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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15825
20 septembre 2023

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

Rapport[1]
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Pieter OMTZIGT, Pays-Bas, Groupe du Parti populaire européen

Résumé

Depuis 2021, différents rapports d'enquête ont révélé que les gouvernements de plusieurs États membres du Conseil de l'Europe avaient fait l'acquisition et fait usage d'un logiciel espion appelé Pegasus. Ce logiciel espion est un outil de surveillance très intrusif, puisqu'il donne à l'utilisateur un accès complet et illimité à toutes les données du téléphone portable ciblé. De plus en plus d'éléments de preuve démontrent que Pegasus ou d'autres logiciels espions similaires ont été utilisés à des fins illicites par plusieurs États membres, notamment contre des journalistes, des opposants politiques et des défenseurs des droits humains. Certains États l'ont également exporté vers des régimes autoritaires hors d'Europe.

L'Assemblée devrait condamner l'utilisation de logiciels espions par les autorités étatiques à des fins politiques, qui constitue une violation du droit au respect de la vie privée et d'autres droits consacrés par la Convention européenne des droits de l'homme. L'utilisation de logiciels espions de type Pegasus devrait être limitée à des situations exceptionnelles, comme mesure de dernier recours, en cas de menaces réelles et graves pour la sécurité nationale ou d'infractions graves précises et définies.

Les États qui auraient utilisé Pegasus à des fins illicites devraient informer l'Assemblée et la Commission de Venise de cette utilisation, mener des enquêtes effectives et offrir réparation aux victimes. Tous les États membres devraient s'abstenir d'utiliser ce type de logiciel espion jusqu'à ce que leur cadre législatif relatif à la surveillance secrète soit pleinement conforme aux exigences de la Convention, selon l'évaluation réalisée par la Commission de Venise.

1. Renvoi en commission: Doc. 15373, Renvoi 4608 du 27 septembre 2021.

Sommaire **Page**

A. Projet de résolution[2]

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'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 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'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, 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 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 spécifique 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. 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'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. 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;

2. Projet de résolution adopté par la commission le 8 septembre 2023.

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'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 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 n^{o} 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^{o} 1 à la Convention (STE n^{o} 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 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 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 contrôle 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 contrôle 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 œuvre sans délai les arrêts *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 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 contrôle 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 contrôle 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'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 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 contrôle 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 contrôle 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 contrôle, les mécanismes de notification et les voies de recours, et 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 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 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 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 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 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 œuvre 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'Azerbaïdjan; 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 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^{o} 223 permettra d'assurer le suivi de la mise en œuvre 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. 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 basées 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.

B. Projet de recommandation[3]

1. L'Assemblée parlementaire se réfère à la Résolution... (2023) «Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État» et recommande au Comité des Ministres:

1.1. d'adopter une recommandation aux États membres du Conseil de l'Europe sur la surveillance secrète et les droits humains, surtout à la lumière des menaces que présentent les nouvelles technologies de surveillance et les logiciels espions, en tenant dûment compte des normes internationales les plus élevées, de la jurisprudence de la Cour européenne des droits de l'homme et du 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, «Convention 108 +»). La recommandation devrait mettre l'accent sur les points suivants:

1.1.1. les conditions d'acquisition de logiciels espions par les agences et organes gouvernementaux des États membres;

1.1.2. les conditions d'utilisation de la technologie des logiciels espions à des fins d'application de la loi et de sécurité nationale;

1.1.3. les conditions de vente et d'exportation de la technologie des logiciels espions vers des pays tiers;

1.1.4. les procédures d'autorisation, les mécanismes de supervision et de contrôle, les mécanismes de notification et les voies de recours applicables à l'utilisation de logiciels espions par les autorités nationales;

1.1.5. les mécanismes garantissant une obligation de rendre des comptes en cas d'utilisation illégale de logiciels espions;

1.1.6. les normes de diligence raisonnable en matière de droits humains pour les entreprises de logiciels espions;

1.1.7. l'aspect transnational de la surveillance numérique et de l'utilisation de logiciels espions;

1.2. d'examiner la faisabilité d'une convention du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions;

1.3. de coordonner ses initiatives avec d'autres organisations internationales, y compris l'Union européenne et l'Organisation des Nations Unies, dans les domaines de la protection des données, de la surveillance ciblée et des logiciels espions, à des fins d'établissement de normes et de coopération.

3. Projet de recommandation adopté à l'unanimité par la commission le 8 septembre 2023.

C. Exposé des motifs par M. Pieter Omtzigt, rapporteur

1. Introduction

1. Le présent rapport fait suite à une proposition de recommandation déposée le 21 septembre 2021, que le Bureau a renvoyée devant la commission des questions juridiques et des droits de l'homme (la commission) pour rapport le 24 septembre 2021[4]. Le 27 septembre 2021, la commission m'a désigné rapporteur.

2. La proposition de recommandation rappelle qu'à la mi-juillet 2021, le consortium de médias Forbidden Stories et ses partenaires internationaux ont fait état de la fuite d'une liste de 50 000 numéros de téléphone proposés par des clients de NSO Group pour en faire d'éventuelles cibles du logiciel espion de NSO, Pegasus. «Bon nombre des téléphones concernés appartiennent à des journalistes, des défenseurs des droits de l'homme, des responsables politiques de l'opposition et des responsables politiques étrangers. [...] Bien que l'existence de Pegasus soit déjà connue, l'utilisation qu'en font apparemment les gouvernements du monde entier et la nature de celle-ci sont choquantes. Les répercussions qu'il pourrait avoir sur la liberté des médias et les institutions démocratiques sont extrêmement préoccupantes». Les révélations concernant Pegasus montrent que des garanties plus rigoureuses contre l'utilisation abusive de cette technologie par des pouvoirs publics, notamment lorsqu'il s'agit de régimes répressifs et autoritaires, sont nécessaires. La proposition demande à l'Assemblée parlementaire d'établir un rapport sur les révélations faites au sujet de Pegasus, en vue de formuler des propositions politiques aux États membres du Conseil de l'Europe et aux autres acteurs pertinents.

3. Dans le roman dystopique de George Orwell, *1984*, toutes les maisons et tous les appartements des citoyens sont équipés de télécrans afin qu'ils puissent être regardés ou écoutés à tout moment. Chaque personne sait qu'elle est observée et c'est un avertissement sévère. Le logiciel espion actuel est beaucoup plus intrusif: le citoyen ne sait pas si et quand il est utilisé et qui l'utilise. Non seulement les informations présentes sont transférées, mais toutes les données du téléphone peuvent également être transférées. C'est tellement intrusif que même Orwell n'est pas allé aussi loin. Pourtant, c'est la réalité de notre monde moderne et cela fait partie des outils utilisés contre les opposants politiques aujourd'hui.

4. Au cours de la préparation du présent rapport, la commission a tenu deux auditions. La première a eu lieu en septembre 2022 à Berne, avec la participation de Tim Engelhardt, responsable des droits humains au Haut-Commissariat des Nations Unies aux droits de l'homme, et de Lars Patrick Berg, député européen et membre de la commission d'enquête chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents du Parlement européen (Commission PEGA). La seconde, qui s'est tenue en décembre 2022, nous a permis d'entendre le témoignage de trois victimes ciblées par Pegasus ou des logiciels espions similaires: Krzysztof Brejza, membre du Sejm polonais pour le parti d'opposition Plateforme civique, Diana Riba, députée européenne espagnole du parti Esquerra Republicana de Catalunya et vice-présidente de la commission PEGA, et Thanasis Koukakis, journaliste d'investigation grec. J'ai également rencontré d'autres victimes en ma qualité de rapporteur. J'ai également pris en considération la proposition de résolution «Enquête sur la surveillance illégale de dirigeants étrangers, d'opposants politiques et de militants en Pologne» du 26 avril 2023.[5]

5. Dans ce rapport, je présenterai d'abord le contexte factuel des allégations d'utilisation abusive de Pegasus et de logiciels espions similaires par les États membres du Conseil de l'Europe, sur la base de différentes sources, notamment les conclusions de la commission PEGA. J'évoquerai ensuite les normes juridiques du Conseil de l'Europe et d'autres normes juridiques internationales susceptibles d'avoir été violées par des États en raison de l'utilisation de logiciels espions commerciaux tels que Pegasus. Enfin, je présenterai les propositions faites par différents acteurs internationaux pour prévenir de nouvelles utilisations abusives des logiciels espions de type Pegasus et mieux traiter leur incidence sur les droits humains.

---

4. Le 14 septembre 2021, notre commission a procédé à un échange de vues sur le «logiciel espion Pegasus et la surveillance secrète opérée par l'État», avec Michelle Bachelet, Haut-Commissaire des Nations Unies aux droits de l'homme; Laurent Richard, fondateur et directeur exécutif de Forbidden Stories, et Tamar Kaldani, Vice-présidente du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, «Convention 108»).

5. Doc. 15751.

2. L'utilisation de Pegasus et de logiciels espions similaires par les États membres du Conseil de l'Europe

2.1. Le logiciel espion Pegasus

6. Pegasus est un logiciel espion développé et commercialisé par la société israélienne NSO Group. Il peut être installé secrètement sur les téléphones mobiles fonctionnant sous la plupart des versions d'iOS et d'Android. La version la plus ancienne de Pegasus, qui a été découverte par des chercheurs en 2016, infectait les téléphones par «harponnage», de SMS ou de courriers électroniques qui incitent une cible à cliquer sur un lien malveillant[6]. Depuis lors, les infections peuvent être réalisées par des attaques dites «zéro-clic», qui ne nécessitent aucune interaction de la part du propriétaire du téléphone pour réussir. Par exemple, en 2019, WhatsApp a révélé que Pegasus avait utilisé une vulnérabilité dans son application pour lancer des attaques «zéro clic». Il suffisait d'appeler le téléphone cible pour que le logiciel espion s'y installe, et celui-ci s'installait même en l'absence d'une réponse à l'appel. Plus récemment, NSO a commencé à exploiter les vulnérabilités du logiciel IMessage d'Apple. Lorsque le harponnage et les attaques «zéro click» ne réussissent pas à l'installer, Pegasus peut également être installé au moyen d'un émetteur-récepteur sans fil situé à proximité d'un appareil cible, ou en obtenant un accès physique à l'appareil[7].

7. Une fois installé sur un téléphone, Pegasus serait capable d'exécuter un code arbitraire, d'extraire des contacts, des journaux d'appels, des messages, des photos, l'historique de navigation sur Internet, des paramètres[8]. Il pourrait aussi recueillir des informations à partir d'applications, notamment les applications de communication iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram et Skype[9]. Il peut secrètement transformer un téléphone portable en un dispositif de surveillance 24 heures sur 24, car il obtient un accès complet à tous les capteurs et à toutes les informations de l'appareil. Pegasus peut lire, envoyer ou recevoir des messages qui sont censés être cryptés de bout en bout, télécharger des photos stockées, et entendre et enregistrer des appels vocaux ou vidéo. Il a un accès complet à l'appareil photo, au microphone et au module de géolocalisation du téléphone[10]. D'une certaine manière, l'auteur de l'écoute peut en savoir plus que le propriétaire du téléphone.

8. Selon le contrôleur européen de la protection des données, Pegasus appartient à une nouvelle catégorie de logiciels espions qui diffèrent des outils d'interception «traditionnels» utilisés par les autorités répressives, sur trois aspects: il accorde un accès complet et illimité à l'appareil ciblé; il est capable de mener une attaque «zéro-clic», ne nécessitant aucune action de l'utilisateur pour être déclenchée; et il est très difficile à détecter[11]. Contrairement aux écoutes téléphoniques classiques, qui ne permettent qu'une surveillance en temps réel des communications, ce type de logiciel espion peut fournir un accès complet et rétroactif aux fichiers et aux messages créés dans le passé, aux mots de passe et aux métadonnées relatives aux communications antérieures.

9. NSO Group affirme que Pegasus ne collecte des données que sur les appareils mobiles de personnes spécifiques pré-identifiées, soupçonnées d'être impliquées dans des activités criminelles graves et terroristes. À cet égard, il est (selon NSO) similaire en principe à une écoute téléphonique traditionnelle et a permis d'empêcher des attaques terroristes, de démanteler des réseaux de pédophilie, de trafic sexuel et de drogue, ou de retrouver et de sauver des enfants kidnappés. NSO octroie des licences du logiciel Pegasus aux services répressifs et de renseignement des États souverains et n'a aucune visibilité sur son utilisation et les cibles de ses clients[12]. Selon NSO, Pegasus n'est pas en mesure de supprimer ou de modifier des données sur un appareil mobile. La société déclare qu'elle exige des clauses de respect des droits humains dans tous les contrats conclus avec les clients, et que ces derniers doivent s'engager à utiliser ses systèmes exclusivement pour la prévention des crimes graves et du terrorisme et pour les enquêtes portant sur de tels crimes, à condition qu'elles soient légitimes et légales. Lorsque la société a terminé sa procédure interne de diligence raisonnable en matière de droits humains pour l'approbation des engagements des clients, les demandes de licences d'exportation doivent être approuvées par l'Agence de contrôle des exportations de

6. «What is Pegasus spyware and how does it hack phones?» | Surveillance | *The Guardian.*
7. Ibid.
8. www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html, 25 août 2016.
9. www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/, 25 août 2016.
10. Voir Contrôleur européen de la protection des données, «Remarques préliminaires sur les logiciels espions modernes», 15 février 2022; page 3 [anglais uniquement].
11. Ibid. pp. 3-4. Les chercheurs spécialisés dans le domaine de la sécurité soupçonnent que les versions récentes de Pegasus ne résident que dans la mémoire temporaire du téléphone, et non dans son disque dur. Dès lors, toute trace du logiciel disparaît lorsque le téléphone est mis hors tension.
12. NSO Group, «Transparency and Responsibility Report», 30 juin 2021, pp 6-7.

défense du ministère israélien de la Défense, qui limite strictement l'octroi de licences du logiciel Pegasus, en menant sa propre analyse des clients potentiels du point de vue des droits humains[13]. En outre, NSO affirme qu'il adapte la configuration du système Pegasus au moyen de paramètres spécifiques à chaque utilisateur final. Ces spécifications personnalisées tiennent compte des restrictions d'utilisation définies dans les politiques internes de l'entreprise en matière de droits humains, ainsi que des conditions énoncées dans la licence d'exportation délivrée par le ministère israélien de la Défense. Toute allégation d'utilisation abusive de Pegasus par un État déclenche un processus d'examen approfondi et une enquête sur les faits signalés. Elle peut conduire à la résiliation du contrat avec un client, si nécessaire. En fait, NSO affirme avoir ouvert des enquêtes à la suite des allégations publiées dans le cadre du «Projet Pegasus» de 2021, notamment en examinant les cadres juridiques nationaux, en interrogeant les utilisateurs finaux et en vérifiant les faits à partir de sources objectives[14].

