CAMERA DEI DEPUTATI

Doc. **XII**-*bis*
n. **85**

ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA

Raccomandazione n. 2513

Pegasus e altri *spyware* simili e la sorveglianza segreta da parte di Stati

Trasmessa il 16 ottobre 2023

PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE

RESOLUTION 2513 (2023) [1]

Provisional version

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. 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 EU export rules.

3. The Parliamentary Assembly notes that Pegasus is a highly intrusive surveillance spyware, which grants the user complete and unrestricted access to all sensors and information 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 require some action on the part of the victim, such as clicking on a link (for instance, Predator) or opening an attachment, Pegasus is installed through a so-called « zero-click attack ». Given its unprecedented level of intrusiveness into the private life of the targeted individual and all their contacts, the Council of Eu-

(1) *Assembly debate* on 13 October 2023 (24th sitting) (see Doc. 15829, report of the Committee on Social Affairs, Health and Sustainable Development, rapporteur: Mr Simon Moutquin). *Text adopted by the Assembly* on 13 October 2023 (24th sitting).

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

5. The Assembly is deeply worried about mounting evidence that Pegasus and similar spyware have been used illegally or for illegitimate purposes by several member States, including against journalists, political opponents, human rights defenders and lawyers. Pegasus and other spyware 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. It 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 and other ministers' phones were infected with Pegasus, allegedly by a third country (Morocco). 65 persons related to the Catalan pro-independence movement were allegedly targeted with Pegasus and/or Candiru, 18 of whom have been confirmed as lawful targets by the Spanish authorities;

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

5.5. spyware companies are or were present in several member States, including Austria, Bulgaria, Cyprus, France, Germany, Greece, 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. Secretly surveilling political opponents, public officials, journalists, human rights defenders and civil society actors for purposes other than those exhaustively enumerated in Article 8.2 of the European Convention on Human Rights (ETS No. 5, « 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 and similar spyware was lawful under domestic law and compliant with the Convention and other international standards. This implies assessing in each individual case whether the interference pursued a legitimate aim under Article 8.2 of the Convention and whether it was strictly necessary in a democratic society and proportionate to that aim. It also means ensuring that all victims of spyware-related abuses have access to effective remedies and redress. In this context, the Assembly urges:

11.1. Poland, to:

11.1.1. inform the Assembly and the 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 on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance;

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

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

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

11.2. Hungary, to:

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

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

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

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

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

11.3. Greece, to:

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

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

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

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

11.4. Spain, to:

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

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

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

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

11.5. Azerbaijan, to:

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

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

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

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

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

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

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

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

14.2. ensure that the implementation of their legislative framework is effectively in line with the case- law of the European

Court of Human Rights on targeted surveillance, with respect to legality, legitimacy, necessity and proportionality of any surveillance measure;

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

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

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 the automatic processing of personal data (CETS No. 223) known as « Convention 108+ », which will apply to the processing of data for national security purposes, and already start implementing its standards in national law;

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

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

14.9. join the Wassenaar Arrangement if they have not yet done so, and for States already participating in this arrangement, develop a human rights-based framework for the transfer of spyware technologies, according to which export licenses would require a human rights impact assessment of the recipient State and the companies' compliance with the 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 the CM/Rec(2016)3 of Committee of Ministers, and implement standards restricting public procurement contracts to only those companies which demonstrate that they apply human rights due diligence.

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

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

17. The Assembly calls on:

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

17.1.1. strengthen its export control mechanisms to ensure that export licenses are denied or revoked with respect to spyware technologies where there is a substantial risk that those technologies could be used for internal or transnational repression and/or 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 Israeli-based companies;

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

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

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

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

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

ASSEMBLÉE PARLEMENTAIRE DU CONSEIL DE L'EUROPE

RÉSOLUTION 2513 (2023) [1]

Version provisoire

Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État

Assemblée parlementaire

1. En juillet 2021, une coalition internationale de journalistes d'investigation coordonnée par Forbidden Stories, avec le soutien technique du laboratoire de sécurité d'Amnesty International (« le Projet Pegasus »), a publié des informations sur une fuite concernant une liste de plus de 50 000 numéros de téléphone désignés comme des cibles potentielles par des clients de NSO Group, une société israélienne qui a développé et commercialise dans le monde entier un logiciel espion appelé Pegasus. Cette liste comprenait des défenseurs des droits humains, des opposants politiques, des avocats, des diplomates, des chefs d'État et près de 200 journalistes de 24 pays. 11 pays dans le monde ont été identifiés comme clients potentiels de NSO, dont deux États membres du Conseil de l'Europe, l'Azerbaidjan et la Hongrie.

2. Des rapports d'enquête ultérieurs, notamment ceux du CitizenLab de l'Université de Toronto, ont révélé que les gouvernements de plusieurs États membres du Conseil de l'Europe ont acquis et utilisé Pegasus pour exercer une surveillance ciblée de leurs propres citoyens. On sait que Pegasus a été vendu à au moins 14 pays de l'Union européenne, dont la Belgique, l'Allemagne (dans une version modifiée), la Hongrie, le Luxembourg, les Pays-Bas, la Pologne et l'Espagne. Il existe des preuves solides que l'Azerbaidjan l'a également utilisé, y compris lors du conflit avec l'Arménie. D'autres États membres ont acquis ou utilisé des logiciels espions similaires, notamment Candiru et Predator. Ces outils ont non seulement été employés dans le cadre de la juridiction des États membres, mais ils ont également été exportés vers des pays tiers ayant des régimes autoritaires et présentant un risque élevé de violations des droits humains, notamment la Libye (sous le régime de Kadhafi), l'Égypte, Madagascar et le Soudan. Ces exportations sont susceptibles d'avoir enfreint les règles de l'Union européenne en matière d'exportation.

