IN-DEPTH ANALYSIS
for the PEGASUS committee

European Parliament

Pegasus and surveillance spyware

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 732.268 - May 2022

EN

Pegasus and surveillance spyware

Abstract

This In-Depth Analysis, drafted by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs for the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, looks into the confirmed or suspected use of the Pegasus spyware and other similar cyber-surveillance instruments in the EU and its Member States or targeting EU citizens or residents, EU reactions and previous activities on issues related to surveillance.

This document was drafted by the Policy Department for Citizens' Rights and Constitutional Affairs for the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

AUTHORS
Ottavio MARZOCCHI, EP, Policy Department for Citizens' Rights and Constitutional Affairs
Martina MAZZINI, trainee, DG IPOL

ADMINISTRATOR RESPONSIBLE
Ottavio MARZOCCHI

EDITORIAL ASSISTANT
Sybille PECSTEEN de BUYTSWERVE

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in May 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

1. PEGASUS

Pegasus is a hacking tool developed and marketed around the world by the **Israeli company NSO Group**. This spyware tool is designed to secretly turn mobile phones - both with Android and iOS operating systems - into 24-hour surveillance devices, as it grants **complete and unrestricted access** to all sensors and information of the targeted device. It can read, send or receive messages that should be end-to-end encrypted, download stored photos, collect passwords, hear and record voice or video calls as, among other things, it has full access to the phone's camera, microphone, and geolocation module.[1] In addition, Pegasus is characterized by the possibility of carrying out the so-called **"zero-click" hacking** attacks, since it does not require any actions by the user to be triggered, and of "**jailbreaking**" into the system by removing manufacturers' access restrictions. Pegasus software is also extremely **difficult to detect** and the intrusions are hard to prove. Due to its unique features, this spyware constitutes a real **game-changer** for the digital monitoring, since it combines a great level of intrusiveness with features capable of rendering the majority of the existing legal and technical safeguards completely ineffective.[2]

Pegasus was first identified in August **2016**, after Ahmed Mansoor, an Arab human rights lawyer, found himself targeted by the cyberattack through a text message promising to reveal secrets regarding torture happening in prisons in the United Arab Emirates. The message was then sent to experts at **Citizen Lab of the University of Toronto**, which discovered the sophisticated cyber weapon.[3] Between 2016 and 2018, Citizens Lab looked for servers associated with NSO Group's Pegasus - finding over 1000 matching IP addresses - and identifying a total of **45 countries** where Pegasus operators may be conducting surveillance operations, many of which are authoritarian regimes.[4]

Accusations that Pegasus had been used by the Saudi regime to target opponents emerged also in relation to the killing of the Saudi human rights activist Jamal **Khashoggi**.[5] In October 2019, **Facebook** sued the NSO Group, accusing it of having used **WhatsApp** to install its Pegasus malware on mobile devices, with Microsoft, Cisco, GitHub, Google, LinkedIn, VMWare and the Internet Association joining the lawsuit on 21 December 2020.[6]

The Pegasus scandal became widely known in **July 2021**, when the **Pegasus project** - a collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by **Forbidden Stories**[7], with the technical support of **Amnesty International** conducting forensic tests on mobile phones to identify traces of the spyware - published information about leaked lists of around **50,000 phone numbers** that had been targeted and attacked using Israeli spyware. Since that moment, it has been reported that the Pegasus spyware had been widely **used by governments all over the world to target human rights activists, opposition figures, lawyers, judges, foreign leaders, etc.** -

---

1 Based on EDPS, *Preliminary Remarks on Modern Spyware*, 15 February 2022, https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf.

2 As explained by EDPS, the attacker might even impersonate the victims by gaining access to their digital credentials and identity.

3 L. Dave, *Who are the hackers who cracked the iPhone?*, BBC News, 26 August 2016, https://www.bbc.com/news/technology-37192670

4 B. Marczak et al., *Hide and seek. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countres*, 18 September 2018, Research report #113, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

5 It later emerged that his wife's phone has also been infected with Pegasus by a UAE agency, https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/

6 https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

7 See https://forbiddenstories.org/case/the-pegasus-project/

including in the EU by targeting EU citizens. Indeed, several EU governments admitted to having bought Pegasus from the NSO Group[8], while EU citizens were targeted by their government, or by foreign governments or authorities. The selling of Pegasus to a foreign country has to be first authorised by the **Israeli Ministry of Defense**, to ensure the sale is in Israel's national interest. NSO states that it also has contractual clauses imposing that it is used only for terrorism and crime. NSO stated that it has sold Pegasus to **60 government agencies in 40 countries**.[9] [10]

On 3 November 2021, the **US blacklisted** the NSO Group for engaging in activities that are contrary to the national security or foreign policy interests of the United States.[11] At the beginning of December 2021, media reported that **U.S. State Department employees in Uganda** had been targeted with Pegasus.[12]

On 23 November 2021, **Apple** filed a lawsuit against the NSO Group for the surveillance and targeting of Apple users.[13]

In November 2021, it emerged that Israel removed 65 countries from its list of countries to whom cyber products can be exported, bringing them from 102 to 37.[14] Still, media reported that Israel re-authorised **Saudi Arabia** to use Pegasus.[15]

On 16 December 2021, **Meta** published a "Threat Report on the Surveillance-for-Hire Industry", whereby it announced that it was taking action against **Cobwebs Technologies, Cognyte, Black Cube, Blue Hawk CI, BellTroX, Cytrox and an unknown Chinese entity**.[16] Many of these companies have offices also in the EU. **Black Cube** is known for having been used by the **Hungarian government to spy on NGOs** and other persons[17] and in Romania to spy in 2016 on **Laura Kodruta Kovesi**, Romanian anti-corruption prosecutor at that time and now EPPO chief prosecutor.[18]

In mid-January 2022, media reported about the fact that the **Israeli Police used NSO Group spyware to track civilians**, including activists and mayors, without judicial oversight. An inquiry is underway,

---

8 EDPS, *ibid*.

9 See https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/#main-content; it was also reported that "there was a presumption that Israel had some access – via a "backdoor" – to intelligence unearthed via such surveillance tools", something NSO denied, https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state.

10 The New Yorker reports that Shalev Hulio, NSO Group's C.E.O., told them that "Almost all governments in Europe are using our tools," and that a former senior Israeli intelligence official added, "NSO has a monopoly in Europe.", https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

11 The press release by the US authorities also states that: "NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order.", see https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

12 https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

13 See https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

14 See https://eurasiantimes.com/pegasus-spyware-controversy-israel-deletes-65-countries-from-its-cyber-export-list/

15 See https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

16 See https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/

17 https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/

18 See https://www.timesofisrael.com/3-israelis-from-black-cube-intel-firm-given-suspended-sentence-in-romania/

while the police did not deny using Pegasus, but stated doing it legally.[19] On 25 January, the head of NSO's board of directors Asher Levy stepped down.

