LA PARTIE IMMERGÉE DE L'ICEBERG

LA RESPONSABILITÉ DES ÉTATS ET DU SECTEUR PRIVÉ DANS LA CRISE DE LA SURVEILLANCE NUMÉRIQUE

AMNESTY INTERNATIONAL

Amnesty International est un mouvement rassemblant 10 millions de personnes qui fait appel à l'humanité en chacun et chacune de nous et milite pour que nous puissions toutes et tous jouir de nos droits humains. Notre vision est celle d'un monde dans lequel les dirigeants et dirigeantes tiennent leurs promesses, respectent le droit international et sont tenu·e·s de rendre des comptes. Essentiellement financée par ses membres et des dons individuels, Amnesty International est indépendante de tout gouvernement, de toute tendance politique, de toute puissance économique et de tout groupement religieux. Nous avons la conviction qu'agir avec solidarité et compassion aux côtés de personnes du monde entier peut rendre nos sociétés meilleures.

© Amnesty International 2021
Sauf exception dûment mentionnée, ce document est sous licence Creative Commons : Attribution-NonCommercial-NoDerivatives-International 4.0.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode
Pour plus d'informations, veuillez consulter la page relative aux autorisation sur notre site : www.amnesty.org.
Lorsqu'une entité autre qu'Amnesty International est détentrice du copyright, le matériel n'est pas sous licence Creative Commons.
L'édition originale de ce document a été publié en 2021
par Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Royaume-Uni.

Index : DOC 10/4491/2021
L'édition originale a été publiée en langue anglaise

amnesty.org

Illustration de couverture : *© Toscanabanana 2021*

AMNESTY INTERNATIONAL

SOMMAIRE

1. INTRODUCTION **4**

2. OBSERVATIONS SUR LE DROIT INTERNATIONAL RELATIF AUX DROITS HUMAINS PAR RAPPORT AUX RÉVÉLATIONS DU PROJET PEGASUS **6**

2.1 UN CIBLAGE D'UNE AMPLEUR DÉMESURÉE AUX CONSÉQUENCES GRAVES SUR LES DROITS HUMAINS 6

2.2 GRAVE INTRUSION ET PROTECTIONS MINIMES 10

2.3 LES FAUTES DES ÉTATS ET LA COMPLICITÉ DES ENTREPRISES 14

3. CONCLUSIONS ET RECOMMANDATIONS **18**

1. INTRODUCTION

Lors du lancement d'une plateforme[1] (développée par Forensic Architecture, avec le soutien d'Amnesty International et du Citizen Lab) conçue pour assurer un suivi du déploiement et des répercussions sur les droits humains des outils de surveillance numérique ciblée de NSO Group, le lanceur d'alerte Edward Snowden a déclaré : « Je pense que cette enquête, qui porte sur NSO Group mais aussi sur le secteur et la technologie dans leur ensemble, est aujourd'hui le sujet le plus important dont les médias ont à s'emparer[2]. » De fait, depuis de nombreuses années, la société civile alerte sur le fait que l'opacité généralisée qui entoure le recours à la surveillance numérique ciblée et le rôle du secteur privé dans sa facilitation empêchent de prendre la mesure des graves répercussions de ce commerce en matière de droits humains et entravent l'obligation de rendre des comptes pour les auteurs de violations. Nous avons alerté quant au fait que les quelques informations que des membres de la société civile, des journalistes et des chercheurs ont réussi à obtenir sur NSO Group et quelques autres entreprises du secteur de la surveillance comme Hacking Team et FinFisher ne représentent que la partie visible de l'iceberg.

Récemment, une enquête collaborative menée par plus de 80 journalistes de 17 médias dans 10 pays et coordonnée par Forbidden Stories avec le soutien technique d'Amnesty International a abouti à la publication de révélations d'une ampleur similaire à celles d'Edward Snowden, mettant en évidence le fait que l'utilisation par certains États d'outils de surveillance numérique ciblée fournis par un des plus importants protagonistes du secteur est complètement hors de contrôle et déstabilise et menace les droits humains, y compris la sécurité physique. L'enquête révèle que des défenseurs des droits humains, des journalistes, des avocats, des militants et des personnalités politiques du monde entier ont été des cibles potentielles de cette attaque presque mondiale de la sphère privée.

Au cours de l'enquête, des spécialistes du Security Lab d'Amnesty Tech ont réussi à identifier des traces d'attaques « zéro clic » (introduction d'un programme malveillant ne nécessitant pas d'interaction avec l'utilisateur ciblé) en procédant à des analyses techniques de pointe, et notamment en faisant le lien entre ces nouveaux incidents et des attaques précédentes à l'encontre de défenseurs des droits humains perpétrées au moyen de logiciels de NSO Group[3]. Ce projet, qui constitue une avancée décisive et très attendue en matière de transparence dans un secteur obstinément réfractaire, a reposé sur l'effort collectif de toutes les personnes impliquées. Il est toutefois important de noter que la réussite des démarches entreprises dans le cadre de l'enquête était loin d'être acquise et que ces révélations ne sauraient suffire à constituer le seul mode de contrôle exercé sur les acteurs du secteur et au niveau des États.

Les articles publiés à la suite de cette collaboration parlent d'eux-mêmes. Avec ce rapport, Amnesty International entend apporter sa contribution en relevant les principaux enseignements du point de vue du droit international et en particulier du droit international relatif aux droits humains qui ressortent des révélations et des analyses techniques. Il s'agit notamment de l'ampleur démesurée du ciblage au regard du droit international relatif aux droits humains qui s'avère également en décalage par rapport à l'argumentation officielle de l'entreprise consistant à affirmer que la vente de ses produits aide ses clients à combattre le

[1] Forensic Architecture, Amnesty International et Citizen Lab, *Digital Violence*, digitalviolence.org.

[2] Aaron Schaffer, The Cybersecurity 202: Group maps alleged victims of NSO Group surveillance tool, *The Washington* Post, 6 juillet 2021, washingtonpost.com/politics/2021/07/06/cybersecurity-202-group-maps-alleged-victims-nso-group-surveillance-tool.

[3] Amnesty International, *Forensic Methodology Report:How to Catch NSO Group's Pegasus*, 18 juillet 2021, amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus.

crime, et notamment les comportements liés au terrorisme ; la nature clandestine de l'outil qui facilite une utilisation et un fonctionnement illégaux ; les violations graves des droits humains qui en ont résulté ; l'impunité totale des États et des entreprises qui utilisent cet outil et l'incapacité des États à remplir leur obligation de protéger la population contre cette surveillance et ces piratages illégaux.

Enfin, Amnesty International formule des recommandations sur les mesures à prendre, compte tenu du besoin manifeste de mettre en place un contrôle indépendant du secteur de la surveillance numérique ciblée, de garantir l'obligation de rendre des comptes pour les violations des droits humains et d'améliorer la transparence. En effet, si les éléments révélés sont ce qu'on peut attendre d'une entreprise qui prétend respecter les droits humains conformément aux Principes directeurs relatifs aux entreprises et aux droits de l'homme (Principes directeurs des Nations unies[4]), quel espoir reste-t-il en ce qui concerne le large éventail d'activités de surveillance rendues possibles par le secteur de la surveillance de manière générale ? Les révélations mènent à la conclusion suivante : ce secteur et les États qui font appel à ses services restent dispensés de rendre compte de leurs actes en la matière et il faut mettre fin aux pratiques sous leur forme actuelle. Nos droits fondamentaux et la sécurité de l'ensemble de l'écosystème numérique en dépendent.

Depuis des années, Amnesty International met en garde contre les dangers pour les droits humains[5] que représentent la surveillance illégale de façon générale et la surveillance ciblée et les pratiques de NSO Group en particulier[6]. Ces révélations apportent un nouvel éclairage sur le besoin urgent d'un véritable contrôle face aux atteintes endémiques dont nous connaissons désormais avec certitude l'existence. Elles montrent que quand les États manquent à leur devoir de respecter les droits humains en exerçant une surveillance et à celui de nous protéger contre les violations des droits humains commises par des entreprises dans le pays ou à l'étranger, ces mêmes entreprises pourront continuer à s'exonérer en toute impunité de leurs responsabilités en matière de droits humains.

[4] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf.

[5] Amnesty International, *« Il suffit que les gens pensent que ça existe » : société civile, culture du secret et surveillance au Bélarus*, (Index : EUR 49/4306/2016), 7 juillet 2016, https://www.amnesty.org/fr/documents/eur49/4306/2016/fr/ ; Amnesty International, « We Will Find You, Anywhere »: The Global Shadow of Uzbekistani Surveillance, *Medium*, 30 mars 2017, medium.com/amnesty-insights/we-will-find-you-anywhere-the-global-shadow-of-uzbekistani-surveillance-254405805860, Amnesty International, « Royaume-Uni. La plus haute juridiction de l'Europe statue que le régime de surveillance de masse du Royaume-Uni a bafoué les droits humains », 25 mai 2021 https://www.amnesty.org/fr/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/.

[6] Amnesty International, *Défendre les droits : une activité sous surveillance :Synthèse de l'impact de la surveillance numérique sur les personnes qui défendes les droits humains,* (Index : ACT 30/1385/2019), 20 décembre 2019, https://www.amnesty.org/fr/documents/act30/1385/2019/fr/ ; Amnesty International, *Pakistan: Human Rights under Surveillance*, (Index: ASA 33/8366/2018), 15 mai 2018, amnesty.org/en/documents/asa33/8366/2018/en; Amnesty International, *Un journaliste marocain victime d'attaques par injection réseau au moyen d'outils conçus par NSO Group*, 22 juin 2020, https://www.amnesty.org/fr/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/.

