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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Résolution 2513 (2023)[1]

Le logiciel espion Pegasus et les 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 qui 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. Quelque 11 pays dans le monde ont été identifiés comme clients potentiels de NSO, dont deux États membres du Conseil de l'Europe, l'Azerbaïdjan 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 avaient 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 selon lesquelles l'Azerbaïdjan l'a également utilisé, y compris lors du conflit avec l'Arménie. D'autres États membres ont acquis ou utilisé des logiciels espions similaires, tels que 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 parlementaire note que Pegasus est un logiciel espion de surveillance 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 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 enquêter sur un acte précis constituant une menace réelle et sérieuse pour la sécurité nationale ou un crime grave spécifique et précisément défini, en ciblant uniquement la personne soupçonnée d'avoir commis ou prévu de commettre ces actes, et elle devrait toujours être soumise à un contrôle juridictionnel.

---

1. *Discussion par l'Assemblée* le 11 octobre 2023 (22e séance) (voir Doc. 15825, rapport de la commission des questions juridiques et des droits de l'homme, rapporteur: M. Pieter Omtzigt). *Texte adopté par l'Assemblée* le 11 octobre 2023 (22e séance).
Voir également la Recommandation 2258 (2023).

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 sur le fait 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'enquête approfondie menée par la Commission d'enquête du Parlement européen chargée d'enquêter 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. L'Assemblée 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). Quelque 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'Azerbaïdjan 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'Azerbaïdjan, à l'encontre de 12 personnes travaillant en Arménie, dont un représentant du Gouvernement arménien, dans ce qui semble être un exemple de surveillance ciblée transnationale.

7. L'Assemblée condamne catégoriquement l'utilisation de logiciels espions par les autorités étatiques 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 n° 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 sûreté 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-même. 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 n° 1 à la Convention (STE n° 9)). 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 au titre 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). Cette protection devrait déclencher en même temps une obligation procédurale de mener une enquête 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'enquête et les tribunaux des États membres accusés d'utiliser abusivement des logiciels espions doivent mener des enquêtes approfondies et déterminer si l'utilisation de Pegasus et de logiciels espions similaires était légale au regard du droit interne et conforme à la Convention et à d'autres normes internationales. Cela implique 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 à 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 aux informations relatives à l'utilisation de logiciels espions aux mécanismes de contrôle et aux personnes ciblées;

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 à 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 aux informations relatives à l'utilisation de logiciels espions aux mécanismes de contrôle et aux personnes ciblées;

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

11.2.5. à mettre en œuvre sans délai les arrêts dans les affaires Szabó et Vissy et Hüttl, 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 à 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 aux informations relatives à l'utilisation de logiciels espions aux mécanismes de contrôle et aux personnes ciblées;

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 à 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 aux informations relatives à l'utilisation de logiciels espions aux mécanismes de contrôle et aux personnes ciblées;

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

11.5. l'Azerbaïdjan:

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 à 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 aux informations relatives à l'utilisation de logiciels espions aux mécanismes de contrôle et aux personnes ciblées;

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 contrôle applicables. Elle 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 contrôle, les mécanismes de notification et les voies de recours, et à les réviser si nécessaire;

14.2. à veiller à ce que la mise en œuvre de leur cadre législatif soit effectivement conforme à la jurisprudence de la Cour européenne des droits de l'homme en matière de surveillance ciblée en ce qui concerne 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 enquêter 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 soupçonnée d'avoir commis ou prévu de commettre ces actes. Les États devraient également mettre en place des mécanismes de contrôle, notamment un contrôle parlementaire, de l'acquisition et de 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 n° 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 œuvre ses normes dans le droit national;

14.7. à ratifier, s'ils ne l'ont pas encore fait, la Convention sur la cybercriminalité (STE n° 185, «Convention de Budapest») et ses protocoles additionnels;

14.8. à s'abstenir d'accorder des licences d'exportation de technologies de logiciels 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 les licences qui ont déjà 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 œuvre des normes limitant l'accès des marchés publics aux 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'Azerbaïdjan; et ensuite l'Allemagne, la Belgique, le Luxembourg, les Pays-Bas et tous les autres États 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 être 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 n° 223 permettra d'assurer le suivi de la mise en œuvre des dispositions pertinentes de la Convention 108+ 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. Israël, 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 enquêtes menées par les États membres du Conseil de l'Europe sur l'utilisation de Pegasus et d'autres logiciels espions exportés d'Israël ou vendus par des sociétés implantées en Israël;

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 enquête 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 surveillance 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.