In April 2022, CitizenLab revealed that a software called **Candiru** had been used to target persons.[20]

The **NSO group** states on its webpage that "In light of the recent planned and well-orchestrated media campaign lead by Forbidden Stories and pushed by special interest groups, and due to the complete disregard of the facts, NSO is announcing it will no longer be responding to media inquiries on this matter and it will not play along with the vicious and slanderous campaign."[21] According to media, the NSO Group is in financial crisis.[22]

[19] See https://www.timesofisrael.com/nso-chairman-steps-down-says-departure-unrelated-to-company-turmoil/

[20] See https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

[21] See https://www.nsogroup.com/Newses/enough-is-enough/

[22] See https://thewire.in/tech/nso-group-worthless-investors-no-new-pegasus-bookings-report

2. PEGASUS AND OTHER SPYWARES' USE IN THE EU

2.1. Hungary

Investigations conducted by **Direkt36**[23], a Hungarian investigative journalism channel, confirmed that around **300 persons** were potentially targeted by Pegasus in Hungary, among which:

- "Photojournalist **Dániel Németh** who has been documenting luxury trips of pro-government businessmen and politicians, such as that of Foreign Minister Szijjártó's on László Szíjj's yacht
- **Four journalists**: two employees of investigative outlet ***Direkt36***, a former journalist of liberal weekly **HVG**, as well as a fourth journalist who has chosen to remain anonymous
- A Hungarian **photographer** who collaborated with an American journalist covering the Russian-led International Investment Bank's affairs in Budapest
- One of Central European University's international students, **Adrien Beauduin**, who was arrested in 2018 for taking part in an anti-government protest
- **Zoltán Varga**, owner of Central Media Group Plc. (publisher of *24.hu* among other outlets), who has allegedly faced multiple attacks from government circles, as well as other businessmen who joined Varga at a dinner meeting in 2018
- Opposition media owner and former Socialist (MSZP) politician, **Zsolt Páva**
- The **son** of former pro-Fidesz oligarch **Lajos Simicska** and a close confidante of Simicska. Simicska initiated an open media campaign against the government during the elections of 2018
- Gödöllő's (opposition-backed) independent mayor **György Gémesi** (formerly centrist MDF's politician)
- Renowned high-profile lawyer **János Bánáti**
- **Attila Chikán**, an economics professor and former Minister of the Economy in the first Orbán administration, known for becoming critical of the Fidesz leader
- Former state secretary of Orbán, **Attila Aszódi,** who got into conflict with the government as the Russians were pushing for the Paks expansion construction's premature start which Aszódi opposed
- An unnamed technical counterintelligence officer of the Special Service for National Security (NBSZ)
- Former deputy head of the Counter-Terrorism Center (TEK), **Zsolt Bodnár**, who became a target after he had to leave the elite police force in 2018, following an inner (perhaps also political) conflict."[24]
- More recently, *Direkt36* revealed that the leaders of the Presidential Guard of the Republic of Hungary and his family were targeted with Pegasus in 2019,[25] as well as Hungary's former ambassador to China and now personal advisor of Viktor Orbán, **Cecília Szilas**, was also targeted by Pegasus spyware before her appointment.[26]

---

[23] See https://telex.hu/direkt36/2021/07/23/az-orban-kormany-allamtitkarat-is-megceloztak-a-pegasusszal-mikozben-belharcokat-vivott-paks-ii-miatt

[24] See https://hungarytoday.hu/fidesz-governement-admit-surveillance-israel-journalist-pegasus-spyware/

[25] See https://www.direkt36.hu/ader-janos-koztarsasagi-elnok-es-csaladja-legkozelebbi-testoreit-is-megceloztak-a-pegasusszal/

[26] See https://telex.hu/direkt36/2022/03/22/pegasusszal-celoztak-meg-a-volt-pekingi-nagykovetet-aki-nem-sokkal-kesobb-bekerult-orban-tanacsadoi-korebe

Hungarian authorities initially denied or not confirmed their involvement and use of Pegasus until **Lajos Kósa, Fidesz MP and Chair of the Hungarian Parliament's Committee on Defense and Law Enforcement**, **admitted** that the Interior Ministry had bought and used Pegasus (before stating that it was used lawfully upon authorization by the judiciary and/or the Minister of Justice).[27]

At the end of January 2022, the **Hungarian National Authority for Data Protection and Freedom of Information** (NAIH) published a report[28] stating that it had investigated hundreds of cases and that all of them met the legal criteria (risk for national security, legal authorisation).[29] The authority also reportedly will file a criminal complaint against those who uncovered the mass surveillance for possibly mishandling data.[30]

On 28 January 2022, the **Hungarian Civil Liberties Union** announced that it initiated proceedings on behalf of six stakeholders in Hungary (Brigitta Csikász, Dávid Dercsényi, Adrien Beauduin, Dániel Németh, Szabolcs Panyi and a sixth person requesting anonymity), before the European Commission and the European Court of Human Rights in Strasbourg, as well as in Israel.[31]

Media also reported that the Hungarian government hired an **ex-Pegasus lobbyist** to prepare for potential US sanctions,[32] that investigations by Israeli media suggest that Pegasus attacks by certain countries overlap with former Israeli PM **Netanyahu** visiting them, including for Hungary,[33] as well as that Pegasus operations began after Orbán's national security expert met Netanyahu in Israel.[34] [35]

2.2. Poland

Already in 2018, Citizens Lab's reported that Poland as one of the Member States that had seen infections by Pegasus originating internally[36] and this has been further confirmed in 2021 by the laboratory. In December 2021, it emerged that Pegasus had been used against Polish personalities:

- **Roman Giertych**, lawyer working for Donald Tusk, leader of Civic Platform (18 intrusions)

- prosecutor **Ewa Wrzosek**[37]

- Civic Platform Senator **Krzysztof Brejza**, coordinating his party's election campaign (33 intrusions)

- agrarian social movement leader **Michal Kolodziejczak**

- author and former collaborator of the Polish secret services **Tomasz Szwejgiert**

---

27 See https://hungarytoday.hu/fidesz-governement-admit-surveillance-israel-journalist-pegasus-spyware/

28 See https://www.naih.hu/adatvedelmi-jelentesek/file/486-jelentes-a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-hivatalbol-inditott-vizsgalatanak-megallapitasai-a-pegasus-kemszoftver-magyarorszagon-torteno-alkalmazasaval-osszefuggesben

29 See https://telex.hu/belfold/2022/01/31/adatvedelem-peterfalvi-pegasus-vizsgalat

30 See https://euobserver.com/rule-of-law/154261

31 See https://ataszjelenti.444.hu/2022/01/28/uj-fejezet-a-pegasus-ugyben-hazai-es-nemzetkozi-lepeseket-teszunk and https://tasz.hu/pegasus.

32 See https://www.euractiv.com/section/politics/short_news/hungary-hires-ex-pegasus-spyware-lobbyist/

33 See https://www.middleeasteye.net/news/israel-pegasus-spyware-hungary-poland-purchase-after-netanyahu-meeting

34 see https://hungarytoday.hu/pm-orban-publicly-asked-pegasus-case-scandal-first-time/

35 Media also reported about Russian hacking into the Hungarian Foreign Affairs Ministry information networks for a decade, also connected to classified information and NATO, upon which an inquiry was recently opened, https://hungarytoday.hu/investigation-launched-into-alleged-russian-cyber-attacks-at-the-foreign-ministry/

36 See https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

37 See https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e

- the **Supreme Audit Office** affirmed that its employers have been put under surveillance[38]

- **Adam Hofman**, former PiS spokesman

- **Dawid Jackiewicz**, former PiS Treasury Minister in the Cabinet of Beata Szydło

- Mariusz Antoni Kamiński, former PiS MP

- **Bartłomiej Misiewicz**, former head of the PiS cabinet and former spokesman of the Ministry of National Defence

- **Katarzyna Kaczmarek**, wife of Tomasz Kaczmarek [pl] (referred to as "agent Tomek"), former policeman and former CBA officer, later a PiS MP. [39]

Initially, the government denied the acquisition of the spyware, but then PiS leader **admitted** in early January 2022 the purchase and the use, underlining that it was used legally and not against the opposition[40]. In January 2022, media reported that the agreement to buy Pegasus was allegedly made by former Prime Minister Beata Szydło in July 2017.[41]

2.3. France

On 22 July 2021 the French authorities stated that they had launched an investigation into allegations that Morocco used Pegasus to spy on President Emmanuel Macron. Traces of Pegasus were found on the mobile phones of at least **five French cabinet ministers.**[42] Other media reported about former French Prime Minister Edouard Philippe and **14 French ministers** targeted by Morocco.[43]

According to MIT Technology Review, France had **negotiated buying Pegasus** from NSO in 2021, but decided to interrupt negotiations after the revelations emerged, something the Foreign Affairs Ministry denied.[44]

On 5 April 2022, the *Fédération internationale pour les droits humains* (**FIDH**), la *Ligue des droits de l'Homme* (**LDH**) and **Salah Hammouri** tabled a lawsuit against NSO Group for having illegally infected the mobile of the French-Palestinian human rights defender Salah Hammouri.

