating in Bulgaria is part of NSO Group, but that the Bulgarian office is not tasked with the development of Pegasus. Circles is reportedly known for development of another software used for tapping phone calls.
[12] See: https://www.bbc.com/news/technology-37192670, 26 August 2016.

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.[13]

10. 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.[14]

11. 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.[15]

2.3. "The Pegasus Project" revelations

12. 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.[16]

13. 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 journalists from 24 countries.[17] 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.[18]

14. According to the investigation, 48 journalists were among those possibly targeted with Pegasus in **Azerbaijan**.[19] These included Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, whose phone had been infected over a two-year period until May 2021, and Khadija Ismayilova, an investigative journalist at the Organized Crime and Corruption Reporting Project, whose phone had been regularly infected for nearly three years.[20] Some reports referred to civil society activists, such as Fatima Movlamli, a female activist whose intimate photographs had been leaked on Facebook in 2019.[21]

15. In **Hungary,** phone numbers of at least 10 lawyers and 5 journalists, and an opposition politician were included on the leaked list of potential Pegasus targets.[22] The phones of Szabolocs Pany and András Szabo, both investigative journalists for Direkt36, had been 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 soon after comment requests by him to

[13] 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.
[14] 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.
[15] See: Phone of top Catalan politician 'targeted by government-grade spyware' | Catalonia | The Guardian, 13 July 2020.
[16] 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.
[17] See: https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/, 18 July 2021.
[18] See: Heads of state found on list of numbers examined by Pegasus Project - The Washington Post, 20 July 2021.
[19] See: Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 July 2021.
[20] https://forbiddenstories.org/journaliste/sevinc-vaqifqizi/
[21] Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 July 2021.
[22] See: https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.

government officials. Other persons identified as potential targets include journalist Dávid Dercseny, Central Media Group owner Zoltán Varga, professor Attila Chikán (former minister in Viktor Orbán's first government and currently a critic), the son and one of the closest confidants of former oligarch Lajos Simicska, János Bánáti, president of the Hungarian Bar Association, and Adrien Beauduin, a Belgian-Canadian PhD student of the Central European University.[23] In this connection, the Hungarian Civil Liberties Union (HCLU) has announced that it will launch legal action on behalf of some of the alleged victims, including a complaint with the Israeli Attorney General and applications with the European Court of Human Rights.[24] In view of these reports, I wrote to the Hungarian authorities, through the chairperson of the Hungarian Assembly delegation, to provide me with some explanations before 20 March 2022 (letter attached hereto).

16. According to the Pegasus Project revelations, two French journalists at *Mediapart,* Edwy Plenel and Lénaïg Bredoux, had their phones infected with Pegasus in 2019 and 2020, allegedly by Moroccan agents.

17. A joint research by German media has also revealed that the German Federal Criminal Police Office (BKA) acquired Pegasus in 2019 in "utmost secrecy".[25]

2.4. Recent disclosures

18. 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, and Ewa Wezosek, a prosecutor involved in a case against the ruling government.[26] Senator Krzystof Brejja's phone had also been compromised numerous times when he was running the Civic Coalition electoral campaign in 2019.[27] Other reported victims include Michal Kolodziejczak, leader of the agrarian movement Agrounia, Tomasz Swejgiert, journalist and alleged former associate of the Central Anticorruption Bureau[28], as well as former Law and Justice (PiS) politicians.[29] 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.[30] In view of these reports, I wrote to the Polish authorities, through the chairperson of the Polish Assembly delegation, asking them to provide me with some explanations before 20 March 2022 (letter attached hereto).

19. In January 2022, it was reported that Pegasus was used by the **Israeli** police against organisers of antigovernment protests, a senior politician, mayors, and employees of government-owned companies, among others.[31] The surveillance was allegedly carried out without judicial authorisation. Further revelations included other targets such as politicians and government officials, heads of corporations, journalists, activists, and even Avner Netanyahu, the son of then-Prime Minister Benjamin Netanyahu.[32]

20. In January 2022, the Finnish foreign ministry reported that several phones of Finnish diplomats abroad had been infected with the Pegasus spyware.[33]

---

[23] 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.
[24] See: https://hclu.hu/en/pegasus-case-foreign-procedures.
[25] See: https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197, 7 September 2021.
[26] See: https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.
[27] See: https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 December 2021.
[28] See: https://apnews.com/article/technology-europe-poland-hacking-spyware-4a410bda35df566632703e3578e5a99d, 25 January 2022.
[29] See: https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true, 18 January 2022.
[30] See: https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true, 7 February 2022.
[31] See: https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html, 18 January 2022.
[32] See: https://www.timesofisrael.com/ministry-heads-netanyahu-associates-activists-said-targeted-by-police-with-spyware/, 7 February 2022.
[33] https://www.euronews.com/2022/01/28/finnish-diplomats-were-targeted-by-pegasus-spyware-says-foreign-ministry, 28 January 2022.