10. Le 3 novembre 2021, le gouvernement des États-Unis (Bureau de l'industrie et de la sécurité du Département du commerce) a ajouté NSO Group à la liste des entités ayant mené des activités contraires à la sécurité nationale ou aux intérêts de la politique étrangère américaine. Cette décision a été prise en se fondant sur des preuves que cette société a développé et fourni des logiciels espions à des gouvernements étrangers qui utilisaient ces outils pour cibler de manière malveillante des responsables gouvernementaux, des journalistes, des hommes et des femmes d'affaires, des militants, des universitaires et des employés d'ambassades, même en dehors de leurs frontières. Gina M. Raimondo, secrétaire au Commerce des États-Unis, a déclaré: «Les États-Unis sont déterminés à utiliser de manière agressive les contrôles à l'exportation pour tenir pour responsables les entreprises qui développent, font le trafic ou utilisent des technologies pour mener des activités malveillantes qui menacent la cybersécurité des membres de la société civile, des dissidents, des responsables gouvernementaux et des organisations ici et à l'étranger[15]». L'exportation de technologies vers la société NSO Group et ses filiales est donc interdite.

11. Des sociétés telles que Meta et Apple ont intenté des procès à NSO Group pour avoir utilisé le logiciel espion Pegasus contre leurs utilisateurs[16]. Une cour d'appel américaine a rejeté l'argument de la société israélienne selon lequel elle devrait être protégée par les lois sur l'immunité souveraine.

12. À la suite des révélations du «Projet Pegasus» et de l'inscription de NSO sur la liste noire des États-Unis, il semble que la liste des pays d'exportation éligibles ait été réduite par le ministère israélien de la Défense, passant de 102 à 37[17].

2.2. Premières allégations concernant l'utilisation abusive de Pegasus

13. La version iOS de Pegasus a été identifiée en août 2016. M. Ahmed Mansoor, défenseur arabe des droits humains, a reçu un SMS contenant un lien promettant des «secrets» sur la torture pratiquée dans les prisons des Émirats arabes unis. M. Mansoor a envoyé le lien au Citizen Lab de l'université de Toronto, qui a enquêté et découvert que si Mansoor avait cliqué sur le lien, son téléphone aurait été «infecté» et le logiciel espion implanté dans celui-ci[18]. Pegasus avait déjà été révélé dans une fuite de documents de Hacking Team, qui indiquait que le logiciel avait été fourni au Gouvernement du Panama en 2015. Certains médias ont également rapporté que les Émirats arabes unis utilisaient ce logiciel espion dès 2013[19].

14. Deux mois après le meurtre du journaliste saoudien Jamal Khashoggi à Istanbul, le dissident saoudien Omar Abdulaziz a intenté une action en justice en Israël contre NSO Group, accusant la société d'avoir fourni au gouvernement saoudien le logiciel de surveillance pour l'espionner, lui et ses amis, dont M. Khashoggi[20]. Cette accusation est rejetée par NSO.

---

13. Ibid. pp. 29-30.
14. Lettre et document sur la position de la société communiqués par NSO Group, 15 août 2022. [anglais uniquement].
15. www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/; www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.
16. www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/, 23 novembre 2021; www.theguardian.com/us-news/2021/nov/08/nso-israeli-spyware-company-whatsapp-lawsuit-ruling, 8 novembre 2021; https://news.bloomberglaw.com/privacy-and-data-security/nso-loses-latest-challenge-to-meta-lawsuit-over-whatsapp-spyware, 6 janvier 2022.
17. Parlement européen, commission PEGA, Rapport relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, 22 mai 2023, paragraphe 463.
18. www.bbc.com/news/technology-37192670, 26 août 2016.
19. www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html, 2 septembre 2016.

15. Des allégations concernant l'utilisation de Pegasus contre des personnes ciblées dans certains États membres du Conseil de l'Europe ont également été signalées avant 2021. Par exemple, selon The Guardian et El País, le logiciel Pegasus a été utilisé pour compromettre les téléphones de plusieurs responsables politiques en Espagne, dont l'ancien président du Parlement de Catalogne, Roger Torrent[21].

2.3. Les révélations du «Projet Pegasus» en 2021

16. En 2020, une liste de plus de 50 000 numéros de téléphone censés appartenir à des personnes considérées comme «des personnes d'intérêt» par des clients de NSO Group a été divulguée à Amnesty International et Forbidden Stories, une organisation à but non lucratif de médias basée à Paris. Ces informations ont été partagées avec 17 organisations de médias d'information dans 11 pays dans le cadre de ce qu'on a appelé le «Projet Pegasus». Pendant plusieurs mois, plus de 80 journalistes de ces organisations médiatiques, dont The Guardian, Le Monde et Radio France, Die Zeit, The Washington Post, Le Soir et Direkt36, ont mené une enquête conjointe sur une éventuelle utilisation abusive de Pegasus contre des personnes ciblées. Le laboratoire de sécurité d'Amnesty International a effectué des analyses technico-légales des téléphones portables de certaines des cibles potentielles[22].

17. Le 18 juillet 2021, des rapports ont commencé à être publiés, révélant que Pegasus avait potentiellement été utilisé contre des défenseurs des droits humains, des opposants politiques, des avocats, des diplomates, des chefs d'État et près de 200 journalistes de 24 pays[23]. Forbidden Stories et ses partenaires ont identifié des clients potentiels de NSO dans 11 pays: Azerbaïdjan, Bahreïn, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda, Arabie saoudite, Togo et Émirats arabes unis. Selon le Washington Post, 14 chefs d'État et de gouvernement anciens ou actuels, dont le président français Emmanuel Macron et l'ancien Premier ministre belge Charles Michel (actuel président du Conseil européen), figuraient sur la liste des cibles potentielles[24].

2.4. Constatations relatives à l'utilisation de Pegasus et de logiciels espions similaires par les États membres du Conseil de l'Europe

18. Des rapports d'enquête ultérieurs et d'autres sources ont démontré que Pegasus et d'autres logiciels espions similaires ont été achetés et utilisés par des États membres du Conseil de l'Europe contre leurs propres citoyens. D'après les informations fournies par NSO Group, on sait que Pegasus a été vendu dans au moins 14 pays de l'Union européenne jusqu'à ce que les contrats avec deux pays soient résiliés. On ne sait pas de quels pays il s'agit, mais on suppose généralement qu'il s'agit de la Pologne et de la Hongrie[25]. Il existe également des preuves que des États membres du Conseil de l'Europe ont exporté Pegasus ou des logiciels espions similaires vers des pays tiers ayant des régimes autoritaires et présentant un risque élevé de violations des droits humains. Les paragraphes ci-après résument certaines des constatations et conclusions de la commission PEGA et d'autres sources, pays par pays.

2.4.1. Pologne

19. En décembre 2021, le Citizen Lab de l'Université de Toronto a annoncé que Pegasus avait été utilisé en Pologne contre Roman Giertych, un avocat représentant les principaux responsables politiques de l'opposition dont Donald Tusk, et Ewa Wrzosek, une procureure impliquée dans une affaire contre le gouvernement en place[26]. Le téléphone du sénateur Krzystof Brejza avait également été piraté à de nombreuses reprises lorsqu'il menait la campagne électorale de la Plateforme civique en 2019[27]. Parmi les

---

20. www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/, 5 décembre 2018. Il a également été signalé que les téléphones d'autres personnes proches de lui avaient été visés avant et après son assassinat.
21. «Phone of top Catalan politician 'targeted by government-grade spyware'» | Catalonia, *The Guardian*, 13 juillet 2020.
22. M. Richard a expliqué, lors de l'échange de vues tenu par la commission le 14 septembre 2021, que les propriétaires de certains des téléphones avaient été contactés et que, dans une grande partie des cas, des traces de Pegasus avaient été trouvées à la suite d'analyses effectuées par des experts du laboratoire de sécurité d'Amnesty International. Voir aussi: Forensic Methodology Report: How to catch NSO Group's Pegasus – Amnesty International, 18 juillet 2021. [anglais uniquement]
23. https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/, 18 juillet 2021.
24. «Heads of state found on list of numbers examined by Pegasus Project», *The Washington Post*, 20 juillet 2021.
25. Rapport de la commission PEGA, paragraphe 11.
26. https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 décembre 2021.
27. https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 décembre 2021.

autres victimes signalées figurent Michal Kolodziejczak, chef du mouvement agraire Agrounia; Tomasz Swejgiert, journaliste et ancien associé présumé du Bureau central de lutte contre la corruption[28]; Andrzej Malinowski, ancien président des Employeurs de Pologne; ainsi que d'anciens responsables politiques du parti Droit et Justice (PiS)[29]. Le 7 février 2022, la Cour des comptes a révélé qu'entre 2020 et 2021, 544 appareils de ses employés ont été sous surveillance dans plus de 7 300 attaques, et que trois d'entre eux auraient pu être infectés par Pegasus[30]. La Cour des comptes enquêtait alors sur l'annulation des élections présidentielles de 2020.

20. Le cas du sénateur Brejza, qui dirigeait la campagne électorale de la Plateforme civique lors des élections européennes et nationales lorsqu'il a été pris pour cible, illustre les liens présumés entre la surveillance et le processus électoral. Son téléphone a en effet subi 33 attaques entre avril et octobre 2019, quelques jours seulement après la fin du cycle électoral. À la suite de ces attaques, des SMS et de la correspondance provenant de son téléphone ont été volés et diffusés sur le réseau de télévision contrôlé par l'État dans le cadre d'une campagne de diffamation qui aurait été orchestrée contre lui. M. Brejza n'a fait l'objet d'aucune accusation, mais sa surveillance aurait été liée à l'enquête criminelle ouverte contre son père (maire d'Inowroclaw) cinq ans auparavant, dans laquelle il n'avait même pas été interrogé en tant que témoin. En 2019, le père de M. Brejza avait lui-même reçu 10 SMS que le laboratoire de sécurité d'Amnesty International avait jugés suspects et qui correspondaient aux caractéristiques de Pegasus. En outre, selon M. Brejza, le tribunal qui a autorisé la surveillance dont il a fait l'objet pendant la campagne électorale n'a pas été informé de l'utilisation de Pegasus[31].

21. Le Gouvernement polonais, qui avait d'abord nié l'acquisition du logiciel espion, a confirmé début 2022 qu'il était en possession de Pegasus. Jarosław Kaczyński, le président du PiS, le parti au pouvoir, a admis que la Pologne avait acquis le logiciel espion Pegasus, mais a rejeté toute allégation concernant son utilisation abusive à des fins politiques, par exemple contre des responsables politiques de l'opposition lors de la campagne des élections législatives de 2019. Le ministre de la Justice, M. Ziobro, a déclaré que toute utilisation de Pegasus était «conforme à la loi»[32]. À cet égard, une commission créée par le Sénat polonais pour enquêter sur l'utilisation de Pegasus (commission extraordinaire du Sénat chargée d'enquêter sur les cas de surveillance illégale, leur impact sur le processus électoral en République de Pologne et la réforme des services spéciaux) a entendu différents témoins et experts, notamment des experts en cybersécurité (de Citizen Lab) et l'ancien président de la Cour des comptes et ensuite, sénateur indépendant, Krzysztof Kwiatkowski. En janvier 2022, il a présenté deux factures à la commission confirmant l'achat de logiciels espions pour le Bureau central de lutte contre la corruption pour un montant de 25 millions de PLN provenant d'un fonds du ministère de la Justice destiné aux victimes d'actes criminels. La législation polonaise prévoyant que les opérations du Bureau central ne peuvent être financées que par le budget de l'État (le fonds susmentionné n'en faisant pas partie), il semble que l'achat de Pegasus ait enfreint la législation polonaise. En ce qui concerne l'utilisation de Pegasus, il n'a pas été explicitement précisé si parmi les personnes qui avaient été ciblées par ce logiciel espion, à ce jour une seule, et encore moins toutes, a été espionnée avec une autorisation judiciaire, comme l'exige la loi. Il semble que seuls les cas d'espionnage de la procureure Ewa Wrzosek et de Krzysztof Brejza aient été examinés par les tribunaux à la suite de leurs plaintes et recours[33].

---

28. https://apnews.com/article/technology-europe-poland-hacking-spyware-4a410bda35df566632703e3578e5a99d, 25 janvier 2022.
29. https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true.18 janvier 2022. Parmi les autres victimes figurent la députée Magdalena Łośko; Paweł Tamborski, vice-ministre du Trésor de 2012 à 2014; Andrzej Długosz, copropriétaire de Cross Media PR Sp. z o.o.; le député Grzegorz Napieralski et Jacek Karnowski, maire de Sopot (tous entendus par la commission extraordinaire du Sénat polonais).
30. https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true, 7 février 2022.
31. Rapport de la commission PEGA, paragraphes 63-68; audition de M. Brejza devant la commission le 12 décembre 2022 (voir l'enregistrement vidéo de l'audition: Des élu.e.s et un journaliste ciblé.e.s par des logiciels espions apportent leur témoignage lors d'une audition de l'APCE à Paris (coe.int)).
32. www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 janvier 2022.
33. Rapport de la commission PEGA, paragraphes 20, 23, 37 et 46. En ce qui concerne le cadre législatif existant, une affaire est en cours devant la Cour européenne des droits de l'homme, dans laquelle les requérants se sont plaints que les systèmes secrets de surveillance des télécommunications, des communications postales et numériques et de collecte de métadonnées entravent leur droit au respect de la vie privée et qu'il n'existe aucun recours effectif contre cette ingérence (*Pietrzak c. Pologne* et *Bychawska-Siniarska et autres c. Pologne:* https://hudoc.echr.coe.int/eng-press?i=003-7444850-10197670).

22. Le 22 février 2022, j'ai écrit aux autorités polonaises, par l'intermédiaire du Président de la délégation polonaise à l'Assemblée, pour leur demander de me fournir quelques explications. Le 22 avril 2022, Stanislaw Zaryn, directeur du département de la sécurité nationale, a répondu qu'il n'y avait aucune preuve de surveillance illégale à l'encontre de qui que ce soit et que chaque cas de contrôle opérationnel par les services spéciaux polonais avait fait l'objet d'une autorisation judiciaire.

23. Lors de ma visite d'information à Varsovie (13-15 mars 2023) dans le cadre de la procédure de suivi concernant la Pologne (Commission pour le respect des obligations et engagements des États membres du Conseil de l'Europe (Commission de suivi)), j'ai rencontré des membres de la commission sénatoriale chargée de clarifier les cas de surveillance illégale et d'autres autorités compétentes. J'ai été informé que le nombre de services secrets et de services répressifs qui sont légalement autorisés à effectuer des surveillances a beaucoup augmenté en Pologne. En conséquence, le contrôle judiciaire et parlementaire est fragmenté et n'est manifestement plus adéquat. Je regrette qu'en dehors de la commission extraordinaire du Sénat, le Sejm n'ait pas tenté d'enquêter sur les allégations de surveillance illégale, y compris de personnalités politiques de premier plan[34]. Il faut noter que la commission sénatoriale n'a pas les pouvoirs d'investigation du Sejm.