A high number of persons have been allegedly spied on with Pegasus:

- Bruno Delport
The phone of the director of Parisian radio station TSF Jazz was found by Citizen Lab to have been infected in 2019, just as he was applying for the presidency of Radio France.

[38] See https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/

[39] See https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true

[40] See https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/ and https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/

[41] See https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba

[42] See https://www.theguardian.com/news/2021/sep/23/spyware-found-on-phones-of-five-french-cabinet-members

[43] See https://www.middleeastmonitor.com/20220106-france-morocco-ties-remain-damaged-by-israel-spyware-claims/

[44] See https://www.technologyreview.com/2021/11/23/1040509/france-macron-nso-in-crisis-sanctions/

- Lénaïg Bredoux
The investigative journalist and general editor of Mediapart was confirmed to have been infected by Pegasus. The confirmation was made by France's computer security agency following Project Pegasus. Bredoux was involved in a story about the head of Morocco's intelligence agency, a known NSO client.

- Edwy Plenel
The investigative journalist with Mediapart was confirmed to have been infected by Pegasus. The confirmation was made by France's computer security agency following Project Pegasus.

- Unnamed France 24 journalist
A senior journalist with France 24 was confirmed to have been infected by Pegasus in May 2019, September 2020 and January 2021. That was confirmed by France's computer security agency after Project Pegasus.

- Claude Mangin
French national whose husband, Naama Asfari, is jailed in Morocco for advocating for Western Saharan independence. As part of Project Pegasus, it was found that at least two of her phones were infected.

- Arnaud Montebourg
A former minister in the government of Manuel Valls, Montebourg was targeted in 2019, most likely by Morocco, an analysis by Amnesty found. Montebourg has given testimony to ANSSI and its investigation into NSO in France.
Suspected operator: "Morocco"[45]

Also former PM **Edouard Philippe and his wife**, an assistant and the councillor **Gilles Boyer**, as well as the ministers in his cabinet: Interior Minister **Christophe Castaner**; Justice Minister **Nicole Belloubet**; Foreign Affairs Minister **Jean-Yves Le Drian**; Economy Minister **Bruno Le Maire**; Education Minister **Jean-Michel Blanquer**; Agriculture Minister **Didier Guillaume**; Budget Minister **Gérald Darmanin**, Cohesion Minister **Jacqueline Gourault**, Minister for the Relations with the Parliament **Marc Fesneau**, Minister for Overseas territories **Annick Girardin**, Culture Minister **Franck Riester**, Ministers **Julien Denormandie** and **Sébastien Lecornu**).[46]

2.4. Spain (Pegasus and Candiru)

According to initial media reports, Spain bought Pegasus, which is used by the intelligence service, including to target Catalan politicians, notably the President of the Parliament of Catalonia Roger Torrent and former member of the Parliament of Catalonia Anna Gabriel i Sabaté.[47] [48]

On 18 April 2022, CitizenLab published a post entitled "CatalanGate, Extensive Mercenary Spyware Operation against Catalans Using Pegasus and **Candiru**" revealing that "at least 63 were targeted or infected with Pegasus, and four others with Candiru. At least two were targeted or infected with both"

[45] See https://www.haaretz.com/israel-news/tech-news/MAGAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510

[46] https://www.franceinter.fr/justice/projet-pegasus-le-gouvernement-et-toute-la-classe-politique-francaise-dans-le-viseur-du-maroc

[47] https://elpais.com/internacional/2021-07-19/pegasus-el-espia-que-desnudo-al-independentismo-catalan.html and https://english.elpais.com/politics/catalonia_independence/2020-07-16/spains-intelligence-service-has-spyware-program-that-targeted-catalan-politicians.html

[48] https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

and that "victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases." It also reported that "The Citizen Lab is not conclusively attributing the operations to a specific entity, but strong circumstantial evidence suggests a nexus with Spanish authorities." A list of targets was published.[49] Candiru is a spyware that the US has blacklisted, together with Pegasus, last November. Victims announced to take legal action in various States and against various actors. El Pais reported that the National Intelligence Centre (CNI), Spain's intelligence agency, acquired the Pegasus in the first half of the 2010s for an initial cost of €6 million.[50]

Spanish authorities replied that surveillance was carried out in full respect of the law and the government promised an internal investigation within the National Intelligence Centre and a report to the committee responsible for state secrets, allowing MPs to access classified information. Also the Spanish ombudsman announced an investigation.[51]

On 2 May 2022, Spain's Minister of the Presidency Félix Bolaños revealed during a press conference that the Spanish Prime Minister Pedro Sanchez and Defence Minister Margarita Robles were targeted by Pegasus attacks in May and June 2021 and data was extracted from their mobiles. These attacks were according to the Minister of the Presidency "illegal and external ... They are alien to state agencies and do not have judicial authorization from any official agency".[52] The *Audiencia Nacional* opened an investigation into these events, while the parliamentary committee on intelligence affairs will examine these cases. According to media, more than 200 Spanish mobile numbers were among possible targets of the Pegasus spyware.[53]

2.5. Finland

On 28 January 2022, the Finnish Foreign Affairs ministry stated that some of its officials abroad had been targeted by Pegasus[54] for a relatively long time.[55]

2.6. Germany

Media reported that the German Federal Criminal Police Office (BKA) admitted during a closed doors session of the Interior Committee of the Bundestag that it had secretly bought Pegasus in 2019 (with some functions disabled) and that the spyware has been used in operations concerning terrorism and organized crime since March 2021. Allegedly, BKA began its negotiations with NSO in 2017.[56]

---

49 https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

50 https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html

51 https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6

52 https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/

53 https://www.theguardian.com/world/2022/may/03/over-200-spanish-mobile-numbers-possible-targets-pegasus-spyware

54 https://www.euronews.com/2022/01/28/finnish-diplomats-were-targeted-by-pegasus-spyware-says-foreign-ministry

55 https://www.helsinkitimes.fi/finland/finland-news/domestic/20894-ministry-for-foreign-affairs-reveals-cyber-espionage-campaign-against-finnish-diplomats.html

56 https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

2.7. Estonia

According to media, Estonia allegedly started negotiations in 2018 and effectively acquired Pegasus in 2019, but following Russian warnings, Israeli authorities and NSO informed the Estonian authorities in August of the same year that the company would **not permit Estonian officials to use the spyware against Russian targets**.[57] Requests to purchase Pegasus made by Ukraine were repeatedly rejected, for fears of angering Russia.

