Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Déclassifié*
AS/Jur (2022) 04
8 avril 2022
fjdoc04 2022

Commission des questions juridiques et des droits de l'homme

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

Note introductive

Rapporteur : M. Pieter Omtzigt, Pays-Bas, Groupe du Parti populaire européen

1. Introduction

1. La présente note d'information fait suite à une proposition de recommandation déposée le 21 septembre 2021 et que le Bureau a renvoyée devant notre commission pour rapport le 24 septembre 2021[1]. 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 le détournement abusif 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 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 la présente note d'information, j'exposerai le contexte factuel du futur rapport concernant les allégations d'utilisation abusive de Pegasus et de logiciels espions similaires, sur la base d'informations provenant de sources publiques existantes, et je résumerai les réactions. Je donnerai également un aperçu des normes pertinentes du Conseil de l'Europe et d'autres normes internationales et je ferai des propositions pour la suite des travaux sur le rapport final.

* Document déclassifié par la Commission le 4 avril 2022.

[1] Doc. 15373, renvoi n° 4608. 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 », auquel ont participé Michelle Bachelet, Haute-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 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) : voir le compte rendu.

2. Les révélations au sujet de Pegasus

2.1. Le logiciel espion Pegasus

4. Pegasus est un logiciel espion développé et commercialisé par la société israélienne NSO Group. Il peut être installé secrètement sur les téléphones portables 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, a infecté des téléphones par « harponnage », une technique qui consiste à envoyer des SMS ou des courriers électroniques qui incitent une cible à cliquer sur un lien malveillant[2]. 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'installe, même sans 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 implanté au moyen d'un émetteur-récepteur sans fil situé à proximité d'un appareil cible, ou en obtenant un accès physique à l'appareil[3].

5. 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 ainsi que des paramètres[4]. Il pourrait aussi recueillir des informations à partir d'applications, notamment les applications de communication iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram et Skype[5]. 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[6]. D'une certaine manière, l'auteur de l'écoute peut en savoir plus que le propriétaire du téléphone.

6. 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[7].

7. La société NSO Group affirme que Pegasus n'est pas un outil de surveillance de masse et qu'il 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 Group vend des licences du logiciel Pegasus aux services répressifs et de renseignement des États souverains et n'a aucune visibilité sur son utilisation[8]. La société déclare qu'elle exige des clauses de respect des droits de l'homme dans tous les contrats conclus avec les clients, et que ces derniers doivent s'engager à utiliser ses systèmes exclusivement pour prévenir les crimes graves et les actes de terrorisme et conduire des enquêtes à cette fin. Elle déclare également qu'elle mène une procédure interne de diligence raisonnable en matière de droits de l'homme pour approuver les engagements des clients et que les demandes de licences d'exportation doivent ensuite être validées par l'Agence de contrôle des exportations de défense

---

[2] Voir : What is Pegasus spyware and how does it hack phones? | Surveillance | The Guardian, 18 juillet 2021.
[3] Ibid.
[4] Voir : https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html, 25 août 2016.
[5] Voir : https://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.
[6] Voir Contrôleur européen de la protection des données, Remarques préliminaires sur les logiciels espions modernes, 15 février 2022 (en anglais) : https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.
[7] 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.
[8] NSO Group, Transparency and Responsibility Report, 30 juin 2021, pp 6-7: https://www.nsogroup.com/governance/transparency/

du ministère israélien de la défense, qui limite strictement la vente de licences du logiciel Pegasus, en procédant à sa propre analyse des clients éventuels du point de vue des droits de l'homme[9].

8. Les rapports de la société NSO Group semblent indiquer que Chypre et la Bulgarie ont accordé des licences d'exportation pour sa technologie[10]. Or les autorités chypriotes et bulgares nient avoir délivré de telles licences à NSO[11].

2.2. Premières allégations concernant l'utilisation abusive de Pegasus

9. La version iOS de Pegasus a été identifiée en août 2016. M. Ahmed Mansoor, défenseur arabe des droits de l'homme, 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 s'il avait cliqué sur le lien, son téléphone aurait été « infecté » et le logiciel espion implanté dans celui-ci[12]. Pegasus avait déjà été mis au jour dans une fuite de documents provenant de la société Hacking Team, qui indiquaient 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[13].

10. 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 Khashoggi[14].

11. 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 pirater les téléphones de plusieurs hommes politiques en Espagne, dont l'ancien président du Parlement de Catalogne, Roger Torrent[15].

2.3. Les révélations du « Projet Pegasus »

12. En 2020, une liste de plus de 50 000 numéros de téléphone censés appartenir à des personnes considérées comme des « personnes intéressantes » 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 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 scientifiques des téléphones portables de certaines des cibles potentielles[16].

