Date : 24 janvier 2022 Index : IOR 40/5179/2022

DROIT À LA LIBERTÉ D'OPINION ET D'EXPRESSION. LES MÉDIAS MENACÉS PAR LA SURVEILLANCE CIBLÉE ILLÉGALE

COMMUNICATION À LA RAPPORTEUSE SPÉCIALE SUR LA PROMOTION ET LA PROTECTION DU DROIT À LA LIBERTÉ D'OPINION ET D'EXPRESSION EN VUE DU RAPPORT PRÉSENTÉ À LA 50ESESSION DU CONSEIL DES DROITS DE L'HOMME

Amnesty International soumet cette communication en réponse à l'appel à contribution[1] de la rapporteuse spéciale des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression en vue du rapport qu'elle présentera à la 50e session du Conseil des droits de l'homme. Bien que les médias soient confrontés à plusieurs défis et risques à l'ère du numérique, cette communication porte spécifiquement sur la menace que représente la surveillance ciblée illégale pour les journalistes. Ce texte présente les perspectives à l'échelle mondiale ainsi que des exemples au niveau national. On ne doit pas considérer cette communication comme un rapport exhaustif des recherches menées par l'organisation sur ces questions.

INTRODUCTION

L'utilisation illégale par les États de technologies de surveillance ciblées contre des journalistes et d'autres membres de la société civile a provoqué une crise de la surveillance numérique. Les États recourent à la surveillance illégale ainsi qu'à toute une série d'autres tactiques pour réduire les journalistes au silence et exercer un effet délétère sur la société civile. Cela constitue une grave menace pour la sûreté et la sécurité des journalistes à travers le monde. Les conséquences pour la liberté des médias sont désastreuses. Les États ont non seulement failli à leur obligation de protéger les journalistes contre ces violations des droits humains, mais ils ont également manqué à leur devoir de respecter les droits fondamentaux, en laissant se déployer ces armes invasives contre des personnes partout dans le monde simplement parce qu'elles veulent exercer leurs droits humains et protéger ceux d'autrui.

Cette tendance mondiale à recourir à des technologies de surveillance ciblées, comme les logiciels espions, pour réprimer les droits à la liberté d'opinion et d'expression est rendue possible par les entreprises privées de surveillance. Comme nous l'avions souligné en février 2019 dans notre précédente communication à l'ancien rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le secteur de la surveillance au niveau international échappe à tout contrôle. Les normes, la surveillance et les mécanismes de contrôle qui existent aux niveaux national, régional et mondial se sont révélés inadéquats pour prévenir les violations des droits humains, et inefficaces pour garantir l'obligation de rendre des comptes et la réparation[2].

La surveillance ciblée illégale viole le droit à la vie privée et les droits à la liberté d'expression, d'opinion, d'association et de réunion pacifique, qui sont protégés à la fois par la Déclaration universelle des droits de l'homme (DUDH) et le Pacte international relatif aux droits civils et politiques (PIDCP). Le PIDCP garantit le droit de ne pas être inquiété pour ses opinions et protège contre les immixtions arbitraires ou illégales dans la vie privée des personnes[3].

Le droit international et les normes connexes prévoient en outre que toute ingérence d'un État dans le droit d'une personne au respect de sa vie privée doit être légale, nécessaire, proportionnée et légitime. La pratique

[1] Appel à contributions : Les opportunités, défis et menaces pour les médias à l'ère numérique, https://www.ohchr.org/FR/Issues/FreedomOpinion/Pages/Report-Media-Digital-Age.aspx

[2] Amnesty International, *The Surveillance Industry and Human Rights: Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression* (22 février 2019, Index : TIGO IOR 40/9868/2019), https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf

[3] PIDCP, articles 17 et 19.

courante des États qui vise à déployer ces outils de manière incontrôlée ne respecte pas ces critères. Le fait de cibler des journalistes et des défenseur·e·s des droits humains au moyen de ces technologies uniquement en raison de leurs activités est contraire au droit international des droits humains, et ce sans équivoque[4].