3. L'Assemblée note que Pegasus est un logiciel espion très intrusif, qui donne à l'utilisateur un accès complet et illimité à tous les capteurs et à toutes les informations du téléphone portable ciblé. Il transforme le smartphone en dispositif de surveillance 24 heures sur 24, en accédant à l'appareil photo et au microphone, aux données de géolocalisation, aux courriers

---

(1) *Discussion par l'Assemblée* le 13 octobre 2023 (24e séance) (voir Doc. 15829, rapport de la commission des questions sociales, de la santé et du développement durable, rapporteur: M. Simon Moutquin). *Texte adopté par l'Assemblée* le 13 octobre 2023 (24e séance).

électroniques, aux messages, aux photos, aux vidéos, aux mots de passe et aux applications. Si certains logiciels espions nécessitent une action de la part de la victime, comme un clic sur un lien (par exemple, Predator) ou l'ouverture d'une pièce jointe, Pegasus est installé par une attaque dite « sans clic ». Compte tenu du degré d'intrusion sans précédent dans la vie privée de la personne ciblée et de tous ses contacts, la Commissaire aux droits de l'homme du Conseil de l'Europe et le Contrôleur européen de la protection des données ont exprimé de sérieux doutes sur le fait que ce type de logiciel puisse satisfaire à l'exigence de proportionnalité et, par conséquent, respecter les droits humains.

4. L'Assemblée partage ces préoccupations et estime que l'utilisation de logiciels espions de type Pegasus devrait être limitée à des situations exceptionnelles et comme mesure de dernier ressort, pour prévenir ou enquéter sur un acte spécifique constituant une menace réelle et sérieuse pour la sécurité nationale ou un crime grave spécifique et précisément défini, en ciblant uniquement la personne soupgonnée d'avoir commis ou prévu de commettre ces actes, et toujours être soumise à un contrôle juridictionnel. Afin de limiter un niveau d'intrusion aussi élevé, les États devraient tenir compte de la proportionnalité des nouveaux logiciels espions avant de les acquérir et de les utiliser; ils devraient également envisager d'utiliser des logiciels espions dépourvus de certaines des caractéristiques les plus invasives de Pegasus ou une version programmée de telle sorte qu'elle limite l'accès au strict nécessaire.

5. L'Assemblée est profondément préoccupée par les preuves de plus en plus nombreuses que Pegasus et des logiciels espions similaires ont été utilisés illégalement ou à des fins illégitimes par plusieurs États membres, notamment contre des journalistes, des opposants politiques, des défenseurs des droits humains et des avocats. Pegasus et d'autres logiciels espions ont également été exportés depuis les États membres vers des régimes autoritaires hors d'Europe, en violation éventuelle des règles de l'Union européenne en matière d'exportation. L'Assemblée se félicite de l'enquéte approfondie menée par la commission d'enquéte du Parlement européen chargée d'enquéter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents (commission PEGA), qui a abouti à l'adoption d'une recommandation par le Parlement européen le 15 juin 2023. Elle note à cet égard que la commission PEGA et le Parlement européen ont constaté ce qui suit:

5.1. en Pologne et en Hongrie, le logiciel espion de surveillance Pegasus a été déployé illégalement à des fins politiques pour espionner des journalistes, des responsables politiques de l'opposition, des avocats, des procureurs et des acteurs de la société civile, apparemment dans le cadre d'un système ou d'une stratégie intégrée;

5.2. en Grèce, il a été confirmé qu'un député européen et un journaliste avaient été mis sur écoute par l'agence de renseignement et ciblés par le logiciel espion Predator, et les médias ont révélé d'autres cibles potentielles de Predator, notamment d'autres personnalités politiques de premier plan. Le logiciel espion semble avoir été utilisé de manière ponctuelle à des fins politiques et financières;

5.3. en Espagne, les téléphones du Premier ministre et d'autres ministres ont été infectés par Pegasus, qui aurait été installé par un pays tiers (le Maroc). 65 personnes liées au mouvement indépendantiste catalan auraient été visées par Pegasus et/ou Candiru, et 18 d'entre elles ont été confirmées comme étant des cibles légales par les autorités espagnoles;

5.4. Chypre et la Bulgarie servent de plaques tournantes pour l'exportation de logiciels espions;

5.5. les sociétés de logiciels espions sont ou étaient présentes dans plusieurs États membres, notamment l'Autriche, la Bulgarie, Chypre, la France, l'Allemagne, la Grèce, l'Irlande, l'Italie, le Luxembourg, la Roumanie et la Suisse.

6. L'Assemblée note en outre que, selon les révélations du « Projet Pegasus », l'Azer-

baidjan a également utilisé Pegasus, notamment contre des journalistes, des propriétaires de médias indépendants et des militants de la société civile. Des rapports récents ont révélé son utilisation dans le cadre du conflit entre l'Arménie et l'Azerbaidjan, à l'encontre de 12 personnes travaillant en Arménie, dont un représentant du gouvernement arménien, dans ce qui semble étre un exemple de surveillance ciblée transnationale.

7. L'Assemblée condamne catégoriquement l'utilisation de logiciels espions par les autorités publiques à des fins politiques. La surveillance secrète des opposants politiques, des agents publics, des journalistes, des défenseurs des droits humains et des acteurs de la société civile à des fins autres que celles énumérées de manière exhaustive à l'article 8.2 de la Convention européenne des droits de l'homme (STE nº 5, « la Convention ») (parmi lesquelles la défense de l'ordre, la prévention des infractions pénales et la protection de la sécurité nationale et de la sureté publique) constitue une violation manifeste du droit au respect de la vie privée (article 8).

8. Si les autorités invoquent des raisons de sécurité nationale pour justifier l'utilisation d'un logiciel espion alors que leur véritable objectif est de cibler et de discréditer un responsable politique de l'opposition ou d'intimider et de réduire au silence un défenseur des droits humains, la surveillance donnera lieu à une violation de l'article 8 en liaison avec l'article 18 de la Convention, qui interdit aux États de restreindre les droits à des fins non prévues par la Convention elle-méme. Un tel abus de pouvoir a un effet dissuasif sur l'exercice d'autres droits humains et libertés fondamentales, notamment la liberté d'expression (article 10), la liberté de réunion et d'association (article 11) et le droit à des élections libres (article 3 du Protocole nº 1 à la Convention (STE nº 009)). Il peut également porter atteinte à l'intégrité des processus électoraux et au libre débat public, et par conséquent aux fondements de nos sociétés démocratiques.