13. Le 18 juillet 2021, les premiers rapports publiés ont révélé que Pegasus avait pu être utilisé contre des défenseurs des droits de l'homme, des opposants politiques, des avocats, des diplomates, des chefs d'État et près de 200 journalistes de 24 pays[17]. Forbidden Stories et ses partenaires ont identifié des clients potentiels de NSO dans 11 pays : Arabie saoudite, Azerbaïdjan, Bahreïn, Émirats arabes unis (EAU), Hongrie, Inde,

---

[9] Ibid. pp. 29-30.
[10] Ibid. p. 4.
[11] https://www.europarl.europa.eu/doceo/document/E-9-2020-005505-ASW_EN.html; http://altanalyses.org/en/2021/07/27/the-pegasus-scandal-9-questions-and-some-answers/?utm_source=rss&utm_medium=rss&utm_campaign=the-pegasus-scandal-9-questions-and-some-answers. Il apparaît que la société Circles, qui exerce ses activités en Bulgarie, fait partie de NSO Group, mais que le bureau bulgare n'est pas chargé du développement de Pegasus. Cette société aurait développé un autre logiciel pour l'écoute des appels téléphoniques.
[12] Voir : https://www.bbc.com/news/technology-37192670, 26 août 2016.
[13] Voir :https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html, 2 septembre 2016.
[14] Voir : https://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.
[15] Voir : Phone of top Catalan politician 'targeted by government-grade spyware' | Catalonia | The Guardian, 13 juillet 2020.
[16] 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 la présence de Pegasus avaient été trouvées à la suite d'analyses effectuées par des experts du laboratoire de sécurité d'Amnesty International. Voir le procès-verbal (lien). Voir aussi : Amnesty International : Comment détecter le logiciel Pegasus, 18 juillet 2021.
[17] Voir : https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/, 18 juillet 2021.

Kazakhstan, Maroc, Mexique, Rwanda et Togo. 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[18].

14. Selon l'enquête, 48 journalistes figurent parmi les personnes susceptibles d'être visées par Pegasus en **Azerbaïdjan**[19]. Il s'agissait notamment de Sevinc Vaqifqizi, journaliste freelance pour le média indépendant Meydan TV, dont le téléphone avait été infecté pendant une période de deux ans jusqu'en mai 2021, et de Khadija Ismayilova, journaliste d'investigation au Projet de signalement de la criminalité organisée et de la corruption, dont le téléphone avait été régulièrement infecté pendant près de trois ans[20]. Certains rapports mentionnaient des militants de la société civile, comme Fatima Movlamli, une militante dont les photos intimes avaient été divulguées sur Facebook en 2019[21].

15. En **Hongrie,** les numéros de téléphone d'au moins dix avocats, cinq journalistes et un homme politique de l'opposition figuraient sur la liste des cibles potentielles de Pegasus qui a fait l'objet d'une fuite[22]. Les téléphones de Szabolocs Pany et d'András Szabo, tous deux journalistes d'investigation pour Direkt36, avaient été infectés avec succès par le logiciel espion, selon l'analyse scientifique d'Amnesty International. Le téléphone de M. Pany avait été piraté à plusieurs reprises par Pegasus au cours d'une période de sept mois en 2019, peu après des demandes de commentaires qu'il avait adressées à des responsables du gouvernement. Parmi les autres personnes identifiées comme cibles potentielles figurent le journaliste Dávid Dercseny, le propriétaire du Central Media Group Zoltán Varga, le professeur Attila Chikán (ancien ministre du premier gouvernement de Viktor Orbán et actuellement critique), le fils et l'un des plus proches confidents de l'ancien oligarque Lajos Simicska, János Bánáti, président du barreau hongrois, et Adrien Beauduin, étudiant belgo-canadien en doctorat à l'Université d'Europe centrale[23]. À cet égard, l'Union hongroise des libertés civiles (HCLU) a annoncé qu'elle engagerait une action en justice au nom de certaines des victimes présumées, notamment une plainte auprès du Procureur général israélien et des requêtes auprès de la Cour européenne des droits de l'homme[24]. Au vu de ces rapports, j'ai demandé par écrit aux autorités hongroises, par l'intermédiaire du président de la délégation de l'Assemblée hongroise, de me fournir quelques explications avant le 20 mars 2022 (lettre jointe en annexe).

16. Selon les révélations du Projet Pegasus, deux journalistes français de *Mediapart,* Edwy Plenel et Lénaïg Bredoux, ont vu leurs téléphones infectés par Pegasus en 2019 et 2020, prétendument par des agents marocains.

17. Une enquête conjointe des médias allemands a également révélé que l'Office fédéral allemand de la police criminelle (BKA) avait acquis Pegasus en 2019 dans « le plus grand secret »[25].

2.4. Révélations récentes

18. 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, et Ewa Wezosek, une procureure impliquée dans une affaire contre le gouvernement en place[26]. Le téléphone du sénateur Krzystof Brejja avait également été piraté à de nombreuses reprises lorsqu'il dirigeait la campagne électorale de la Coalition civique en 2019[27]. Parmi les 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], ainsi que d'anciens hommes politiques du parti Droit et Justice

[18] Voir : Heads of state found on list of numbers examined by Pegasus Project - The Washington Post, 20 Juillet 2021.
[19] Voir : Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 juillet 2021.
[20] https://forbiddenstories.org/journaliste/sevinc-vaqifqizi/.
[21] Pegasus project: spyware leak suggests lawyers and activists at risk across globe | Human rights | The Guardian, 19 juillet 2021.
[22] Voir : https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juillet 2021.
[23] Voir : https://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.
[24] Voir : https://hclu.hu/en/pegasus-case-foreign-procedures.
[25] Voir : https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197, 7 septembre 2021.
[26] Voir : https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 décembre 2021.
[27] Voir : https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 décembre 2021.
[28] Voir : https://apnews.com/article/technology-europe-poland-hacking-spyware-4a410bda35df566632703e3578e5a99d, 25 janvier 2022.