24. La commission PEGA a conclu que «l'utilisation de Pegasus [en Pologne] fait partie intégrante et est un élément déterminant d'un système de surveillance de l'opposition et des détracteurs du gouvernement à des fins politiques. (...). Le champ de la surveillance en Pologne a été considérablement élargi au cours des dernières années, par l'affaiblissement ou la suppression des garanties et des dispositions en matière de contrôle. Au fil des modifications législatives systématiques et ciblées adoptées par la majorité au pouvoir, les droits des victimes ont été réduits au minimum et les voies de recours ont été de fait vidées de leur sens. Les contrôles *ex ante* et *ex post* effectifs, ainsi que les mécanismes de surveillance indépendants, ont été *de facto* éliminés.»[35] Le Parlement européen, dans sa recommandation du 15 juin 2023 sur l'enquête relative à l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, a noté que «le logiciel espion de surveillance Pegasus a été déployé illégalement à des fins politiques pour espionner des journalistes, des responsables politiques, des avocats, des procureurs et des acteurs de la société civile».

2.4.2. Hongrie

25. En 2021, le projet Pegasus a révélé, et Amnesty International a confirmé, que plus de 300 Hongrois auraient été ciblés par Pegasus. Les numéros de téléphone d'au moins dix avocats et de cinq journalistes, d'un responsable politique de l'opposition, ainsi que de militants et d'entrepreneurs de renom figuraient sur la liste divulguée des cibles potentielles de Pegasus[36]. Il a été confirmé depuis qu'un certain nombre de cibles ont été piratées avec succès. Le téléphone de Szabolcs Pany, journaliste d'investigation pour Direkt36, a été infecté par le logiciel espion, selon l'analyse technico-légale d'Amnesty International. Le téléphone de M. Pany a été piraté à plusieurs reprises par Pegasus au cours d'une période de sept mois en 2019, l'infection ayant eu lieu peu après qu'il a demandé des commentaires à des responsables gouvernementaux (notamment sur un article qu'il avait écrit concernant le déménagement d'une banque russe à Budapest). Parmi les autres personnes identifiées comme cibles figurent le journaliste Dávid Dercsény; le propriétaire de Central Media Group, Zoltán Varga; le professeur Attila Chikán (ancien ministre du premier gouvernement de Viktor Orbán et actuellement critique), le fils et l'avocat de l'un des anciens amis (aujourd'hui opposant) de Viktor Orbán, Lajos Simicska; János Bánáti, président de l'Association du Barreau de Hongrie; Adrien Beauduin, un doctorant belgo-canadien de l'Université d'Europe centrale qui a été arrêté après avoir participé à une manifestation à Budapest; l'avocate Ilona Patócs; le maire de Gödöllö György Gémesi; Brigitta Csikász, l'un des journalistes hongrois les plus expérimentés en matière de criminalité; ainsi que des personnes faisant partie du cercle rapproché du Fidesz[37].

26. Au début de l'année 2022, un groupe de six journalistes et militants a entamé des actions en justice auprès des autorités hongroises et de la Commission européenne. L'Union hongroise des libertés civiles (HCLU) les représente[38]. Au moment de la rédaction du présent rapport, la Cour suprême et la Cour constitutionnelle avaient toutes deux rejeté les demandes de la HCLU.

---

34. https://rm.coe.int/note-information-pologne-mars-2023/1680ab69c2
35. Rapport de la commission PEGA, paragraphes 79-80.
36. www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juillet 2021.
37. www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/, 19 juillet 2021. Voir aussi: https://telex.hu/direkt36/2021/07/20/pegasus-nso-surveillance-hungary-lawyers-bar-association-janos-banati, 20 juillet 2021. Dans certains de ces cas, les téléphones présentaient des traces de piratages potentiels de Pegasus, mais il n'a pas été possible de confirmer si l'infection avait réussi.

27. Dans un premier temps, les autorités hongroises n'ont ni commenté ni démenti l'utilisation de Pegasus. En novembre 2021, Lajos Kósa, président de la Commission parlementaire de la défense et de l'application de la loi, a admis que le ministère de l'Intérieur avait acheté Pegasus, mais a déclaré qu'il n'avait jamais été utilisé contre des citoyens hongrois[39]. Le ministère de l'Intérieur a acheté indirectement Pegasus pour 6 millions EUR par l'intermédiaire de Communication Technologies Ltd à la société de NSO Group enregistrée au Luxembourg en 2017. Le 31 janvier 2022, l'Autorité nationale hongroise pour la protection des données et la liberté d'information (NAIH) a présenté les conclusions d'une enquête ouverte d'office sur l'utilisation de Pegasus par les autorités hongroises. Elle a conclu que Pegasus était utilisé par le service de sécurité nationale pour surveiller plusieurs personnes dont les noms avaient paru dans la presse, mais toujours dans le respect du cadre juridique (avec une autorisation du ministère de la Justice ou d'un tribunal) et pour des motifs de sécurité nationale. Les 300 citoyens hongrois dont le téléphone figurait sur la liste ayant fait l'objet d'une fuite n'ont pas tous fait l'objet d'une enquête de la part de NAIH, puisque, selon son président, Amnesty International ne lui a pas fourni cette liste[40]. Les motifs de l'enquête resteront classifiés jusqu'en 2050.

28. En février 2022, j'ai écrit aux autorités hongroises, par l'intermédiaire du Président de la délégation hongroise à l'Assemblée, pour leur demander de me fournir quelques explications. Je n'ai, malheureusement, pas reçu de réponse à ce jour.

29. D'autres sociétés de logiciels espions, telles que Black Cube et Cytrox, semblent également avoir des liens avec la Hongrie. Black Cube est intervenue en Hongrie lors des élections de 2018, au cours desquelles elle a espionné différentes ONG et des personnes qui avaient des liens avec George Soros[41]. En 2015, des fichiers divulgués par Hacking Team ont révélé que le gouvernement hongrois était un client.

30. La commission PEGA a conclu que «L'utilisation de Pegasus en Hongrie semble s'inscrire dans le cadre d'une campagne stratégique et orchestrée du gouvernement visant à saper la liberté des médias et la liberté d'expression. Le gouvernement a utilisé ce logiciel espion pour instaurer facilement un régime de harcèlement, de chantage, de menaces et de pressions à l'encontre des journalistes indépendants, des médias, des opposants politiques et des organisations de la société civile, sans crainte de contestations.»[42] Dans sa recommandation du 15 juin 2023, le Parlement européen est parvenu à la même conclusion qu'avec la Pologne, à savoir que «le logiciel espion de surveillance Pegasus a été déployé illégalement à des fins politiques pour espionner des journalistes, des responsables de l'opposition, des avocats et des acteurs de la société civile».

2.4.3. Grèce

31. En mars 2022, Citizen Lab a révélé que le téléphone du journaliste d'investigation Thanasis Koukakis avait été infecté par le logiciel espion Predator en 2021[43]. Contrairement à Pegasus, Predator est un code d'exploitation dans lequel il faut que la cible clique une fois sur un lien pour que le logiciel espion infecte le téléphone. Predator a été développé par Cytrox, une société basée à l'époque en Macédoine du Nord. Cytrox a ensuite été rachetée par Tal Dilian (ancien membre des forces de défense israéliennes qui a la nationalité maltaise) avant de devenir membre de l'alliance Intellexa, un consortium de vendeurs de logiciels espions ayant des représentations à Chypre, en France, en Grèce et en Irlande. En juillet 2022, le député européen et chef du parti d'opposition grec PASOK Nikos Androulakis a annoncé qu'il portait plainte contre les tentatives visant à infecter son téléphone par Predator. Les tentatives d'installation du logiciel espion ont été découvertes lors d'un contrôle de son téléphone par le service informatique du Parlement européen. Ces tentatives ont eu lieu lorsque M. Androulakis était candidat à la direction du PASOK. En novembre 2022, les médias grecs ont révélé une liste de 33 cibles de Predator, toutes des personnalités de premier plan, dont des membres du gouvernement, l'ancien Premier ministre Antonis Samaras et l'ancien commissaire européen Avramopoulos. En février 2023, le président de l'Autorité grecque chargée de la protection des données (Hellenic Data Protection Authority, HDPA) a confirmé que 300 SMS liés au logiciel espion Predator avaient été envoyés à une centaine d'appareils[44]. Parmi les cibles confirmées de Predator figurent Christos Spiritzis, ancien ministre des Infrastructures et député du parti Syriza, et Artemis Seaford, une ancienne employée gréco-américaine de Meta qui avait écrit sur un cas de harcèlement sexuel de la part d'un homme politique.

---

38. https://hclu.hu/en/pegasus-case-foreign-procedures.
39. www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217, 4 novembre 2021.
40. https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/, 31 janvier 2022.
41. Rapport de la commission PEGA, paragraphes 129-131.
42. Rapport de la commission PEGA, paragraphe 132.
43. M. Koukakis a participé à une audition devant la commission le 12 décembre 2022 (enregistrement vidéo à l'adresse suivante): Des élu.e.s et un journaliste ciblé.e.s par des logiciels espions apportent leur témoignage lors d'une audition de l'APCE à Paris (coe.int)).

32. Koukakis et Androulakis ont tous deux tenté d'obtenir des informations ou des réparations auprès des autorités nationales compétentes, notamment en s'adressant à l'Autorité grecque chargée de la sécurité des communications et de la vie privée (ADAE) et en déposant des plaintes pénales. Ils ont également introduit des requêtes auprès de la Cour européenne des droits de l'homme.

33. En août 2022, le gouvernement grec a admis que le service de renseignement national (EYP)[45] avait surveillé (au moyen d'écoutes téléphoniques classiques) MM. Koukakis et Androulakis, mais il a nié avoir jamais acheté le programme Predator ou l'avoir utilisé contre eux. Le 8 août, le Premier ministre Kyriakos Mitsotakis a déclaré que la surveillance de M. Androulakis avait été «légale» mais «politiquement inacceptable». Il n'a fait aucune référence au cas de M. Koukakis ou à d'autres cas présumés. Après les premières révélations, le directeur de l'EYP et Grigoris Dimitriadis, le secrétaire général du gouvernement, ont démissionné. L'ancien directeur de l'EYP a déclaré que les écoutes téléphoniques de M. Androulakis avaient été lancées à la demande des services de renseignement de l'Arménie et de l'Ukraine, compte tenu de sa participation à la commission du commerce international du Parlement européen, qui traite des relations commerciales entre l'Union européenne et la Chine. Il est possible que Predator n'ait pas été acheté directement par l'État, mais par d'autres canaux[46].

34. Il a également été confirmé que le gouvernement grec avait accordé des licences d'exportation à Intellexa pour la vente du logiciel espion Predator à des gouvernements tels que Madagascar et le Soudan, ce qui aurait pu constituer une violation du règlement de l'Union européenne sur les biens à double usage[47].

35. La commission PEGA a conclu que «certains schémas suggèrent que le gouvernement grec autorise l'utilisation de logiciels espions envers des journalistes, des responsables politiques et des hommes et femmes d'affaires. Il permet également l'exportation de logiciels espions vers des pays dont le bilan en matière de droits de l'homme est mauvais (...) Bien que l'utilisation de logiciels espions soit illégale en Grèce, l'enquête sur l'origine des attaques de logiciels espions n'a pris de l'ampleur qu'à l'été 2022. (...) Les dirigeants politiques les plus haut placés du pays utilisent les logiciels espions comme un outil de pouvoir et de contrôle politiques, dans certains cas en parallèle à une interception légale, ou après celle-ci. (...) Contrairement à d'autres cas, tels que la Pologne, l'utilisation abusive de logiciels espions ne semble pas faire partie d'une stratégie autoritaire à part entière, mais plutôt être utilisée de manière opportuniste pour des gains politiques et financiers.» Le Parlement européen, dans sa recommandation du 15 juin 2023, a ajouté «qu'il est très probable que ce dernier ait été utilisé par des personnes très proches du bureau du Premier ministre».

2.4.4. Espagne

36. En avril 2022, Citizen Lab a publié un rapport (CatalanGate Report) selon lequel les téléphones mobiles de 65 personnes avaient été ciblés ou infectés par Pegasus ou un logiciel espion similaire entre 2017 et 2020: 63 avec Pegasus, quatre avec Candiru (un autre logiciel espion vendu par la société Candiru, enregistrée en Israël) et au moins deux personnes avec les deux. Les appareils d'au moins 51 personnes ont été infectés. Toutes ces personnes étaient des membres du mouvement indépendantiste catalan (députés européens, présidents catalans, législateurs, avocats et membres de la société civile) ou des membres de leur famille et de leur personnel. Citizen Lab n'a pas attribué les attaques à une entité spécifique, mais a suggéré que les preuves indiquaient «un lien étroit avec une ou plusieurs entités au sein du gouvernement espagnol». En mai 2022, les autorités espagnoles ont admis avoir ciblé, avec l'autorisation d'un juge de la Cour suprême, 18 personnes sur les 65 cas présumés. L'ancienne directrice du Centre national du renseignement espagnol (CNI), Paz Esteban, s'est présentée devant la commission des secrets officiels du Congrès des députés lors d'une réunion à huis clos pour justifier la surveillance de ces 18 personnes, mais les mandats judiciaires n'ont jamais été rendus publics. Parmi les cibles confirmées figurent l'actuel président de la Catalogne Pere Aragonès, l'ancien président et actuel député européen Carles Puigdemont (ciblage relationnel), les anciens présidents de l'ANC (organisation de la société civile catalane soutenant l'indépendance) Jordi Sanchez et Elisenda Paluzie, ainsi que l'ancien vice-président de l'ONG Omnium Cultural Marcel Mauri. Certaines des cibles confirmées ont fait l'objet de poursuites pénales liées au référendum sur l'indépendance de 2017 et aux événements qui ont suivi. D'autres auraient été visées au

---

44. Rapport de la commission PEGA, paragraphe 136.
45. Sous le contrôle direct du Premier ministre après une modification de la loi suite à la victoire de Néa Dimokratia en 2019.
46. Une possibilité serait de passer par Keytak, le Centre pour le support, le développement et l'innovation technologiques créé par l'ancien directeur de l'EYP. Voir le rapport de la commission PEGA, paragraphes 141 et 142, également en ce qui concerne les liens entre Intellexa, la société propriétaire de Predator, et l'État grec.
47. Rapport de la commission PEGA, paragraphes. 153-155.

moment des manifestations publiques et des blocages de routes organisés par les Comités de défense de la République (CdR) en réaction à la condamnation pénale des dirigeants catalans impliqués dans le référendum illégal. Les autorités ont invoqué des motifs de confidentialité et de sécurité nationale pour ne pas s'étendre sur les motifs de la surveillance. Le gouvernement n'a fait aucun commentaire sur les 47 personnes restantes et il n'est pas avéré que ces personnes aient été légalement visées par une décision de justice. Certaines des cibles se trouvaient en dehors de l'Espagne au moment de l'infection, notamment en Belgique et en Suisse[48]. Selon certaines sources, le Gouvernement espagnol a acheté Pegasus au cours de la première moitié des années 2010 pour un montant estimé à 6 millions EUR[49].