2.5. Some reactions to the revelations

2.5.1. The NSO Group

21. Following *Pegasus Project* revelations in July 2021, NSO Group denied "false claims made in [the] report which many of them are uncorroborated theories that raise serious doubts about the reliability of [the] sources". It stated that it does not operate the systems it sells to vetted government customers, and does not have access to the data of its customers' targets. It added that due to contractual and national security considerations, NSO cannot confirm or deny the identity of their government customers, as well as the identity of customers whose system they have shut down.[34] The CEO of NSO Group categorically denied that the leaked list of 50,000 phone numbers had anything to do with them and the Pegasus spyware.[35]

2.5.2. States

22. In **France**, an investigation into the matter was launched by the Government, as well as by the public prosecutor's office in Paris following a complaint by the two targeted journalists from *Mediapart*.[36] France's national agency for information systems security (Anssi) confirmed that Pegasus had been found on the phones of three journalists, Mr Plenel, Ms Bredoux and a journalist of France 24, in what was the first time an official authority corroborated the findings of the Pegasus Project investigation.[37]

23. In **Hungary,** Lajos Kósa, Member of Parliament and Vice President of Fidesz, member of the Parliamentary Defence and Law Enforcement Committee, admitted that the Ministry of Interior had purchased and used the Pegasus software.[38] 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 list.[39] The investigation's reasoning will remain classified until 2050.

24. In **Israel,** the head of the Knesset's Foreign Affairs and Defence Committee announced the creation of a commission to investigate the allegations of misuse of Pegasus.[40] Following the most recent reports concerning the use of Pegasus by the Israeli Police, the Minister of Public Security has announced that he will set up a government-appointed commission of inquiry to investigate the allegations.[41]

25. The **Moroccan** government has denied claims of acquiring and using Pegasus and "categorically rejects and condemns these unfounded and false allegations".[42] Morocco has also sued Amnesty International and Forbidden Stories, as well as media participating in the joint investigation, for defamation.[43]

26. In **Poland**, 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".[44] In this connection, a committee set up by the Polish Senate to investigate the use of Pegasus has heard different witnesses and experts, among which cybersecurity experts (from Citizen Lab) and the president of the Supreme Audit Office, Mr

[34] See: https://www.washingtonpost.com/investigations/2021/07/18/nso-group-response-pegasus-project/, 18 July 2021.
[35] See: https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html, 20 July 2021.
[36] See: https://www.aa.com.tr/en/world/france-launches-investigation-into-pegasus-spyware/2311661, 22 July 2021.
[37] See: https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms, 2 August 2021.
[38] See: https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217, 4 November 2021.
[39] See: https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/, 31 January 2022.
[40] See: https://www.aljazeera.com/news/2021/7/22/israel-launches-commission-to-probe-pegasus-spyware-legislator, 22 July 2021.
[41] See: https://www.timesofisrael.com/police-minister-establishes-commission-to-probe-explosive-nso-spying-claims/, 7 February 2022.
[42] See: https://www.washingtonpost.com/investigations/2021/07/18/responses-countries-pegasus-project/, 19 July 2021.
[43] See: https://www.france24.com/en/africa/20210722-morocco-files-libel-suit-in-france-against-ngos-alleging-it-used-pegasus-spyware, 22 July 2021.
[44] See: https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 January 2022.

Banas. Mr Banas has said before the committee that the Central Anti-Corruption Bureau had secretly purchased Pegasus using a Ministry of Justice fund meant for crime victims.[45]

27. On 3 November 2021, the **United States** government (Commerce Department's Bureau of Industry and Security) added NSO Group and three other foreign companies 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 organizations here and abroad".[46]

2.5.3. Companies

28. Companies such as Meta and Apple have filed lawsuits against NSO Group for using the Pegasus spyware against their users.[47] A US appeals court has rejected the Israeli company's claim that it should be protected under sovereign immunity laws.