9. Le fait de prendre pour cible des journalistes a une incidence sur la confidentialité de leurs sources et, par conséquent, sur leur liberté de communiquer des informations. Le fait de prendre pour cible des communications entre un avocat et son client porte atteinte à l'exercice des droits de la défense et au droit à un procès équitable garanti par l'article 6 de la Convention, qui est un principe fondamental de l'État de droit.

10. L'Assemblée souligne que les États membres ont des obligations à la fois négatives et positives nées de la Convention. Les obligations positives dans ce domaine devraient inclure la protection des personnes relevant de leur juridiction contre une surveillance ciblée illégale par des acteurs non étatiques et des États tiers (surveillance transnationale). Celle-ci devrait déclencher en méme temps une obligation procédurale de mener une enquéte effective sur tous les cas d'allégations de surveillance numérique illégale par des acteurs tiers ciblant des personnes vivant sur le territoire d'un État membre. L'Assemblée renvoie à ce propos à la Recommandation CM/Rec(2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises, adoptée le 2 mars 2016, qui rappelle que les États membres ont le devoir de protéger les personnes contre les violations des droits humains commises par des tiers, y compris des entreprises.

11. L'Assemblée considère que les autorités nationales d'enquéte et les tribunaux des États membres accusés d'utiliser abusivement des logiciels espions doivent mener des enquétes approfondies et déterminer si l'utilisation de Pegasus et de logiciels espions similaires était légal au regard du droit interne et conforme à la Convention et à d'autres normes internationales. Cela implique également d'évaluer dans chaque cas si l'ingérence poursuivait un but légitime au sens de l'article 8.2 de la Convention et si elle était strictement nécessaire dans une société démocratique et proportionnée à ce but. Cela implique aussi de veiller à ce que toutes les victimes d'abus liés aux logiciels espions aient accès à des

voies de recours et à des réparations effectives. Dans ce contexte, l'Assemblée exhorte:

11.1. la Pologne:

11.1.1. à informer l'Assemblée et la Commission européenne pour la démocratie par le droit (Commission de Venise) de l'utilisation de Pegasus et de logiciels espions similaires, dans un délai de trois mois;

11.1.2. à mener des enquêtes effectives, indépendantes et rapides sur tous les cas avérés et supposés d'utilisation abusive de logiciels espions et offrir une réparation suffisante aux victimes ciblées en cas de surveillance illégale;

11.1.3. à s'abstenir d'invoquer des règles générales de confidentialité pour refuser l'accès des mécanismes de contróle et des personnes ciblées aux informations relatives à l'utilisation de logiciels espions;

11.1.4. à appliquer des sanctions appropriées, pénales ou administratives, en cas d'abus;

11.1.5. à se conformer à l'avis de la Commission de Venise relatif à la loi de 2016 sur la police;

11.2. la Hongrie:

11.2.1. à informer l'Assemblée et la Commission de Venise de l'utilisation de Pegasus et de logiciels espions similaires, dans un délai de trois mois;

11.2.2. à mener des enquêtes effectives, indépendantes et rapides sur tous les cas avérés et supposés d'utilisation abusive de logiciels espions et offrir une réparation suffisante aux victimes ciblées en cas de surveillance illégale;

11.2.3. à s'abstenir d'invoquer des règles générales de confidentialité pour refuser l'accès des mécanismes de contróle et des personnes ciblées aux informations relatives à l'utilisation de logiciels espions;

11.2.4. à appliquer des sanctions appropriées, pénales ou administratives, en cas d'abus;

11.2.5. à mettre en reuvre sans délai les arréts *Szabó et Vissy* et *Huttl*, comme l'exige le Comité des Ministres dans l'exercice de ses compétences au titre de l'article 46.2 de la Convention;

11.3. la Grèce:

11.3.1. à informer l'Assemblée et la Commission de Venise de l'utilisation de Predator et de logiciels espions similaires, dans un délai de trois mois;

11.3.2. à mener des enquêtes effectives, indépendantes et rapides sur tous les cas avérés et supposés d'utilisation abusive de logiciels espions et offrir une réparation suffisante aux victimes ciblées en cas de surveillance illégale;

11.3.3. à s'abstenir d'invoquer des règles générales de confidentialité pour refuser l'accès des mécanismes de contróle et des personnes ciblées aux informations relatives à l'utilisation de logiciels espions;

11.3.4. à appliquer des sanctions appropriées, pénales ou administratives, en cas d'abus;

11.4. l'Espagne:

11.4.1. à informer l'Assemblée et la Commission de Venise de l'utilisation de Pegasus, Candiru et de logiciels espions similaires, dans un délai de trois mois;

11.4.2. à mener des enquêtes effectives, indépendantes et rapides sur tous les cas avérés et supposés d'utilisation abusive de logiciels espions et offrir une réparation suffisante aux victimes ciblées en cas de surveillance illégale;

11.4.3. à s'abstenir d'invoquer des règles générales de confidentialité pour refuser l'accès des mécanismes de contróle et des personnes ciblées aux informations relatives à l'utilisation de logiciels espions;

11.4.4. à appliquer des sanctions appropriées, pénales ou administratives, en cas d'abus;

11.5. l'Azerbaidjan:

11.5.1. à informer l'Assemblée et la Commission de Venise de l'utilisation de Pegasus et de logiciels espions similaires, dans un délai de trois mois;

11.5.2. à mener des enquêtes effectives, indépendantes et rapides sur tous les cas avérés et supposés d'utilisation abusive de logiciels espions et offrir une réparation suffisante aux victimes ciblées en cas de surveillance illégale;

11.5.3. à s'abstenir d'invoquer des règles générales de confidentialité pour refuser l'accès des mécanismes de contróle et des personnes ciblées aux informations relatives à l'utilisation de logiciels espions;

11.5.4. à appliquer des sanctions appropriées, pénales ou administratives, en cas d'abus.