2. OBSERVATIONS SUR LE DROIT INTERNATIONAL RELATIF AUX DROITS HUMAINS PAR RAPPORT AUX RÉVÉLATIONS DU PROJET PEGASUS

2.1 UN CIBLAGE D'UNE AMPLEUR DÉMESURÉE AUX CONSÉQUENCES GRAVES SUR LES DROITS HUMAINS

Les États sont tenus légalement de protéger la population contre les atteintes commises par des entreprises privées comme NSO Group telles que celles qui ont été dévoilées. Cependant, les révélations confirment également ce que l'on sait depuis longtemps : de nombreux États se montrent peu enclins à respecter et encore moins à protéger les droits humains quand il s'agit de surveillance. Faute d'un contrôle suffisant exercé par les États sur NSO Group, des atteintes aux droits humains à grande échelle ont pu être commises.

OBLIGATIONS RESPECTIVES DES ÉTATS ET DES ENTREPRISES EN MATIÈRE DE DROITS HUMAINS

En vertu du droit international relatif aux droits humains, les États ont l'obligation de protéger les personnes des atteintes à leurs droits que pourraient commettre des tiers[7]. Les États sont ainsi tenus de réglementer la conduite des entreprises qui sont domiciliées sur leur territoire ou qui se trouvent sous leur contrôle effectif, afin de les empêcher de causer des atteintes aux droits humains ou d'y contribuer, y compris lorsque celles-ci se produisent dans d'autres pays[8].

Comme l'indiquent les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, les entreprises sont tenues de respecter les droits humains quel que soit l'endroit dans le monde où elles mènent leurs activités. Ces Principes directeurs imposent aux entreprises de prendre des mesures proactives pour s'assurer de ne pas causer d'atteintes aux droits humains ni d'y contribuer dans le cadre de leurs opérations internationales et pour remédier à de telles atteintes lorsqu'elles se produisent. Pour remplir cette obligation, les entreprises doivent faire preuve de diligence raisonnable en matière de droits humains pour « identifier leurs incidences sur les droits de l'homme, prévenir ces incidences et en atténuer les effets, et rendre compte de la manière dont elles y remédient ». Cette responsabilité qu'ont les entreprises de respecter les droits humains est indépendante des capacités et de la détermination des États de remplir leurs propres obligations en la matière, et prévaut sur le respect des lois et règlements nationaux qui protègent les droits fondamentaux. Ainsi, le guide interprétatif des Principes directeurs des Nations unies précise que l'on peut considérer qu'une entreprise peut contribuer à une atteinte aux droits humains si elle fournit « des données sur les utilisateurs des services Internet à un gouvernement qui les utilise pour retracer et poursuivre les dissidents politiques, et ce en opposition avec les droits de l'homme[9]. »

Par ailleurs, il est possible qu'une entreprise qui vend des équipements de surveillance soit complice des violations des droits humains perpétrées à l'aide de ces équipements. Un groupe d'experts de la Commission internationale de juristes a étudié de manière approfondie la question de la complicité des entreprises dans les violations des droits humains et a clarifié la responsabilité juridique – civile et pénale – que pourrait représenter une telle complicité. Cette commission a estimé que le lien pourrait s'établir relativement facilement en droit si la conduite de l'entreprise permettait, aggravait ou facilitait la perpétration d'atteintes et si celle-ci savait, ou aurait raisonnablement dû savoir, que ces atteintes seraient commises. Une entreprise pourrait permettre, aggraver ou faciliter les atteintes, entre autres, par la fourniture de biens et de services[10].

NSO Group a souvent affirmé, pour justifier son existence (et son opacité), que l'« unique raison d'être de NSO est de fournir des technologies aux services de renseignement gouvernementaux agréés et aux organismes d'application des lois pour les aider à lutter contre le terrorisme et les crimes graves[11]. » En vue de rallier des soutiens publics et officiels et de mener ses activités sans entrave, l'entreprise a fait valoir

[7] Comité des droits de l'homme des Nations unies, Observation générale n° 31 [80] :« La Nature de l'obligation juridique générale imposée aux États parties au Pacte », doc. ONU CCPR/C/21/Rev.1/Add.13, § 8.

[8] Les États sont responsables de la protection contre les violations perpétrées par les entreprises privées, même au-delà de leurs frontières. Ce principe est largement accepté et directement applicable aux droits enfreints dans les cas révélés par ce projet. Voir par exemple Comité des droits économiques, sociaux et culturels, Observation générale n°14, Obligations des États en vertu du Pacte international relatif aux droits économiques, sociaux et culturels dans le contexte des activités des entreprises, 10 août 2017, doc. ONU E/C.12/GC/24, § III.C.2. ; Comité des droits de l'homme des Nations unies, Observation générale n°36, Droit à la vie, 3 septembre 2019, doc. ONU CCPR/C/GC/36, § 63 ; voir également Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi, 19 juin 2019, doc. ONU A/HRC/41/CRP.1.

[9] Haut-Commissariat des Nations unies aux droits de l'homme, *La responsabilité des entreprises de respecter les droits de l'homme : Guide interprétatif*, https://www.ohchr.org/Documents/Publications/HR_PUB_12_2_fr.pdf, p. 19.

[10] International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1er janvier 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[11] NSO Group, "NSO Group Statement on Facebook Lawsuit", *CISION PR Newswire*, 30 octobre 2019, prnewswire.com/il/news-releases/nso-group-statement-on-facebook-lawsuit-832166037.html. Voir aussi NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, traduction d'un extrait de la partie Contract Provisions (dispositions contractuelles), p. 31. « L'utilisateur final déclare et garantit par la présente que lui et ses employés et agents respectifs ... (iii) utiliseront le Système uniquement à des fins de prévention et d'enquête légitimes et légales de crimes graves et de terrorisme, tels qu'ils sont définis dans le tableau F ou en droit national de manière similaire en substance au contenu du tableau F, et les définitions du tableau F priment en cas de conflit matériel entre les définitions de tels crimes en droit national et dans le tableau F[.] ».

l'argument d'un recours légitime à un outil essentiel pour lutter contre le terrorisme et arrêter des criminels. Les révélations du Projet Pegasus démolissent ce raisonnement.

Depuis plusieurs années, nous dénonçons le fait que cet outil, qui peut certes être commercialisé à des fins légitimes, telles que le « recueil de données provenant d'appareils mobiles appartenant à des personnes soupçonnées d'être coupables de graves crimes[12] », est utilisé en parallèle contre des membres de la société civile et d'autres personnes de manière incompatible avec le droit international relatif aux droits humains. Les révélations de cette enquête collaborative confirment l'ampleur démesurée de cet usage parallèle, ainsi que les répercussions déstabilisantes que pourrait avoir l'outil non seulement sur les droits humains, mais aussi sur la sécurité de l'environnement numérique de manière générale.

Le ciblage illégal au moyen du logiciel de NSO Group dévoilé dans ce projet s'étend dans le monde entier et touche potentiellement des dirigeants, des personnalités politiques, des défenseurs des droits humains et des journalistes. À partir des données divulguées et des enquêtes qu'ils ont conduites, Forbidden Stories et ses partenaires dans les médias ont identifié des clients potentiels de NSO dans les 11 pays suivants : Arabie saoudite, Azerbaïdjan, Bahreïn, Émirats arabes unis, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda et Togo.

Les attaques ciblées contre la famille, les amis et les associés du journaliste assassiné Jamal Khashoggi montrent non seulement un mépris complet des droits des personnes ciblées, mais aussi l'impunité manifeste avec laquelle les États déploient cet outil. D'après des déclarations, quatre mois avant le meurtre de Jamal Khashoggi, le téléphone de son épouse, Hanan Elatr, avait été ciblé par le logiciel espion Pegasus[13]. Quelques jours seulement après son assassinat, le téléphone de la fiancée du journaliste, Hatice Cengiz, a été infecté par Pegasus à plusieurs reprises. Le téléphone d'un autre associé de Jamal Khashoggi, l'ancien journaliste d'Al Jazeera, Wadah Khanfar, a été également infecté par Pegasus[14].

Ce cas est emblématique des nombreux préjudices causés par l'utilisation de l'outil de NSO Group. Il permet d'espionner non seulement des cibles illégitimes, comme des journalistes, mais il peut également facilement toucher leurs associés, leurs familles ou leurs réseaux, ce qui a un effet dévastateur dans le monde réel s'étendant bien au-delà de l'atteinte à la vie privée de la cible. Comme le souligne le Washington Post dans son enquête sur ces attaques, « [l]'irruption dans la vie des deux femmes qui partageaient la vie de Jamal Khashoggi montre les répercussions que même la peur de l'espionnage peut avoir. Toutes deux étaient épanouies et indépendantes avant d'entretenir une relation amoureuse avec lui. Désormais, elles vivent cachées et ont été abandonnées par des amis qui craignent pour leur propre sécurité parce qu'ils savent que les autorités sont capables faire le lien entre eux en inspectant leurs téléphones, comptes sur les réseaux sociaux, messages et autres communications[15]. »

Bien qu'il soit impossible de connaître avec certitude l'ampleur réelle du ciblage permis par cet outil, il ressort clairement qu'à ce jour son utilisation parallèle cachée, à savoir une surveillance non conforme aux droits humains et dangereuse pour les personnes, a une part bien plus importante que ce que le discours sur la lutte contre le crime et le terrorisme de l'entreprise laisse entendre. Ce groupe de victimes, de personnes ciblées et de personnes susceptibles d'intéresser les clients de NSO Group pourrait en fait représenter un pourcentage non négligeable du nombre total de licences délivrées à l'entreprise par le ministère israélien de la Défense (seul un audit indépendant des licences concernant le logiciel espion Pegasus délivrées à NSO Group permettrait de vérifier les chiffres avec certitude). De plus, comme le

[12] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 7.

[13] Comme Hanan Elatr utilisait un téléphone Android, les experts en technologie d'Amnesty International n'ont pas été en mesure de confirmer si son ciblage avait réussi.

[14] Dana Priest, Souad Mekhennet et Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post*, 18 juillet 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[15] Dana Priest, Souad Mekhennet et Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post*, 18 juillet 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

démontrent les cas révélés et nos explications détaillées ci-après, l'entreprise avait connaissance ou aurait dû avoir connaissance d'une telle utilisation finale de nature invasive et inappropriée[16].