(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]. Au vu de ces rapports, j'ai demandé par écrit aux autorités polonaises, par l'intermédiaire du président de la délégation de l'Assemblée polonaise, de me fournir quelques explications avant le 20 mars 2022 (lettre jointe en annexe).

19. En janvier 2022, il a été signalé que Pegasus avait été utilisé par la police **israélienne** contre des organisateurs de manifestations antigouvernementales, un haut responsable politique, des maires et des employés d'entreprises publiques, entre autres[31]. La surveillance aurait été effectuée sans autorisation judiciaire. D'autres révélations ont porté sur d'autres cibles, notamment des hommes politiques et des responsables publics, des dirigeants d'entreprises, des journalistes, des militants et même Avner Netanyahu, le fils du Premier ministre de l'époque, Benjamin Netanyahu[32].

20. En janvier 2022, le ministère finlandais des Affaires étrangères a signalé que plusieurs téléphones de diplomates finlandais à l'étranger avaient été infectés par le logiciel espion Pegasus[33].

2.5. Quelques réactions aux révélations

2.5.1. La société NSO Group

21. Suite aux révélations du *Projet Pegasus* en juillet 2021, la société NSO Group a démenti « les fausses affirmations présentées dans [le] rapport, dont beaucoup sont des théories non corroborées qui soulèvent de sérieux doutes sur la fiabilité des sources ». Elle a déclaré qu'elle n'exploitait pas les systèmes qu'elle vend à des clients gouvernementaux contrôlés et qu'elle n'avait pas accès aux données des cibles de ses clients. La société a ajouté que, pour des raisons contractuelles et de sécurité nationale, elle ne pouvait pas confirmer ni infirmer l'identité de ses clients gouvernementaux, ni celle des clients dont elle avait mis le système hors service[34]. Le PDG de NSO Group a catégoriquement nié que la liste de 50 000 numéros de téléphone qui a fait l'objet d'une fuite ait un rapport avec sa société et le logiciel espion Pegasus[35].

2.5.2. Les États

22. En **France**, une enquête a été ouverte par le gouvernement, ainsi que par le parquet de Paris, à la suite d'une plainte déposée par les deux journalistes de *Mediapart* visés[36]. L'Agence nationale de la sécurité des systèmes d'information (Anssi) a confirmé que Pegasus avait été détecté sur les téléphones de trois journalistes, M. Plenel, M[me] Bredoux et un journaliste de France 24. C'est la première fois qu'une autorité officielle corrobore les conclusions de l'enquête menée dans le cadre du Projet Pegasus[37].

23. En **Hongrie,** Lajos Kósa, membre du Parlement et vice-président du Fidesz, membre de la commission parlementaire de la défense et de l'application de la loi, a reconnu que le ministère de l'Intérieur avait acheté et utilisé le logiciel Pegasus[38]. Le 31 janvier 2022, l'Autorité nationale hongroise pour la protection des données et la liberté de l'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 les services de sécurité 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 raisons de sécurité nationale. Les 300 citoyens hongrois dont le téléphone figurait sur la liste qui avait fuité n'ont pas tous

[29] Voir : https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true, 18 janvier 2022.
[30] Voir : https://wyborcza.pl/7,75398,28081346,cyberatak-na-najwyzsza-izbe-kontroli-dzis-poznamy-szczegoly.html?disableRedirects=true, 7 février 2022.
[31] Voir : https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html, 18 janvier 2022.
[32] Voir : https://www.timesofisrael.com/ministry-heads-netanyahu-associates-activists-said-targeted-by-police-with-spyware/, 7 février 2022.
[33] https://www.euronews.com/2022/01/28/finnish-diplomats-were-targeted-by-pegasus-spyware-says-foreign-ministry, 28 janvier 2022.
[34] Voir : https://www.washingtonpost.com/investigations/2021/07/18/nso-group-response-pegasus-project/, 18 juillet 2021.
[35] Voir : https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html, 20 juillet 2021.
[36] Voir : https://www.aa.com.tr/en/world/france-launches-investigation-into-pegasus-spyware/2311661, 22 juillet 2021.
[37] Voir : https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms, 2 août 2021.
[38] Voir : https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217, 4 novembre 2021.

fait l'objet d'une enquête de la part de la NAIH puisque, selon son président, Amnesty International ne lui a pas fourni cette liste[39]. Le raisonnement du contenu de l'enquête restera classifié jusqu'en 2050.

24. En **Israël,** le chef de la commission des affaires étrangères et de la défense de la Knesset a annoncé la création d'une commission d'enquête sur les allégations d'utilisation abusive de Pegasus[40]. Suite aux rapports les plus récents concernant l'utilisation de Pegasus par la police israélienne, le ministre de la Sécurité publique a annoncé qu'il allait mettre en place une commission d'enquête nommée par le gouvernement pour procéder à des investigations sur les allégations[41].

25. Le gouvernement **marocain** a nié les allégations d'acquisition et d'utilisation de Pegasus et « rejette et condamne catégoriquement ces allégations infondées et fausses »[42]. Le Maroc a également poursuivi en justice Amnesty International et Forbidden Stories, ainsi que les médias participant à l'enquête conjointe, pour diffamation[43].