12. L'Assemblée considère que les élections législatives polonaises de 2019 n'ont pas été équitables car Pegasus a été utilisé contre des opposants politiques pendant la campagne électorale.

13. L'Assemblée appelle les États membres qui semblent avoir acquis ou utilisé Pegasus, notamment l'Allemagne, la Belgique, le Luxembourg et les Pays-Bas, à clarifier le cadre de son utilisation et les mécanismes de contróle applicables. Elles les invite à envoyer ces informations, ainsi que toute statistique sur l'utilisation de Pegasus, à l'Assemblée et à la Commission de Venise dans un délai de trois mois.

14. Afin de prévenir de futures utilisations abusives de logiciels espions et des violations des droits humains en Europe et ailleurs, l'Assemblée appelle tous les États membres:

14.1. à veiller à ce que leur législation nationale sur la surveillance secrète soit pleinement conforme aux exigences de la Cour européenne des droits de l'homme et de la Commission de Venise en ce qui concerne la qualité de la législation, les procédures d'autorisation, les mécanismes de supervision et de contróle, les mécanismes de notification et les voies de recours, et les réviser si nécessaire;

14.2. à veiller à ce que la mise en reuvre de leur cadre législatif soit effectivement conforme à la jurisprudence de la Cour européenne des droits de l'homme en matière de surveillance ciblée s'agissant de la légalité, la légitimité, la nécessité et la proportionnalité de toute mesure de surveillance;

14.3. dans l'attente de l'évaluation de leur cadre législatif et de leurs pratiques par la Commission de Venise, à s'abstenir d'utiliser des outils tels que Pegasus, Candiru, Predator ou des logiciels espions similaires;

14.4. à moyen terme, à réglementer spécifiquement l'acquisition et l'utilisation de logiciels espions par les services de police et de renseignement, en limitant l'utilisation de logiciels espions de type Pegasus à des situations exceptionnelles comme mesure de dernier ressort, pour prévenir ou enquéter sur un acte précis constituant une menace réelle et sérieuse pour la sécurité nationale ou un crime grave spécifique et précisément défini, et en ciblant uniquement la personne soupgonnée d'avoir commis ou prévu de commettre ces actes. Les États devraient également mettre en place des mécanismes de contróle, notamment parlementaire, de l'acquisition et l'utilisation des technologies de logiciels espions, et intégrer l'obligation de prendre en compte des considérations de proportionnalité avant d'acquérir et d'utiliser de nouveaux logiciels espions;

14.5. à ériger en infraction la vente et l'utilisation de logiciels espions par des acteurs non étatiques;

14.6. à ratifier, s'ils ne l'ont pas encore fait, le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (STCE nº 223), connu sous le nom de « Convention 108+ », qui s'appliquera au traitement des données à des fins de sécurité nationale, et à commencer d'ores et déjà à mettre en reuvre ses normes dans le droit national;

14.7. à ratifier, s'ils ne l'ont pas encore fait, la Convention sur la cybercriminalité (STE nº 185, « Convention de Budapest ») et ses protocoles additionnels;

14.8. à s'abstenir d'accorder des licences d'exportation de technologies de logi-

ciels espions à des pays où il existe un risque important que ces technologies soient utilisées à des fins de répression interne ou transnationale et/ou pour commettre des violations des droits humains, et à annuler celles qui ont été accordées dans de tels cas;

14.9. à adhérer à l'Arrangement de Wassenaar s'ils ne l'ont pas encore fait et, pour les États qui participent déjà à cet arrangement, à élaborer un cadre fondé sur les droits humains pour le transfert des technologies de logiciels espions, en vertu duquel les licences d'exportation seraient soumises à une évaluation de l'impact sur les droits humains de l'État destinataire et à la vérification du respect par les entreprises des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme;

14.10. à exiger que toutes les entreprises de logiciels espions domiciliées ou menant des activités importantes dans leur juridiction appliquent une diligence raisonnable en matière de droits humains dans l'ensemble de leurs opérations ou en ce qui concerne ces activités, conformément à la recommandation CM/Rec(2016)3 du Comité des Ministres, et à mettre en reuvre des normes limitant l'accès des marchés publics aux seules entreprises qui démontrent qu'elles appliquent une diligence raisonnable en matière de droits humains.

15. L'Assemblée demande à la Commission de Venise d'évaluer le cadre législatif et la pratique en matière de surveillance ciblée de tous les États membres (en priorité la Pologne, la Hongrie, la Grèce, l'Espagne, et l'Azerbaidjan; et ensuite l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas et tous les autres Etats membres), afin de déterminer si ce cadre contient des garanties appropriées et effectives contre tout abus éventuel de logiciels espions, eu égard à la Convention et à d'autres normes du Conseil de l'Europe. Compte tenu du degré d'intrusion de Pegasus et des logiciels espions similaires, une législation claire et précise, des mécanismes de contrôle solides, des garanties procédurales et des recours effectifs doivent étre en place avant que les États membres puissent continuer à utiliser ces outils.

16. L'Assemblée est convaincue que le mécanisme d'évaluation et de contrôle prévu dans le Protocole STCE nº 223 permettra d'assurer le suivi de la mise en reuvre des dispositions pertinentes de la Convention 108+ à dans le domaine de la surveillance ciblée à des fins de sécurité nationale et d'application de la loi, y compris l'utilisation de logiciels espions.