37. Les députés catalans indépendantistes du Parlement européen font partie des groupes ciblés. Nous avons entendu le cas de Diana Riba lors de l'audition en commission le 12 décembre 2022. Elle affirme que son téléphone a été infecté par Pegasus à deux reprises. La première a eu lieu en juin 2019, alors qu'elle venait de prendre son siège d'eurodéputée et pendant les discussions politiques sur le siège vacant d'Oriol Junqueras, qui n'a pas pu prendre ses fonctions d'eurodéputé parce qu'il était en détention provisoire pour son implication dans le référendum catalan illégal de 2017. La deuxième infection a eu lieu en octobre 2019, après l'arrêt de la Cour suprême contre les dirigeants indépendantistes, notamment son propre partenaire et ancien ministre catalan, Raül Romeva. La majorité de ses appels téléphoniques concernaient cette affaire, y compris des conversations avec les avocats de l'ancien ministre[50].

38. Parmi les 65 autres personnes ciblées figurent Marta Rovira, secrétaire générale du parti ERC vivant en Suisse, Elena Jiménez, représentante internationale d'Omnium Cultural faisant partie de l'équipe juridique de Jordi Cuixart (ancien président d'Omnium Cultural); ainsi que des avocats représentant certains responsables politiques catalans indépendantistes emprisonnés à l'époque.

39. Parallèlement, en mai 2022, peu après les révélations du CatalanGate, le Gouvernement espagnol a révélé que les téléphones du Premier ministre Pedro Sánchez, de la ministre de la Défense Margarita Robles et du ministre de l'Intérieur Fernando Grande-Marlaska avaient été infectés par le logiciel espion Pegasus en 2020-2021. Le ministre de l'Agriculture, Luis Planas, qui exerçait auparavant les fonctions de diplomate au Maroc, a également été ciblé par le logiciel espion, mais n'a constaté aucune infection. Bien que l'origine de ces attaques n'ait pas été confirmée, les autorités marocaines (qui auraient utilisé Pegasus contre des cibles en France) sont soupçonnées d'en être à l'origine, compte tenu de la crise diplomatique entre les deux pays à l'époque.

40. À la suite des révélations du CatalanGate, le Médiateur espagnol a ouvert une enquête d'office. Le 18 mai 2022, il a conclu que les 18 cibles confirmées avaient été surveillées conformément à la loi puisque les interceptions avaient été approuvées par un juge de la Cour suprême et que l'autorisation était accompagnée de la motivation requise. Il avait eu accès aux documents classifiés mais n'a pas commenté sur le fond les motifs contenus dans les mandats judiciaires ni la proportionnalité de la surveillance[51]. Bien que le Congrès espagnol ait voté contre une proposition de création d'une commission d'enquête sur l'utilisation de Pegasus en 2022, les récentes élections tenues en juillet 2023 ont modifié la position du parti socialiste au pouvoir (PSOE), qui a finalement accepté de créer une commission d'enquête sur Pegasus en échange du soutien des partis indépendantistes catalans à la présidente du Congrès nouvellement élue[52]. Le Parlement catalan avait déjà créé une commission d'enquête en 2022[53].

41. Différentes plaintes pénales ont été déposées auprès des tribunaux d'instruction de Barcelone par certaines des personnes concernées, des organisations de la société civile et même le Parlement catalan[54]. Cependant, les enquêtes ne progressent pas aussi rapidement que prévu et il est difficile de prouver l'existence des infections. Il semble que les juges d'instruction n'acceptent pas toujours les expertises présentées par les plaignants et que les procureurs demandent que les téléphones portables infectés soient vérifiés par la police. La Cour suprême a rejeté les recours déposés par certaines des cibles confirmées et qui souhaitaient avoir accès aux mandats judiciaires et aux documents relatifs à leur surveillance[55]. En effet, la

48. Rapport de la commission PEGA, paragraphes 329-331; 338-346. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.
49. «El CNI compró el sistema Pegasus para espiar en el extranjero» | España | *El País* (elpais.com).
50. Enregistrement vidéo de l'audition: Des élu.e.s et un journaliste ciblé.e.s par des logiciels espions apportent leur témoignage lors d'une audition de l'APCE à Paris (coe.int).
51. «El Defensor del Pueblo concluye que el CNI espió 'conforme a la Constitución'» (elnacional.cat).
52. «Spain: Pedro Sánchez's socialist candidate wins crucial vote for control of parliament» |*Euronews*.
53. «Constituïda la comissió d'investigació sobre l'espionatge amb els programes Pegasus i Candiru» – Parlament de Catalunya.
54. «El Parlament presenta la denúncia pels fets relacionals amb el programa d'espionatge Pegasus» – Parlament de Catalunya.

législation espagnole prévoit que les informations relatives aux services de renseignement et à leurs activités sont classifiées[56]. L'affaire de la surveillance du Premier ministre Pedro Sánchez et d'autres ministres a également été portée devant l'Audience nationale à Madrid. Le juge d'instruction de ce tribunal a adressé une demande formelle d'entraide judiciaire internationale (commission rogatoire) au gouvernement israélien afin d'obtenir des informations sur différents aspects du logiciel Pegasus. Cependant, le juge a récemment décidé de clore provisoirement cette affaire «en raison du manque total de coopération d'Israël»[57].

42. La commission PEGA a conclu que les 47 personnes ciblées mentionnées dans le rapport CatalanGate devraient avoir accès à la justice et qu'une enquête devrait être ouverte. En ce qui concerne les 18 cas ayant fait l'objet d'une autorisation judiciaire, leur proportionnalité et leur nécessité restent encore à être vérifiées par un tribunal, étant donné que le Médiateur n'a vérifié que leur légalité (formelle). Dans sa recommandation du 15 juin 2023, le Parlement européen a appelé l'Espagne à inviter Europol, qui pourrait apporter une expertise technique, à s'associer aux enquêtes.

2.4.5. Azerbaïdjan

43. Selon les révélations du «Projet Pegasus» de 2021, l'Azerbaïdjan fait partie des pays qui utilisent Pegasus. Au moins 48 journalistes auraient été désignés comme cible potentielle de ce logiciel espion[58]. Il s'agissait notamment de Sevinc Vaqifqizi, journaliste freelance pour le média indépendant Meydan TV, dont le téléphone a été infecté pendant deux ans (2019-2020) et de Khadija Ismayilova, journaliste d'investigation au Projet de signalement de la criminalité organisée et de la corruption (OCCRP), dont le téléphone a été régulièrement infecté pendant près de trois ans (2019-2021)[59]. Certains rapports mentionnent également des militants de la société civile, comme Fatima Movlamli, dont des photos intimes ont été divulguées sur Facebook en 2019[60]. À cet égard, la publication de photos et de conversations privées et intimes de femmes soulève des inquiétudes particulières et illustre les dangers spécifiques liés au genre de la surveillance ciblée des femmes journalistes et défenseures des droits humains.

44. L'enquête menée par le consortium OCCRP a révélé que plus de 1 000 numéros azerbaïdjanais figuraient sur la liste du Projet Pegasus. Au total, 245 numéros de téléphone ont été identifiés. Sur cette liste, un cinquième appartenait à des journalistes, des rédacteurs en chef ou des propriétaires d'entreprises de médias[61]. Environ 62 personnes ont porté plainte devant le bureau du procureur général, affirmant que leurs téléphones avaient été illégalement infiltrés par le logiciel espion Pegasus et que cela constituait une violation de leur droit au respect de la vie privée garanti par la Convention européenne des droits de l'homme (STE n° 5). Le bureau du procureur général a répondu que leurs plaintes devaient être adressées à la Direction des enquêtes du service de sécurité de l'État (SSS). Celui-ci a refusé de donner une réponse écrite officielle et les responsables ont informé oralement les avocats des requérants individuels qu'ils n'avaient pas utilisé ce logiciel espion contre eux. Les requérants ont engagé des poursuites contre le bureau du procureur général et le SSS pour leur inaction et leur refus d'ouvrir une enquête pénale. Si certaines plaintes sont toujours pendantes devant les tribunaux nationaux à différentes instances, certaines sont déjà parvenues à la Cour européenne des droits de l'homme[62].

---

55. Informations qui m'ont été communiquées par Omnium Cultural. Notamment l'affaire de son ancien vice-président Marcel Mauri, qui a déposé une plainte auprès de la Cour constitutionnelle lui demandant d'ordonner à la Cour suprême de lui accorder l'accès à ces documents.
56. «El govern espanyol nega espiar dos diputats d'ERC, però no desclassifica informació de Pegasus» (elnacional.cat). Le gouvernement a cependant répondu positivement à la demande du juge d'instruction de recueillir le témoignage oral de l'actuelle présidente du CNI. Le gouvernement avait annoncé en 2022 qu'il réformerait le cadre juridique du CNI pour renforcer ses garanties et avait présenté un nouvel avant-projet de loi sur les informations classifiées (la loi actuelle sur les secrets officiels date de 1968).
57. «Spain closes Pegasus investigation over 'lack of cooperation' from Israel» | Spain | *The Guardian*.
58. Voir «Pegasus project: spyware leak suggests lawyers and activists at risk across globe» | Human rights | *The Guardian*, 19 juillet 2021.
59. https://forbiddenstories.org/journaliste/sevinc-vaqifqizi/.
60. «Pegasus project: spyware leak suggests lawyers and activists at risk across globe» | Human rights | *The Guardian*, 19 juillet 2021.
61. www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything. [anglais uniquement] Lors de l'audition de la commission sur les «Menaces d'atteinte à la vie et à la sécurité des journalistes et des défenseurs des droits humains en Azerbaïdjan» (avril 2023), Ulvi Hasanli, fondateur et directeur exécutif d'AbzasMedia, a déclaré que lui-même et l'actuel rédacteur en chef avaient été espionnés par Pegasus (procès-verbal déclassifié).
62. Informations reçues en juin 2023.

45. Des rapports récents ont révélé que Pegasus avait été utilisé lors du conflit entre l'Arménie et l'Azerbaïdjan. Les téléphones de 12 personnes travaillant en Arménie, dont le porte-parole du ministère arménien des Affaires étrangères, un représentant de l'ONU et plusieurs militants de la société civile et journalistes arméniens (dont la plupart avaient fait des reportages sur le conflit), auraient été infectés par Pegasus entre octobre 2020 et décembre 2022[63]. Aucune preuve n'indique que l'Arménie ait déjà été un utilisateur de Pegasus (l'achat possible du Predator de Cytrox est évoqué ci-après). CitizenLab a identifié un opérateur Pegasus présumé en Azerbaïdjan qui aurait pu atteindre des cibles en Arménie.

2.4.6. Chypre

46. Selon le Parlement européen, «Chypre est un important pôle d'exportation à l'échelle européenne pour le secteur de la surveillance et représente un endroit attrayant pour les entreprises qui vendent des technologies de surveillance». Tal Dilian, ancien membre des forces de défense israéliennes, a commencé une carrière d'expert du renseignement à Chypre, où il a lancé Aveledo Ltd, qui deviendra plus tard WS WiSpear Systems Ltd. Il a également lancé Intellexa Alliance, un consortium de fournisseurs d'équipements de surveillance. En 2019, Tal Dilian aurait conclu un accord non contractuel avec Hermes Airports en vue de l'utilisation de son équipement Wispear dans le but d'améliorer le signal Wi-Fi mis à la disposition des passagers de l'aéroport international de Larnaca. Il semble que la véritable raison de cet accord était de tester la technologie d'interception de la société WiSpear, qui a été condamnée à une amende de 76 000 EUR par la Cour d'assises le 22 février 2022 pour surveillance illégale de communications privées et violation de la protection des données. Les poursuites pénales contre Tal Dilian et d'autres employés de WiSpear ont été abandonnées. À la suite de cette affaire, M. Dilian a transféré les activités d'Intellexa en Grèce, bien qu'il n'ait jamais quitté Chypre[64].

47. Bien que le gouvernement chypriote nie l'exportation de Pegasus et l'enregistrement de toute entité de NSO Group à Chypre, les rapports de NSO Group indiquent que Chypre a accordé des licences d'exportation pour sa technologie[65]. Selon un document transmis par le parti d'opposition AKEL au Parlement européen, NSO Group aurait exporté Pegasus par l'intermédiaire d'une de ses filiales à Chypre vers une société implantée aux Émirats arabes unis. En 2017, une réunion entre des responsables de NSO et des clients saoudiens a eu lieu à l'hôtel Four Seasons de Limassol dans le but de présenter les dernières capacités de Pegasus. Les clients saoudiens l'ont immédiatement acheté, un an avant l'assassinat de Jamal Khashoggi au consulat saoudien d'Istanbul et la surveillance présumée de ses proches par Pegasus[66].

48. Selon la commission PEGA, «dans la pratique, il semblerait que les règles soient faciles à contourner et qu'il existe des liens étroits entre les responsables politiques, les agences de sécurité et le secteur de la surveillance. C'est apparemment l'application laxiste des règles qui fait de Chypre un endroit aussi attrayant pour le commerce de logiciels espions».[67]

2.4.7. Autres États membres[68]

49. Le gouvernement autrichien a déclaré que l'Autriche n'a pas été un client de NSO. Or, son ancien chancelier Sébastien Kurz entretient des liens étroits avec le fondateur de NSO Group, Shalev Hulio. En octobre 2022, ils ont lancé une société de cybersécurité appelée Dream Security. En outre, une société spécialisée dans les logiciels espions, Decision Supporting Information Research and Forensic (DSIRF), est basée en Autriche. En juillet 2022, Microsoft a découvert qu'un outil logiciel de DSIRF (appelé Subzero) était utilisé pour attaquer des cabinets d'avocats, des banques et des cabinets de conseil stratégique en Autriche, au Royaume-Uni et au Panama. Compte tenu de l'absence de licence d'exportation pour DSIRF, le parquet de Vienne a ouvert une enquête préliminaire. En effet, le logiciel aurait pu être utilisé par un acteur étranger, ce qui reviendrait à une violation des restrictions à l'exportation par DSIRF[69].