Ces cas illustrent également le lien troublant qui existe entre la surveillance numérique ciblée, les atteintes au respect de la vie privée et d'autres violations des droits humains. En termes de capacités opérationnelles, cet outil de surveillance n'a aucune limite : toute donnée qui passe par un appareil infecté est accessible, alors que le logiciel efface ses traces, car il est conçu pour éviter de laisser ou pour détruire toute preuve de son utilisation. Au regard des personnes ciblées, de l'historique et du contexte, on peut conclure que les données personnelles les plus sensibles, comme la localisation physique, les contenus vidéo enregistrés à l'insu des personnes, les contacts, les photos, les conversations privées et les informations médicales personnelles, ont été recueillies et exploitées en vue de leur causer du tort, sans notification ultérieure ou possibilité de contester la surveillance. Un tel ciblage peut avoir des effets désastreux, en particulier en ce qui concerne l'interception de données personnelles privées et leur exploitation en vue d'exercer un chantage émotionnel.

En outre, l'ampleur du ciblage en lui-même pourrait en réalité ne révéler qu'une partie des diverses atteintes aux droits humains qu'il induit. Plusieurs raisons appuient cette affirmation. Tout d'abord, comme l'illustrent clairement les cas évoqués, la surveillance illégale peut toucher d'autres personnes au-delà des cibles-mêmes, notamment parmi le cercle de leur famille, de leurs amis ou de leurs collègues et autres. Le journaliste hongrois András Szabó y a pensé lorsqu'il a été informé de l'infection de son téléphone par le logiciel Pegasus : « J'ai commencé à réfléchir à ce que ces hackers avaient pu découvrir sur moi grâce aux données de mon téléphone. Étaient-ils à la recherche de mes sources ? L'une d'elles a-t-elle eu des ennuis par la suite[17] ? » Le Organized Crime and Corruption Reporting Project fait état d'une réaction similaire de la part de la journaliste d'investigation azerbaïdjanaise Khadija Ismayilova lorsqu'elle a appris avoir été ciblée :

> **« Immédiatement, elle s'est préoccupée de savoir si elle avait compromis quelqu'un d'autre. Elle y a pensé toute la nuit. Elle essayait de se souvenir ce qu'elle avait envoyé et à qui.**
>
> **"C'est bouleversant, a-t-elle déclaré le lendemain. Tout le monde devient une cible."**
>
> **Alors qu'elle fait défiler la liste de plus de 1 000 numéros azerbaïdjanais ayant fuité, elle reconnaît des numéros les uns après les autres. Une nièce. Un ami. Son chauffeur de taxi.**
>
> **"Lui aussi, se lamente-t-elle encore et encore. Elle aussi[18]. " »**

Ensuite, il est également vrai que les atteintes au droit au respect de la vie privée entraînent des répercussions sur de nombreux autres droits humains. Par exemple, la Haute-Commissaire des Nations unies aux droits de l'homme a noté que « [l]a surveillance utilisant les moyens technologiques met sérieusement en péril l'exercice des droits de l'homme dans le contexte des rassemblements pacifiques, et contribue pour beaucoup au rétrécissement de l'espace civique dans beaucoup de pays[19]. » Il en est de même pour le droit à la liberté d'expression et d'association et d'autres droits humains, et la surveillance pourrait avoir des effets négatifs imprévus sur certains groupes, en particulier sur ceux qui sont victimes de discrimination au motif de leur identité ou de leurs identités.

---

[16]Un groupe d'experts de la Commission internationale de juristes (ICJ) a étudié de manière approfondie la question de la complicité des entreprises dans les violations des droits humains et a clarifié la responsabilité juridique – civile et pénale – pouvant découler d'une telle complicité. Le groupe d'experts a estimé que le lien pourrait s'établir relativement facilement en droit si la conduite de l'entreprise avait permis, aggravé et facilité des atteintes et si celle-ci savait, ou aurait raisonnablement dû savoir, qu'il y aurait des atteintes. Une entreprise pourrait permettre, aggraver ou faciliter des atteintes, entre autres, par la fourniture de biens et de services. International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 janvier 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[17] Organized Crime and Corruption Reporting Project (OCCRP), *András Szabó: Hungarian Journalist*, 18 juillet 2021, occrp.org/en/the-pegasus-project/andras-szabo-hungarian-journalist.

[18] Miranda Patrucic et Kelly Bloss, "Life in Azerbaijan's Digital Autocracy, 'They Want to be in Control of Everything'", *OCCRP*,18 juillet 2021, occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything.

[19] Rapport de la Haute-Commissaire des Nations Unies aux droits de l'homme : *Incidence des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris des manifestations pacifiques*, 24 juin 2020, doc. ONU A/HRC/44/24, §24.

De plus, quand la surveillance est exercée sans faire l'objet d'une supervision, de protections et d'une transparence suffisantes, les répercussions de la surveillance illégale s'étendent bien au-delà des personnes directement visées. Il est bien connu que « [l]a possibilité qu'une information relative à des communications soit interceptée constitue même à elle seule une immixtion dans la vie privée et peut être attentatoire à des droits, y compris ceux relatifs à la liberté d'expression et d'association[20]. » Face à l'opacité et au manque de protections, en particulier dans des situations où il est notoire qu'une surveillance est exercée de manière illégale ou qu'il existe des soupçons de celle-ci, les défenseurs des droits humains sont contraints de s'autocensurer par crainte d'être criminalisés pour leur travail, même dans le cas où une telle surveillance n'existe en fait peut-être pas. De nombreux rapports de recherche d'Amnesty International démontrent l'effet délétère considérable de cette peur sur la société civile d'une manière générale. Comme un défenseur des droits humains bélarussien s'exprimant au sujet de l'influence de la surveillance secrète sur le travail des défenseurs l'a souligné : « [i]l suffit que les gens pensent que ça existe[21]. »

En permettant une utilisation du logiciel de NSO Group exempte de tout contrôle et en négligeant de prendre les mesures nécessaires pour protéger nos droits, les États ont laissé se développer cette situation scandaleuse aux répercussions tellement vastes sur les droits d'un nombre incalculable de personnes à travers le monde que nous ne serons jamais en mesure d'en répertorier l'ensemble.

2.2 GRAVE INTRUSION ET PROTECTIONS MINIMES

Les révélations du Projet Pegasus brossent le portrait d'une entreprise et de méthodes de surveillance numérique ciblée qui sont passées entre les (certes grandes) mailles du filet des cadres juridiques et règlementaires existants aux niveaux national, régional et international. Le logiciel Pegasus est conçu pour empiéter sur le droit à la vie privée. Et pourtant, les États et l'entreprise mettent en place très peu de protections en vue de rendre les immixtions que les révélations ont dénoncées proportionnées et donc légales. Le logiciel de surveillance numérique ciblée de NSO Group est conçu et utilisé de telle façon que les violations dont nous avons été témoins sont malheureusement prévisibles.

Il est important de souligner qu'il n'est en aucun cas possible d'utiliser les outils de surveillance numérique ciblée tels que Pegasus sans qu'il y ait d'effets sur le droit à la vie privée reconnu par le droit international et, par extension, souvent sur de nombreux autres droits[22]. L'utilisation du logiciel espion Pegasus a par essence des conséquences sur le droit à la vie privée : l'outil est furtif, fonctionne sans l'autorisation du détenteur de droit et a la capacité de collecter et de transmettre toutes les données personnelles et privées sans restriction (ainsi que des données concernant tout contact avec qui la cible de la surveillance interagit).

Il existe des mesures techniques qui pourraient permettre de procéder à des vérifications quant à cet outil invasif, mais aucun élément n'indique que NSO Group y ait recours. Dans son rapport sur la transparence et la responsabilité, par exemple, l'entreprise déclare :

> **« Les préoccupations [relatives aux droits humains] sont renforcées car il ne nous est pas possible de contrôler l'utilisation en temps réel et nous n'avons pas encore déterminé s'il serait possible techniquement d'empêcher le ciblage de populations vulnérables par nos clients. Pour compenser, nous imposons des conditions contractuelles rigoureuses visant à établir des modalités conformes aux normes internationales et un meilleur processus d'évaluation pour écarter les clients quand l'état de**

[20] Rapport du Haut-Commissariat des Nations unies aux droits de l'homme : *Le droit à la vie privée à l'ère du numérique*, 30 juin 2014, doc. ONU A/HRC/27/37, § 20.

[21] Amnesty International, *« Il suffit que les gens pensent que ça existe » : société civile, culture du secret et surveillance au Bélarus*, (Index : EUR 49/4306/2016), 7 juillet 2016, https://www.amnesty.org/fr/documents/eur49/4306/2016/fr/

[22] Cour de justice de l'Union européenne, affaire n° C-311/18 (« Schrems II »), 16 juillet 2020, § 171 : « La Cour a déjà jugé que la communication de données à caractère personnel à un tiers, tel qu'une autorité publique, constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. » Voir aussi Cour européenne des droits de l'homme, *Szabo* § 53, *Zakharov § 179, Klass* § 41.

droit est affaibli, que le droit local ne concorde pas avec les normes internationales ou lorsque les clients ne peuvent ou ne veulent pas fournir des garanties suffisantes[23]. »

En comptant sur des engagements contractuels de la part d'États entretenant sciemment un bilan désastreux en termes de respect de leurs autres obligations légales, y compris en vertu du droit international relatif aux droits humains, NSO Group exerce un contrôle manifestement insuffisant sur l'utilisation abusive pouvant être faite de ses produits.

De plus, au lieu d'enquêter de manière proactive sur les allégations de violations, NSO Group affirme attendre d'être avertie pour diligenter des enquêtes. L'entreprise a certes déclaré avoir mis fin ou renoncé à plusieurs contrats ces dernières années, mais compte tenu des difficultés rencontrées lorsqu'il s'agit d'identifier des cas d'utilisation abusive d'un outil aussi opaque ainsi que du manque de voies de recours et de protections pour les victimes, cette garantie s'avère peu efficace et contraire aux meilleures pratiques.