2.5.4. International bodies

29. There have been numerous negative reactions from international bodies concerning the use of the Pegasus spyware.

30. The **European Parliament** (EP) awarded the 2021 Daphne Caruana Galizia journalism prize to "The Pegasus Project". The EP's Civil Liberties (LIBE) Committee is examining the issue from the perspective of what the Pegasus revelations mean for fundamental rights. It has so far held two hearings with experts and persons affected.[48] The EP's Special Committee on Foreign Interference in all Democratic Processes in the EU including Disinformation held a hearing on "Foreign interference and spying on European politicians and institutions", which also addressed the matter of the Pegasus revelations.[49] According to the most recent information, the EP is preparing to launch a committee of inquiry on the abuse of Pegasus by EU Governments, on the basis of an initiative from the Renew Europe group.[50]

31. Didier Reynders, the **European Union's Justice Commissioner**, stated that the European Commission "totally condemns any illegal access to systems or any kind of illegal trapping or interception of community user communications. It's a crime in the whole of the EU". He added: "any indication that such intrusion of privacy actually occurred needs to be thoroughly investigated and all responsible for a possible breach have to be brought to justice".[51]

32. 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 proposes a ban on the development and the deployment

---

[45] See: https://www.usnews.com/news/business/articles/2022-01-17/polish-senators-question-cyber-experts-in-hacking-inquiry, 18 January 2022.
[46] 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.
[47] 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.
[48] On 29 November 2021, the LIBE Committee heard Laurent Richard, Executive Director of Forbidden Stories, Etienne Maynier, technologist at Amnesty International's Security Lab, and Wojciech Wiewiórowski, the European Data Protection Supervisor. On 1 February 2022, the LIBE Committee heard Szabolcs Pany, Hungarian journalist, Ewa Wrzosek, Polish prosecutor, and Ozturan Gürkan, from the European Centre for Press and Media Freedom.
[49] On 9 September 2021, with Robert Dover, professor of Criminology at the University of Hull, Margarita Robles Carrillo, professor at the University of Granada, Laurent Richard and Sandrine Rigaud, Executive Director and Editor-in-Chief of Forbidden Stories.
[50] See: EU to launch rare inquiry into Pegasus spyware scandal | European Union | The Guardian, 10 February 2022.
[51] See: EU commissioner calls for urgent action against Pegasus spyware | Surveillance | The Guardian, 15 September 2021.

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.[52]

33. The **United Nations High Commissioner for Human Rights**, Ms Bachelet, has 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.[53] She has also called on States to investigate cases of targeted surveillance and provide redress to the victims.

2.5.5. Journalists and civil society

34. Journalists and non-governmental organisations around the world have reacted strongly to the revelations concerning the misuse of Pegasus against journalists, opposition leaders and activists.[54] They have called for investigations, accountability and regulation of the global trade in surveillance technology. Edward Snowden has called for governments to impose a global moratorium on international trade in spyware.[55]

3. Similar spyware

35. Pegasus is not the only spyware tool available that has been used by governments. There have been allegations concerning the abuse of other spyware tools. For instance, software marketed by the Israeli company Candiru has been reported to target critics of autocratic regimes, including some readers of a London-based news website.[56] Unlike Pegasus, Candiru's malware is believed to infect computers, and in some cases the malware user can launch an exploit that allows them to take over an individual target's computer. Candiru has in fact been added, together with NSO Group, to the US's trade blacklist for supplying spyware to foreign governments which then used it to malicious ends (see paragraph 25 above).

36. FinFisher, also known as FinSpy, is a surveillance software marketed by Lench IT Solutions plc., which has a UK-based branch (Gamma International Ltd) and a German-based branch (Gamma International GmbH). FinFisher's use by governments for monitoring political dissidents was first reported in Egypt in 2011. Its use was later reported also in Bahrein (2010-2012) and against Ethiopian dissidents in exile. Civil society organisations have filed criminal complaints against Gamma Group in the United Kingdom and Germany.

4. Relevant/Applicable legal standards

4.1. Council of Europe standards

37. 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").[57] According to the case-law of the European Court of Human Rights ("the Court"), secret surveillance of an individual can only be justified under

---

[52] 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.

[53] 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.