2.8. Bulgaria and Cyprus

In 2019, the **NGO Access Now** asked Bulgarian[58] and Cypriot authorities[59] to clarify whether they gave the NSO Group (which has offices in Israel, Bulgaria and Cyprus and employs also EU citizens) the authorisation to export Pegasus.[60] The authorities of both Member States **denied** having given such authorisation.[61] Still, media report that one of the servers of the network infrastructure over which Pegasus attacks are conducted is located in a Bulgarian datacentre, owned by a Bulgarian company owned by NSO group, Circles, which has received export licences from the authorities.[62] [63] The Sofia City Prosecutor's Office is investigating whether state services have illegally used the Pegasus spyware to target Bulgarian citizens.[64]

2.9. Belgium / European Union

In 2019, **Charles Michel**, current President of the European Council and then former Belgian PM, as well as his father **Louis Michel** then MEP, were among the persons targeted by the Moroccan client of NSO.[65]

Also journalist **Peter Verlinden and his wife Marie Bamutese** were targeted with Pegasus, allegedly by Rwandan authorities.[66]

---

57 https://amp.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia and https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html.

58 https://www.accessnow.org/cms/assets/uploads/2019/05/Access-Now-letter-to-Bulgaria-Government-on-NSO-Group-export-licence.pdf

59 https://www.accessnow.org/cms/assets/uploads/2019/05/Access-Now-letter-to-Cyprus-Government-on-NSO-Group-export-licence.pdf

60 NSO Group Transparency and Responsibility Report published in 2021 states: "Additional layers of approval are provided by select government regulatory authorities. NSO Group is closely regulated by export control authorities in the **countries from which we export our products**: Israel, **Bulgaria and Cyprus**. The Defense Export Controls Agency ("DECA") of the Israeli Ministry of Defense strictly restricts the licensing of some of our products and it conducts its own analysis of potential customers from a human rights perspective."

61 https://www.accessnow.org/is-nso-groups-infamous-pegasus-spyware-being-traded-through-the-eu/

62 https://www.mediapool.bg/bulgaria-mozhe-da-se-ozove-v-tsentara-na-shpionskata-afera-pegasus-news324368.html

63 https://newsbeezer.com/bulgariaeng/bulgaria-could-be-at-the-center-of-the-pegasus-espionage-affair/

64 https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria

65 https://www.lemonde.fr/pixels/article/2021/07/20/projet-pegasus-le-telephone-de-charles-michel-selectionne-quand-il-etait-premier-ministre-de-la-belgique_6088962_4408996.html

66 https://www.timesofisrael.com/rwanda-believed-to-have-used-nso-spyware-against-belgian-journalist-wife/

More recently, it emerged that also **Didier Reynders**, current EU Commissioner for Justice, as well as other senior officials of the Commission, were targeted with Pegasus in 2021.[67]

2.10. Greece (Predator)

According to a forensic report by CitizensLab, a spyware similar to Pegasus called **Predator,** that was initially developed by the North Macedonian company **Cytrox** (reportedly now owned by a Cyprus-based company, **WiSpear** then renamed **Passitora Ltd**, recently fined in Cyprus for illegal surveillance of private communications through the use of a "spy van"; the main company is **Intellexa**, which has headquarters in Greece and whose website it is stated that it is an "EU based and regulated company, with six sites and R&D labs throughout Europe") is likely to be used by the Greek authorities (together with Armenia, Egypt, Indonesia, Madagascar, Oman, Saudi Arabia and Serbia).[68]

In November 2021, media reported that **Stavros Malichudis**, a journalist following migration issues, had been under surveillance.[69]

More recently, it was reported that a Greek journalist, **Thanasis Koukakis,** working also for CNN and Financial Times, was informed by CitizensLab that he had been targeted with **Predator**, for 10 weeks between July 12 and September 24 in 2021, while he was working on alleged money laundering and corruption cases. He had in 2020, 2021 and 2022 suspicions of being under surveillance and complained to the Hellenic Authority for Communications Security and Privacy.[70] In all cases, the government denied being behind these surveillance operations. Media organisations have written to the government to ask them to explain the fact that Koukakis private communications were intercepted by the Greek National Intelligence Service (EYP), a body overseen by the office of the Prime Minister, in 2020. The organisations also raised questions in relation to some legislative changes introduced related to the EYP. [71]

2.11. Other non-EU States: USA, UK

Among the many States somehow associated with Pegasus, we focus here on the US and the UK.

As already recalled, in December 2021, Reuters reported that at least 9 **U.S. State Department employees in Uganda** had been targeted with Pegasus.[72] According to a statement released by the **FBI** and by declarations of FBI Director Christopher Wray given at the US House Intelligence Committee, the US agency obtained a licence to test and evaluate Pegasus for counter-intelligence purposes, but

---

67 https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/

68 https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

69 https://ipi.media/greece-journalist-thanasis-koukakis-surveilled-for-10-weeks-with-powerful-new-spyware-tool/ and https://www.investigate-europe.eu/en/2021/stavros-malichudis-journalist-being-watched-by-the-greek-secret-service-press-freedom/

70 https://cpj.org/2022/04/greek-journalist-thanasis-koukakis-targeted-by-predator-spyware/

71 https://ipi.media/greece-letter-to-government-after-spyware-surveillance-of-journalist-thanasis-koukakis/

72 https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

never used it for operational support of investigations as it decided not to purchase it.[73] [74] It also appears that the New York Police Department Intelligence Bureau was given a demonstration on Pegasus.[75]

On 18 April 2022, CitizensLab stated that in 2020 and 2021 they observed and notified the **UK** government of multiple suspected instances of Pegasus spyware infections within official UK networks, notably including the **Prime Minister's Office** (associated with a Pegasus operator linked to the UAE) and **the Foreign and Commonwealth/Development Office** (associated with Pegasus operators that they link to the UAE, India, Cyprus, and Jordan; the infection could have been taken place abroad)**.**[76]

[73] https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware

[74] https://www.jpost.com/international/article-700689

[75] https://www.vice.com/en/article/m7vp93/nso-group-pegasus-demo-nypd

[76] https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/

3. EU REACTIONS

3.1. European Commission

European Commission President **Ursula von der Leyen** stated on 19 July 2021 that "What we could read so far, and this has to be verified, but if it is the case, it is completely unacceptable. Against any kind of rules we have in the European Union...Freedom of media, free press is one of the core values of the EU. It is completely unacceptable if this [hacking] were to be the case".[77]

Justice **Commissioner Reynders** stated on 20 July 2021 that "We are starting to collect information to see what are the possible uses of such a kind of application in one of those member states. We have seen the comments in the press about that" and added that the Commission Directorate-General for Communications Networks, Content and Technology (DG CNECT) would coordinate the work, gathering information also on investigations by judicial authorities and data protection watchdogs.