En outre, comme indiqué plus haut, une violation du droit à la vie privée peut produire des effets en cascade sur d'autres droits. La question est donc de savoir si la fonction particulière de cet outil constitue une **atteinte admissible au droit à la vie privée**[24]. Comme il sera démontré ci-après, il est évident, au vu des révélations, que tel n'est pas le cas.

En vertu du droit international relatif aux droits humains, tout déploiement de cet outil doit remplir les critères caractérisant les restrictions autorisées d'un droit garanti : il doit être conforme aux principes de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi. Autrement dit, la simple affirmation d'un intérêt potentiellement légitime n'est pas suffisante pour justifier des restrictions du droit à la vie privée, sauf si les autres critères édictés par le droit international relatif aux droits humains sont remplis. Ce fait juridique communément admis transparait, entre autres, dans la Stratégie antiterroriste mondiale de l'Organisation des Nations Unies, qui reconnaît les « [m]esures garantissant le respect des droits de l'homme et la primauté du droit en tant que base fondamentale de la lutte antiterroriste » comme un de ses quatre piliers. Elle réaffirme « que les États doivent veiller à ce que toutes les mesures prises pour lutter contre le terrorisme soient conformes aux obligations qu'ils assument en vertu du droit international, en particulier du droit international des droits de l'homme, du droit international des réfugiés et du droit international humanitaire[25]. » En outre, l'examen le plus récent de la Stratégie « [d]emande aux États de revoir, alors même qu'ils luttent contre le terrorisme et s'efforcent de prévenir l'extrémisme violent conduisant au terrorisme, leurs procédures, leurs pratiques et leur législation en matière de surveillance et d'interception des communications et de collecte de données personnelles, notamment à grande échelle, de façon à défendre le droit à la vie privée prévu à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques, en veillant à s'acquitter effectivement de l'intégralité de leurs obligations au regard du droit international des droits de l'homme[26]. »

Cependant, en pratique, il n'existe pas de cadre global garantissant le respect de ces exigences dans le contexte des opérations de surveillance numérique ciblée[27]. En effet, de nombreux États ont cherché à

---

[23] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 18-19.

[24] « Les limitations ne sont justifiées que si elles visent à protéger des intérêts précis » (voir Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Recours au chiffrement et à l'anonymat dans le domaine des échanges numériques*, 22 mai 2015, doc. ONU A/HRC/29/32, § 33).

« Il faut que la limitation soit nécessaire pour atteindre cet objectif légitime, qu'elle soit proportionnée à cet objectif et qu'elle constitue l'option la moins intrusive possible. En outre, aucune limitation du droit à la vie privée ne peut vider de son sens le principe de ce droit » (voir Note du Secrétaire général des Nations unies, *promotion et protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, 23 septembre 2014, doc. ONU A/69/397, § 51) ; rapport du haut-commissaire des Nations Unies aux droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, doc ONU A/HRC/39/29, 3 août 2018, § 10.

[25]Assemblée générale des Nations unies (AGNU), Résolution 16/288 : La Stratégie antiterroriste mondiale de l'Organisation des Nations Unies, 8 septembre 2006, doc. ONU A/RES/60/288.

[26] Assemblée générale des Nations unies (AGNU), Résolution 72/284 : Examen de la Stratégie antiterroriste mondiale des Nations Unies, 26 juin 2018, doc. ONU A/RES/72/284, § 20.

[27] Comme le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression l'a souligné : « Dire que le mécanisme global de contrôle de l'utilisation des technologies de surveillance ciblée ne fonctionne pas est un euphémisme. En réalité, ce mécanisme est pratiquement inexistant. Bien que le droit des droits de l'homme restreigne expressément l'utilisation des outils de surveillance, certains États exercent une surveillance illicite sans avoir à craindre de conséquences juridiques. En effet, il existe un cadre

conserver une grande marge de manœuvre sur leur territoire et à l'étranger et à maintenir le secret autour des outils de surveillance numérique ciblée à leur disposition. Les États se sont reposés sur la réglementation en matière d'exportation comme moyen principal de contrôle du déploiement de cet outil. Cependant, comme on pouvait s'y attendre, cette approche n'a pas eu pour effet de freiner les violations des droits humains. Les décisions concernant la délivrance des licences d'exportation sont à la discrétion de l'État et elles ne reposent pas sur des critères disqualifiants objectifs (à l'exception des régimes de sanctions qui s'appliquent à une poignée de pays), ce qui laisse la porte ouverte à une approbation de l'État en fonction de priorités concurrentes et laisse à ce dernier une grande flexibilité en la matière[28]. Certains États, ainsi que l'Union européenne, ont essayé d'imposer des critères relatifs aux droits humains en ce qui concerne les exportations de technologies de surveillance. Cependant, cette initiative s'est également avérée insuffisante pour garantir un véritable contrôle. Par exemple, malgré des appels de la société civile, l'Union européenne a adopté son règlement final sur les exportations de biens à double usage[29], qui se contente d'imposer aux États de « prendre en considération » les critères relatifs aux droits humains dans leur évaluation concernant la délivrance des licences d'exportation, mais les laisse malgré tout libres de les accorder. De tels vides juridiques permettent aux États de faire fi des risques relatifs aux droits humains liés à l'exportation de ces outils. Même si, en théorie, d'autres réglementations de l'Union européenne imposent la prise en compte des droits humains dans le cadre des exportations, ce n'est pas le cas en pratique, comme en témoignent les nombreux exemples de recours à des technologies provenant de l'Union européenne en vue de réprimer les droits[30].

De plus, en intégrant le recours à un logiciel comme Pegasus, qualifié d'outil d'« interception légale », dans leurs activités de renseignement au sens large qui échappent traditionnellement à l'obligation de rendre des comptes, les États ont brouillé les limites de l'usage autorisé de l'outil, aux dépens des principes de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi. L'entreprise NSO Group a elle-même reconnu que son outil pourrait avoir des fins illicites et contribuer à des effets néfastes sur les droits humains[31]. Cependant, même face à une longue liste d'exemples d'atteintes documentées, l'entreprise a déclaré qu'elle pourrait continuer d'équiper ses clients sans vraiment vérifier l'utilisation finale, en raison d'intérêts liés à la sécurité nationale censés primer[32].

L'entreprise s'est contentée d'invoquer la sécurité nationale, sans mentionner le respect des principes obligatoires de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi[33], pour justifier la poursuite de la distribution et l'utilisation de l'outil. Il est à noter que si l'entreprise évoque

juridique visant à protéger les droits de l'homme, mais pas de cadre permettant de garantir le respect des restrictions imposées. » Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Surveillance et droits de l'homme*, doc. ONU A/HRC/41/35, 28 mai 2019, § 46.

[28] Access Now et autres organisations, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules*, mars 2021, hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf.

[29] Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte), https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=FR.

[30] Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*, (Index: EUR 01/2556/2020), 21 septembre 2020, amnesty.org/fr/documents/EUR01/2556/2020/en.

[31] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 9 ; 17-19.

[32] Voir par exemple NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 9-10 (« Nos clients sont exclusivement des services de renseignement autorisés et des organismes d'application des lois chargés d'enquêter et, le cas échéant, de prévenir des crimes graves et des actes terroristes. Afin de mener ces opérations efficacement, ces agences doivent agir discrètement pour (i) infiltrer les réseaux criminels et terroristes en vue d'obtenir des informations essentielles pour empêcher les actes illégaux, et (ii) éviter de donner par inadvertance une chance aux criminels et terroristes de contrarier ces activités préventives. C'est pourquoi nos clients exigent une confidentialité stricte de notre part comme de tous les autres fournisseurs de services de notre secteur. Notre capacité d'action est également limitée par le fait que nous n'avons pas de visibilité sur les utilisations précises faites de nos produits, à moins que le client ne nous accorde un accès à ces informations (tel que prescrit dans les contrats en cas d'enquête liée à des soupçons d'utilisation illégale des produits). Néanmoins, ce rapport fournit un aperçu de la manière dont nous effectuons notre mission et contribuons à un équilibre entre le devoir incombant aux États de protéger leur population de menaces physiques et criminelles et leurs obligations vis-à-vis de la liberté d'expression, le droit à la vie privée et d'autres droits humains. »)

[33] Ni l'entreprise ni les autorités en charge des exportations du pays n'ont expliqué comment elles vérifiaient si ces obligations étaient respectées par l'utilisateur final dans le cadre des procédures de diligence raisonnable et d'atténuation des risques de l'entreprise ou des décisions concernant l'octroi de licences d'exportation.

régulièrement les exigences liées à la lutte contre le terrorisme dans son discours, elle n'a cependant jamais expliqué de quelle manière son logiciel, dans sa conception et son utilisation, se conformait à l'ensemble considérable de textes législatifs, de politiques et de travaux développés ces dernières années en matière de promotion et de protection des droits humains dans le cadre de la lutte anti-terroriste (par exemple, la Stratégie antiterroriste mondiale des Nations unies[34] et le travail approfondi du Rapporteur spécial des Nations unies sur les droits de l'homme et la lutte contre le terrorisme, y compris sur des sujets tels que les meilleures pratiques pour les services de renseignement[35]). En lieu et place, dans son rapport sur la transparence et la responsabilité publié en juin 2021, NSO Group identifiait de manière incongrue une « absence de bonnes pratiques et de conseils à la fois pour les États et pour notre secteur afin de trouver un équilibre approprié entre les droits humains et les libertés individuelles d'une part et les exigences liées à la lutte contre les crimes graves et le terrorisme d'autre part[36] ». De la sorte, l'entreprise balayait sommairement des décennies d'initiatives sur la question et les normes du droit en matière de droits humains. L'affirmation de NSO Group est fausse. En effet, le Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression s'est adressé au secteur de la surveillance en général et a écrit à NSO Group en particulier afin de les inciter à adopter des normes conformes au droit international relatif aux droits humains dans leur travail, y compris, entre autres, en ayant recours à des limitations techniques dans le but de réduire la possibilité d'effets négatifs sur les droits humains[37].