---

63. www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.
64. Rapport de la commission PEGA, paragraphe 268-280.
65. NSO Group, «Transparency and Responsibility Report», 30 juin 2021, p. 4.
66. Rapport de la commission PEGA, paragraphes 285-286. Cette affirmation est contestée par NSO.
67. Rapport de la commission PEGA, paragraphe 302.
68. Il s'agit uniquement des États membres pour lesquels il y a eu des allégations concernant l'utilisation de Pegasus ou de logiciels espions similaires par des autorités nationales ou des pays tiers, l'achat ou l'exportation avérés de ces logiciels espions, ou le registre des sociétés de logiciels espions. J'ai exclu ceux qui se sont montrés intéressés par l'achat ou l'utilisation de logiciels espions, mais qui ont finalement été refusés (voir: «Israel Blocked Sale of Pegasus Spyware to Ukraine and Estonia», *The New York Times* (nytimes.com).
69. Rapport de la commission PEGA, paragraphes 403- 405, 403-509.

50. Il semble que la Belgique soit l'un des 14 États de l'Union européenne qui ont acheté Pegasus. Un ancien responsable des services de renseignement israéliens a révélé que la police belge utilisait Pegasus dans ses opérations. En septembre 2021, le ministre de la Justice a indiqué que ce logiciel espion pouvait être utilisé de manière légale, mais n'a pas confirmé si les services belges étaient des clients de NSO. Parmi les personnes ciblées par Pegasus sur le territoire belge (très probablement par des pays tiers) figurent l'ancien Premier ministre et actuel président du Conseil européen Charles Michel ainsi que son père Louis Michel; El Mahjoub Maliha, défenseur des droits humains originaire du Sahara occidental; Carine Kanimba, fille d'un militant politique rwandais; l'actuel commissaire européen à la justice Didier Reynders ainsi que des membres du personnel de la Commission européenne[70].

51. En Bulgarie, les autorités nationales nient avoir accordé des licences d'exportation à NSO Group ou à ses filiales. Cependant, les rapports de cette société indiquent que ses produits sont ou ont été exportés de Chypre et de Bulgarie[71]. Selon les médias, certains des serveurs de la structure de réseau à partir desquels les attaques Pegasus sont menées sont situés dans un centre de traitement de données bulgare appartenant à une société bulgare, Circle Bulgaria, elle-même détenue par NSO Group. Cette société fournit des services de recherche et de développement aux filiales chypriotes depuis la Bulgarie et exporte des produits vers des administrations publiques. Le bureau du procureur de la ville de Sofia enquête pour savoir si les services de l'État ont utilisé illégalement Pegasus contre des citoyens bulgares[72].

52. En France, le Projet Pegasus a permis de révéler que plusieurs tentatives de piratage par Pegasus avaient eu lieu, et que le président Macron avait notamment été visé. Des traces d'infections par Pegasus ont été confirmées sur les téléphones de cinq ministres et d'un député, du directeur de la station de radio parisienne TSF Jazz Bruno Delport, des journalistes d'investigation Edwy Plenel et Lénaïg Bredoux, ainsi que d'avocats et de proches de militants sahraouis. Dans la plupart des cas, il semble que le Maroc soit à l'origine des attaques.

53. En outre, la France abrite plusieurs sociétés spécialisées dans les logiciels espions, telles que Nexa Technologies (qui fait partie de l'alliance Intellexa de Tal Dilian) et Amesys. En juillet 2021, à la suite de plusieurs plaintes déposées par des organisations de défense des droits humains, quatre cadres d'Amesys et de Nexa Technologies ont été inculpés pour vente de technologies de surveillance aux gouvernements de Libye (sous le régime de Kadhafi) et d'Égypte. On ignore si des licences d'exportation ont été accordées pour l'exportation de logiciels espions vers ces pays[73].

54. En Allemagne, les médias ont rapporté que l'Office fédéral de la police criminelle (BKA) avait acquis une version modifiée de Pegasus (avec un accès uniquement aux communications en direct, pour qu'il soit conforme à la législation allemande) fin 2020. Toujours selon les médias, le vice-président du BKA a confirmé l'achat du logiciel espion lors d'une réunion *à huis clos* de la commission de l'Intérieur du Bundestag et qu'il était utilisé depuis mars 2021. Le service de renseignement extérieur allemand a également acheté une version modifiée de Pegasus. Les informations relatives à ces opérations restent confidentielles. Avant les révélations sur Pegasus, le BKA et la police berlinoise LKA avaient acheté FinSpy à FinFisher (basé à Munich) en 2012 et 2013, également dans une version modifiée avec un accès uniquement aux communications en direct. D'anciens dirigeants de FinFisher ont été inculpés par le parquet de Munich pour avoir exporté des technologies de surveillance vers la Türkiye sans licence d'exportation. FinFisher a annoncé sa faillite et ses activités ont cessé. Plus récemment, il a été signalé que le gouvernement (par l'intermédiaire de l'Office central des technologies de l'information dans le secteur de la sécurité: ZITiS) avait été en contact avec d'autres sociétés de logiciels espions (l'italienne RCS Lab, l'autrichienne DSIRF, Candiru, Intellexa ou Cytrox), mais il n'a pas été confirmé que des logiciels espions supplémentaires avaient été effectivement acquis.

55. En ce qui concerne l'Italie, aucun rapport sur l'achat ou l'utilisation éventuels de logiciels espions par les autorités n'a été publié. Cependant, des sociétés de logiciels espions telles que Tykelab et RCS Lab sont basées en Italie. Hacking Team, aujourd'hui appelé Memento Labs, a exporté le logiciel espion RCS vers des pays dont les régimes sont autoritaires[74].

56. Aux Pays-Bas, les médias ont rapporté en juin 2022 que le service de renseignement néerlandais avait utilisé Pegasus pour aider la police à retrouver Ridouan Tagh, principal suspect de plusieurs meurtres liés à la criminalité organisée. Le gouvernement néerlandais s'est refusé à tout commentaire. D'autres reportages

---

70. Rapport de la commission PEGA, paragraphes 360- 361 361.
71. NSO Group, Transparency and Responsibility Report, op. cit., p. 4.
72. Rapport de la commission PEGA, paragraphes 409-410.
73. Rapport de la commission PEGA, paragraphes 376-390.
74. Rapport de la commission PEGA, paragraphes 400-402.

dans les médias ont révélé qu'en 2019, le ministère néerlandais de la Défense était sur le point de signer un accord avec WiSpear, la société détenue par Tal Dilian. Rien ne permet de confirmer cependant que le contrat ait été signé ou que des logiciels espions aient été acquis[75].

57. Le Luxembourg, l'Irlande, Malte et la République tchèque entretiennent des liens importants avec le secteur des logiciels espions. Le Luxembourg héberge neuf entités directement liées à NSO Group, mais le ministre des Affaires étrangères a confirmé qu'aucune d'entre elles n'avait été autorisée à exporter des produits de surveillance à partir du Luxembourg. En octobre 2021, le Premier ministre Xavier Bettel a confirmé que le Luxembourg avait acheté et utilisé Pegasus «pour des motifs liés à la sécurité de l'État». L'Irlande héberge certaines des sociétés de logiciels espions mentionnées (Intellexa et Thalestris Limited, sa société mère) parce que sa législation fiscale serait favorable. Plusieurs personnalités du secteur du commerce des logiciels espions, dont Tal Dilian, ont obtenu des passeports maltais. Enfin, c'est à Prague que se tient le salon européen annuel du secteur des logiciels espions, l'«ISS World», également baptisé «The Wiretappers' Ball» (La foire aux écoutes)[76].

58. Selon le rapport de CitizenLab, des clients probables de Predator ont été trouvés en Arménie. Il semble que des acteurs soutenus par le gouvernement aient acheté des produits Cytrox[77].

59. La Roumanie a acheté le logiciel espion FinFisher, comme d'autres pays de l'Union européenne (Belgique, République tchèque, Estonie, Allemagne, Hongrie, Italie, Pays-Bas, Slovaquie, Slovénie et Espagne). Black Cube a été impliqué dans un scandale de piratage informatique: les dirigeants de la société ont admis avoir espionné l'ancien procureure en chef de la Direction nationale anticorruption de Roumanie, Laura Kövesi; l'ancien agent roumain Daniel Dragomir aurait été le commanditaire de cette mission. D'autres sociétés de logiciels espions (Cognyte, QuaDream) opéreraient depuis la Roumanie[78].

60. Selon certains rapports, la Serbie a été cliente de Circles Technologies (appartenant à NSO Group), de Predator, de Cognyte et de FinFisher[79].

61. Des filiales de la société Thalestris, société mère d'Intellexa Alliance, sont situées en Suisse. DigiTask (Allemagne) a vendu des logiciels espions aux autorités suisses, selon des informations divulguées en 2011[80].

62. La Türkiye a utilisé FinSpy de FinFisher en 2017. Le logiciel était déguisé en application téléchargeable recommandée aux participants aux manifestations antigouvernementales[81]. Des procureurs allemands ont accusé quatre anciens dirigeants d'entreprise de vendre illégalement des logiciels aux services secrets de Türkiye.

63. Selon CitizenLab, des téléphones de représentants du gouvernement du Royaume-Uni, y compris du cabinet du Premier ministre et du ministère des Affaires étrangères et du Commonwealth, ont été infectés par Pegasus en 2020-2021. Les infections suspectes liées au ministère des Affaires étrangères étaient associées à des opérateurs Pegasus liés à des pays tiers, notamment les Émirats arabes unis, l'Inde, Chypre et la Jordanie[82].

3. Normes juridiques pertinentes

3.1. La Convention européenne des droits de l'homme

64. La surveillance secrète ciblée, y compris l'interception des communications par téléphone mobile, constitue une atteinte au droit au respect de la vie privée et de la correspondance consacré par l'article 8.1 de la Convention européenne des droits de l'homme (STE n° 5, «La Convention»)[83]. Selon la jurisprudence de la Cour européenne des droits de l'homme («la Cour»), la surveillance secrète d'un individu ne peut se justifier au regard de l'article 8.2 que si elle est «prévue par la loi», vise un ou plusieurs des «buts légitimes»

75. Rapport de la commission PEGA, paragraphes 354-359.
76. Rapport de la commission PEGA, paragraphes 370- 375, 391-399.
77. https://carnegieendowment.org/programs/democracy/commercialspyware.
78. Rapport de la commission PEGA, paragraphes 473, 487, 495, 513.
79. Rapport de la commission PEGA, paragraphes 287 et 483.
80. Rapport de la commission PEGA, paragraphe 487; https://carnegieendowment.org/programs/democracy/commercialspyware.
81. Rapport de la commission PEGA, paragraphe 514.
82. https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/.

mentionnés dans ce paragraphe (parmi lesquels la défense de l'ordre, la prévention des infractions pénales et la protection de la sécurité nationale et de la sûreté publique) et est «nécessaire dans une société démocratique» pour atteindre ces buts[84].

65. En ce qui concerne la première exigence, cela signifie que la surveillance doit avoir un fondement juridique en droit interne qui doit être accessible à la personne concernée et prévisible quant à ses effets. La loi doit être suffisamment claire pour donner aux citoyens une indication adéquate des circonstances et des conditions dans lesquelles les autorités publiques sont habilitées à recourir à des mesures de surveillance secrète. Dans sa jurisprudence relative à ces mesures, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer: la nature des infractions susceptibles de donner lieu à un mandat d'interception; la définition des catégories de personnes susceptibles d'être mises sur écoute; la fixation d'une limite à la durée d'exécution de la mesure; la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies; les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements[85]. La Cour a confirmé que ces garanties minimales s'appliquent dans les cas où l'interception avait pour but de prévenir ou de détecter des infractions pénales, mais aussi dans ceux où la mesure a été ordonnée pour des raisons de sécurité nationale[86]. Elle a cependant admis que l'exigence de «prévisibilité» de la loi n'allait pas jusqu'à imposer aux États l'obligation d'édicter des dispositions juridiques énumérant dans le détail tous les comportements pouvant conduire à la décision de soumettre un individu à une surveillance secrète pour des motifs de «sécurité nationale». De par leur nature même, les menaces pour la sécurité nationale peuvent varier et être imprévues ou difficiles à définir à l'avance. La loi doit au moins indiquer avec suffisamment de clarté l'étendue de tout pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice[87].

66. La deuxième condition requise pour qu'une ingérence soit justifiée au regard de l'article 8.2 est que la mesure soit «nécessaire dans une société démocratique» pour poursuivre l'un des buts énoncés dans le deuxième alinéa (sécurité nationale, sûreté publique, défense de l'ordre et prévention des infractions pénales, etc.). Le pouvoir d'ordonner la surveillance en secret des citoyens n'est tolérable au regard de l'article 8 que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques[88]. En outre, la mesure doit être strictement nécessaire à l'obtention de renseignements vitaux dans le cadre d'une opération individuelle. Afin de s'assurer que les mesures de surveillance secrète ne sont appliquées que lorsqu'elles sont «nécessaires dans une société démocratique», la Cour doit également être convaincue qu'il existe des garde-fous suffisants et effectifs contre les abus. Cela implique d'évaluer, *entre autres,* les procédures d'autorisation, les modalités du contrôle de l'application de mesures de surveillance secrète, ainsi que tout mécanisme de notification et de recours prévus en droit interne[89].

67. En ce qui concerne les procédures d'autorisation, bien que l'autorisation judiciaire préalable puisse constituer une garantie importante contre la surveillance abusive, la Cour examine également avec soin son champ d'application (si le juge applique un test de «nécessité» ou de «proportionnalité») et le contenu de l'autorisation d'interception (c'est-à-dire la mention de personnes ou de locaux spécifiques). L'autorité d'autorisation doit en effet être en mesure de vérifier l'existence d'un soupçon raisonnable à l'encontre de la personne concernée, en particulier s'il existe des indices concrets permettant de soupçonner cette personne de préparer, de commettre ou d'avoir commis des actes criminels ou d'autres actes pouvant donner lieu à une surveillance secrète, tels que, par exemple, des actes mettant en péril la sécurité nationale[90]. Il est en principe souhaitable de confier le contrôle à un juge, car le contrôle juridictionnel offre les meilleures garanties d'indépendance et d'impartialité, ainsi qu'une procédure appropriée. Cependant, le contrôle exercé par des organes non judiciaires peut également être considéré comme conforme à la Convention si l'organe de

---

83. L'ingérence peut également porter atteinte au droit d'un tiers dont les communications avec la personne visée ont été interceptées (voir *Lambert c. France*, Requête n° 23628/94, arrêt du 24 août 1998, paragraphe 21). La simple collecte et le stockage de données par les services de sécurité sur des individus particuliers, y compris le lieu où se trouve la personne et ses déplacements dans la sphère publique, constituent également une ingérence dans la vie privée (voir *Shimovolos c. Russie*, Requête n° 30194/09, arrêt du 21 juin 2011, paragraphe 65).