On 15 September 2021, he stated during a debate in the EP plenary that "the Commission totally condemns any illegal access to systems or any kind of illegal trapping or interception of community users communications. It's a crime in the whole of the European Union". He also added that "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. This is, of course, the responsibility of each and every member state of the EU, and I expect that in the case of Pegasus, the competent authorities will thoroughly examine the allegations and restore trust."[78]

On 19 April 2022, the EU Commission stated that it **will not investigate Member States that used Pegasus** to spy on politicians, journalists and other individuals, as "this is really something for the national authorities," and that the EU commission cannot deal with national security issues: people should seek justice at national courts' level.[79]

3.2. European Parliament

The **European Parliament** debated Pegasus in various occasions:[80]

- during a session of the **INGE Committee** (Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation) on **9 September 2021**;[81]

- in **Plenary, during the September 2021 session**, on 15 September (debate on the Pegasus spyware scandal);[82]

- In **October 2021**, the **European Parliament awarded** the first Daphne Caruana Prize for Journalism to journalists from the Pegasus Project coordinated by the Forbidden Stories Consortium;

---

77 https://www.dw.com/en/pegasus-spying-reports-completely-unacceptable-says-eus-von-der-leyen/a-58318756

78 https://www.theguardian.com/news/2021/sep/15/eu-poised-to-tighten-privacy-laws-after-pegasus-spyware-scandal

79 https://euobserver.com/digital/154752

80 The EPP group also held on 10 February 2022 a public hearing on the threats posed by the Pegasus spyware to democracy and rule of law, https://www.eppgroup.eu/newsroom/events/epp-group-public-hearing-pegasus-spyware-scandal-and-its-impact-on-democracy-in-the-eu; various MEPs tabled parliamentary questions on Pegasus, see https://www.europarl.europa.eu/plenary/en/parliamentary-questions.html#sidesForm.

81 https://multimedia.europarl.europa.eu/en/webstreaming/special-committee-on-foreign-interference-in-all-democratic-processes-in-european-union-including-di_20210909-0900-COMMITTEE-INGE

82 https://www.europarl.europa.eu/doceo/document/CRE-9-2021-09-15-ITM-009_EN.html

- On Monday **29th November 2021**, the **LIBE Committee** held a meeting with Laurent Richard, Founder and executive director of Forbidden Stories with Sandrine Rigaud, Editor-in-chief of Forbidden Stories; Etienne Maynier, Technologist at Amnesty International's Security Lab; and Wojciech Wiewiórowski, European Data Protection Supervisor;

- The **LIBE Committee** on **1st February 2022** held an exchange of views on the impact on fundamental rights of the Pegasus spyware, with the participation of Szabolcs Panyi, Investigative journalist, Hungary, targeted with Pegasus; Gürkan Özturan, European Centre for Press and Media Freedom, Germany; and Ewa Wrzosek, Prosecutor, Poland, targeted with Pegasus;

- The European Parliament heard the Council and Commission statements and debated in **plenary on 15 February 2022** "The surveillance of politicians, prosecutors, lawyers and journalists, and other persons and entities in EU Member States using cyber surveillance software";

- On 17 February 2022, the EP adopted a **resolution on human rights and democracy in the world** and the European Union's policy on the matter – annual report 2021, where it rang the alarm on Pegasus and on the misuse of surveillance technology and its impact on human rights and called for stronger regulation; [83]

- On **9 March 2022**, the EP adopted the resolution of the INGE committee **on foreign interference in all democratic processes in the European Union, including disinformation**, condemning the use of Pegasus and similar spyware to target journalists, human rights defenders and politicians and calling the Commission to take measures in various fields, from trade to revision of relevant EU laws; [84]

- The EP voted on **10 March 2022** to set up a **Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware;**[85] it then voted on 24 March 2022 on the membership of the special committee, which consists of 38 members, with a 1-year-long mandate, which can be extended. During its first meeting taking place on 19 April 2022, the Chair and the rapporteur were elected, Jeroen Lenaers (EPP, NL) and Sophie In't Veld (Renew, NL), as well as the Vice-chairs. [86]

- The EP held a **plenary debate on 4 May 2022**, on the **Use of the Pegasus Software by EU Member States against individuals including MEPs and the violation of fundamental rights**.

---

[83] See https://www.europarl.europa.eu/doceo/document/TA-9-2022-0041_EN.html, "43. Stresses that recent revelations such as the NSO Pegasus scandal confirm that spying against human rights defenders and journalists, among others, is an extremely alarming matter and appear to confirm the dangers of the misuse of surveillance technology to undermine human rights; calls for the promotion of a safe and open space and greater capacity for civil society organisations, human rights defenders, journalists and other individuals concerned in order to protect them from cyber surveillance and interference; underlines the need for more robust national and international regulation in this area;"

[84] See paragraphs 100 to 106 of the resolution.

[85] See https://www.europarl.europa.eu/doceo/document/TA-9-2022-0071_EN.html; the decision to set up the committee originated from a campaign led by Renew Europe with the support of other groups; the vote in plenary gathered a very large support, with 635 MEPs in favor, 36 against and 20 abstentions.

[86] See the PEGA committee website, https://www.europarl.europa.eu/committees/en/pega/home/highlights. The members of the committee are: PPE (10): Arłukowicz Bartosz, Bilčík Vladimír, Braunsberger-Reinhold Karolin, Falcă Gheorghe, Lenaers Jeroen, Novak Ljudmila, Virkkunen Henna, Vuolo Lucia, Warborn Jörgen, Zoido Álvarez Juan Ignacio; S&D (8): Barley Katarina, Cozzolino Andrea, Guillaume Sylvie, Heide Hannes, Hristov Ivo, Kohut Łukasz, López Aguilar Juan Fernando, Rónai Sándor; Renew (6): Donáth Anna Júlia, In 'T Veld Sophia, Körner Moritz, Thun Und Hohenstein Róża, Tudorache Dragoş, Yenbou Salima; Greens (4): Bricmont Saskia, Delbos-Corfield Gwendoline, Neumann Hannah, Riba I Giner Diana; ID (3): Anderson Christine, Androuët Mathilde, Lebreton Gilles; ECR (3): Kanko Assita, Kempa Beata, Tarczyński Dominik; The Left (2): Ernst Cornelia, Georgiou Giorgos; NI (2): Hidvéghi Balázs, Puigdemont I Casamajó Carles.

3.3. European Data Protection Supervisor

On 15 February 2022, the European Data Protection Supervisor (EDPS) published the paper ***Preliminary Remarks on Modern Spyware***. EDPS states that "revelations made about the Pegasus spyware raised very serious questions about the possible impact of modern spyware tools on fundamental rights, and particularly on the rights to privacy and data protection. This paper aims to contribute to the ongoing assessment in the EU and globally of the **unprecedented risks** posed by this type of surveillance technology. It comes from the EDPS' conviction that the use of Pegasus might lead to an **unprecedented level of intrusiveness**, which threatens the **essence of the right to privacy**, as the spyware is able to interfere with the most intimate aspects of our daily lives." EDPS clearly underlines in the paper that such risks are not only to the right to privacy, but to fundamental freedoms, democracy and the rule of law, as evidence has showed that Pegasus has been used to spy on politicians, journalists, lawyers, opposition leaders, activists and human rights defenders in several Member States.

EDPS underlines that while Art. 4(2) TEU states that "national security remains the sole responsibility of each Member State", Member States have to respect the European Convention on Human Rights and the jurisprudence of the European Court of Human rights, which sets limits to surveillance activities for national security. Furthermore, when used for law enforcement purposes, surveillance has to comply with EU law and notably the **EU Charter of Fundamental Rights**[87] and by EU directives such as the **ePrivacy directive**[88] and the **law enforcement directive.**[89]

EPDS then examines whether Pegasus could be used legally in the scope of EU law and concludes that "regular deployment of Pegasus or similar highly intrusive spyware technology would **not be compatible** with the EU legal order" also because it would encroach on the right to fair trial. The EU should, according to EDPS, **adopt a** "**ban** on the development and deployment of spyware with the capability of Pegasus" and if still used in exceptional situations, a series of guarantees against unlawful use should be adopted and implemented (strengthening the oversight of surveillance measures, full implementation of EU privacy and data protection law, judicial review, criminal procedural rights, no import of illegal intelligence, no political abuse of national security, addressing rule of law problems, support civil society). Also, EDPS states that the **EU dual use regulation** should be strengthened to condition exports of cyber-surveillance items to fundamental rights and privacy, and to cover also imports.[90]

---

87 Art. 7 - 8 - 52(1).

88 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

89 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

90 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). The Regulation was published in the Official Journal on 11 June 2021 and enters into force on 8 September 2021, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821&qid=1651479588233. Also UN bodies (see further in the briefing) and Edward Snowden called for governments to impose a global moratorium on the international spyware trade in order to avoid pervasive violation of privacy and connected abuses, see https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations.