26. En **Pologne**, 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 personnalités 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 se faisait « conformément à la loi »[44]. À cet égard, une commission mise en place par le Sénat polonais pour enquêter sur l'utilisation de Pegasus a entendu différents témoins et experts, parmi lesquels des experts de la cybersécurité (de Citizen Lab) et le président de la Cour des comptes, M. Banas. Celui-ci a déclaré devant la commission que le Bureau central de lutte contre la corruption avait secrètement acheté Pegasus en utilisant des fonds du ministère de la Justice destinés aux victimes de la criminalité[45].

27. 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 et trois autres sociétés étrangères 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 tenant compte d'éléments prouvant que cette société avait développé et fourni des logiciels espions à des gouvernements étrangers qui utilisaient ces programmes pour cibler de manière malveillante des responsables publics, des journalistes, des hommes d'affaires, des militants, des universitaires et des employés d'ambassades, même en dehors de leurs frontières. M[me] Gina M. Raimondo, secrétaire au Commerce des États-Unis, a déclaré : « Les États-Unis sont résolus à courir énergiquement aux contrôles à l'exportation pour mettre devant leurs responsabilités les entreprises qui développent, commercialisent illégalement ou utilisent des technologies visant à mener des activités malveillantes qui menacent la cybersécurité des membres de la société civile, des dissidents, des représentants du gouvernement et des organisations à l'intérieur du pays et à l'étranger[46] ».

2.5.3. Les entreprises

28. Des sociétés telles que Meta et Apple ont intenté des procès à NSO Group pour avoir utilisé le logiciel espion Pegasus contre leurs utilisateurs[47]. Une cour d'appel américaine a réfuté l'argument de la société israélienne selon lequel elle devait être protégée par la législation sur l'immunité souveraine.

---

[39] Voir : https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/, 31 janvier 2022.
[40] Voir : https://www.aljazeera.com/news/2021/7/22/israel-launches-commission-to-probe-pegasus-spyware-legislator, 22 juillet 2021.
[41] Voir : https://www.timesofisrael.com/police-minister-establishes-commission-to-probe-explosive-nso-spying-claims/, 7 février 2022.
[42] Voir : https://www.washingtonpost.com/investigations/2021/07/18/responses-countries-pegasus-project/, 19 juillet 2021.
[43] Voir : https://www.france24.com/en/africa/20210722-morocco-files-libel-suit-in-france-against-ngos-alleging-it-used-pegasus-spyware, 22 juillet 2021.
[44] Voir : https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 janvier 2022.
[45] Voir : https://www.usnews.com/news/business/articles/2022-01-17/polish-senators-question-cyber-experts-in-hacking-inquiry, 18 janvier 2022.
[46] https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/; https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.
[47] Voir : https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/, 23 novembre 2021; https://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.

2.5.4. Les organismes internationaux

29. L'utilisation du logiciel espion Pegasus a suscité de nombreuses réactions négatives de la part des organismes internationaux.

30. Le **Parlement européen** (PE) a décerné le prix du journalisme Daphne Caruana Galizia 2021 au « Projet Pegasus ». La commission des libertés civiles (LIBE) du PE examine la question sous l'angle des conséquences pour les droits fondamentaux de ces révélations au sujet de Pegasus. Elle a jusqu'à présent procédé à deux auditions d'experts et de personnes concernées[48]. La commission spéciale du PE sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'UE, y compris la désinformation, a procédé à une audition sur « l'ingérence étrangère et l'espionnage de personnalités politiques et d'institutions européennes », qui a également abordé la question des révélations au sujet de Pegasus[49]. Selon les informations les plus récentes, le PE se prépare à lancer une commission d'enquête sur le détournement de l'usage de Pegasus par les gouvernements de l'UE, sur la base d'une initiative du groupe Renew Europe[50].

31. Didier Reynders, **commissaire européen chargé de la Justice**, a déclaré que la Commission européenne « condamne fermement tout accès illégal aux systèmes ou toute forme d'interception illégale des communications des utilisateurs. En fait, c'est un crime dans toute l'Union ». Il a ajouté que « toute indication qu'une telle intrusion dans la vie privée a effectivement eu lieu doit faire l'objet d'une enquête approfondie et tous les responsables d'une éventuelle violation doivent être traduits en justice »[51].

32. Le **Contrôleur européen de la protection des données**, dans ses observations préliminaires publiées le 15 février 2022, a déclaré que, compte tenu du niveau d'ingérence dans le droit à la vie privée et de la difficulté de satisfaire aux exigences de proportionnalité, le déploiement régulier de Pegasus ou d'une technologie similaire de logiciels espions particulièrement intrusifs n'est pas compatible avec l'ordre juridique de l'UE. Il propose donc d'interdire le développement et le déploiement de ces logiciels espions dans l'UE et, à titre subsidiaire (si ces outils sont néanmoins utilisés dans des situations exceptionnelles), de prendre certaines mesures pour empêcher leur utilisation illégale[52].

33. La **Haut-Commissaire des Nations Unies aux droits de l'homme**, M[me] Bachelet, a estimé que les gouvernements devraient instaurer un moratoire sur la vente et le transfert de technologies de surveillance jusqu'à ce que des garanties adéquates soient mises en place en matière de droits de l'homme[53]. Elle a également appelé les États à enquêter sur les cas de surveillance ciblée et à accorder réparation aux victimes.