84. Cour européenne des droits de l'homme, *Roman Zakharov c. Russie*, Requête n° 47143/06, arrêt du 4 décembre 2015 (Grande Chambre), paragraphe 232. Voir le Guide sur la jurisprudence relative à l'article 8 de la Convention, 2022.

85. Ibid., paragraphe 228-231, ainsi que d'autres références *infra*.

86. Ibid., paragraphes 231 et 246-248; *Big Brother Watch et autres c. Royaume-Uni,* Requêtes n° 58170/13 et autres, arrêt du 25 mai 2021 (Grande Chambre).

87. *Roman Zakharov c. Russie*, paragraphe 247. Dans cette affaire, la Cour a critiqué le fait que la loi en question laissait aux autorités une latitude quasi illimitée lorsqu'il s'agit de déterminer quels faits ou actes représentent une menace, et si celle-ci est grave au point de justifier une surveillance secrète.

88. *Klass et autres c. Allemagne* Requête n° 5029/71, arrêt du 6 septembre 1978, paragraphe 42.

89. *Roman Zakharov c. Russie*, paragraphes 235-238.

contrôle est indépendant des autorités chargées de l'opération et est doté de pouvoirs suffisants pour exercer un contrôle effectif et permanent[91]. Appliquant ces principes, la Cour a estimé dans l'affaire *Szabó et Vissy c. Hongrie*[92] que l'autorisation et le contrôle des mesures de surveillance secrète par le ministre de la Justice (sans autorisation judiciaire préalable) étaient, par essence, incapables d'assurer l'appréciation requise de la stricte nécessité. Pour la Cour, le contrôle par un membre politiquement responsable de l'exécutif n'offre pas les garanties nécessaires. En outre, lorsqu'un juge ou un tribunal qui exerce la fonction de contrôle fait preuve de passivité et se contente d'approuver, sans véritable vérification des faits, les actions des services de sécurité, ce contrôle n'est pas compatible avec l'article 8[93].

68. Une fois la surveillance terminée, la question de la notification ultérieure des mesures de surveillance est inextricablement liée au caractère effectif des recours devant les tribunaux. Les possibilités de recours devant les tribunaux par l'individu concerné sont en principe limitées, sauf si ce dernier est informé des mesures prises à son insu et peut en contester la légalité *a posteriori*, ou sauf si la personne qui soupçonne que ses communications sont ou ont été interceptées peut saisir un tribunal, de sorte que la compétence de celui-ci ne dépend pas de la notification au sujet qui a fait l'objet de l'interception. Les informations devraient toutefois être communiquées en principe au sujet après la fin des mesures de surveillance «dès que la notification peut être effectuée sans compromettre l'objectif de la restriction»[94].

69. La Cour a constaté des violations de l'article 8 dans des affaires concernant la surveillance secrète de militants des droits humains[95], de membres d'organisations non gouvernementales[96], d'avocats[97]et de journalistes[98], entre autres.

70. En ce qui concerne les journalistes, les mesures de surveillance ciblée visant à découvrir leurs sources journalistiques peuvent également porter atteinte à leur droit à la liberté d'expression, tel que garanti par l'article 10 de la Convention, en l'absence de garanties adéquates dans la loi[99] ou de toute exigence impérieuse d'intérêt public justifiant de telles mesures dans le cas concret[100]. La Cour a constamment considéré que le droit pour les journalistes de protéger leurs sources fait partie de la liberté de «recevoir ou de

---

90. Ibid., paragraphes 257-267. Dans cette affaire, la Cour a critiqué un système qui permettait aux services secrets et à la police d'intercepter directement les communications de n'importe quel citoyen sans leur imposer l'obligation de présenter une autorisation d'interception au fournisseur de services de communication ou à quiconque (paragraphe 270). La Cour a conclu que les pratiques de surveillance abusives indiquées par le requérant semblaient être dues à l'insuffisance des garanties offertes par la législation russe, qui ne répondait pas aux exigences de l'article 8 (paragraphes 303-304). Voir également *Ekimdzhiev et autres c. Bulgarie,* Requête n° 70078/12, arrêt du 11 janvier 2022, où la Cour a contesté le fait que les tribunaux bulgares délivrant des mandats de surveillance n'ont donné aucun motif ou ont donné des motifs généraux et globaux (paragraphes 307-322).

91. Ibid., paragraphes 233-275.

92. *Szabó et Vissy c. Hongrie,* Requête n° 37138/14, arrêt du 12 janvier 2016, paragraphes 75-77. L'exécution de cet arrêt est toujours placée sous la surveillance du Comité des Ministres (procédure renforcée); le gouvernement a reconnu que des modifications de la législation s'imposent (voir Résolution intérimaire du Comité des Ministres du 9 mars 2023: https://hudoc.echr.coe.int/eng?i=001-223724).

93. Voir, par exemple, *Zoltán Varga c. Slovaquie,* Requête n° 58361/12 et 2 autres, arrêt du 20 juillet 2021, paragraphes 155-163.

94. *Roman Zakharov c. Russie*, paragraphes 234-287. Dans cette affaire, l'absence d'obligation de notification ou de toute autre possibilité de demander et d'obtenir des informations sur les interceptions a compromis l'efficacité des recours applicables. En revanche, dans *l'affaire Kennedy c. Royaume-Uni,* arrêt du 18 mai 2010, la compétence des tribunaux ne dépendant pas de la notification au sujet de l'interception, l'absence de notification a été jugée compatible avec la Convention.

95. *Shimovolos c. Russie,* Requête n° 30194/09, arrêt du 21 juin 2011.

96. *Association '21 décembre 1989' et autres c. Roumanie*, Requête n° 33810/07, arrêt du 24 mai 2011.

97. *Vasil Vasilev c. Bulgarie,* Requête n° 7610/15, arrêt du 16 novembre 2021. La Cour a constamment estimé que l'article 8 offre une protection renforcée aux communications entre avocat et client, dont l'interception peut également avoir des répercussions sur les droits consacrés à l'article 6 (procès équitable) du client de l'avocat.

98. *Azer Ahmadov c. Azerbaïdjan,* Requête n° 3409/10, arrêt du 22 juillet 2021.

99. *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas,* Requête n° 39315/06, arrêt du 22 novembre 2012, paragraphes 84-102: absence de contrôle préalable par un organe indépendant ayant le pouvoir d'empêcher la mesure ou d'y mettre fin. La Cour a récemment identifié des critères concernant la protection du matériel journalistique au titre de l'article 10 lorsqu'il s'agit de régimes d'interception de masse, en établissant une distinction entre l'accès intentionnel et l'accès non intentionnel à ce matériel *(Big Brother Watch et autres c. Royaume-Uni*, paragraphes 447-450; en ce qui concerne la différence entre l'interception ciblée et l'interception de masse, voir paragraphes 343-347).

100. *Sedletska c. Ukraine,* Requête n° 42634/18, arrêt du 1 avril 2021, paragraphes 64-73, concernant l'accès aux données de communication d'une journaliste stockées par son opérateur de téléphonie mobile. Dans cette affaire, il est intéressant de noter que la Cour a indiqué au gouvernement, en vertu de l'article 39 du règlement de la Cour et au cours de la procédure à Strasbourg, qu'il devait veiller à ce que les autorités publiques s'abstiennent d'accéder à l'une quelconque des données spécifiées dans l'ordonnance rendue par le juge d'instruction concernant la requérante.

communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques» consacrée par l'article 10 et qui en constitue l'une des garanties essentielles. Il s'agit là d'une pierre angulaire de la liberté de la presse, sans laquelle les sources pourraient se montrer réticentes à aider la presse à informer le public sur des questions d'intérêt général. Une ingérence susceptible de conduire à la divulgation d'une source ne saurait donc être considérée comme «nécessaire» au sens de l'article 10 que si elle se justifie par une exigence impérieuse d'intérêt public[101].

71. La communication entre un avocat et son client est particulièrement protégée par l'article 8 de la Convention. En principe, les communications orales et la correspondance entre un avocat et son client sont privilégiées et doivent rester confidentielles. Il s'agit également d'une garantie importante des droits de la défense et du droit à un procès équitable garantis par l'article 6[102]. L'utilisation de logiciels espions a également des conséquences négatives sur l'exercice d'autres droits de la Convention, en particulier par les défenseurs des droits humains et les militants politiques, notamment le droit à la liberté de réunion et d'association (article 11), le droit à des élections libres (article 3 du Protocole n° 1 à la Convention (STE nº 009)) et, dans les cas les plus extrêmes, le droit à l'intégrité physique et mentale et le droit à la vie (articles 2 et 3).

72. La question de savoir si les cas d'infections par Pegasus décrits dans la section ci-dessus ont violé les droits de la Convention, et en particulier le droit au respect de la vie privée, devra être tranchée par les différents tribunaux nationaux saisis et, en dernier ressort, par la Cour. Un certain nombre de requêtes individuelles ont déjà été introduites devant la Cour. Bien qu'il n'y ait pas encore eu de décision ou de jurisprudence sur l'utilisation de Pegasus, l'utilisation de ce logiciel espion ou d'un logiciel espion similaire par les autorités de l'État soulève de nouvelles questions sur d'éventuelles incidences sur les droits humains. Donner accès à tous les contenus et fonctionnalités d'un smartphone (localisation, appels téléphoniques, SMS et messages vocaux, courriels, photos, vidéos, mots de passe, historique de navigation sur le web, ou possibilité d'utiliser à distance l'appareil photo et le microphone en temps réel) conduit à un niveau d'intrusion sans précédent. Cela révèle les informations les plus sensibles (notamment sur la santé, la vie sexuelle, les opinions politiques, les croyances religieuses ou autres) non seulement sur les personnes ciblées, mais aussi sur leur famille, leurs collègues, leurs amis, leurs clients, etc. À cet égard, le Contrôleur européen de la protection des données, dans ses remarques préliminaires publiées le 15 février 2022, a déclaré qu'étant donné le niveau d'ingérence dans le droit au respect de la vie privée et la difficulté de satisfaire aux exigences de proportionnalité, le déploiement régulier de Pegasus ou d'autres technologies de logiciel espion similaires très intrusives ne paraît pas compatible avec l'ordre juridique de l'Union européenne. Il a donc proposé d'interdire le développement et le déploiement de ces logiciels espions dans l'Union européenne et, à titre subsidiaire (si de tels outils sont néanmoins utilisés dans des situations exceptionnelles), de prendre certaines mesures pour empêcher leur utilisation illégale (renforcement du contrôle des mesures de surveillance, mise en œuvre intégrale de la législation européenne en matière de protection de la vie privée et des données, contrôle judiciaire, pas d'utilisation abusive de l'exception relative à la sécurité nationale pour des motifs politiques, etc.)[103]. La Commissaire aux droits de l'homme du Conseil de l'Europe a également exprimé de sérieux doutes quant à la compatibilité de l'utilisation de Pegasus ou de logiciels espions similaires avec la jurisprudence de la Cour, compte tenu de leur degré d'intrusion[104]. En tout état de cause, et indépendamment de l'évaluation de la proportionnalité de l'utilisation de ces logiciels espions dans chaque cas d'espèce, la Cour devra d'abord examiner la qualité du cadre législatif concerné, comme elle le fait souvent dans les affaires de surveillance au titre de l'article 8. Selon différentes études, le cadre législatif de certains des pays qui ont utilisé Pegasus est insuffisant ou inefficace, notamment en ce qui concerne les mécanismes de contrôle *ex ante* et *ex post*, ainsi que les voies de recours[105]. Dans certains cas, les lacunes ont déjà été recensées par la Cour dans des affaires antérieures de surveillance sans rapport avec Pegasus (Hongrie, par exemple l'absence d'obligation de notification après la fin de la surveillance[106] et les pouvoirs de contrôle

---

101. *Sanoma Uitgevers B.V. c. Pays-Bas,* Requête n° 38224/03, arrêt du 14 septembre 2010 (Grande Chambre), paragraphes 50-51.
102. *Altay c. Turquie (n ° 2),* Requête n° 11236/09, arrêt du 9 avril 2019, paragraphes 49-50.
103. European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 février 2022, [anglais uniquement].
104. Carnet des droits de l'homme, «Highly intrusive spyware threatens the essence of human rights» (Les logiciels espions très intrusifs menacent l'essence des droits de l'homme), 27 janvier 2023.
105. Parlement européen, Département thématique des droits des citoyens et des affaires constitutionnelles, février 2023, «The use of Pegasus and equivalent surveillance spyware» (L'utilisation de Pegasus et de logiciels espions de surveillance équivalents). Pour un aperçu détaillé des réformes législatives récentes dans le domaine des services de renseignement, en particulier en ce qui concerne les mécanismes de contrôle et les recours, voir l'Agence des droits fondamentaux de l'Union européenne (FRA), «Surveillance par les services de renseignement: protection des droits fondamentaux et voies de recours dans l'Union européenne – mise à jour 2023». [anglais uniquement].

limités de l'autorité chargée de la protection des données[107]). Dans d'autres (Pologne, Grèce), ces études ont conduit la commission PEGA et le Parlement européen à relever les lacunes qui semblent soulever des inquiétudes au regard des normes de la Convention. Par exemple, en Grèce, un amendement législatif de 2021 a supprimé la possibilité pour l'ADAE d'informer les citoyens de la levée de la confidentialité des communications. En ce qui concerne la Pologne, la Commission européenne pour la démocratie par le droit (Commission de Venise) a constaté que la loi de 2016 sur la police régissant la surveillance des citoyens (toujours en vigueur) ne contenait pas de garanties suffisantes pour prévenir les abus[108].