17. L'Assemblée appelle:

17.1. Israel, qui bénéficie du statut d'observateur auprès de l'Assemblée:

17.1.1. à renforcer ses mécanismes de contrôle des exportations afin de s'assurer que les licences d'exportation sont refusées ou annulées pour les technologies des logiciels espions lorsqu'il existe un risque important que ces technologies soient utilisées à des fins de répression interne ou transnationale et/ou pour commettre des violations des droits humains;

17.1.2. à coopérer pleinement aux enquétes menées par les États membres du Conseil de l'Europe sur l'utilisation de Pegasus et d'autres logiciels espions exportés d'Israel ou vendus par des sociétés basées en Israel;

17.1.3. à publier son cadre sur le contrôle des exportations et à en informer l'Assemblée dans un délai de six mois;

17.2. le Maroc, qui bénéficie du statut de partenaire pour la démocratie auprès de l'Assemblée:

17.2.1. à informer l'Assemblée, dans un délai de trois mois, s'il a utilisé Pegasus ou un logiciel espion similaire dans son pays et à l'étranger;

17.2.2. à ouvrir dans un délai de trois mois une enquéte totalement indépendante sur l'utilisation présumée de Pegasus par les autorités de l'État contre des cibles au Maroc et des cibles relevant de la juridiction des États membres du Conseil de l'Europe.

18. L'Assemblée appelle également les entreprises de logiciels espions et de sur-

veillance domiciliées dans les États membres du Conseil de l'Europe ou menant des activités importantes dans leur juridiction à faire preuve de diligence raisonnable en matière de droits humains dans l'ensemble de leurs opérations ou en ce qui concerne ces activités et à améliorer la transparence, conformément à la recommandation CM/Rec(2016)3 du Comité des Ministres et aux Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme;

19. L'Assemblée invite l'Union européenne à signer et à ratifier la Convention 108 +, à utiliser l'expertise du Conseil de l'Europe dans ce domaine, et à collaborer avec ses organes compétents dans des domaines tels que la protection des données, la surveillance ciblée et les logiciels espions, à des fins d'établissement de normes, de suivi et de coopération.

ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA

RACCOMANDAZIONE 2513 (2023) [1]

Pegasus e altri spyware simili e la sorveglianza segreta da parte di Stati

ASSEMBLEA PARLAMENTARE

1. Nel luglio 2021, una coalizione internazionale di giornalisti investigativi coordinata da *Forbidden Stories*, con il supporto tecnico del Security Lab di Amnesty International (« Progetto Pegasus »), ha pubblicato informazioni su un elenco, che era trapelato, di oltre 50.000 numeri di telefono identificati come potenziali obiettivi dai clienti di una società israeliana, NSO Group, che ha sviluppato e commercializza a livello globale uno spyware chiamato Pegasus. L'elenco comprendeva difensori dei diritti umani, oppositori politici, avvocati, diplomatici, capi di Stato e quasi 200 giornalisti di 24 Paesi. Undici Paesi del mondo sono stati identificati come potenziali clienti di NSO, compresi due Stati membri del Consiglio d'Europa, l'Azerbaigian e l'Ungheria.

2. Successivi rapporti investigativi, tra cui quello del CitizenLab dell'Università di Toronto, hanno rivelato che i governi di diversi Stati membri del Consiglio d'Europa hanno acquistato e utilizzato Pegasus per la sorveglianza mirata dei propri cittadini. È noto che Pegasus è stato venduto ad almeno 14 Paesi dell'Unione Europea, tra cui Belgio, Germania (in una versione modificata), Ungheria, Lussemburgo, Paesi Bassi, Polonia e Spagna. Ci sono solide prove che anche l'Azerbaigian lo abbia utilizzato, compreso durante il conflitto con l'Armenia. Altri Stati membri hanno acquisito o usato spyware simili, come Candiru e Predator. Questi strumenti non sono stati utilizzati solo all'interno della giurisdizione degli Stati membri, ma sono stati anche esportati in Paesi terzi con regimi autoritari ad alto rischio di violazione dei diritti umani, tra cui Libia (sotto il regime di Gheddafi), Egitto, Madagascar e Sudan. Queste esportazioni hanno potenzialmente violato le norme dell'UE in materia.

3. L'Assemblea parlamentare osserva che Pegasus è uno spyware di sorveglianza altamente intrusivo, che garantisce all'utente un accesso completo e illimitato a tutti i sensori e alle informazioni del telefono cellulare preso di mira. Trasforma lo smartphone in un dispositivo di sorveglianza attivo 24 ore su 24, accedendo a fotocamera e microfono, dati di geolocalizzazione, e-mail, messaggi, foto, video, password e applicazioni. Mentre alcuni spyware richiedono un'azione da parte della vittima, come cliccare su un link (ad esempio, Predator) o aprire un allegato, Pegasus viene installato attraverso un cosiddetto « attacco zero-click ». Dato il livello di intrusione senza precedenti nella privacy dell'individuo preso di mira e di tutti i suoi contatti, il Commissario per i diritti umani

---

(1) Dibattito in Assemblea del 13 ottobre 2023 (24° seduta) (V. Doc.15829, relazione della Commissione Affari sociali, salute e sviluppo sostenibile, relatore: Simon Moutquin). Testo adottato dall'Assemblea il 13 ottobre 2023 (24° seduta).
V. anche la Risoluzione 2521 (2023).

del Consiglio d'Europa e il Garante europeo per la protezione dei dati hanno espresso seri dubbi sulla possibilità che il suo utilizzo potrà mai soddisfare il requisito di proporzionalità e quindi essere conforme ai diritti umani.

4. L'Assemblea condivide queste preoccupazioni e ritiene che l'uso di spyware tipo Pegasus dovrebbe essere limitato a situazioni eccezionali, come misura utilizzata in ultima istanza per prevenire o indagare su un atto specifico che rappresenta una minaccia grave e reale alla sicurezza nazionale o su un reato grave specifico e definito con precisione e solo per colpire la persona sospettata di aver commesso o di pianificare di commettere tali atti e sempre sotto controllo giudiziario. Per limitare un livello così elevato di intrusività, gli Stati dovrebbero prendere in considerazione la proporzionalità dei nuovi software spia prima di acquisirli e utilizzarli; dovrebbero inoltre considerare l'utilizzo di spyware privi di alcune delle caratteristiche più invasive di Pegasus o di una versione programmata in modo tale da limitare l'accesso allo stretto necessario.