2.5.5. Les journalistes et la société civile

34. Les journalistes et les organisations non gouvernementales du monde entier ont vivement réagi aux révélations concernant l'utilisation abusive de Pegasus contre des journalistes, des dirigeants de l'opposition et des militants[54]. Ils ont demandé demander l'ouverture d'enquêtes, l'obligation de rendre compte et une

[48] Le 29 novembre 2021, la commission LIBE a entendu Laurent Richard, directeur exécutif de Forbidden Stories, Etienne Maynier, technologue au laboratoire de sécurité d'Amnesty International, et Wojciech Wiewiórowski, Contrôleur européen de la protection des données. Le 1er février 2022, la commission LIBE a entendu Szabolcs Pany, journaliste hongrois, Ewa Wrzosek, procureure polonaise, et Ozturan Gürkan, du Centre européen pour la liberté de la presse et des médias.
[49] Le 9 septembre 2021, à laquelle ont participé Robert Dover, professeur de criminologie à l'Université de Hull, Margarita Robles Carrillo, professeure à l'Université de Grenade, Laurent Richard et Sandrine Rigaud, directrice exécutive et rédactrice en chef de Forbidden Stories.
[50] Voir : EU to launch rare inquiry into Pegasus spyware scandal | European Union | The Guardian, 10 février 2022.
[51] Voir : EU commissioner calls for urgent action against Pegasus spyware | Surveillance | The Guardian, 15 septembre 2021.
[52] Voir : Voir Contrôleur européen de la protection des données, Remarques préliminaires sur les logiciels espions modernes, 15 février 2022 (en anglais), https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.
[53] Déclaration faite lors de l'échange de vues de la commission du 14 septembre 2021. Voir : OHCHR | Commission des questions juridiques et des droits de l'homme, Assemblée parlementaire Conseil de l'Europe : audition sur les implications du logiciel espion Pegasus 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.
[54] Committee to Protect Journalists (Spyware reform critical as at least 180 journalists revealed as potential Pegasus targets - Committee to Protect Journalists (cpj.org)); International Press Institute (Pegasus Project: Full investigation needed after 180 journalists targeted by spyware - International Press Institute (ipi.media)); Human Rights Watch (Human Rights Watch Among Pegasus Spyware Targets | Human Rights Watch (hrw.org)) ; Amnesty International (La partie immergée de l'iceberg. La responsabilité des États et du secteur privé dans la crise de la surveillance numérique - Amnesty International).

réglementation du commerce mondial des technologies de surveillance. Edward Snowden a appelé les gouvernements à imposer un moratoire mondial sur le commerce international des logiciels espions[55].

3. Logiciels espions similaires

35. Pegasus n'est pas le seul outil d'espionnage disponible qui ait été utilisé par des gouvernements. D'autres logiciels espions auraient été utilisés de façon abusive. Par exemple, un logiciel commercialisé par la société israélienne Candiru aurait ciblé les détracteurs de régimes autocratiques, notamment certains lecteurs d'un site d'information basé à Londres[56]. Contrairement à Pegasus, qui infecte les téléphones portables, le logiciel malveillant de Candiru est censé infecter les ordinateurs. Dans certains cas, l'utilisateur de ce logiciel peut lancer un programme ou un code (« un exploit ») qui lui permet d'exploiter une vulnérabilité logicielle pour prendre le contrôle de l'ordinateur d'une cible visée. Le Département du commerce américain a placé sur liste noire la société Candiru, ainsi que NSO Group, pour avoir fourni des logiciels espions à des gouvernements étrangers qui les ont ensuite utilisés à des fins malveillantes (voir paragraphe 25 ci-dessus).

36. FinFisher, également connu sous le nom de FinSpy, est un logiciel de surveillance commercialisé par Lench IT Solutions plc., qui possède une succursale basée au Royaume-Uni (Gamma International Ltd) et une autre basée en Allemagne (Gamma International GmbH). L'utilisation de FinFisher par les gouvernements pour surveiller des dissidents politiques a été signalée pour la première fois en Égypte en 2011. Son utilisation a ensuite été signalée également au Bahreïn (2010-2012) et contre des dissidents éthiopiens en exil. Des organisations de la société civile ont déposé plainte au pénal contre Gamma Group au Royaume-Uni et en Allemagne.

4. Normes juridiques pertinentes et applicables

4.1. Normes du Conseil de l'Europe

37. La surveillance secrète ciblée, notamment l'interception des communications par téléphone mobile, constitue une ingérence dans le 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 »)[57]. 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 » mentionnés dans ce paragraphe et est « nécessaire dans une société démocratique » pour atteindre ces buts[58].

38. En ce qui concerne la première exigence, cela signifie que la surveillance doit avoir un fondement en droit interne et que ce droit doit être accessible à la personne concernée et prévisible quant à ses effets. La loi doit user de termes assez clairs et détaillés 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, une 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[59]. La Cour a réaffirmé que ces garanties minimales s'appliquent dans les cas où l'interception avait pour but de prévenir ou de déceler des infractions pénales, mais aussi dans ceux où la mesure a été ordonnée pour des raisons de sécurité nationale[60]. Elle a cependant admis que l'exigence de « prévisibilité » de la loi n'allait pas jusqu'à imposer aux États l'obligation d'édicter

---

[55] Voir : Edward Snowden calls for spyware trade ban amid Pegasus revelations | Edward Snowden | The Guardian, 19 juillet 2021.

[56] Israeli firm's spyware linked to attacks on websites in UK and Middle East | Malware | The Guardian, 16 novembre 2021. Voir aussi : Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus - The Citizen Lab.