3.2. Autres normes du Conseil de l'Europe

73. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), seul instrument international juridiquement contraignant dans le domaine de la protection des données ayant une portée mondiale (ratifiée par 55 Parties, dont 9 non membres du Conseil de l'Europe), accorde une protection supplémentaire pour tout traitement de données effectué par le secteur privé et le secteur public, y compris le traitement des données par les autorités judiciaires et autres autorités d'application de la loi. Toutefois, les États peuvent faire des déclarations visant à exclure du champ d'application de la Convention certains types de traitement des données (par exemple, à des fins de sécurité nationale et de défense)[109]. À cet égard, M[me] Kaldani, Vice-Présidente du Comité consultatif de la Convention, a rappelé lors de l'audition du 14 septembre 2021 que la Convention 108 modernisée (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, «Convention 108+», ouvert à la signature le 10 octobre 2018 et non encore entré en vigueur[110]) supprime cette possibilité. La Convention 108+ établit également des exigences plus strictes concernant la licéité du traitement, la proportionnalité et la minimisation des données, rappelant que les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées[111]. Elle renforce les droits des individus et impose des exigences de plus grande transparence[112], qui peuvent toutefois être restreintes lorsque cela est prescrit par la loi, respecte l'essence des droits et libertés fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique à des «objectifs essentiels d'intérêt public général», y compris la protection de la sécurité nationale, la défense, la sûreté publique ou la prévention, l'investigation et la répression des infractions pénales[113]. La Convention 108+ renforce également les pouvoirs d'enquête et de correction ainsi que l'indépendance des autorités chargées de la protection des données. Elle prévoit toutefois un nombre limité d'exceptions dans le domaine de la sécurité nationale et de la défense, pour autant qu'elles soient prévues par la loi et nécessaires dans une société démocratique[114]. Les activités de traitement à des fins de sécurité nationale et de défense doivent en tout cas faire l'objet d'un contrôle et d'une supervision indépendants effectifs selon la législation nationale[115].

74. Depuis son ouverture à la signature en 2001, la Convention sur la cybercriminalité (STE n° 185, également connue sous le nom de «Convention de Budapest» ou «Convention sur la cybercriminalité»), a attiré la participation de pays de toutes les régions du monde. Elle contient des dispositions relatives au droit

---

106. *Szabó et Vissy c. Hongrie,* Requête n° 37138/14, arrêt du 12 janvier 2016.
107. *Hüttl c. Hongrie,* Requête n° 58032/16, arrêt de comité du 29 septembre 2022.
108. www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-f.
109. Voir l'article 3.2. Par exemple, la déclaration d'Andorre qui exclut, entre autres, les données à caractère personnel relatives à la sécurité de l'État et à l'investigation et la prévention des infractions pénales.
110. À ce jour, 27 États l'ont ratifié. Le nombre requis de ratifications pour l'entrée en vigueur (38) devrait être atteint en 2024. Voir aussi Conseil de l'Europe, Département de la société de l'information DGI(2022)04, «Le logiciel espion Pegasus et ses répercussions sur les droits de l'homme», juin 2022.
111. Article 5.
112. Articles 8 et 9.
113. Article 11.1.
114. Articles 11.3 et 15.2, notamment en ce qui concerne les pouvoirs d'enquête et d'intervention ou le pouvoir de rendre des décisions en cas de violation de la Convention.
115. Article 11.3. M[me] Kaldani a déclaré qu'une réflexion était en cours au sein du comité pour fournir un document sur l'utilisation pratique des principes de protection des données dans le contexte de la surveillance. Il a également été avancé que la Convention 108+ ne répond pas pleinement et explicitement à certains des défis posés à notre ère numérique par des capacités de surveillance sans précédent et qu'il est nécessaire de renforcer les garanties au niveau international (par exemple, un instrument international global des droits humains encadrant les opérations des services de renseignement). Voir à cet égard la déclaration conjointe d'Alessandra Pierucci, Présidente du Comité de la Convention 108, et de Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe, intitulée «Mieux protéger les personnes dans un contexte de flux international de données: La nécessité d'une supervision démocratique et effective des services de renseignement», 7 septembre 2020, voir https://rm.coe.int/declaration-conjointe-schrems-ii-finale/16809f79ca.

pénal matériel et au droit procédural, ainsi qu'à la coopération internationale, en matière de criminalité informatique. La notion de «système informatique» définie à l'article 1.a couvre les téléphones mobiles modernes, les smartphones, les tablettes ou des dispositifs similaires, qui ont la capacité de produire, de traiter et de transmettre des «données informatiques»[116]. Parmi les abus que la Convention impose aux États parties d'incriminer, ceux qui sont pertinents pour notre sujet sont l'«accès illégal» (article 2), l'«interception illégale» (article 3) et l'«utilisation abusive de dispositifs» (article 6). L'«interception illégale» s'applique à toutes les formes de transfert électronique de données (par exemple par téléphone), mais l'interception doit être effectuée «intentionnellement» et «sans droit». À cet égard, l'interception est justifiée si elle est légalement autorisée dans l'intérêt de la sécurité nationale ou de la détection d'infractions par les autorités chargées de l'enquête[117]. L'«utilisation abusive de dispositifs» fait référence à la production, la vente, l'acquisition pour utilisation, l'importation, la distribution ou toute autre mise à disposition d'un dispositif, y compris un programme informatique, conçu ou adapté principalement dans le but de commettre l'une des autres infractions; ou d'un mot de passe informatique, d'un code d'accès ou de données similaires permettant d'accéder au système informatique. Le Comité de la Convention sur la cybercriminalité (T-CY) a précisé que toutes les formes de logiciels malveillants sont couvertes par ces dispositions, en fonction de ce que le logiciel malveillant fait réellement[118]. La Convention de Budapest pourrait entrer en jeu dans les cas où l'interception au moyen d'un logiciel espion n'est manifestement pas légale au titre du droit interne, auquel cas elle pourrait être assimilée à une «interception illégale» et devrait être érigée en infraction pénale[119]. En outre, la Convention de Budapest contient des dispositions spécifiques sur l'interception des données relatives au contenu des communications («en ce qui concerne un éventail d'infractions graves à définir en droit interne») et sur l'entraide entre les États en la matière (articles 21 et 34). L'interception doit en tout état de cause être soumise aux garanties relatives aux droits de l'homme, y compris celles découlant de la Convention et d'autres traités internationaux, et en particulier au principe de proportionnalité, à la supervision judiciaire ou d'autres formes de supervision indépendante, aux motifs justifiant l'application et à la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question (article 15).

75. Les travaux antérieurs de l'Assemblée sur ce sujet montrent qu'elle a toujours été favorable au maintien du plus haut niveau possible de protection du droit à la vie privée, tant contre la surveillance ciblée que contre la surveillance de masse. Dans ce contexte, il convient de se référer à la Résolution 1843 (paragraphe 18) et à la Recommandation 1984 (2011) «La protection de la vie privée et des données à caractère personnel sur l'Internet et les médias en ligne»; à la Résolution 1986 (paragraphe 6.1) et à la Recommandation 2041 (2014) «Améliorer la protection et la sécurité des utilisateurs dans le cyberespace» (paragraphes 2.1 et 2.9)[120]; et à la Résolution 2256 (2019) «Gouvernance de l'Internet et droits de l'homme» (paragraphe 7).

76. Dans la Résolution 2045 (2015) «Les opérations de surveillance massive», adoptée à la suite des révélations faites par M. Edward Snowden sur les pratiques de surveillance de masse des États-Unis et de certains États membres du Conseil de l'Europe, l'Assemblée a exhorté les États membres et observateurs à: «veiller à ce que leur droit interne autorise la collecte et l'analyse des données à caractère personnel (...) uniquement avec le consentement de l'intéressé ou à la suite d'une décision de justice rendue sur la base de motifs raisonnables de soupçonner la cible de prendre part à des activités criminelles; il importe d'incriminer la collecte et le traitement illégaux des données de la même manière que la violation du secret de la correspondance classique (...)»; «veiller, pour faire respecter ce cadre juridique, à ce que leurs services de renseignement soient soumis à des mécanismes de contrôle judiciaire et/ou parlementaire appropriés. (...)»; «convenir d'un 'code du renseignement' multilatéral, destiné à leurs services de renseignement, qui définisse les principes régissant la coopération aux fins de lutte contre le terrorisme et la criminalité organisée (...)»; et «s'abstenir d'exporter vers les régimes autoritaires une technologie de pointe en matière de surveillance»

---

116. Note d'orientation n°1 du T-CY sur la notion de «système informatique», article 1.a de la Convention de Budapest sur la cybercriminalité, décembre 2012: https://rm.coe.int/16806f94b1.
117. Rapport explicatif de la Convention, paragraphe 58.
118. «Note d'orientation n° 7 du T-CY, Nouvelles formes de logiciels malveillants», 5 juin 2013. Selon l'Organisation de coopération et de développement économiques, «le terme 'logiciel malveillant' est un terme générique qui désigne un programme introduit dans un système d'information pour endommager celui-ci ou d'autres systèmes associés, ou encore pour détourner ces systèmes de l'utilisation initialement prévue par leurs propriétaires».
119. La commission PEGA a noté, par exemple, que l'infection d'un appareil par un logiciel espion constituait une infraction pénale en vertu du Code pénal grec, de même que la production, la vente, la fourniture, l'utilisation, l'importation, la détention et la distribution de logiciels malveillants, y compris les logiciels espions (rapport du comité PEGA, paragraphe 166).
120. L'Assemblée a invité le Comité des Ministres à examiner la possibilité d'élaborer un Protocole additionnel à la Convention sur la cybercriminalité concernant les violations graves des droits fondamentaux des utilisateurs de services en ligne. Elle a aussi invité le Comité des Ministres à établir, sur la base des éléments divulgués par Edward Snowden concernant les violations massives du droit à la vie privée, consacré par l'article 8 de la Convention européenne des droits de l'homme, un plan d'action visant à prévenir pareilles violations.

(paragraphe 19). Dans sa Recommandation 2067 (2015) «Les opérations de surveillance massive», l'Assemblée a invité le Comité des Ministres à envisager d'adresser une recommandation aux États membres en vue de garantir la protection de la vie privée à l'ère du numérique et la sécurité d'internet à la lumière des menaces que représentent les techniques de surveillance massive qui ont fait l'objet de récentes révélations, et de poursuivre l'étude des problèmes de sécurité sur internet que posent les pratiques de surveillance massive et d'intrusion, sous l'angle des droits de l'homme des usagers de l'internet (paragraphes 2.1 et 2.2).

77. Le Comité des Ministres a également adopté des textes importants dans ce domaine: la Déclaration de 2013 sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux; la Recommandation n° R(87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police; la Recommandation CM/Rec(2014)6 sur un Guide des droits de l'homme pour les utilisateurs d'internet (Annexe, paragraphes 65-85), et la Recommandation CM/Rec(2016)5 sur la liberté d'internet (Annexe, paragraphe 4.2).Le Comité des Ministres a rappelé que toute mesure prise dans l'intérêt de la sécurité nationale doit rigoureusement respecter les exigences de la Convention, notamment en ce qui concerne les articles 8, 10 et 11. Il a également souligné que les États membres ont à la fois des obligations négatives et des obligations positives, notamment la protection contre les restrictions arbitraires imposées par des acteurs non étatiques[121].

78. Enfin, la Commission de Venise a établi des normes pertinentes pour les services de sécurité. L'accent a été mis sur l'obligation de rendre des comptes, à savoir devant le parlement et la justice[122].

3.3. Autres normes internationales

79. Le 28 mai 2019, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a publié un rapport sur la surveillance et les droits de l'homme, qui indique que le logiciel espion Pegasus est un exemple de piratage d'appareils mobiles utilisé comme outil de surveillance ciblée dans 45 pays. Le rapport donne un aperçu général des obligations des États en matière de droits de humains au niveau des Nations Unies qui protègent contre la surveillance ciblée, parmi lesquelles les articles 12 (droit à la vie privée) et 19 (liberté d'expression) de la Déclaration universelle des droits de l'homme, les articles 17(1) (droit à la vie privée) et 19 (liberté d'expression) du Pacte international relatif aux droits civils et politiques. Il affirme qu'en plus de l'obligation primaire de ne pas interférer avec ces droits, les États ont le devoir de protéger les particuliers contre l'interférence de tiers, y compris en ce qui concerne la surveillance transnationale exercée par des entités étrangères sur leurs propres citoyens. Le rapport fait également référence aux Principes directeurs relatifs aux entreprises et aux droits de l'homme: mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies, adoptés par le Conseil des droits de l'homme en 2011, qui sont pertinents tant pour les États que pour le secteur privé de la surveillance (processus de diligence raisonnable en matière de droits de l'homme, mesures correctives, etc.) En ce qui concerne le contrôle des exportations, il mentionne l'Arrangement non contraignant de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage. Les États participants à cet Arrangement sont censés appliquer des contrôles à l'exportation à tous les articles de la liste des biens et technologies à double usage, y compris les articles liés aux «logiciels d'intrusion» et aux systèmes de surveillance des communications du réseau du protocole Internet depuis 2013. Le Rapporteur spécial des Nations Unies regrette toutefois que l'Arrangement ne comporte pas de lignes directrices ou de mesures d'application qui traiteraient directement des violations des droits humains causées par les outils de surveillance[123].

80. En ce qui concerne la législation de l'Union européenne, outre la Charte des droits fondamentaux (articles 7, 8, 11, 41, 42, 47 et 52, paragraphe 1)[124], la directive «vie privée et communications électroniques»[125] et la directive «Police-Justice»[126], il convient de mentionner le règlement de l'Union sur les

---

121. Voir Réponse à la Recommandation, Doc. 13911, 14 octobre 2015.
122. Commission de Venise, Rapport sur le contrôle démocratique des services de sécurité, adopté en juin 2007 et mis à jour en mars 2015, CDL-AD(2015)010.
123. A/HRC/41/35: «Surveillance et droits de l'homme», Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, HCDH.
124. Droit au respect de la vie privée et familiale; protection des données à caractère personnel; liberté d'expression et d'information; droit à une bonne administration; droit d'accès aux documents; portée des droits garantis/limitations.
125. JO L 201, 31 juillet 2002, p. 37-47.
126. Directive (UE) 2016/680 du 27 avril 2016, JO L 119 du 4 mai 2016, p. 89-131, article 30.1. Cette directive s'applique au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (article 1.1), domaine qui est exclu du champ d'application du règlement général sur la protection des données (RGPD).

biens à double usage (refonte), qui a introduit de nouveaux contrôles à l'exportation pour les «éléments de cybersurveillance», lorsqu'ils risquent d'être utilisés dans le cadre de la répression interne ou de la commission de violations graves des droits de l'homme et du droit international humanitaire[127]. Dans sa recommandation du 15 juin 2023 sur l'enquête Pegasus, le Parlement européen a conclu, par exemple, qu'il existait des preuves «d'une mauvaise administration dans l'application du règlement de l'Union sur les biens à double usage à Chypre», sur la base de rapports montrant que Chypre était devenue une plaque tournante pour l'exportation de logiciels espions vers des pays tiers répressifs.

4. La voie à suivre: propositions visant à prévenir l'utilisation abusive des logiciels espions et à mieux traiter leurs incidences sur les droits humains

81. À la suite des révélations concernant Pegasus, différents acteurs internationaux ont formulé des propositions pour prévenir l'utilisation abusive des logiciels espions et mieux traiter les risques qu'ils présentent pour les droits humains.