3.4. Council of Europe

The Council of Europe's Parliamentary Assembly has appointed Dutch MEP Pieter Omtzigt (EPP) as rapporteur for the Committee on Legal Affairs and Human Rights on "Pegasus and similar spyware and secret state surveillance".[91]

3.5. United Nations

On 19 July 2022, the **UN High Commissioner for Human Rights Michelle Bachelet** expressed serious concern on spying on journalists, human rights defenders, opposition, and called on companies to exert due human rights diligence, States to protect the right to privacy of persons and for better regulation of the sale, transfer and use of surveillance technologies and ensure strict oversight and authorization for spyware and surveillance.[92]

On 12 August 2021, **UN human rights experts** called on all States to impose a global moratorium on the sale and transfer of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards.[93]

3.6. NGOs

Amnesty International is one of three pillars leading the work on the Pegasus Project in collaboration with Citizens Lab and Forbidden Stories to disclose spyware and surveillance in the world through Pegasus and other spyware. It has also stated that the scale of secretive cyber surveillance is an international human rights crisis in which the NSO Group is complicit.[94]

Human Rights Watch urged to regulate the global trade in surveillance technology and called on governments to ban the sale, export, transfer, and use of surveillance technology until human rights safeguards are in place.[95]

The **International Press Institute** (IPI)[96] denounced the abuse of spying on journalists, calling for formal investigations and accountability. Likewise, the **Media Freedom Rapid Response** (MFRR), a Europe-wide mechanism, which tracks, monitors, and reacts to violations of press and media freedom in the EU Member States and Candidate Countries, called for an immediate investigation into the

---

91 A draft memorandum is available at https://storage.googleapis.com/pieter-omtzigt-website/documenten/Pegasus-memorandum-Omtzigt.pdf.

92 https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner?LangID=E&NewsID=27326 and https://news.un.org/en/story/2021/07/1096142

93 The UN experts are Ms. Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of expression; Ms. Mary Lawlor, Special Rapporteur on the situation of human rights defenders; Mr. Clement Nyaletsossi Voulé, Special Rapporteur on the rights to freedom of peaceful assembly and of association; and UN Working Group on the issue of human rights and transnational corporations and other business enterprises (known as the Working Group on Business and Human Rights), Mr. Surya Deva (Chairperson), Ms. Elzbieta Karska (Vice-Chairperson), Mr. Githu Muigai, Mr. Dante Pesce, and Ms. Anita Ramasastry. See https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=

94 https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/

95 press release of 8 September 2021, https://www.hrw.org/news/2021/09/08/eu-robustly-implement-new-export-rules-surveillance-tech#_ftn4

96 https://ipi.media/pegasus-project-full-investigation-needed-after-180-journalists-targeted-by-spyware/

alleged use of the spyware against journalists by Hungarian authorities and urged the implementation of new EU rules on the export of cyber-surveillance technology around the world. [97]

[97] https://ipi.media/mfrr-eu-action-needed-to-tackle-spyware-abuses-after-pegasus-revelations/

ANNEX 1: EP MAIN ACTIONS ON SURVEILLANCE AND SPYWARE

Echelon

On 5 September 2001, the EP adopted a resolution on the **existence of a global system for the interception of private and commercial communications (ECHELON interception system)**.[98] The draft resolution had been drafted and approved by the temporary committee on the ECHELON system, set up by the EP in 2000. ECHELON was uncovered by media and through STOA researches. It is an interception system using satellite receiver stations and spy satellites with the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents on the basis of searches for keywords.

The system allegedly operated worldwide since the early 1970s on the basis of cooperation agreement involving the UK, the USA, Canada, Australia and New Zealand. It involved not only intelligence on security issues, but also economic and business intelligence, gathered by the authorities of these countries and exchanged among them.[99] The EP called Member States to review their legislation to strengthen privacy guarantees for citizens, as well as against industrial espionage, and enhance the oversight of intelligence services

Prism

In **2013**, the EP adopted a resolution on **the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy**,[100] after the publication of reports in the international press based on information leaked by Edward Snowden, revealing evidence that through programmes such as PRISM, the US authorities are accessing and processing on a large scale the personal data of EU citizens using US internet service providers. The EP condemned such programmes and called for an inquiry by LIBE, which led to the adoption of EP **resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs.**[101] In 2015 the EP adopted another resolution **of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens.**[102]

Hacking team

In 2015, a series of leaks concerning the activities of the Italian company **Hacking Team** revealed that their remote computer surveillance software had been bought by the governments of Hungary, Italy, Germany, Luxembourg, Poland, Spain, Cyprus, the Czech Republic and Switzerland, along with Saudi Arabia, Kazakhstan, Turkey and Sudan, among others. The Italian government restricted the licence of the company to export their products. A few days later, the European Parliament voted to review

98 https://www.europarl.europa.eu/doceo/document/TA-5-2001-0440_EN.html

99 See The Echelon Affair study https://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf, the explanatory statement of the report, https://www.europarl.europa.eu/doceo/document/A-5-2001-0264_EN.html#title3 and the STOA studies listed below.

100 https://www.europarl.europa.eu/doceo/document/TA-7-2013-0322_EN.html

101 https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.html?redirect

102 https://www.europarl.europa.eu/doceo/document/TA-8-2015-0388_EN.html?redirect

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of **dual-use items** (recast).[103]

Other areas of EU and EP activity on Article 2 TEU values, internal security, and cybersecurity

The issue of Pegasus and similar spyware is also related to the respect of the European values listed in **Article 2 TEU** and in the Charter of Fundamental Rights: democracy, rule of law, fundamental rights, notably privacy and data protection. Internal security and cybersecurity are also areas of relevance, notably in the framework of the 2020-2025 **EU Security Union Strategy**[104] covering cybersecurity, notably through the **Network and Information Systems Directive** (NIS).[105] The recent Commission proposal for a Directive on **corporate sustainability due diligence** aiming at fostering sustainable and responsible corporate behaviour throughout global value chains including in relation to human rights could also be of particular relevance.[106]

[103] The Regulation was published in the Official Journal on 11 June 2021 and enters into force on 8 September 2021, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821&qid=1651479588233

[104] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[105] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/0359(COD)&l=en

[106] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1145

ANNEX 2: LIST OF SPYWARE

Among the various spyware and surveillance products that are on the market, the following are mentioned in publicly available reports: Pegasus by NSO group, Cobwebs Technologies, Cognyte, Black Cube, Blue Hawk CI, BellTroX, Cytrox[107], Predator, Candiru, Reign / QuaDream, Paragon[108]; Dark Basin, Circles system, SS7 attack, Cobalt Strike, FinSpy, NetWire, P6 intercept, Galileo, PC 360, Karma, Epeius, StealthAgent, Crimson, Invisible Man, Unlimited Interception System, Skylock, Windshield, Phoreal, Soundbite, OceanLotus tester, Ocean Lotus encryptor, Ocean Lotus Cloudrunner, Ocean Lotus MAC, Komprogo.[109] Among the companies mentioned : Cellebrite, FinFisher, Blue Coat, Hacking Team, CyberPoint, L3 Technologies, Verint and of course NSO Group.[110]