[54] Committee to Protect Journalists (Spyware reform critical as at least 180 journalists revealed as potential Pegasus targets - Committee to Protect Journalists (cpj.org)); International Press Institute (Pegasus Project: Full investigation needed after 180 journalists targeted by spyware - International Press Institute (ipi.media)); Human Rights Watch (Human Rights Watch Among Pegasus Spyware Targets | Human Rights Watch (hrw.org)) ; Amnesty International (Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector - Amnesty International).

[55] See: Edward Snowden calls for spyware trade ban amid Pegasus revelations | Edward Snowden | The Guardian, 19 July 2021.

[56] Israeli firm's spyware linked to attacks on websites in UK and Middle East | Malware | The Guardian, 16 November 2021. See also: Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus - The Citizen Lab.

[57] 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).

Article 8.2 if it is "in accordance with the law", pursues one or more of the "legitimate aims" to which this paragraph refers and is "necessary in a democratic society" in order to achieve such aims.[58]

38. 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.[59] 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.[60] 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.[61]

39. 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.[62] 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.[63]

40. As regards authorisation procedures, although prior judicial authorisation may be an important safeguard against indiscriminate surveillance, the Court 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).[64] 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.[65] Applying these principles, the Court found in *Szabó and Vissy v. Hungary*[66] 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.[67]

---

[58] 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, 2021.
[59] Ibid., paragraphs 228-231, with further references therein.
[60] 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).
[61] *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.
[62] *Klass and Others v. Germany,* Application No. 5029/71, judgment of 6 September 1978, paragraph 42.
[63] *Roman Zakharov v. Russia*, paragraphs 235-238.
[64] 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 (not final), 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).
[65] Ibid., paragraph 233.
[66] *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: https://hudoc.exec.coe.int/eng?i=004-10745).
[67] See, for instance, *Zoltán Varga v. Slovakia,* Application No. 58361/12 and 2 others, judgment of 20 July 2021, paragraphs 155-163.

41. The Court has found violations of Article 8 in cases concerning secret surveillance of human rights activists,[68] members of non-governmental organisations,[69] lawyers,[70] and journalists,[71] among others.

42. 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[72] or any overriding requirement in the public interest justifying such measures in the concrete case.[73] 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.[74]

43. 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 8 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).[75] As recalled by Mr 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[76]) 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.[77] It provides individuals with stronger rights and imposes greater transparency requirements,[78] which may however be restricted when this is prescribed by law and constitutes a necessary measure in a democratic society for "essential objectives of general public interest", including the protection of national security, defence or the investigation and prosecution of criminal offences.[79] 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.[80]

---

[68] *Shimovolos v. Russia,* Application No. 30194/09, judgment of 21 June 2011.
[69] *Case of Association "21 December 1989" and Others v. Romania,* Application No. 33810/07, judgment of 24 May 2011.
[70] *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.
[71] *Azer Ahmadov v. Azerbaijan,* Application No. 3409/10, judgment of 22 July 2021.
[72] *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).
[73] *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.
[74] *Sanoma Uitgevers B.V. v. the Netherlands,* Application No. 38224/03, judgment of 14 September 2010 (Grand Chamber), paragraphs 50-51.
[75] 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.
[76] To date, 16 States have ratified it.
[77] Article 5.
[78] Articles 8 and 9.
[79] Article 11.1.
[80] Article 11.3. Mr 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 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.

44. The **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 (66 ratifications as of February 2022). 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".[81] 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.[82] 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.[83]

45. 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),[84] and Resolution 2256 (2019) "Internet governance and human rights" (paragraph 7).

46. 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 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).

47. 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 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.[85]

---

[81] 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.
[82] Explanatory report to the Convention, § 58.
[83] 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".
[84] 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.
[85] See Reply to Recommendation, Doc. 13911, 14 October 2015.

4.2. Other international standards

48. 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 which had been 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). The report asserts that in addition to the primary obligations not to interfere with these rights, States have duties to protect individuals against third-party interference, including with regard to transnational surveillance committed by foreign entities against one's own citizens. It 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.).