[57] 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, par les services de sécurité, de données sur des individus précis, notamment le lieu où se trouve la personne et ses déplacements dans l'espace public, constituent également une ingérence dans la vie privée (voir *Shimovolos c. Russie,* requête n° 30194/09, arrêt du 21 juin 2011, paragraphe 65).

[58], 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, 2021.

[59] Ibid., paragraphe 228-231, avec d'autres références.

[60] 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).

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 »[61].

39. La deuxième condition requise pour qu'une ingérence soit justifiée au titre de l'article 8.2 est que la mesure soit « nécessaire dans une société démocratique » pour atteindre 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 de surveiller en secret les citoyens n'est tolérable d'après l'article 8 que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques[62]. 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 garanties et 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, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne[63].

40. Pour ce qui est des procédures d'autorisation, bien que l'autorisation judiciaire préalable puisse constituer une garantie importante contre la surveillance abusive, la Cour examine minutieusement son champ d'application (si le juge applique un critère de « nécessité » ou de « proportionnalité ») et le contenu de l'autorisation d'interception (si des personnes ou des locaux spécifiques sont mentionnés)[64]. 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[65]. En appliquant ces principes, la Cour a estimé dans l'affaire *Szabó et Vissy c. Hongrie*[66] 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[67].

41. La Cour a constaté des violations de l'article 8 dans des affaires de surveillance secrète de militants des droits de l'homme[68], de membres d'organisations non gouvernementales[69], d'avocats[70]et de journalistes[71], entre autres.

42. 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, consacré par l'article 10 de la Convention, en l'absence de garanties adéquates dans la loi[72] ou de tout impératif prépondérant d'intérêt

---

[61] *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 pareille menace, et si celle-ci est grave au point de justifier une surveillance secrète.

[62] *Klass et autres c. Allemagne* requête n° 5029/71, arrêt du 6 septembre 1978, paragraphe 42.

[63] *Roman Zakharov c. Russie*, paragraphes 235-238.

[64] 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 qu'ils soient tenus 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 l'affaire *Ekimdzhiev et autres c. Bulgarie,* requête n° 70078/12, arrêt du 11 janvier 2022 (non définitif), dans laquelle la Cour a critiqué le fait que les tribunaux bulgares délivrant des mandats de surveillance ne donnaient aucun motif ou donnaient des motifs généraux et globaux (paragraphes 307-322).

[65] Ibid., paragraphe 233.

[66] *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 : https://hudoc.exec.coe.int/eng?i=004-10745).

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

[68] *Shimovolos c. Russie,* requête n° 30194/09, arrêt du 21 juin 2011.

[69] *Affaire « Association '21 décembre 1989' et autres c. Roumanie » (groupe d'affaires*), requête n° 33810/07, arrêt du 24 mai 2011.

[70] *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.

[71] *Azer Ahmadov c. Azerbaïdjan,* requête n° 3409/10, arrêt du 22 juillet 2021.

[72] *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 défini des critères applicables à 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

public justifiant de telles mesures dans un cas concret[73]. La Cour a constamment considéré que le droit pour les journalistes de protéger leurs sources fait partie de la liberté de « recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques » consacrée par l'article 10 et qu'il en constitue l'une des garanties essentielles. Il s'agit là d'une pierre angulaire de la liberté de la presse, dont l'absence pourrait dissuader les sources d'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 un impératif prépondérant d'intérêt public[74].

43. La **Convention de 1981 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 qui ait une portée mondiale (ratifiée par 55 Parties, dont 8 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 réalisé par les autorités judiciaires et autres autorités répressives. 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)[75]. À cet égard, M. Kaldani, Vice-Président du Comité consultatif de la Convention, a rappelé lors de l'audition du 14 septembre 2021 que la **Convention 108 modernisée** (Protocole STCE n ° 223, ouvert à la signature le 10 octobre 2018 et non encore entré en vigueur[76]) supprime cette possibilité. La Convention modernisée établit également des exigences plus strictes pour 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[77]. Elle renforce les droits des personnes et impose des exigences de plus grande transparence[78], qui peuvent toutefois être restreintes lorsque cette mesure est prévue par la loi et constitue, dans une société démocratique, une mesure nécessaire à la poursuite d'« objectifs essentiels d'intérêt public général », notamment la protection de la sécurité nationale, la défense ou l'investigation et la répression des infractions pénales[79]. Les activités de traitement à des fins de sécurité nationale et de défense doivent en tout cas faire l'objet d'un contrôle indépendant effectif prévu par la législation nationale de chaque Partie[80].

44. La **Convention sur la cybercriminalité** (STE n° 185, également connue sous le nom de « Convention de Budapest » ou « Convention Cybercriminalité »), ouverte à la signature en 2001, rassemble des parties de toutes les régions du monde (66 ratifications en février 2022). Elle contient des dispositions sur le droit pénal matériel et le droit procédural, ainsi que sur la coopération internationale en matière de délits informatiques. 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 »[81]. Parmi les abus que la Convention impose aux États parties

---

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).

[73] *Sedletska c. Ukraine,* requête n° 42634/18, arrêt du 1er 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, au titre de l'article 39 de son règlement 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 le mandat délivré par le juge d'instruction à l'égard de la requérante.

[74] *Sanoma Uitgevers B.V. c. Pays-Bas,* requête n° 38224/03, arrêt du 14 septembre 2010 (Grande Chambre), paragraphes 50-51.