Cette communication explique en détail comment la surveillance ciblée illégale a été utilisée contre des journalistes et préconise des mesures pour mettre fin à cette pratique.

UTILISATION DE LA SURVEILLANCE CIBLÉE ILLÉGALE CONTRE DES JOURNALISTES

Ces dernières années, on a commencé à voir apparaître des cas d'utilisation de la surveillance ciblée illégale contre des journalistes. Depuis les premiers rapports faisant état de l'utilisation d'écoutes téléphoniques aux tentatives d'hameçonnage, en passant par les messages SMS contenant des liens malveillants, on arrive aujourd'hui à des attaques ciblées plus sophistiquées au moyen par exemple de logiciels espions « zéro clic ». À mesure que les technologies ont évolué, les tactiques de répression numérique ciblée ont elles aussi évolué. Les journalistes sont donc confrontés à de nouvelles menaces contre lesquelles il est plus difficile de se protéger, qui sont plus difficiles à détecter et pour lesquelles il est encore plus difficile d'établir les responsabilités en la matière.

De nombreux cas d'utilisation de technologies de surveillance ciblée visant des journalistes ont été recensés à travers le monde. Au Royaume-Uni, des rapports laissent entendre que la police a placé des journalistes sous surveillance numérique[5]. En Colombie, la police nationale aurait mis des journalistes de radio sous surveillance numérique[6]. Le laboratoire de recherche Citizen Lab a détecté des attaques numériques qui ont été perpétrées ces dernières années contre des journalistes par divers acteurs de menace en Chine, en Russie, en Éthiopie et au Mexique[7]. Amnesty International avait précédemment recensé des informations sur des attaques menées au moyen de logiciels malveillants contre des blogueurs vietnamiens et un journaliste indien[8]. En 2020, Citizen Lab a également découvert que le célèbre logiciel espion Pegasus du fournisseur de services de surveillance NSO Group avait été utilisé pour pirater les téléphones personnels de 36 employés d'Al Jazeera, d'un journaliste d'Al Araby TV et d'un journaliste du *New York Times*[9]. Le laboratoire de sécurité d'Amnesty International a révélé que Maati Monjib, cofondateur de l'Association marocaine du journalisme d'investigation, et Omar Radi, un éminent militant et journaliste marocain aujourd'hui emprisonné, avaient été pris pour cible à l'aide d'outils conçus par NSO Group[10].

À la suite de ces rapports initiaux, le Projet Pegasus a été rendu public en juillet 2021. L'ampleur et la portée des conclusions de ce Projet ont mis en évidence la gravité de la menace que représente la surveillance ciblée illégale pour la liberté de la presse. Le Projet Pegasus est une enquête collaborative sans précédent menée par plus de 80 journalistes de 17 médias dans 10 pays et coordonnée par Forbidden Stories, une association à but non lucratif basée à Paris qui travaille dans le secteur des médias, avec le soutien technique d'Amnesty International, qui a mené des analyses techniques de pointe visant à détecter des traces du logiciel espion Pegasus dans des téléphones portables. Le Projet Pegasus a mis en évidence la manière dont un seul logiciel espion, celui du fournisseur de services de surveillance NSO Group, a été utilisé par des États clients pour

---

[4] Comité des droits de l'homme des Nations unies, Observation générale n° 34, doc. ONU CCPR/C/GC/34, § 23

[5] Dominic Ponsford, "Surveillance court says Met grabs of Sun reporters' call records 'not compatible' with human rights law", 17 décembre 2015, http://www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources

[6] Committee to Protect Journalists, "Claims police spied on two journalists revive surveillance fears of Colombia's press", 2016, https://cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php.