NSO Group, l'État d'Israël (en tant qu'État dans lequel NSO Group est domicilié) et les États identifiés dans les cas exposés qui ont eu recours à cet outil pour atteindre un large éventail de cibles, font primer la restriction sur le droit lorsqu'ils distribuent et/ou utilisent cet outil de surveillance numérique ciblée. Cependant, comme l'a souligné le Haut-Commissaire des Nations unies aux droits de l'homme, « les restrictions ne doivent pas porter atteinte à l'essence même du droit[38] ». Dans le sillage de cette inversion, la surveillance numérique ciblée est devenue une pratique courante et un secteur d'activité échappant dans les faits à toute obligation de rendre des comptes fondée sur les régimes juridiques et la réglementation existants.

Par exemple, les outils de surveillance numérique ciblée fournis par NSO Group sont de nos jours construits autour de failles dans les applications et plateformes numériques utilisées par les consommateurs. Les États ont incité activement les acteurs du secteur privé à chercher des failles dans les appareils et applications numériques populaires et à trouver des moyens de les exploiter à des fins malveillantes, au lieu de les encourager à une divulgation responsable. En conséquence, les capacités de surveillance sont renforcées, les autres fournisseurs de technologie sont discrédités et la sécurité de l'environnement numérique est compromise pour les utilisateurs du monde entier. Alors que les entreprises de surveillance tirent des bénéfices de cette activité, les fournisseurs tiers touchés (dont un grand nombre sont des sociétés cotées en bourse) doivent consacrer des ressources considérables à la résolution des failles découvertes afin de

---

[34] La Stratégie antiterroriste mondiale des Nations unies compte parmi ses quatre piliers les « [m]esures garantissant le respect des droits de l'homme et la primauté du droit en tant que base fondamentale de la lutte antiterroriste ». Elle réaffirme « que les États doivent veiller à ce que toutes les mesures prises pour lutter contre le terrorisme soient conformes aux obligations qu'ils assument en vertu du droit international, en particulier du droit international des droits de l'homme, du droit international des réfugiés et du droit international humanitaire. » Assemblée générale des Nations unies (AGNU), Résolution 16/288 : La Stratégie antiterroriste mondiale de l'Organisation des Nations Unies, 8 septembre 2006, doc. ONU A/RES/60/288.

[35] Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte antiterroriste, Martin Scheinin, *Compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste*, 17 mai 2010, doc. ONU A/HRC/14/46.

[36] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 30. De plus, la notion de « trouver un équilibre » entre les droits humains et la sécurité est en soi inopportune. Comme le Rapporteur spécial des Nations unies sur les droits de l'homme et la lutte contre le terrorisme l'a expliqué, « une action efficace contre le terrorisme et la protection des droits de l'homme sont des objectifs non pas contradictoires mais complémentaires et synergiques. Cette position reflète également la souplesse du droit des droits de l'homme. Grâce à l'application rigoureuse de ce droit, il est possible de faire face efficacement aux problèmes que pose la lutte antiterroriste tout en respectant les droits de l'homme. Il n'est pas nécessaire dans ce processus de rechercher un équilibre entre les droits de l'homme et la sécurité, car le bon équilibre peut et doit être trouvé au sein même du droit des droits de l'homme – le droit étant la balance, et non le poids à évaluer. » Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Martin Scheinin, *Dix pratiques optimales en matière de lutte antiterroriste*, 22 décembre 2010, doc. ONU A/HRC/16/51, § 12.

[37] Lettre du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, à Shalev Hulio, NSO Group, 18 octobre 2019, spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24905.

[38] Comité des Nations unies des droits de l'homme, Observations générales adoptées par le Comité des droits de l'homme au titre du paragraphe 4 de l'article 40 du Pacte international relatif aux droits civils et politiques, observation générale n°27, article 12 (liberté de circulation), 1er novembre 1999, doc. ONU CCPR/C/21/Rev.1/Add.9, § 13.

garantir à leurs clients que leur sécurité est assurée et ainsi de les conserver. Pegasus est capable de contourner les dispositifs de sécurité des nouveaux modèles de l'iPhone d'Apple, ce qui pourrait menacer la sécurité de tous les utilisateurs d'iPhone. De plus, en proposant l'installation un programme malveillant par le biais d'attaques « zéro clic » (introduction d'un programme malveillant ne nécessitant pas d'interaction avec l'utilisateur ciblé), NSO Group a créé un outil aux répercussions dévastatrices sur la vie privée, qui dans le même temps ne demande que très peu d'efforts de la part des gouvernements qui cherchent à cibler un grand nombre de personnes au moyen de la surveillance illégale[39].

Quand on lui demande ce que l'on peut faire pour se protéger de Pegasus, le lanceur d'alerte Edward Snowden répond : « [q]u'est-ce que les gens peuvent faire pour se protéger des armes nucléaires[40] ? » De fait, il n'existe aucune démarche permettant aux utilisateurs de se protéger contre les attaques « zéro clic » de Pegasus. La seule véritable protection réside dans une protection collective assurée par des lois et des réglementations robustes, mais, comme cette enquête l'a bien montré, la législation en l'état se révèle insuffisante. Les États eux-mêmes en ont pâti, en étant touchés par la démonstration saisissante de l'impact extraterritorial et du potentiel d'immixtion dans les droits de l'outil, même dans d'autres pays. D'après l'enquête du Washington Post, des centaines de personnalités politiques, y compris 14 chefs d'État, ont été des cibles potentielles de cette contamination[41]. Depuis plusieurs années, la question de l'adoption de normes visant à réguler le cyberespace et celle de l'application du droit international en ce qui concerne les cyberopérations menées par les États font l'objet d'un débat au niveau international[42]. Cependant, les normes relatives à l'espionnage numérique en temps de paix ne sont pas encore complètement figées. D'après ces révélations, il apparait clairement que des États ciblent des personnes en raison de l'exercice de leurs droits fondamentaux reconnus en droit international, et empiètent sur la capacité d'autres États de conduire leurs propres affaires et de remplir leurs obligations en matière de droits humains[43].

2.3 LES FAUTES DES ÉTATS ET LA COMPLICITÉ DES ENTREPRISES

Ces révélations, qui correspondent à des recherches menées sur des années et ont dévoilé de graves répercussions sur les droits humains et un non-respect manifeste du droit international et des normes connexes, n'ont pour autant entraîné aucune conséquence ou changement dans l'activité de l'entreprise ou de ses clients. Cela nous mène dès lors à la conclusion que **les États et entreprises se livrent à la surveillance numérique ciblée en toute impunité**.

Une culture de l'impunité spécifique à la surveillance numérique ciblée s'est développée en l'absence d'un cadre légal et d'un contrôle à la hauteur de l'enjeu. Comme l'a souligné l'ancien Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « [l]a surveillance numérique n'est plus réservée aux pays dont les ressources leur permettent d'exercer une surveillance de masse et une surveillance ciblée avec des technologies qu'ils ont conçues eux-mêmes. Le secteur privé est entré dans le jeu et agit sans être soumis à aucun contrôle, et donc presque en toute impunité. » Plus loin, il déclare :

---

[39] Amnesty International, « Projet Pegasus : des iPhones infectés par le logiciel espion de NSO Group », 19 juillet 2021, https://www.amnesty.org/fr/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware-2/.

[40] David Pegg et Paul Lewis, "Edward Snowden calls for spyware trade ban amid Pegasus revelations", *The Guardian*, 19 juillet 2021, theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations.

[41] Craig Timberg, Michael Birnbaum, Drew Harwell et Dan Sabbagh, "On the list: Ten prime ministers, three presidents and a king", *The Washington Post*, 20 juillet 2021, washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware.

[42] Par exemple, les travaux du Groupe d'experts gouvernementaux des Nations unies et du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Voir Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", *Just Security*, 10 juin 2021, justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace; Bureau des affaires de désarmement, *Groupe de travail à composition non limitée*, un.org/disarmament/open-ended-working-group; Bureau des affaires de désarmement, *Les progrès de l'informatique et de la télématique et la question de la sécurité internationale*, https://www.un.org/disarmament/fr/informatique-et-telematique/.

[43] Rapporteuse spéciale sur les exécutions extrajudiciaires, sommaires ou arbitraires, Annex to the Report: *Investigation into the unlawful death of Mr. Jamal Khashoggi*, 19 juin 2019, doc. ONU A/HRC/41/CRP.1.

« [d]ire que le mécanisme global de contrôle de l'utilisation des technologies de surveillance ciblée ne fonctionne pas est un euphémisme. En réalité, ce mécanisme est pratiquement inexistant[44]. »

Cette culture de l'impunité repose sur la finalité et l'offre de la technologie elle-même : l'action est invisible (contrairement aux outils conventionnels, cette technologie est conçue pour empêcher que le ciblage puisse être détecté et prouvé) ; il existe peu de restrictions véritablement appliquées en matière de fonctionnement ; la responsabilité est très difficile à établir (la technologie est conçue pour brouiller l'identité de l'opérateur) ; de vastes capacités de surveillance sont à portée indépendamment du niveau de connaissances techniques du client. Les acteurs étatiques opèrent ainsi sans contrainte et sans redouter de réelles conséquences. Il suffit de prendre en considération l'ampleur du ciblage dévoilé par les révélations du Projet Pegasus (voir ci-dessus) pour prendre la mesure de cette impunité.

NSO Group nie avoir eu connaissance d'informations relatives aux cibles révélées par le Projet Pegasus. Toutefois, de très nombreux nouveaux cas ont été découverts dans des pays connus pour leurs programmes de surveillance illégale, et même dans des pays où des utilisations illégales du logiciel de NSO Group avaient précédemment été révélées. Ainsi, même si l'entreprise NSO Group n'avait pas connaissance de ces atteintes liées à l'utilisation de son produit en particulier, elle aurait raisonnablement dû savoir dans ces circonstances que des atteintes en résulteraient[45].

[44] *Surveillance et droits de l'homme*, Rapport du rapporteur spécial sur la promotion du droit à la liberté d'opinion et d'expression, 28 mai 2019, doc. ONU A/HRC/41/35, § 6 et 46.