5. L'Assemblea è profondamente preoccupata per le prove sempre più evidenti che Pegasus e spyware simili sono stati usati illegalmente o per scopi illegittimi da diversi Stati membri, anche contro giornalisti, oppositori politici, difensori dei diritti umani e avvocati. Pegasus e altri software spia sono stati anche esportati dagli Stati membri verso regimi autoritari al di fuori dell'Europa, potenzialmente in violazione delle norme dell'Unione Europea in materia di esportazioni. L'Assemblea accoglie con favore l'indagine approfondita condotta dalla Commissione d'inchiesta del Parlamento europeo incaricata di esaminare l'uso di Pegasus e di spyware di sorveglianza equivalenti (Commissione PEGA), che ha portato all'adozione di una raccomandazione da parte del Parlamento europeo il 15 giugno 2023. A questo proposito, rileva che la commissione PEGA e il Parlamento europeo hanno riscontrato che:

5.1. in Polonia e Ungheria, il software di sorveglianza Pegasus è stato utilizzato illegalmente a fini politici per spiare giornalisti, politici dell'opposizione, avvocati, procuratori e attori della società civile, apparentemente come parte di un sistema o di una strategia integrata;

5.2. in Grecia, è stato confermato che un membro del Parlamento europeo e un giornalista sono stati intercettati dall'agenzia di intelligence e presi di mira con lo spyware Predator e i media hanno rivelato ulteriori possibili obiettivi di Predator, tra cui altri politici di alto profilo. Sembra che lo spyware sia stato utilizzato *ad hoc* per ottenere vantaggi politici e finanziari;

5.3. in Spagna, i telefoni del Primo Ministro e di altri ministri sono stati infettati da Pegasus, presumibilmente da un Paese terzo (Marocco). 65 persone legate al movimento indipendentista catalano sono state presumibilmente prese di mira con Pegasus e/o Candiru, 18 delle quali sono state confermate come obiettivi legittimi dalle autorità spagnole;

5.4. Cipro e la Bulgaria fungono da *hub* per l'esportazione di spyware;

5.5. le aziende produttrici di spyware sono o erano presenti in diversi Stati membri, tra cui Austria, Bulgaria, Cipro, Francia, Germania, Grecia, Irlanda, Italia, Lussemburgo, Romania e Svizzera.

6. L'Assemblea osserva inoltre che, secondo le rivelazioni del « Progetto Pegasus », anche l'Azerbaigian ha utilizzato Pegasus, tra gli altri contro giornalisti, proprietari di media indipendenti e attivisti della società civile. Recenti rapporti hanno rivelato il suo utilizzo in relazione al conflitto tra Armenia e Azerbaigian, contro 12 persone che lavoravano in Armenia, tra cui un funzionario del governo armeno, in quello che sembra essere un esempio di sorveglianza mirata transnazionale.

7. L'Assemblea condanna inequivocabilmente l'uso di spyware da parte delle autorità statali a scopi politici. Sorvegliare segretamente oppositori politici, funzionari pubblici, giornalisti, difensori dei diritti umani e attori della società civile per scopi diversi da quelli esaustivamente elencati all'articolo 8.2 della Convenzione europea

dei diritti dell'uomo (STE n. 5, « la Convenzione ») (tra cui la prevenzione di disordini o crimini e la protezione della sicurezza nazionale e della pubblica sicurezza) equivale a una chiara violazione del diritto al rispetto della privacy (articolo 8).

8. Se le autorità invocano motivi di sicurezza nazionale come giustificazione per l'utilizzo di software spia, ma il loro vero scopo è quello di colpire e screditare un politico dell'opposizione o intimidire e mettere a tacere un difensore dei diritti umani, la sorveglianza equivale a una violazione dell'articolo 8 in combinato disposto con l'articolo 18 della Convenzione, che vieta agli Stati di limitare i diritti per scopi non previsti dalla Convenzione stessa. Un tale abuso di potere ha un effetto dissuasivo sull'esercizio di altri diritti umani e libertà fondamentali, tra cui la libertà di espressione (articolo 10), la libertà di riunione e di associazione (articolo 11) e il diritto a libere elezioni (articolo 3 del Protocollo n. 1 della Convenzione (STE n. 009)). Può anche minare l'integrità dei processi elettorali e il libero dibattito pubblico e, quindi, le fondamenta stesse delle nostre società democratiche.

9. Il fatto di prendere di mira i giornalisti ha un impatto sulla riservatezza delle loro fonti e, di conseguenza, sulla libertà di informare. L'intercettazione delle comunicazioni tra avvocati e clienti compromette l'esercizio dei diritti della difesa e il diritto a un processo equo garantito dall'articolo 6 della Convenzione, che è un principio fondamentale dello Stato di diritto.

10. L'Assemblea sottolinea che gli Stati membri hanno obblighi sia negativi che positivi ai sensi della Convenzione. Gli obblighi positivi in questo settore dovrebbero includere la protezione degli individui all'interno della loro giurisdizione dalla sorveglianza illegale mirata da parte di attori non statali e di Stati terzi (sorveglianza transnazionale). Ciò dovrebbe far scattare, al tempo stesso, l'obbligo procedurale di indagare efficacemente su tutti i casi di presunta sorveglianza digitale illegale da parte di attori terzi nei confronti di persone che vivono sul territorio di uno Stato membro. L'Assemblea fa riferimento, in questo contesto, alla Raccomandazione CM/Rec(2016)3 del Comitato dei Ministri agli Stati membri sui diritti umani e le imprese, adottata il 2 marzo 2016, che ricorda che gli Stati membri hanno il dovere di proteggere gli individui dalle violazioni dei diritti umani da parte di terzi, comprese le imprese commerciali.