[75] 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 la recherche et la prévention des infractions pénales.

[76] À ce jour, 16 États l'ont ratifié.

[77] Article 5.

[78] Articles 8 et 9.

[79] Article 11.1.

[80] Article 11.3. M. Kaldani a déclaré qu'une réflexion était en cours au sein de sa commission 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 répondait pas pleinement et expressément à certains des défis posés à notre époque numérique par des capacités de surveillance sans précédent, et que des garanties plus solides au niveau international (par exemple, un instrument complet de droit international des droits de l'homme encadrant les opérations des services de renseignement) étaient nécessaires. Voir à cet égard la déclaration conjointe du 7 septembre 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 » : https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb..

[81] 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 : http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e7.

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[82]. 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 réalise réellement[83].

45. 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. A ce propos, il convient de renvoyer à la Résolution 1843 (paragraphe 18) et à la Recommandation 1984 (2011) sur 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)[84], ainsi qu'à la Résolution 2256 (2019) « Gouvernance de l'internet et droits de l'homme » (paragraphe 7).

46. Dans sa 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 adoptées par les États-Unis et 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 ; 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 » (paragraphe 17). 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, notamment sous l'angle des droits de l'homme et des libertés fondamentales des usagers de l'internet (paragraphes 2.1 et 2.2).

47. 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 CM/Rec(2014)6 sur un Guide des droits de l'homme pour les utilisateurs d'internet (Annexe, §§ 65-85) et la Recommandation CM/Rec(2016)5 sur la liberté d'internet (Annexe, § 4.2). Le Comité des Ministres a rappelé que toute mesure prise dans l'intérêt de la sécurité nationale devait satisfaire rigoureusement aux exigences énoncées dans 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

[82] Rapport explicatif de la Convention,§ 58.

[83] Note d'orientation n °7 du T-CY, Nouvelles formes de logiciels malveillants, 5 juin 2013 : http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b5. Selon l'Organisation de coopération et de développement économiques (OCDE), « le terme 'logiciel malveillant' est un terme générique qui désigne un fragment de code 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 ».

[84] 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 à propos des violations massives du droit au respect de 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.

négatives et des obligations positives, notamment la protection contre les restrictions arbitraires imposées par des acteurs non étatiques[85].

4.2. Autres normes internationales

48. 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 de protection contre la surveillance ciblée faites aux États par les Nations Unies en matière de droits de l'homme, et notamment par les articles 12 (droit à la vie privée) et 19 (liberté d'expression) de la Déclaration universelle des droits de l'homme, ainsi que les articles 17(1) (droit à la vie privée) et 19 (liberté d'expression) du Pacte international relatif aux droits civils et politiques (PIDCP). Le rapport affirme qu'en plus de l'obligation première de s'abstenir de toute ingérence dans ces droits, les États ont le devoir de protéger les particuliers contre l'ingérence de tiers, notamment pour ce qui est de la surveillance transnationale exercée par des entités étrangères sur leurs propres citoyens. Il évoque également les Principes directeurs relatifs aux entreprises et aux droits de l'homme concernant la 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, en ajoutant que ces principes 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.).

49. Afin d'améliorer le respect de ces normes et de combler les lacunes de leur mise en œuvre, le Rapporteur spécial propose dans son rapport un cadre juridique et stratégique permettant de réglementer le secteur privé de la surveillance et de faire en sorte que les principes de responsabilité et de transparence y soient respectés. Il appelle à une réglementation plus stricte de l'exportation et de l'utilisation de technologies, mais aussi à l'instauration d'un moratoire immédiat sur la vente et le transfert de licences d'exportation de technologies de surveillance jusqu'à ce que l'utilisation de ces technologies puisse être techniquement limitée à des fins légales et conformes aux droits de l'homme, ou jusqu'à ce que l'on puisse garantir 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[86].

50. En ce qui concerne la **législation de l'Union européenne**, outre la Charte des droits fondamentaux (articles 7, 8, 11, 47 et 52, paragraphe 1) et la directive « vie privée et communications électroniques »[87], il convient de mentionner le règlement de l'Union sur les biens à double usage (refonte), qui a mis en place 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[88]. Je tiens également à examiner dans le rapport la pertinence de la Directive en matière de protection des données dans le domaine répressif, qui établit par exemple l'obligation de notifier toute violation de données à caractère personnel qui présente un risque pour les droits et libertés individuels à l'autorité de contrôle dans un délai de 72 heures au plus tard[89].

5. Conclusions préliminaires et prochaines étapes

51. Les révélations au sujet de Pegasus ont apporté la preuve que ce logiciel espion a été utilisé comme un outil de piratage et de surveillance de journalistes, d'avocats, d'hommes politiques et de militants des droits de l'homme dans plusieurs États membres du Conseil de l'Europe et dans d'autres pays. Compte tenu du niveau d'intrusion de ce logiciel, qui accorde un accès à distance non autorisé (« zéro-clic ») et sans restriction au téléphone portable et à toutes les données à caractère personnel et privé qu'il contient, son utilisation a de graves répercussions sur les droits fondamentaux des personnes effectivement visées, notamment leur droit

[85] Voir Réponse à Recommandation, Doc. 13911, 14 octobre 2015.
[86] OHCHR | Rapport 2019 du Rapporteur spécial au Conseil des droits de l'homme des Nations Unies Voir aussi Haut-Commissaire des Nations Unies aux droits de l'homme, 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, §§ 24-40 ; et rapport : *Le droit à la vie privée à l'ère du numérique*, 30 juin 2014. Voir la Résolution 73/179 de l'Assemblée générale des Nations Unies du 17 décembre 2018.
[87] OJ L 201, 31/07/2002, p. 37-47.
[88] OJ L 206, 11/06/2021, p. 1-461.
[89] Directive UE 2016/680 du 27 avril 2016, JO L 119 du 04/05/2016, 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).