[45] Comme cela est expliqué dans les orientations accompagnant les Dix principes du Pacte mondial des Nations unies, être complice, pour les entreprises, signifie « être impliqué » dans les atteintes aux droits humains. La complicité est constituée « généralement » de deux éléments : une action effectuée par une entreprise ou son représentant qui « aide » un tiers « d'une certaine manière, à commettre une atteinte aux droits humains » et la « connaissance par l'entreprise du fait que son action ou son omission pourrait fournir une telle assistance ». Cette formulation implique donc seulement que l'action de l'entreprise facilite les atteintes aux droits humains mais n'indique pas nécessairement que l'aide apportée soit conséquente ou la véritable cause de la violation. Selon cette formulation, la complicité réside également dans la connaissance du fait que cette aide *pourrait* faciliter les atteintes aux droits humains. Il n'est pas nécessaire que l'entreprise sache que cela facilitera réellement ces atteintes. United Nations Global Compact, "Principle Two: Human Rights", *The Ten Principles of the UN Global Compact*, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

Les entreprises ne peuvent pas échapper à la complicité par l'aveuglement volontaire. On peut déduire le niveau de connaissance de l'entreprise à partir des éléments qui étaient généralement connus et par conséquent de ce que toute entreprise raisonnable devrait savoir et sait probablement. La démarche est comparable à celle qui est suivie pour établir la négligence de la part d'une entreprise : on se demande si « une personne raisonnable, à la place de l'entreprise, avec les informations raisonnablement disponibles sur le moment, aurait su qu'il existait un risque que son action porte atteinte à une personne. Cela signifie qu'[on] regardera à la fois ce que l'entreprise elle-même savait et ce qu'une entreprise raisonnable aurait su à sa place sur le risque de voir survenir cette atteinte. » Les informations disponibles dans le domaine public et les informations portées à l'attention de l'entreprise sont pertinentes pour établir la connaissance de l'entreprise. L'entreprise n'a pas besoin de connaitre « l'étendue réelle des violations flagrantes des droits humains auxquelles elle contribue, à condition que certaines violations soient connues. » International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1er janvier 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes, 20-22.

LA COMPLICITÉ DES ENTREPRISES AUX TERMES DU DROIT INTERNATIONAL ET DES NORMES S'Y RAPPORTANT

La complicité, dans son acception légale, prend plusieurs formes, dont celle de la responsabilité pénale ou civile individuelle telles que définies en droit national, et elle est également une notion couverte par le droit pénal international notamment en ce qui concerne le rôle des entreprises dans les crimes internationaux.

Dans le cadre de ce rapport, le terme « complicité » doit être compris selon les évolutions des normes du droit international et des normes applicables aux entreprises privées ou « personnes morales » qui est le terme consacré dans les systèmes de droit de certains pays.

Le principe, qui a évolué, transparait dans plusieurs normes internationales majeures et est applicable de différentes façons aux crimes internationaux et à d'autres atteintes aux droits humains. Les commentaires accompagnant les principes du Pacte mondial des Nations unies précisent clairement que la complicité dans ce contexte comprend deux éléments principaux :

- « Une action ou omission (manquement à l'action) par une entreprise, ou une personne représentant une entreprise, qui « aide » (facilite, légitime, assiste, encourage, etc.) un tiers, d'une certaine manière, à commettre une atteinte aux droits humains ; et
- la connaissance par l'entreprise que son action ou omission pourrait fournir cette assistance[46]. »

Pour dissiper tout doute, il est précisé : « Si une entreprise tire un avantage de violations commises par les autorités, ou les incite, les encourage ou les soutient dans la perpétration de violations des droits humains, la complicité de l'entreprise est manifeste[47]. »

Il appartient aux États, qui sont tenus d'offrir des voies de recours aux victimes des violations révélées par le Projet Pegasus, de répondre à la question de savoir si la complicité manifeste de NSO Group dans les violations des droits humains perpétrées par des États constitue un fondement pour engager sa responsabilité civile ou pénale au regard du droit national, régional ou international.

Le Projet Pegasus a révélé de nouvelles preuves de contaminations par le logiciel espion Pegasus ciblant des personnes marocaines, alors même qu'en 2020, l'utilisation du logiciel de NSO Group contre le journaliste marocain Omar Radi avait été établie[48]. De même, alors que NSO Group nie toute implication dans le meurtre de Jamal Khashoggi, des tentatives d'infection du téléphone de son épouse avant son meurtre et du téléphone de sa fiancée, même après son assassinat, ont été attestées par l'enquête[49]. D'après certaines informations, en 2019, au moins six dissidents ayant des liens avec le Rwanda ont été avertis par WhatsApp qu'ils avaient été ciblés par le logiciel espion Pegasus. D'après de nouvelles révélations, des Rwandais continuent d'être visés aujourd'hui, et notamment la fille du militant emprisonné Paul Rusesabagina, Carine Kalimba[50].

Ailleurs, même s'il n'existe pas de preuves d'atteintes précédentes pouvant être reliées à NSO Group, comme en Azerbaïdjan, la gravité des violations liées à la surveillance commises dans le passé aurait dû alerter l'entreprise quant aux risques vis-à-vis des droits humains. Par exemple, Amnesty International avait

[46] United Nations Global Compact, "Principle Two: Human Rights", *The Ten Principles of the UN Global Compact*, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

[47] Andrew Clapham, "On Complicity" in M. Henzelin and R. Roth (editors), *Le droit pénal à l'épreuve de l'internationalisation*, 2002, ssrn.com/abstract=1392988, p. 241-275.

[48] Amnesty International, « Un journaliste marocain victime d'attaques par injection réseau au moyen d'outils conçus par NSO Group », 22 juin 2020, https://www.amnesty.org/fr/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/.

[49] Dana Priest, Souad Mekhennet et Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post,* 18 juin 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[50] Stephanie Kirchgaessner, "Hotel Rwanda activist's daughter placed under Pegasus surveillance", *The Guardian*, 19 juillet 2021, theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance.

déjà fait état de cas de surveillance de défenseurs des droits humains azerbaïdjanais dans le pays ou à l'étranger[51]. De nombreux cas de chantage visant réduire au silence des femmes défenseures des droits humains par l'utilisation d'images personnelles ou intimes ont été recensés[52], ce qui aurait dû être un avertissement suffisant pour NSO Group sur les risques liés à cette vente. Et pourtant, cet avertissement a été ignoré. Le cas de NSO Group prouve que même les entreprises qui ont connaissance ou auraient dû avoir connaissance de violations continuent de fournir leur technologie de surveillance et ne font face qu'à peu de conséquences, encore une fois.

NSO Group affirme ne pas disposer d'informations relatives aux cibles sélectionnées par les clients. Ce n'est pas une réponse acceptable. L'absence manifeste de prise en considération de risques facilement identifiables liés à la vente d'outils de surveillance à ses clients démontre un manquement criant de la part de l'entreprise en matière de diligence raisonnable. Une entreprise ne peut se soustraire à ses responsabilités par un tel « aveuglement volontaire » face aux risques induits par ses ventes et la nature de ses produits alors que toute personne raisonnable le comprendrait[53].

Selon certaines informations, les autorités israéliennes ont diligenté une enquête au sujet des révélations du Projet Pegasus[54]. Amnesty International appelle les autorités israéliennes à révoquer immédiatement toutes les licences d'exportation accordées à NSO Group, à veiller à ce que l'enquête soit indépendante, impartiale, transparente et à même de déterminer l'ampleur du ciblage illégal et enfin à communiquer publiquement les résultats des efforts entrepris et les mesures identifiées pour prévenir de nouveaux préjudices.

Les États ont fait le choix de préserver la souplesse qui leur permet de mener des attaques numériques offensives et de s'appuyer sur le secteur privé pour augmenter leur capacité de surveillance, au détriment des personnes ciblées par cette surveillance intrusive, de l'environnement numérique dans son ensemble et même des intérêts de sécurité nationale sur le long-terme. Parallèlement, les entreprises de surveillance comme NSO Group semblent résolues à adopter un rôle complice en vue d'accroitre leurs profits. Leurs ventes et leurs produits ont rendu possibles des violations à grande échelle, alors même que les éléments attestant de ce risque étaient facilement consultables, que ces entreprises aient choisi d'en tenir compte ou non. Les normes internationales relatives aux droits humains servent à empêcher l'externalisation des responsabilités en matière de droits humains dans des situations où les liens entre l'État et le monde de l'entreprise se brouillent. En effet, même face à ces révélations choquantes, des questionnements demeurent : les États se tiendront-ils responsables les uns les autres ? L'entreprise NSO Group finira-t-elle par avoir à rendre des comptes ?

[51] Amnesty International, « Des militants visés par une cyberattaque attribuée au gouvernement », 10 mars 2017, https://www.amnesty.org/fr/latest/press-release/2017/03/azerbaijan-activists-targeted-by-government-sponsored-cyber-attack/.

[52]Amnesty International, « Azerbaïdjan. Il faut mettre un terme à la violente campagne de diffamation et de représailles fondées sur le genre ciblant des militantes », 12 mai 2021, https://www.amnesty.org/fr/latest/press-release/2021/05/azerbaijan-stop-the-vicious-campaign-of-gendered-smears-and-reprisals-against-women-activists/

[53] International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1er janvier 2008, § 2.2.4, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[54] Dan Williams, "Israel appoints task force to assess NSO spyware allegations – sources", *Reuters*, 21 juillet 2021, reuters.com/technology/israels-national-security-council-looking-into-nso-spyware-allegations-2021-07-21.

3. CONCLUSIONS ET RECOMMANDATIONS

Les nouvelles révélations au sujet de NSO Group démontrent le besoin urgent d'une réglementation et d'un changement radical en ce qui concerne les pratiques de surveillance numérique ciblée des États et la contribution du secteur privé à ces pratiques. Ces réformes indispensables comprennent :

UN CONTRÔLE INDÉPENDANT À LA FOIS DU MARCHÉ DE LA SURVEILLANCE ET DES PRATIQUES DE SURVEILLANCE DES ÉTATS.

