Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 2513 (2023)[1]

Pegasus and similar spyware and secret State surveillance

Parliamentary Assembly

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

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

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

4. The Assembly shares these concerns and believes that the use of Pegasus-type spyware should be limited to exceptional situations, as a measure of last resort, to prevent or investigate a specific act amounting to a genuine and serious threat to national security or a specific and precisely defined serious crime, targeting only the person suspected of committing or planning to commit those acts, and always under court supervision. In order to limit such a high level of intrusiveness, States should take into account the proportionality of new spyware before acquiring and using it; they should also consider using spyware without some of the most invasive features of Pegasus or a version that is programmed in such a way that it limits access to what is strictly necessary.

---

1. *Assembly debate* on 11 October 2023 (22nd sitting) (see Doc. 15825, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Pieter Omtzigt). *Text adopted by the Assembly* on 11 October 2023 (22nd sitting).
See also Recommendation 2258 (2023).

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

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

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

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

5.4. Cyprus and Bulgaria serve as export hubs for spyware;

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

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

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

8. If the authorities invoke national security grounds as a justification for using spyware but their real purpose is to target and discredit an opposition politician or to intimidate and silence a human rights defender, the surveillance will give rise to a violation of Article 8 in conjunction with Article 18 of the Convention, which prohibits States from restricting rights for purposes not prescribed by the Convention itself. Such a misuse of power has a chilling effect on the exercise of other human rights and fundamental freedoms, including the freedom of expression (Article 10), the freedom of assembly and association (Article 11) and the right to free elections (Article 3 of Protocol No. 1 to the Convention (ETS No. 9)). It may also undermine the integrity of electoral processes and free public debate, and therefore the foundations of our democratic societies.

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

10. The Assembly underlines that member States have both negative and positive obligations under the Convention. Positive obligations in this area should include the protection of individuals within their jurisdiction from unlawful targeted surveillance by non-state actors and third States (transnational surveillance). This should trigger at the same time a procedural obligation to effectively investigate all cases of alleged unlawful digital surveillance by third actors targeting persons living in the territory of a member State. The Assembly refers in this context to Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business, adopted on 2 March 2016, which recalls that member States have a duty to protect individuals against human rights abuses by third parties, including business enterprises.

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

11.1. Poland, to:

11.1.1. inform the Assembly and the European Commission for Democracy through Law (Venice Commission) about the use of Pegasus and similar spyware, within three months;

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

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

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

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

11.2. Hungary, to:

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

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

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

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

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

11.3. Greece, to:

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

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

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

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

11.4. Spain, to:

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

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

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

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

11.5. Azerbaijan, to:

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

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

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

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

12. The Assembly considers that the Polish parliamentary election of 2019 was unfair as Pegasus was used against political opponents during the electoral campaign.

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

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

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

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

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

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

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

14.6. ratify, if they have not yet done so, the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), known as “Convention 108+”, which will apply to the processing of data for national security purposes, and already start implementing its standards in national law;

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

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

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

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

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

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

17. The Assembly calls on:

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

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

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

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

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

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

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

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

19. The Assembly invites the European Union to sign and ratify Convention 108+, make use of the Council of Europe’s expertise in this field, and engage with its relevant bodies in areas such as data protection, targeted surveillance and spyware, for the purposes of standard setting, monitoring and co-operation.