49. In order to improve compliance with these standards and address the gaps in implementation, the Special Rapporteur proposes in his report a legal and policy framework for regulation, accountability and transparency within the private surveillance industry. He calls for tighter regulation of surveillance exports and regulations on their use, as well as for an immediate moratorium on granting export licenses for surveillance technologies until the use of those technologies can be technically restricted to lawful purposes that are consistent with human rights, or until it can be ensured that those technologies will only be exported to countries in which their use is subject to authorization (granted in accordance with due process and the standards of legality, necessity and legitimacy) by an independent and impartial judicial body.[86]

50. In terms of **European Union legislation**, apart from the Charter of Fundamental Rights (Articles 7, 8, 11, 47 and 52(1)) and the ePrivacy Directive,[87] 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 or the commission of serious violations of human rights and international humanitarian law.[88] I would also like to examine in the report the relevance of the Law Enforcement Directive, which establishes for instance an obligation to notify any personal data breach which poses a risk to individual rights and freedoms to the data protection authority within 72 hours.[89]

5. Preliminary conclusions and next steps

51. The Pegasus revelations have provided evidence that this spyware has been used as a hacking and surveillance tool on journalists, lawyers, politicians and human rights activists in several Council of Europe member States and beyond. Given the 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 effectively targeted, 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. In any event, serious questions must be answered on whether the surveillance of such persons had any legal basis and could at all be justified, either on national security grounds or for the purposes of a criminal investigation. In this regard, as mentioned before, I have already sent letters with questions addressed to the Hungarian and Polish authorities, in light of growing evidence that Pegasus has been used in both countries against several individuals, allegedly for political purposes. I intend to send similar letters to all delegations, even in the absence of concrete allegations on the use of Pegasus in order to obtain complete information about its possible acquisition and use (or that of a similar spyware) by any of the Council of Europe's member States. I also envisage sending letters requesting information to other actors, including the NSO Group. I will

[86] OHCHR | The Special Rapporteur's 2019 report to the United Nations Human Rights Council. See also UN High Commissioner for Human Rights, 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.
[87] OJ L 201, 31/07/2002, p. 37-47.
[88] OJ L 206, 11/06/2021, p. 1-461.
[89] 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).

also follow closely the hearings and debates which are currently being held on Pegasus before the European Parliament, with the possibility of making a working visit to ensure coordination

52. Apart from shedding light on specific allegations concerning the use of Pegasus in some member States, its scale and implications, the other main purpose of my report will be to take stock of the existing Council of Europe and international standards on targeted digital surveillance (seeking complementarity, for instance between the European Convention on Human Rights, Convention 108 and the Cybercrime Convention), including on the issue of the global trade in privately developed surveillance tools and the relevant positive obligations of States to regulate and restrict this trade. I intend to identify the loopholes in the existing legal framework, with a view to making concrete proposals for a coordinated Council of Europe response to the misuse of surveillance tools by state authorities against targeted individuals and for stronger safeguards in this field.

53. In order to complete my mandate, I should like to hold another hearing before the committee, with a representative from an NGO having filed complaints on behalf of some of the victims, a technical/IT expert who participated in the investigations (Amnesty International Security Lab, or Citizen Lab at the University of Toronto), and a MEP involved in the EP's hearings on this topic. I also propose to conduct a fact-finding mission to Israel, to meet with representatives of NSO Group, the Defence Export Controls Agency of the Israeli Ministry of Defence, members of the Knesset involved in efforts to investigate alleged abuses of NSO and similar spyware and an Israeli lawyer who has made several attempts to sue the NSO Group over Pegasus (Mr Eitay Mack).

54. Finally, I propose that this introductory memorandum be declassified immediately after the committee meeting.

Appendix

Questions sent to Hungarian and Polish authorities:

1. Can your authorities confirm whether they have acquired the Pegasus spyware and provide information on any other spyware they may have obtained?
2. What is the legal basis governing the application of such spyware and how is compliance with this legislation assured?
3. Has the Pegasus spyware been used against any of the persons mentioned in the letter, or other individuals, and if so on what legal basis?
4. Against how many people has the Pegasus spyware been used by the government?
5. Can you indicate which government agencies have the ability to use such spyware and against which category of people it has been used?
6. What steps have been taken by your authorities to prevent the misuse of spyware against persons such as those referred to in the letter?
7. What official investigations have been undertaken, or planned, on the misuse of spyware, and what results (provisional or otherwise) are available?
8. Are there plans to change the legal framework concerning the use of Pegasus or similar spyware in the future and improve compliance over its use and prevent possible abuse?
9. What measures are envisaged to eventually sanction those misusing such spyware?