11. L'Assemblea ritiene che le autorità investigative e i tribunali nazionali degli Stati membri accusati di uso abusivo di spyware debbano indagare a fondo e stabilire se l'uso di Pegasus e di spyware equivalenti fosse legittimo ai sensi del diritto nazionale e conforme alla Convenzione e ad altri standard internazionali. Ciò implica valutare in ogni singolo caso se l'interferenza perseguisse uno scopo legittimo ai sensi dell'articolo 8.2 della Convenzione e se fosse strettamente necessaria in una società democratica e proporzionata a tale scopo. Significa anche garantire che tutte le vittime di abusi legati ai software spia abbiano accesso a mezzi di ricorso e risarcimenti efficaci. In questo contesto, l'Assemblea esorta:

11.1. la Polonia a:

11.1.1. informare l'Assemblea e la Commissione europea per la democrazia attraverso il diritto (Commissione di Venezia) sull'uso di Pegasus e di spyware equivalenti, entro tre mesi;

11.1.2. condurre indagini efficaci, indipendenti e tempestive su tutti i casi confermati e presunti di abuso di spyware e fornire un risarcimento sufficiente alle vittime nei casi di sorveglianza illegale;

11.1.3. astenersi dall'utilizzare regole di segretezza generalizzate per negare ai meccanismi di controllo e alle persone coinvolte l'accesso alle informazioni sull'uso degli spyware;

11.1.4. comminare sanzioni adeguate, penali o amministrative, in caso di abuso;

11.1.5. conformarsi al parere della Commissione di Venezia sulla legge sulla polizia del 2016;

11.2. l'Ungheria, a:

11.2.1. informare l'Assemblea e la Commissione di Venezia sull'uso di Pegasus e di spyware equivalenti, entro tre mesi;

11.2.2. condurre indagini efficaci, indipendenti e tempestive su tutti i casi confermati e presunti di abuso di spyware e fornire un risarcimento sufficiente alle vittime nei casi di sorveglianza illegale;

11.2.3. astenersi dall'utilizzare regole di segretezza generalizzate per negare ai meccanismi di supervisione e alle persone interessate l'accesso alle informazioni sull'uso degli spyware;

11.2.4. comminare adeguate sanzioni, penali o amministrative, nei casi di abuso;

11.2.5. dare attuazione senza indugi alle sentenze *Szabó e Vissy e Huttl*, come richiesto dal Comitato dei Ministri nell'esercizio dei suoi poteri ai sensi dell'articolo 46.2 della Convenzione;

11.3. la Grecia, a:

11.3.1. informare l'Assemblea e la Commissione di Venezia sull'uso di Predator e di spyware equivalenti, entro tre mesi;

11.3.2. condurre indagini efficaci, indipendenti e tempestive su tutti i casi confermati e presunti di abuso di spyware e fornire un risarcimento sufficiente alle vittime nei casi di sorveglianza illegale;

11.3.3. astenersi dall'utilizzare regole di segretezza generalizzate per negare ai meccanismi di controllo e alle persone interessate l'accesso alle informazioni sull'uso degli spyware;

11.3.4. comminare sanzioni adeguate, penali o amministrative, nei casi di abuso;

11.4. la Spagna, a:

11.4.1. informare l'Assemblea e la Commissione di Venezia sull'uso di Pegasus, Candiru e altri spyware equivalenti, entro tre mesi;

11.4.2. condurre indagini efficaci, indipendenti e tempestive su tutti i casi confermati e presunti di abuso di spyware e fornire un risarcimento sufficiente alle vittime nei casi di sorveglianza illegale;

11.4.3. astenersi dall'utilizzare regole di segretezza generalizzate per negare ai meccanismi di controllo e alle persone coinvolte l'accesso alle informazioni sull'uso dei spyware;

11.4.4. comminare sanzioni adeguate, penali o amministrative, in caso di abuso;

11.5. l'Azerbaigian, a:

11.5.1. informare l'Assemblea e la Commissione di Venezia sull'uso di Pegasus e di spyware equivalenti, entro tre mesi;

11.5.2. condurre indagini efficaci, indipendenti e tempestive su tutti i casi confermati e presunti di abuso di spyware e fornire un risarcimento sufficiente alle vittime nei casi di sorveglianza illegale;

11.5.3. astenersi dall'utilizzare regole di segretezza generalizzate per negare l'accesso alle informazioni sull'uso degli spyware ai meccanismi di controllo e alle persone coinvolte;

11.5.4. comminare sanzioni adeguate, penali o amministrative, in caso di abuso.

12. L'Assemblea ritiene che le elezioni parlamentari polacche del 2019 non siano state eque in quanto Pegasus è stato utilizzato contro gli avversari politici durante la campagna elettorale.

13. L'Assemblea invita gli Stati membri che sembrano aver acquisito o utilizzato Pegasus, tra cui Germania, Belgio, Lussemburgo e Paesi Bassi, a chiarire il quadro del suo utilizzo e i meccanismi di controllo applicabili. Li invita a inviare queste informazioni, nonché eventuali statistiche sull'uso di Pegasus, all'Assemblea e alla Commissione di Venezia entro tre mesi.

14. Al fine di prevenire futuri usi impropri di spyware e violazioni dei diritti umani in Europa e altrove, l'Assemblea invita tutti gli Stati membri a:

14.1. garantire che le loro leggi nazionali sulla sorveglianza segreta siano piena-

mente conformi ai requisiti della Corte europea dei diritti dell'uomo e della Commissione di Venezia, per quanto riguarda la qualità della legge, le procedure di autorizzazione, la supervisione e i meccanismi di controllo, i meccanismi di notifica e i mezzi di ricorso e rivederle se necessario;

14.2. garantire che l'attuazione del loro quadro legislativo sia effettivamente in linea con la giurisprudenza della Corte europea dei diritti dell'uomo sulla sorveglianza mirata, per quanto riguarda la legalità, la legittimità, la necessità e la proporzionalità di qualsiasi misura di sorveglianza;

14.3. in attesa della valutazione del loro quadro legislativo e della loro prassi da parte della Commissione di Venezia, astenersi dall'utilizzare strumenti come Pegasus, Candiru, Predator o altri spyware simili;