Ce qui se produit quand des gouvernements qui opèrent hors de tout contrôle indépendant et de mécanismes de responsabilisation prennent possession de ces outils n'a rien d'un mystère : ils les utilisent pour renforcer leur pouvoir aux dépens des droits humains. Il s'agit d'un fait irréfutable au regard des dernières révélations. Il n'est évidemment pas surprenant de constater que les gouvernements qui utilisent le logiciel pour porter atteinte aux droits humains s'autorisent également à retourner ces mêmes outils contre d'autres États, et de la sorte portent préjudice aux droits humains également dans ces pays. Alors que NSO Group affirme que ses outils sont uniquement utilisés à des fins d'enquête sur des comportements liés au terrorisme et d'autres crimes, il est plus clair que jamais que l'entreprise n'a pas la volonté ni/ou la capacité de garantir que ce soit le cas. Et pourtant, les entreprises ont bel et bien la responsabilité indépendante de respecter les droits humains, indépendamment de la situation ou des actions du gouvernement du pays où elles opèrent ou sont domiciliées. Les Principes directeurs des Nations unies précisent que cette responsabilité « existe indépendamment des capacités ou de la volonté des États de remplir leurs propres obligations en matière de droits de l'homme, et ne restreint pas ces dernières. Elle prévaut en outre sur le respect des lois et règlements nationaux qui protègent les droits de l'homme. » Il est clair que tel n'est pas le cas et qu'il est grand temps d'instaurer des mécanismes de contrôle, des lois et des réglementations solides adaptés à la surveillance numérique ciblée.

DES VOIES DE RECOURS POUR LES PERSONNES CIBLÉES AU MÉPRIS DE LEURS DROITS FONDAMENTAUX

Nous commençons seulement à saisir l'ampleur et la gravité réelles des impacts de cette technologie sur les droits humains, comme nous l'avons découvert avec ces révélations. Il est indispensable d'offrir des voies de recours à toutes les personnes dont les droits fondamentaux reconnus par le droit international ont été bafoués par le ciblage, et notamment aux victimes dont le cas a été révélé au grand jour. Les Principes directeurs relatifs aux entreprises et aux droits de l'homme sont clairs sur la question : « [s]auf si les États prennent des mesures appropriées pour enquêter sur les atteintes aux droits de l'homme commises par les entreprises et, lorsqu'elles se produisent, en punir les auteurs et les réparer, l'obligation de protéger incombant à l'État peut être affaiblie voire même être vidée de son sens[55]. » Cependant, l'accès à des voies de recours s'est révélé excessivement difficile dans le contexte de la surveillance numérique, compte tenu du secret associé aux opérations de surveillance et des obstacles techniques et juridiques rencontrés par

[55] Haut-Commissariat des Nations unies aux droits de l'homme, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : Cadre de référence « Protéger, respecter et réparer » des Nations unies, 2011,* Principes 4 et 5.

ceux qui ont cherché à obtenir des preuves ou à former des recours en justice contre des États ou des entreprises privées de surveillance. Les États doivent apporter leur soutien aux personnes touchées qui cherchent à obtenir la justice et des réparations – à la fois de la part des États exerçant une surveillance et des entreprises qui les approvisionnent - et prendre des mesures pour prévenir de nouvelles tentatives de surveillance à l'encontre de ces personnes , y compris en prévoyant des moyens d'action dans la législation nationale et dans les règles normatives internationales relatives à la surveillance numérique ciblée[56].

UNE PLUS GRANDE TRANSPARENCE

De façon assez alarmante à l'aune de ces révélations, la tendance actuelle dans le domaine de la surveillance consiste non pas à améliorer mais à réduire la transparence. Les évolutions techniques dans le fonctionnement des logiciels espion, comme l'intégration des attaques « zéro clic » et des attaques par injection réseau rendent encore plus difficiles la détection des attaques ciblées et la visibilité en ce qui les concerne. Dans le même temps, les investissements privés dans le secteur de la surveillance, par des sociétés de capital-investissement ou d'autres fonds privés, aggravent le manque de contrôle indépendant[57].

NSO Group a certes publié son premier rapport sur la transparence et la responsabilité (*Transparency and Responsibility Report*) en juin 2021, mais celui-ci n'a servi qu'à montrer où s'arrête la tolérance du secteur de la surveillance en matière de transparence. Le rapport reprend quelques statistiques sans les contextualiser ni les interpréter et il fournit peu de détails concernant l'application pratique et les aboutissements des procédures de diligence raisonnable en matière de droits humains, des mesures d'atténuation des risques et des mécanismes de traitement des plaintes mis en place par l'entreprise. Le rapport omet d'évoquer les actions en justice antérieures et en cours contre l'entreprise ou les informations rendues publiques concernant l'utilisation abusive de ses produits. Il y est également écrit que « la sphère dans laquelle nous opérons nécessite que quelques détails-clés, en particulier l'identification directe de nos clients ou clients potentiels, restent confidentiels en raison de considérations strictes relatives à la sécurité nationale et contractuelles[58]. »

La transparence est un aspect clé de la responsabilité qui incombe aux entreprises de respecter les droits humains, comme le stipulent les Principes directeurs des Nations unies, qui énoncent que les entreprises doivent avoir « des politiques et des procédures par lesquelles elles peuvent à la fois connaître les droits de l'homme et montrer qu'elles les respectent dans la pratique. Qui dit montrer dit communiquer, en assurant un certain degré de transparence et de responsabilité aux individus ou aux groupes susceptibles d'être touchés et aux autres acteurs pertinents, y compris les investisseurs. » Le secteur n'a fait preuve d'aucune initiative significative en matière de transparence. Les États et les citoyens doivent agir dès à présent pour contrecarrer ces tendances.

En conséquence, Amnesty International formule les recommandations suivantes :

Tous les États doivent :

a. instaurer un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies d'espionnage numérique. Compte tenu de l'ampleur de ces révélations, il est urgent de mettre un terme aux activités des États et des entreprises jusqu'à ce qu'un cadre réglementaire solide et respectueux des droits humains soit mis en place ;

b. mener immédiatement une enquête indépendante, transparente et impartiale sur tous les cas de surveillance illégale révélés par le Projet Pegasus et, le cas échéant, engager des démarches judiciaires pour offrir réparation aux victimes et demander des comptes aux responsables, conformément aux normes internationales relatives aux droits humains ;

---

[56] *Surveillance et droits de l'homme*, Rapport du rapporteur spécial sur la promotion du droit à la liberté d'opinion et d'expression, 28 mai 2019, doc. ONU A/HRC/41/35.

[57] Voir Amnesty International et autres, *Operating from the Shadows: Inside NSO Group's Corporate Structure*, (Index: DOC 10/4182/2021), 31 mai 2021, amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF.

[58] NSO Group, *Transparency and Responsibility Report 2021*, 30 juin 2021, p. 4.

c. mener sans délai une enquête indépendante, transparente et impartiale sur toutes les licences d'exportation accordées pour des technologies d'espionnage numérique et résilier les autorisations de mise sur le marché et d'exportation dès lors qu'il existe un risque substantiel que ces technologies contribuent à des atteintes aux droits humains ;

d. adopter et faire appliquer un cadre juridique imposant aux entreprises privées de surveillance de faire preuve de diligence raisonnable en matière de droits humains dans leurs activités partout dans le monde, dans leurs chaînes d'approvisionnement et en ce qui concerne l'utilisation de leurs produits et services. En vertu de cette législation, les entreprises de surveillance doivent avoir l'obligation d'identifier, de prévenir et d'atténuer les risques relatifs aux droits humains découlant de leurs activités et de leurs relations commerciales ;

e. adopter et mettre en application un cadre juridique exigeant la transparence des sociétés de surveillance privées, avec notamment l'obligation de fournir des informations sur leur identification et enregistrement, sur les produits et services qu'elles proposent et sur leurs ventes ;

f. veiller à ce que toutes les entreprises domiciliées sur leur territoire aient l'obligation d'agir de manière responsable et soient tenues de rendre des comptes en ce qui concerne leurs impacts néfastes en matière de droits humains. Les États doivent imposer par la loi à ces entreprises de mener des procédures de diligence raisonnable dans le cadre de leurs opérations partout dans le monde. Cela doit comprendre la responsabilité pour les préjudices causés et l'accès des populations touchées à des voies de recours dans les États d'origine des entreprises. Les États doivent par conséquent élaborer ou soutenir les législations sur la responsabilité des entreprises proposées à l'échelle nationale ;

g. informer sur les contrats qui ont été, sont et seront passés avec des sociétés privées de surveillance, soit en répondant aux demandes d'informations, soit de leur propre initiative ;

h. en outre, les États doivent, *a minima*, mettre en œuvre les recommandations suivantes si le moratoire sur la vente et le transfert des technologies d'espionnage numérique est levé :

    a. réglementer l'exportation des technologies de surveillance, y compris :

        i. ne pas accorder d'autorisations d'exportation lorsqu'il existe un risque substantiel que la technologie en question soit utilisée pour porter atteinte aux droits humains ou lorsque le pays de destination ne dispose pas de garanties juridiques, procédurales et techniques suffisantes pour prévenir les atteintes aux droits humains. Les États devraient mettre à jour les critères de contrôle des exportations pour tenir compte du bilan de l'utilisateur final en matière de droits humains et de la légalité du recours à des outils de surveillance sophistiqués dans le pays de destination, en stipulant que les demandes seront rejetées s'il existe un risque substantiel d'atteinte aux droits humains ;

        ii. veiller à ce que toutes les technologies concernées fassent l'objet d'un examen approfondi visant à identifier les risques relatifs aux droits humains dans le processus d'attribution des licences ;

        iii. garantir la transparence au sujet du volume, de la nature, de la valeur, de la destination et du pays de l'utilisateur final des transferts de technologies de surveillance, par exemple en publiant des rapports annuels sur les importations et les exportations de telles technologies ;

        iv. réviser toute législation en vigueur qui impose des restrictions démesurées en ce qui concerne la révélation de ce type d'informations ;

        v. faire en sorte que les outils de chiffrement et les recherches légitimes dans le domaine de la sécurité ne soient pas soumis à des contrôles à l'exportation ;

vi. appliquer une législation nationale qui impose une protection contre les atteintes aux droits humains causées par la surveillance numérique et crée des mécanismes d'obligation de rendre des comptes destinés à offrir une voie de recours aux victimes de surveillance abusive ;

vii. appliquer des normes d'achat qui limitent les contrats gouvernementaux pour des technologies et services de surveillance aux seules entreprises qui sont en mesure de prouver qu'elles respectent les droits humains conformément aux Principes directeurs des Nations unies et qu'elles ne vendent pas à des clients qui utilisent la surveillance de façon abusive ;

viii. participer aux principaux efforts multilatéraux (par exemple en soutien à l'appel de la Rapporteuse spéciale des Nations unies en faveur d'un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies de surveillance) visant à élaborer des normes rigoureuses en matière de droits humains afin d'encadrer le développement, la vente, le transfert et l'utilisation des équipements de surveillance et à définir des cibles inacceptables en matière de surveillance numérique.