82. Le 27 janvier 2023, à l'occasion de la Journée européenne de la protection des données, la Commissaire aux droits de l'homme du Conseil de l'Europe a publié un Carnet des droits de l'homme intitulé «Des logiciels espions très intrusifs menacent l'essence des droits de l'homme». La Commissaire a observé que 18 mois après la divulgation de la fuite de plus de 50 000 numéros de téléphone désignés comme cibles potentielles de surveillance au moyen du logiciel espion Pegasus, des défenseurs des droits humains, des journalistes et des responsables politiques de l'opposition continuaient d'être ciblés par de puissants outils de piratage en mode «zéro clic» qui donnent un accès complet et illimité à leur vie privée mettant en péril leur sécurité personnelle ainsi que l'exercice de leurs droits fondamentaux. Tout en se félicitant des enquêtes en cours sur l'exportation, la vente, le transfert et l'utilisation de logiciels espions aussi intrusifs que Pegasus, la Commissaire a appelé les États membres à prendre des mesures pour prévenir de nouveaux abus, à imposer un moratoire strict sur l'exportation, la vente, le transfert et l'utilisation de logiciels espions «zéro clic» tels que Pegasus, et à mettre en place un cadre législatif complet et respectueux des droits humains qui s'applique à l'utilisation des technologies de surveillance modernes. Ce cadre devrait prévoir de véritables garanties procédurales, un contrôle juridictionnel et parlementaire qui s'exerce avant et après la mise en œuvre de la mesure de surveillance, et des mécanismes de recours effectifs pour les victimes. La Commissaire a également réfléchi à la nécessité de sensibiliser davantage le public à la menace omniprésente que le secteur des logiciels espions non contrôlés et un fonctionnement opaque des services de sécurité nationale font peser sur les droits humains, notamment les droits au respect de la vie privée, à la liberté d'expression et à la participation au débat public.

83. Le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a proposé (en 2019) un cadre juridique et politique pour la réglementation, l'obligation de rendre des comptes et la transparence dans le secteur privé de la surveillance, afin d'améliorer le respect des normes internationales et de combler les lacunes dans leur mise en œuvre. Il a appelé à une réglementation plus stricte de l'exportation d'équipements de surveillance et à ce que leur utilisation soit réglementée, mais aussi à l'instauration d'un moratoire immédiat sur l'exportation, la vente, le transfert, l'utilisation ou l'entretien des outils de surveillance jusqu'à ce que l'utilisation de ces technologies puisse être techniquement limitée à des fins légales et conformes aux droits humains, ou jusqu'à ce que la garantie soit apportée que ces technologies ne seront exportées que vers des pays où leur utilisation est soumise à une autorisation accordée conformément à une procédure régulière et aux normes de légalité, de nécessité et de légitimité par un organe judiciaire indépendant et impartial. Les États participant à l'Arrangement de Wassenaar devraient élaborer un cadre dans lequel l'octroi de licences pour toute technologie serait subordonné à un examen national de son incidence sur les droits humains et au respect par les entreprises des Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme[128].

84. L'ancienne Haut-Commissaire des Nations Unies aux droits de l'homme, M[me] Bachelet, a estimé que, jusqu'à ce que le respect des normes relatives aux droits humains soit garanti, les gouvernements devraient mettre en œuvre un moratoire sur la vente et le transfert de technologies de surveillance[129]. Un rapport récent préparé par le Bureau du Haut-Commissaire des Nations Unies aux droits de l'homme, outre qu'il

---

127. JO L 206, 11 juin 2021, p. 1-461.

128. OHCHR, Rapport 2019 du Rapporteur spécial au Conseil des droits de l'homme des Nations Unies; «Logiciels espions: des experts demandent un moratoire sur les technologies de surveillance», 12 août 2021. Voir également HCDH, Rapport: «Impact des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris les manifestations pacifiques», 24 juin 2020, paragraphes 24-40; et Rapport: «Le droit à la vie privée à l'ère numérique», 30 juin 2014. Voir également la Résolution 73/179 de l'Assemblée générale des Nations Unies du 17 décembre 2018.

réitère les appels précédents à mettre en œuvre un moratoire sur la vente et l'utilisation (nationales et transnationales) des systèmes de surveillance, recommande que le piratage des dispositifs personnels ne soit utilisé qu'en dernier recours, pour prévenir ou enquêter sur un acte spécifique constituant une menace grave pour la sécurité nationale ou sur un crime grave précis, en ciblant étroitement le suspect; de telles mesures devraient également être soumises à un contrôle indépendant strict et nécessiter l'approbation préalable d'un organe judiciaire[130].

85. Dans sa recommandation de juin 2023 faisant suite à son enquête sur l'utilisation de Pegasus, le Parlement européen a formulé d'importantes recommandations à l'intention des États membres de l'Union européenne, des institutions de l'Union européenne et d'autres acteurs concernés. Outre des recommandations spécifiques aux principaux États membres de l'Union européenne concernés (Pologne, Hongrie, Grèce, Espagne et Chypre), notamment en ce qui concerne leur cadre législatif et leurs enquêtes, il préconise de «définir les conditions applicables pour l'utilisation, la vente, l'acquisition et le transfert légaux de logiciels espion» et fixe un délai à tous les États membres (fin 2023) pour remplir quatre conditions, afin d'être autorisés à continuer de les utiliser. Ces conditions sont les suivantes: a) enquête et résolution sans délai des cas d'utilisation abusive de logiciels espions; b) conformité du cadre juridique national avec les normes de la Commission de Venise, et la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme; c) engagement exprès d'associer Europol dans leurs enquêtes; et d) abrogation des licences d'exportation qui ne sont pas conformes au règlement sur les biens à double usage. Le respect de ces conditions devrait être évalué par la Commission européenne d'ici le 30 novembre 2023. En ce qui concerne l'action à long terme, le Parlement européen a estimé qu'en raison de la dimension européenne de l'utilisation des logiciels espions (coopération judiciaire en matière pénale et marché intérieur), il est nécessaire d'établir des normes européennes communes qui devraient réglementer et limiter l'utilisation des logiciels espions. Par exemple, l'autorisation d'utiliser des logiciels espions ne devrait être accordée que dans des cas exceptionnels, dans le cadre d'enquêtes portant sur une «liste limitée et fermée d'infractions graves clairement définies qui constituent une menace réelle pour la sécurité nationale». Les autres recommandations du Parlement européen comprennent, entre autres, les éléments suivants:

– La ratification de la Convention 108 + du Conseil de l'Europe par tous les États membres et l'application immédiate de ses normes dans le droit national, et l'adhésion de l'Union européenne elle-même;

– Une législation européenne supplémentaire qui imposerait aux entreprises produisant et/ou exportant des technologies de surveillance d'intégrer des cadres relatifs aux droits humains et de diligence raisonnable, conformément aux Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme;

– La participation d'Europol aux enquêtes sur les allégations d'abus de logiciels espions, notamment en proposant aux autorités nationales d'ouvrir, de mener ou de coordonner une enquête;

– Une meilleure mise en œuvre et application des règles de l'Union européenne en matière d'exportation afin d'éviter les «achats liés au régime d'exportation»;

– Une meilleure gestion de l'aide au développement de l'Union européenne afin de prévenir l'utilisation abusive des technologies de surveillance par les pays tiers;

– La création d'un laboratoire technologique de l'Union européenne qui serait chargé de découvrir et d'exposer l'utilisation illégale de logiciels à des fins de surveillance illicite, et de fournir une assistance technique aux particuliers en détectant les traces de logiciels espions dans leurs appareils;

– L'intégration de l'utilisation illégale de logiciels espions par les États membres de l'Union européenne dans les rapports sur l'État de droit de la Commission européenne.

86. Les ONG et la société civile ont également formulé des propositions en vue d'une réglementation plus poussée dans ce domaine, appelant à un moratoire immédiat sur la vente, le transfert et l'utilisation de logiciels espions jusqu'à ce qu'un tel cadre réglementaire soit mis en place[131]. Certains ont estimé que les

---

129. Déclaration faite lors de l'échange de vues tenu par la commission le 14 septembre 2021. Voir: OHCHR | Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe, Hearing on the implications of the Pegasus spyware. Voir aussi: OHCHR, «Use of spyware to surveil journalists and human rightsdefenders»; Statement by UN High Commissioner for Human Rights Michelle Bachelet, 19 juillet 2021. [anglais uniquement].
130. A/HRC/51/17 (undocs.org), 4 août 2022.
131. Amnesty International, 2021: «La partie immergée de l'iceberg. La responsabilité des États et du secteur privé dans la crise de la surveillance numérique»; Déclaration de Genève sur la surveillance ciblée et les droits humains, septembre 2022: «The Geneva Declaration on Targeted Surveillance & Human Rights» (accessnow.org).

recommandations du Parlement européen n'allaient pas assez loin, par exemple, notant le fait qu'il subsiste des doutes quant à la poursuite de l'utilisation légale, de la vente, de l'acquisition et du transfert de logiciels espions pendant l'évaluation des quatre conditions par la Commission européenne, qu'aucune mesure d'exécution ne soit prévue en cas de non-respect de ces conditions, ou simplement que le Parlement européen n'ait pas demandé une interdiction totale de l'utilisation de cette forme intrusive de logiciels espions[132].

5. Conclusions

87. Les révélations concernant Pegasus ainsi que les enquêtes qui les ont suivi ont apporté la preuve que ce logiciel espion et d'autres types de logiciels similaires (par exemple Candiru, Predator) ont été utilisés comme un outil de piratage et de surveillance visant des journalistes, des avocats, des responsables politiques et des militants des droits humains dans plusieurs États membres du Conseil de l'Europe et dans d'autres pays encore. Compte tenu du niveau d'intrusion sans précédent de ce logiciel, qui accorde un accès à distance non autorisé («zéro-clic») et sans restriction à un téléphone portable et à toutes les données à caractère personnel et privé qu'il contient, son utilisation a de graves incidences sur les droits fondamentaux des personnes effectivement visées et de tous leurs contacts, notamment leur droit au respect de la vie privée et leur droit à la liberté d'expression, ainsi que, plus généralement, sur la liberté des médias et les institutions démocratiques. D'aucuns ont fait valoir que son utilisation même pourrait difficilement satisfaire aux exigences de proportionnalité que toute ingérence dans ces droits devrait respecter, compte tenu précisément de son degré d'intrusion et de furtivité. J'ai tendance à être d'accord avec ceux qui ont fait part de ces préoccupations, notamment la Commissaire aux droits de l'homme du Conseil de l'Europe et le Contrôleur européen de la protection des données. En tout état de cause, les autorités nationales d'enquête et les tribunaux des pays concernés doivent encore faire la lumière sur la question de savoir si ces ingérences très intrusives dans les droits des personnes concernées poursuivaient un but légitime (sécurité nationale, prévention des infractions pénales) ou étaient principalement fondées sur des considérations politiques, et si elles étaient en l'occurrence nécessaires et proportionnées pour atteindre ce but dans chaque cas concret, comme l'exigent la Convention européenne des droits de l'homme et d'autres normes internationales. L'espionnage des responsables politiques, des journalistes et des défenseurs des droits humains à des fins purement politiques n'est manifestement pas conforme aux valeurs du Conseil de l'Europe, aux droits humains, à l'État de droit et aux principes démocratiques. Il a non seulement un effet dissuasif sur l'exercice des droits fondamentaux par les acteurs de la société civile, les responsables politiques et les journalistes, mais il affecte également l'essence et l'intégrité des processus électoraux et le débat public. Les victimes devraient avoir accès à des recours effectifs dans tous les cas de surveillance ciblée illégale, ce qui suppose d'avoir accès aux informations pertinentes une fois que la mesure de surveillance a pris fin. Or, dans de nombreux pays concernés, les victimes ont rencontré des obstacles pour prouver que leurs appareils étaient infectés ou ciblés, en partie à cause du manque de transparence et de coopération des autorités nationales, qui invoquent des motifs de confidentialité et de sécurité nationale. Les cadres législatifs et les systèmes de contrôle des activités de surveillance dans certains États membres sont insuffisants ou inefficaces, et il est manifestement nécessaire de renforcer la réglementation et les garanties et d'améliorer la mise en œuvre et le suivi.

88. L'Assemblée devrait adresser des recommandations spécifiques aux États membres qui ont acquis et utilisé Pegasus ou des logiciels espions équivalents, notamment la Pologne, la Hongrie, la Grèce et l'Espagne. Elle devrait également adresser des recommandations générales à tous les États membres, dont beaucoup ont utilisé ou utilisent encore des logiciels espions similaires, en s'inspirant des normes établies par la Cour européenne des droits de l'homme dans ce domaine. Les États devraient s'abstenir d'utiliser des logiciels espions à moins que leur cadre législatif, leurs mécanismes de contrôle et leur système de recours ne soient pleinement conformes à ces normes. À cet égard, l'Assemblée devrait inviter tous les États membres à faire rapport aux organes compétents du Conseil de l'Europe (qu'il s'agisse du Comité consultatif de la Convention 108+, une fois le Protocole d'amendement entre en vigueur, ou de la Commission de Venise) sur la conformité de leurs cadres réglementaires et de leur mise en œuvre avec les normes du Conseil de l'Europe, et à partager leurs bonnes pratiques. En attendant cette évaluation, les États membres devraient imposer un moratoire immédiat sur la surveillance et les droits humains qui porterait notamment sur l'acquisition et l'utilisation d'outils d'espionnage très intrusifs tels que Pegasus. Le Comité des Ministres

132. «Union européenne. Après la proposition du Parlement européen de réglementer les logiciels espions, des 'mesures plus fortes' sont nécessaires pour protéger les droits humains» – Amnesty International; «PEGA Committee does not go all the way on spyware regulation» – European Digital Rights (EDRi). Un précédent projet de recommandation du Parlement européen, rédigé par la rapporteure Sophie in 't Veld, appelait à l'adoption immédiate d'un moratoire conditionnel, qui devrait être levé pays par pays si les quatre conditions étaient remplies.

devrait également être invité à rédiger une recommandation à l'intention des États membres sur la surveillance et les droits humains qui porterait notamment sur l'acquisition, l'utilisation, l'exportation et le transfert de logiciels espions, en tenant dûment compte de toutes les normes juridiques internationales et du Conseil de l'Europe. Toutes ces normes gagneraient à être regroupées sous forme de compilation à des fins de clarté. Cette recommandation codifierait également les normes les plus élevées dans ce domaine, en s'inspirant par exemple des textes existants des Nations Unies et du Conseil de l'Europe sur les droits de l'homme et les entreprises (Recommandation CM/Rec(2016)3) et en les adaptant au contexte du secteur des logiciels espions. À un stade ultérieur, le Comité des Ministres pourrait examiner la faisabilité de l'élaboration d'une nouvelle Convention du Conseil de l'Europe sur l'acquisition, l'utilisation, l'exportation et le transfert de logiciels espions, assortie d'un mécanisme de suivi.