à 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 remplir, compte tenu précisément de son degré d'intrusion et de furtivité. En tout état de cause, il convient de répondre à la grave question de savoir si la surveillance de ces personnes avait un fondement juridique et pouvait être justifiée, que ce soit pour des raisons de sécurité nationale ou aux fins d'une enquête pénale. À cet égard, comme nous l'avons indiqué précédemment, j'ai déjà posé un certain nombre de questions dans des lettres adressées aux autorités hongroises et polonaises, à la lumière des éléments de preuve de plus en plus nombreux de l'utilisation de Pegasus dans les deux pays contre plusieurs personnes, utilisation qui aurait été motivée par des considérations politiques. J'ai l'intention d'envoyer des courriers identiques à toutes les délégations, même en l'absence d'allégations concrètes sur l'utilisation de Pegasus, afin d'obtenir des informations complètes sur son éventuelle acquisition et utilisation (ou celle d'un logiciel espion similaire) par l'un des États membres du Conseil de l'Europe. J'envisage également d'envoyer des demandes d'informations à d'autres acteurs, notamment à la société NSO Group. Je suivrai également de près les auditions et les débats qui se tiennent actuellement devant le Parlement européen au sujet de Pegasus, et j'envisage la possibilité d'effectuer une visite de travail pour assurer la coordination.

52. Outre la mise en évidence d'allégations spécifiques de l'utilisation de Pegasus dans certains États membres, de son ampleur et de ses implications, l'autre objectif principal de mon rapport sera de faire le point sur les normes internationales et du Conseil de l'Europe en vigueur en matière de surveillance numérique ciblée (en recherchant la complémentarité, par exemple, de la Convention européenne des droits de l'homme, de la Convention 108 et de la Convention sur la cybercriminalité), notamment sur la question du commerce mondial des outils de surveillance développés par le secteur privé et sur les obligations positives pertinentes faites aux États de réglementer et de restreindre ce commerce. J'ai l'intention de relever les lacunes du cadre juridique existant en vue de formuler des propositions concrètes visant à élaborer une réponse coordonnée du Conseil de l'Europe à l'utilisation abusive des outils de surveillance par les autorités publiques contre des individus ciblés et à prévoir des garanties plus strictes dans ce domaine.

53. Afin de réaliser pleinement mon mandat, je souhaite procéder à une autre audition par la commission d'un représentant d'une ONG ayant déposé des plaintes au nom de certaines des victimes, d'un expert technique/informatique qui a participé aux enquêtes (Amnesty International Security Lab, ou Citizen Lab à l'Université de Toronto) et d'un député européen ayant participé aux auditions du PE sur ce sujet. Je propose également d'effectuer une mission d'information en Israël, afin de rencontrer les représentants de NSO Group, de l'Agence de contrôle des exportations de la défense du ministère israélien de la Défense, des membres de la Knesset qui prennent part aux initiatives d'enquête sur les allégations d'utilisation abusive du logiciel de NSO et de logiciels espions similaires, ainsi qu'un avocat israélien qui a tenté à plusieurs reprises de poursuivre le groupe NSO au sujet de Pegasus (M. Eitay Mack).

54. Enfin, je propose que cette note d'information soit déclassifiée immédiatement après la réunion de la commission.

Annexe

Questions envoyées aux autorités hongroises et polonaises :

1. Vos autorités peuvent-elles confirmer qu'elles ont acquis le logiciel espion Pegasus et fournir des informations sur tout autre logiciel espion qu'elles ont pu obtenir ?
2. Quel est le fondement juridique qui régit l'application de ces logiciels espions et comment la conformité à cette législation est-elle assurée ?
3. Le logiciel espion Pegasus a-t-il été utilisé contre l'une des personnes mentionnées dans la lettre, ou contre d'autres individus, et si oui, sur quel fondement juridique ?
4. Contre combien de personnes le logiciel espion Pegasus a-t-il été utilisé par le gouvernement ?
5. Pouvez-vous indiquer quels sont les organismes gouvernementaux qui ont la possibilité d'utiliser ces logiciels espions et contre quelle catégorie de personnes ils ont été utilisés ?
6. Quelles sont les mesures qui ont été prises par vos autorités pour empêcher l'utilisation abusive de logiciels espions contre des personnes telles que celles mentionnées dans la lettre ?
7. Quelles sont les enquêtes officielles qui ont été ouvertes, ou sont prévues, sur l'utilisation abusive des logiciels espions, et quelles sont les conclusions (provisoires ou non) qui sont disponibles ?
8. Prévoyez-vous de modifier le cadre juridique de l'utilisation de Pegasus ou de logiciels espions similaires à l'avenir, d'améliorer la conformité de son usage et de prévenir les abus éventuels ?
9. Quelles sont les mesures envisagées pour que ceux qui font un usage abusif de ces logiciels espions soient finalement sanctionnés ?