ANNEX 3: STUDIES ON SURVEILLANCE AND SPYWARE

European Parliament studies

Digital technologies as a means of repression and social control (2021), Policy Department for External Relations,
https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653636

Authors: Dorota GŁOWACKA, Richard YOUNGS, Adela PINTEA, Ewelina WOŁOSIK. Administrator responsible: Monika LERCH

Abstract: The proliferation of new and emerging technologies over the past two decades has significantly expanded states' toolkit for repression and social control, deepening human rights problems. While these technologies still have the potential to positively enhance democratic values and human rights, they are now also actively deployed and shaped by many repressive regimes to their own strategic advantage. Globally and regionally, efforts have been made to tackle the challenges that digital technologies pose to human rights, but a lot remains to be done. The EU must enrich global legal and standard-setting efforts, as well as improve its own core foreign policy instruments. The EU's foreign policy toolbox has become more comprehensive in the last several years, with the addition of a number of different strands to its efforts against 'digital authoritarianism'. The challenge related to the use of digital technologies by authoritarian regimes has continued to deepen, however. The EU must therefore continue to find ways to fine-tune and add to this toolbox. A core finding that runs through this report is that the EU has undertaken many valuable and well-designed policy initiatives in this field, but still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level.

[107] These products (together with an unknown Chinese entity) are mentioned in the 16 December 2021 Meta "Threat Report on the Surveillance-for-Hire Industry", see https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/

[108] Mentioned in: https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

[109] These spywares are mentioned in: https://www.top10vpn.com/research/global-spyware-market-index/ (containing a detailed spreadsheet with interesting information).

[110] https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019 and https://data.mendeley.com/datasets/csvhpkt8tm/2.

Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (**2017**), Policy Department for Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137

Authors: Mirja GUTHEIL, Quentin LIGER, Aurélie HEETMAN, James EAGER, Max CRAWFORD, Optimity Advisors. Official responsible: Kristiina MILT

Abstract: the Study, commissioned by the EP's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, presents concrete policy proposals on the use of hacking techniques by law enforcement across the EU Member States. A comparative examination of the legal frameworks for hacking by law enforcement across 6 Member States - France, Germany, Italy, Netherlands, Poland, UK - and 3 non-EU countries - Australia, Israel, US - is conducted, and it is combined with analyses of the international and EU-level debates on the topic and the EU legal basis for intervention in the sector.

Surveillance and censorship: The impact of technologies on human rights (2015), Policy Department, Directorate-General for External Policies, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf

Authors: Ben WAGNER, Centre for Internet and Human Rights, European University Viadrina, GERMANY Joanna BRONOWICKA, Centre for Internet and Human Rights, European University Viadrina, GERMANY Cathleen BERGER, Centre for Internet and Human Rights, European University Viadrina, GERMANY Thomas BEHRNDT, Centre for Internet and Human Rights, European University Viadrina, GERMANY. Official Responsible: Anete BANDON

Abstract: As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This report argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere. It also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The report concludes that EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies

Mass Surveillance - Part 1: Risks and opportunities raised by the current generation of network services and applications (2015), STOA, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf

Authors: Company: TECNALIA Research and Investigation Authors: Arkaitz Gamino Garcia Concepción Cortes Velasco Eider Iturbe Zamalloa Erkuden Rios Velasco Iñaki Eguía Elejabarrieta Javier Herrera Lotero Jason Mansell (Linguistic Review) José Javier Larrañeta Ibañez Stefan Schuster (Editor), Responsible administrator: Peter Ide-Kostic

Abstract: This document identifies the risks of data breaches for users of publicly available Internet services such as email, social networks and cloud computing, and the possible impacts for them and the European Information Society. It presents the latest technology advances allowing the analysis of

user data and their meta-data on a mass scale for surveillance reasons. It identifies technological and organisational measures and the key stakeholders for reducing the risks identified. Finally the study proposes possible policy options, in support of the risk reduction measures identified by the study.

Mass Surveillance - Part 2: Technology foresight, options for longer term security and privacy improvements (2015), STOA
https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf

Authors: Company: Capgemini Consulting Authors: M. van den Berg P. de Graaf (editor) P.O. Kwant T. Slewe. Responsible administrator: Peter Ide-Kostic

Abstract : The main objective of part two of this study is to provide the European Parliament with policy options, based on technology foresight, with regard to the protection of the European Information Society against mass surveillance from a perspective of technology and organisational foresight. Four scenarios with two to four technology options each were developed in this study, leading to twenty-three policy options.

National security and secret evidence in legislation and before the courts: exploring the challenges (2014), Policy Department Citizens' Rights and Constitutional Affairs,
https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf

Authors: Prof. Didier Bigo, Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London Dr Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs Section, Centre for European Policy Studies, CEPS Mr Nicholas Hernanz, Researcher, Justice and Home Affairs Section, CEPS Dr Amandine Scherrer, European Studies Coordinator and Associate Researcher at CCLS. Responsible administrator: Darren NEVILLE

Abstract At the request of the LIBE committee, this study provides a comparative analysis of the national legal regimes and practices governing the use of intelligence information as evidence in the United Kingdom, France, Germany, Spain, Italy, the Netherlands and Sweden. It explores notably how national security can be invoked to determine the classification of information and evidence as 'state secrets' in court proceedings and whether such laws and practices are fundamental rights- and rule of law compliant. The study finds that, in the majority of Member States under investigation, the judiciary is significantly hindered in effectively adjudicating justice and guaranteeing the rights of the defence in 'national security' cases. The research also illustrates that the very term 'national security' is nebulously defined across the Member States analysed, with no national definition meeting legal certainty and "in accordance with the law" standards and a clear risk that the executive and secret services may act arbitrarily. The study argues that national and transnational intelligence community practices and cooperation need to be subject to more independent and effective judicial accountability and be brought into line with EU 'rule of law' standards.

National Programme for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law (2013), Policy Department Citizens' Rights and Constitutional Affairs,
https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

Authors: Prof. Didier Bigo, Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London Dr. Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs Section, Centre for European Policy Studies, CEPS Mr. Nicholas

Hernanz, Research Assistant, Justice and Home Affairs Section, CEPS Dr. Julien Jeandesboz, Assistant Professor at the University of Amsterdam and Associate Researcher at CCLS Ms. Joanna Parkin, Researcher, Justice and Home Affairs Section, CEPS Dr. Francesco Ragazzi, Assistant Professor in International Relations, Leiden University Dr. Amandine Scherrer, European Studies Coordinator and Associate Researcher at CCLS. Responsible administrator: Alessandro Davoli.

Summary: In the wake of the disclosures surrounding PRISM and other US surveillance programmes, this study makes an assessment of the large-scale surveillance practices by a selection of EU member states: the UK, Sweden, France, Germany and the Netherlands. Given the large-scale nature of surveillance practices at stake, which represent a reconfiguration of traditional intelligence gathering, the study contends that an analysis of European surveillance programmes cannot be reduced to a question of balance between data protection versus national security, but has to be framed in terms of collective freedoms and democracy. It finds that four of the five EU member states selected for in-depth examination are engaging in some form of large-scale interception and surveillance of communication data, and identifies parallels and discrepancies between these programmes and the NSA-run operations. The study argues that these surveillance programmes do not stand outside the realm of EU intervention but can be engaged from an EU law perspective via (i) an understanding of national security in a democratic rule of law framework where fundamental human rights standards and judicial oversight constitute key standards; (ii) the risks presented to the internal security of the Union as a whole as well as the privacy of EU citizens as data owners, and (iii) the potential spillover into the activities and responsibilities of EU agencies. The study then presents a set of policy recommendations to the European Parliament.