a. exiger la création immédiate d'organismes indépendants, composés de diverses parties concernées, chargés de superviser toutes les entreprises de surveillance privées. Ces organismes doivent être une condition à la poursuite de l'activité de ces entreprises, et compter parmi leurs membres des groupes de défense des droits humains et d'autres acteurs de la société civile ;

b. mettre en place des conseils de surveillance publique issus de la société civile chargés de superviser et d'approuver l'acquisition ou l'utilisation des nouvelles technologies de surveillance, qui auraient le pouvoir d'approuver ou de rejeter les demandes sur la base des obligations de l'État en matière de droits humains, des dispositions relatives aux avis publics et des comptes rendus ;

c. réformer les lois existantes qui font obstacle à l'octroi de réparations aux victimes de surveillance illégale et veiller à ce que des voies de recours judiciaires et non judiciaires soient concrètement disponibles.

La Bulgarie, Israël et d'autres pays dans lesquels NSO Group est présent :

a. les Etats exportateurs, y compris Israël et la Bulgarie, doivent immédiatement résilier les autorisations de mise sur le marché et d'exportation dont bénéficie actuellement NSO Group, mener sans délai une enquête indépendante, impartiale et transparente visant à déterminer l'ampleur du ciblage illégal et enfin communiquer publiquement les résultats des efforts entrepris et les mesures identifiées pour prévenir de nouveaux préjudices.

NSO Group et son principal investisseur Novalpina Capital doivent, *a minima* :

a. mettre immédiatement un terme à l'utilisation, la maintenance et la vente de Pegasus dans les États où le logiciel de surveillance numérique a été utilisé à mauvais escient pour cibler illégalement des défenseurs des droits humains, des journalistes et des membres de la société civile, comme l'enquête du Projet Pegasus l'a démontré ;

b. proposer une indemnisation adéquate ou d'autres formes de réparations effectives aux victimes de surveillance illégale exercée au moyen des produits de NSO Group ;

c. prendre de toute urgence des mesures proactives pour veiller à ne pas entraîner ni favoriser des violations des droits humains – notamment celles évoquées dans le cadre de l'enquête du Projet Pegasus – et pour y remédier si elles se produisent. Pour s'acquitter de cette responsabilité, NSO Group est tenu de faire preuve de diligence raisonnable en matière de

droits humains et de faire le nécessaire pour que les défenseurs des droits humains, les journalistes et les membres de la société civile ne soient plus la cible d'une surveillance illégale ;

d. résilier ou suspendre ses contrats avec les gouvernements qui ont utilisé ses outils pour exercer une surveillance ciblée illégale ou commettre d'autres violations des droits humains ;

e. faire preuve de transparence en ce qui concerne le volume, la nature, la valeur, la destination et l'utilisateur final des transferts de technologies de surveillance.

Les investisseurs dans l'entreprise NSO Group doivent :

a. veiller à ne pas contribuer à des violations des droits humains par la détention de participations dans des entreprises privées de surveillance comme NSO Group. Ils devraient pour cela exiger de l'entreprise NSO Group qu'elle fasse preuve d'une transparence rigoureuse et de diligence raisonnable en matière de droits humains et qu'elle rende des comptes ;

b. enquêter pour déterminer si les fonds de placement du secteur privé ou d'autres supports d'investissement dans lesquels ils envisagent d'investir comptent ou prévoient de compter des entreprises de surveillance dans leur portefeuille, et exiger d'être avertis de tout changement de stratégie d'investissement qui pourrait aboutir à un investissement dans ce type d'entreprises ;

c. veiller à ce que les sociétés financées par les investissements n'aient pas de répercussions négatives sur les droits humains, en exigeant des entreprises de surveillance qu'elles fassent preuve d'une transparence rigoureuse et en exerçant une diligence raisonnable en matière de droits humains avant d'investir dans cette catégorie de sociétés ;

d. user de leur influence sur les entreprises de surveillance figurant dans les portefeuilles pour veiller à ce qu'elles mettent en place toutes les recommandations susmentionnées qui leur sont applicables.

Le secteur privé de la surveillance ciblée doit :

a. mettre en place un système solide de diligence raisonnable en matière de droits humains pour tous les transferts proposés de technologies de surveillance et le rendre public ;

b. renoncer à exporter des technologies de surveillance dès lors qu'il existe un risque substantiel que les utilisateurs finaux y aient recours pour commettre des atteintes aux droits humains ;

c. veiller à la transparence des ventes et des contrats ;

d. consulter les détenteurs de droits dans les pays de destination avant de signer des contrats, afin d'identifier et d'évaluer les risques en matière de droits humains et d'élaborer des mesures d'atténuation ;

e. veiller à intégrer des engagements publics en faveur des droits humains dans la politique de l'entreprise ;

f. mettre en œuvre des protections contractuelles contre les atteintes aux droits humains ;

g. faire des choix en matière de conception et d'ingénierie qui intègrent des normes relatives aux droits humains et des garanties en la matière ;

h. veiller à ce que les processus de vérification soient soumis à des audits réguliers, dont les résultats doivent être rendus publics ;

i. disposer de mécanismes de réclamation et d'un processus de notification approprié pour signaler les utilisations abusives de leurs technologies ;

j. mettre en œuvre de solides mécanismes d'indemnisation ou d'autres formes de réparation pour les cibles de surveillance illégale ;

k. respecter les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme et les Principes directeurs de l'Organisation de coopération et de développement économiques (OCDE) à l'intention des entreprises multinationales.

Les investisseurs dans des entreprises de surveillance doivent :

a. exercer une diligence raisonnable en matière de droits humains exhaustive dans le cadre de la procédure de diligence raisonnable appliquée dans la phase précédant les investissements et de manière continue ;

b. enquêter pour déterminer si les fonds de placement du secteur privé ou d'autres supports d'investissement dans lesquels ils envisagent d'investir comptent ou prévoient de compter des entreprises de surveillance dans leur portefeuille, et exiger d'être avertis de tout changement de stratégie d'investissement qui pourrait aboutir à un investissement dans ce type d'entreprises ;

c. veiller à ce que les sociétés financées par les investissements n'aient pas de répercussions négatives sur les droits humains, en exigeant des entreprises de surveillance qu'elles fassent preuve d'une transparence rigoureuse et en exerçant une diligence raisonnable en matière de droits humains avant d'investir dans cette catégorie de sociétés ;

d. user de leur influence sur les entreprises de surveillance figurant dans les portefeuilles pour veiller à ce qu'elles mettent en place toutes les recommandations susmentionnées qui leur sont applicables.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DEFENSE DES DROITS HUMAINS. LORSQU'UNE INJUSTICE TOUCHE UNE PERSONNE, NOUS SOMMES EGALEMENT CONCERNES.

Traduction d'Amnesty International France, octobre 2021

NOUS CONTACTER

info@amnesty.org

+44 (0)20 7413 5500

PRENDRE PART A LA CONVERSATION

www.facebook.com/AmnestyGlobal

@Amnesty

LA PARTIE IMMERGÉE DE L'ICEBERG

LA RESPONSABILITÉ DES ÉTATS ET DU SECTEUR PRIVÉ DANS LA CRISE DE LA CYBERSURVEILLANCE

Le Projet Pegasus est une enquête collaborative menée par plus de 80 journalistes de 17 médias dans 10 pays et coordonnée par Forbidden Stories, avec le soutien technique d'Amnesty International. Les révélations montrent que l'utilisation par les Etats des outils de surveillance numérique ciblée fournis par NSO Group est hors de contrôle et déstabilise et menace les droits des personnes, y compris leur sécurité physique.

Les articles publiés à la suite de cette collaboration parlent d'eux-mêmes. Avec ce rapport, Amnesty International entend apporter sa contribution en relevant les principaux enseignements du point de vue du droit international et en particulier du droit international relatif aux droits humains qui ressortent des révélations et des analyses techniques. Il s'agit notamment de l'ampleur démesurée du ciblage au regard du droit international relatif aux droits humains qui s'avère également en décalage par rapport à l'argumentation officielle de l'entreprise consistant à affirmer que la vente de ses produits aide ses clients à combattre le crime, et notamment les comportements liés au terrorisme ; la nature clandestine de l'outil qui facilite une utilisation et un fonctionnement illégaux ; les violations graves des droits humains qui en ont résulté ; l'impunité totale des États et des entreprises qui utilisent cet outil et l'incapacité des États à remplir leur obligation de protéger la population contre cette surveillance et ces piratages illégaux.

Enfin, Amnesty International formule des recommandations sur les mesures à prendre, compte tenu du besoin manifeste de mettre en place un contrôle indépendant du secteur de la surveillance numérique ciblée, de garantir l'obligation de rendre des comptes pour les violations des droits humains et d'améliorer la transparence.

INDEX : DOC 10/4491/2021
JUILLET 2021
LANGUE ORIGINALE : ANGLAIS

amnesty.org

AMNESTY INTERNATIONAL