14.4. a medio termine, regolamentare specificamente l'acquisizione e l'uso di spyware da parte delle forze dell'ordine e delle agenzie di intelligence, limitando l'uso di spyware tipo Pegasus a situazioni eccezionali, come misura a cui ricorrere, in ultima istanza, per prevenire o indagare su un atto specifico che rappresenti una minaccia grave e reale alla sicurezza nazionale o un reato grave specifico e definito con precisione e avendo come obiettivo esclusivamente la persona sospettata di aver commesso o di pianificare di commettere tali atti. Gli Stati dovrebbero inoltre istituire meccanismi di controllo, compreso il controllo parlamentare, sull'acquisizione e l'uso di tecnologie spyware e incorporare l'obbligo di tener conto di considerazioni di proporzionalità prima di acquisire e utilizzare nuovi spyware;

14.5. considerare reato la vendita e l'uso di spyware da parte di attori non statali;

14.6. ratificare, se non l'hanno ancora fatto, il Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 223), noto come « Convenzione 108+ », che si applicherà al trattamento dei dati per scopi di sicurezza nazionale, e iniziare già ad attuare le sue norme nel diritto nazionale;

14.7. ratificare, se non l'hanno ancora fatto, la Convenzione sulla criminalità informatica (STE n. 185, « Convenzione di Budapest ») e i suoi Protocolli aggiuntivi;

14.8. astenersi dal concedere licenze di esportazione di tecnologie spyware a Paesi in cui esiste un rischio sostanziale che tali tecnologie possano essere utilizzate per la repressione interna o transnazionale e/o per commettere violazioni dei diritti umani e revocare dette licenze in tali casi;

14.9. aderire all'Intesa di Wassenaar, se non l'hanno ancora fatto, e, per gli Stati che già vi partecipano, sviluppare un quadro di riferimento basato sui diritti umani per il trasferimento di tecnologie spyware, in base al quale le licenze di esportazione richiedano una valutazione dell'impatto sui diritti umani dello Stato destinatario e il rispetto da parte delle aziende dei Principi Guida delle Nazioni Unite su Imprese e Diritti Umani;

14.10. richiedere che tutte le aziende produttrici di spyware domiciliate o che conducono attività sostanziali all'interno della loro giurisdizione applichino la dovuta diligenza sui diritti umani in tutte le loro operazioni o in relazione a tali attività, in linea con la CM/Rec(2016)3 del Comitato dei Ministri, e applichino standard che limitino i contratti di appalto pubblico solo a quelle aziende che dimostrino di applicare la *due diligence* sui diritti umani.

15. L'Assemblea chiede alla Commissione di Venezia di valutare il quadro legislativo e la prassi in materia di sorveglianza mirata di tutti gli Stati membri (in via prioritaria Polonia, Ungheria, Grecia, Spagna e Azerbaigian; e in seguito Germania, Belgio, Lussemburgo, Paesi Bassi e tutti gli altri Stati membri), al fine di valutare se tale quadro contenga garanzie adeguate ed efficaci contro ogni possibile abuso di spyware, tenendo conto della Convenzione e di altri standard del Consiglio d'Europa. Dato il livello di intrusività di

Pegasus e di altri software spia equivalenti, prima che gli Stati membri possano continuare a utilizzare questi strumenti è necessario disporre di una legislazione chiara e precisa, di solidi meccanismi di controllo, di garanzie procedurali e di mezzi di ricorso efficaci.

16. L'Assemblea confida che il meccanismo di valutazione e revisione previsto nella modifica del Protocollo STCE n. 223 garantirà il monitoraggio dell'attuazione delle pertinenti disposizioni della Convenzione 108+ in materia di sorveglianza mirata a fini di sicurezza nazionale e di applicazione della legge, compreso l'uso di spyware.

17. L'Assemblea invita:

17.1. Israele, che gode dello status di osservatore presso l'Assemblea, a:

17.1.1. rafforzare i propri meccanismi di controllo delle esportazioni per garantire che le licenze di esportazione in relazione alle tecnologie spyware siano negate o revocate laddove esista un rischio sostanziale che tali tecnologie possano essere utilizzate per la repressione interna o transnazionale e/o per commettere violazioni dei diritti umani;

17.1.2. cooperare pienamente con le indagini condotte dagli Stati membri del Consiglio d'Europa sull'uso di Pegasus e di altri spyware esportati da Israele o venduti da società con sede in Israele;

17.1.3. pubblicare il proprio quadro normativo sul controllo delle esportazioni e informarne l'Assemblea entro sei mesi;

17.2. il Marocco, che gode dello status di partner per la democrazia con l'Assemblea, a:

17.2.1. informare l'Assemblea, entro tre mesi, sull'eventuale utilizzo di Pegasus o di spyware analoghi in patria e all'estero;

17.2.2. avviare entro tre mesi un'indagine completamente indipendente sul presunto uso di Pegasus da parte delle autorità statali contro obiettivi in Marocco e obiettivi nella giurisdizione degli Stati membri del Consiglio d'Europa;

18. L'Assemblea invita inoltre le aziende produttrici di software spia e di sorveglianza con sede negli Stati membri del Consiglio d'Europa o che conducono attività sostanziali all'interno della loro giurisdizione ad applicare la dovuta diligenza in materia di diritti umani in tutte le loro operazioni o in relazione a tali attività e a migliorare la trasparenza, in linea con la CM/Rec(2016)3 del Comitato dei Ministri e con i Principi guida delle Nazioni Unite su imprese e diritti umani;

19. L'Assemblea invita l'Unione Europea a firmare e ratificare la Convenzione 108+, ad avvalersi dell'esperienza del Consiglio d'Europa in questo campo e ad impegnarsi con i suoi organi competenti in settori quali la protezione dei dati, la sorveglianza mirata e gli spyware, ai fini della definizione di standard, del monitoraggio e della cooperazione.