The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights (2013), Policy Department Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

Summary: In light of the recent PRISM-related revelations, this briefing note analyzes the impact of US surveillance programmes on European citizens' rights. The note explores the scope of surveillance that can be carried out under the US FISA Amendment Act 2008, and related practices of the US authorities which have very strong implications for EU data sovereignty and the protection of European citizens' rights.

Authors: Caspar BOWDEN (Independent Privacy Researcher) , Introduction by Didier BIGO (King's College London / Centre d'Etudes sur les Conflits, Liberté et Sécurité – CCLS, Paris, France). Responsible administrator: Alessandro DAVOLI

Impact of surveillance programmes on EU citizen's rights to privacy (2013), At a Glance, Library briefing, https://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130585/LDM_BRI(2013)130585_REV1_EN.pdf

Author: Franziska ZIBOLD

Summary : On 6 June 2013, articles in the Guardian and Washington Post based on information from former US National Security Agency employee Edward Snowden stoked up the debate on internet data surveillance. Further allegations that US and UK intelligence agencies had accessed and stored large quantities of data followed.

Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011), Policy Department Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

Authors: Aidan WILLS (Geneva Centre for the Democratic Control of Armed Forces - DCAF) and Mathias VERMEULEN (European University Institute - EUI)

Abstract This study evaluates the oversight of national security and intelligence agencies by parliaments and specialised non-parliamentary oversight bodies, with a view to identifying good practices that can inform the European Parliament's approach to strengthening the oversight of Europol, Eurojust, Frontex and, to a lesser extent, Sitcen. The study puts forward a series of detailed recommendations (including in the field of access to classified information) that are formulated on the basis of in-depth assessments of: (1) the current functions and powers of these four bodies; (2) existing arrangements for the oversight of these bodies by the European Parliament, the Joint Supervisory Bodies and national parliaments; and (3) the legal and institutional frameworks for parliamentary and specialised oversight of security and intelligence agencies in EU Member States and other major democracies.

Development of Surveillance Technology and Risk of Abuse of Economic Information - Appraisal of Technologies of Political Control (Volume 1 to 5) (1999), STOA, https://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf

Authors: Peggy Becker (visiting researcher, Directorate General for Research, European Parliament) - Volume 1 Duncan Campbell (IPTV Ltd., Edinburgh, the UK) - Volume 2 Franck Leprevost (Technische Universität Berlin, Germany) - Volume 3 Chris Elliot - Volume 4 and Volume 5 Nikos Bogolikos (Zeus E.E.I.G)

Summary: Volume 1 - Presentation and Analysis. Containing four studies, this volume, commissioned by STOA, on electronic surveillance and the risk of abuse of economic information compares and contrasts the legislation covering fundamental freedoms with the respect for human rights. Volume 2 - The state of the art in communications. Communications Intelligence (COMINT) of automated processing for intelligence purposes of inrtercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition. Volume 3 - Encryption and cryptosystems in electronic surveillance : a survey of the technology assessment issues. Volume 4 - The legality of the interception of electronic communications. A concise survey of the principal legal issues and instruments under international, European and national law. Volume 5 - The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception : Survey of opinions of experts.

Other studies

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

Abstract: The revelations made about the Pegasus spyware raised very serious questions about the possible impact of modern spyware tools on fundamental rights, and particularly on the rights to

privacy and data protection. This paper aims to contribute to the ongoing assessment in the EU and globally of the unprecedented risks posed by this type of surveillance technology. It comes from the EDPS' conviction that the use of Pegasus might lead to an unprecedented level of intrusiveness, which threatens the essence of the right to privacy, as the spyware is able to interfere with the most intimate aspects of our daily lives.

UN, Report of the Working Group on the use of mercenaries, The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities (July 2021), https://www.ohchr.org/en/documents/thematic-reports/a76151-human-rights-impacts-mercenaries-mercenary-related-actors-and

This Report, submitted to the UN General Assembly, examines the provision of military and security products and services in cyberspace by mercenaries, mercenary-related actors and private military and security companies and its human rights impacts. The present thematic study aims towards exploring the manifestations and activities of actors who benefit from developing, maintaining and operating cybercapabilities, which might be used in the conduct of hostilities, in conflict and in non-conflict settings. It assesses the impacts that this may have on human rights, including the right of peoples to self-determination, as well as examines the issue of regulating the provision of military and security products and services in cyberspace.

Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

Abstract: The Special Rapporteur calls "for tighter regulation of surveillance exports and restrictions on their use, as well as a call for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways."

Fundamental Rights Agency, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update (2.73 MB) , 2017

Abstract: This report is FRA's second publication addressing a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic, and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including its oversight.

The country reports are available at: https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu#country-related

Fundamental Rights Agency, Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union - Mapping Member States' legal frameworks (1.93 MB), 2015

This report, drafted in response to the European Parliament's call for thorough research on fundamental rights protection in the context of surveillance, maps and analyses the legal frameworks on surveillance in place in EU Member States.

Ten standards for oversight and transparency of national intelligence services, Institute for Information Law, 2015, https://www.ivir.nl/publicaties/download/1591.pdf

Authors: Sarah Eskens Ot van Daalen Nico van Eijk, Institute for Information Law

Abstract: The main goal of this report is to contribute to the policy debate on surveillance by intelligence services from the perspective of oversight and transparency. Both are considered essential for devising checks and balances in which human rights are respected. By offering this concise list of ten standards, we intend to provide practical guidance for those who seek further input for discussions, policymaking and the review of existing legislation. These standards are based on our analysis and interpretation of relevant jurisprudence, literature and selected policy documents. Standard 1: Intelligence services need to be subject to oversight that is complete. Standard 2: Oversight should encompass all stages of the intelligence cycle. Standard 3: Oversight of the intelligence services should be independent. Standard 4: Oversight should take place prior to the imposition of a measure. Standard 5: Oversight bodies should be able to declare a measure unlawful and provide for redress. Standard 6: Oversight should incorporate the adversary principle. Standard 7: Oversight bodies should have sufficient resources to perform effective oversight. Standard 8: Intelligence services and their oversight bodies should provide layered transparency. Standard 9: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance. Standard 10: Companies and other private legal entities should be able to publish aggregate information on surveillance orders they receive.

Report on the democratic oversight of signals intelligence agencies, European Commission for Democracy through Law - Venice Commission, 2015, on the basis of comments by Mr **Iain Cameron** (Member, Sweden),
https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e

The study looks into democratic control, jurisdiction, accountability including in relation to the ECtHR jurisprudence, internal and governmental controls, parliamentary and judicial reviews and authorisations, accountability to expert bodies, complaint mechanisms.

This In-Depth Analysis, drafted by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs for the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, looks into the confirmed or suspected use of the Pegasus spyware and other similar cyber-surveillance instruments in the EU and its Member States or targeting EU citizens or residents, EU reactions and previous activities on issues related to surveillance.

PE 732.268
Print ISBN 978-92-846-9429-7 | doi: 10.2861/985996 | QA-09-22-184-EN-C
PDF ISBN 978-92-846-9430-3 | doi: 10.2861/165499 | QA-09-22-184-EN-N