[7] Voir Marczak et.al., *The Great iPwn*, décembre 2020, (https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/) et Marczak et.al., *Stopping the Press New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator*, janvier 2020, (https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/)

[8] Voir Amnesty International, *Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks*, février 2021 (https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/) et Amnesty International, *India: Human Rights Defenders Targeted by a Coordinated Spyware Operation*, juin 2020, (https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/)

[9] Marczak et.al., *The Great iPwn*, décembre 2020, https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

[10] Voir Amnesty International, *Maroc. Des défenseurs des droits humains ciblés par un logiciel espion de NSO Group*, octobre 2019, (https://www.amnesty.org/fr/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/) et Amnesty International, *Un journaliste marocain victime d'attaques par injection réseau au moyen d'outils conçus pas NSO Group*, juin 2020 (https://www.amnesty.org/fr/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/)

commettre des atteintes aux droits humains d'une grande ampleur partout dans le monde. Cette enquête a identifié des clients potentiels de l'entreprise NSO Group dans les 11 pays suivants : Arabie saoudite, Azerbaïdjan, Bahreïn, Émirats arabes unis, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda et Togo. Ces révélations viennent démentir les affirmations de l'entreprise NSO Group selon lesquelles ces attaques sont rares ou inhabituelles, ou liées à une utilisation frauduleuse de sa technologie. Bien que NSO Group soutienne que son logiciel espion est utilisé exclusivement à des fins légitimes d'enquêtes pénales et terroristes, il est clair que sa technologie favorise des atteintes systématiques des droits humains, auxquelles l'entreprise semble être complice[11].

Au moment de la publication des résultats du Projet Pegasus, les organes de presse ont révélé qu'au moins 180 journalistes provenant de 20 pays avaient été sélectionnés pour être potentiellement la cible du logiciel espion de NSO Group entre 2016 et juin 2021[12]. Le Projet Pegasus a identifié au moins 25 journalistes mexicains ayant été désignés comme cibles potentielles en l'espace de deux ans, parmi lesquels la journaliste d'investigation Carmen Aristegui qui a été visée[13]. Le logiciel espion Pegasus a été utilisé en Azerbaïdjan, un pays où il ne reste plus qu'une poignée de médias indépendants. Selon l'enquête, plus de 40 journalistes azerbaïdjanais figuraient parmi les cibles potentielles visées. En Inde, au moins 40 journalistes travaillant pour les principaux médias du pays ont été sélectionnés comme cibles potentielles entre 2017 et 2021. L'enquête a également identifié parmi les cibles potentielles des journalistes travaillant pour de grands médias internationaux, comme Associated Press, CNN, *le New York Times* et Reuters[14].

Grâce à des analyses techniques sophistiquées, le Security Lab d'Amnesty International a confirmé que les téléphones portables de nombreux journalistes ont été ciblés et/ou infectés. En Azerbaïdjan, les téléphones des journalistes Sevinc Vaqifqizi et Khadija Ismayilova ont été infectés par le logiciel espion Pegasus. En Inde, des analyses techniques de pointe ont révélé que les téléphones des journalistes Siddharth Varadarajan, MK Venu, Paranjoy Guha Thakurta, Sushant Singh et SNM Abdi étaient infectés. En Hongrie, les téléphones des journalistes Szabolcs Panyi, Daniel Nemeth, András Szabó, Brigitta Csikász et du propriétaire du média Zoltan Pava[15] se sont révélés infectés. Les téléphones de journalistes basés en France, notamment Hicham Mansouri, Lénaïg Bredoux et Edwy Plenel, ont aussi été contaminés[16].

Il est donc clair que le logiciel espion Pegasus de NSO Group est une arme de choix entre les mains des gouvernements pour faire taire les journalistes[17]. L'utilisation de logiciels espion a un effet dissuasif et instaure un climat de peur intense pour celles et ceux qui osent s'exprimer. Même lorsque la présence d'une surveillance ne peut être prouvée, le simple fait d'en soupçonner l'existence incite les journalistes à s'autocensurer. La surveillance présente des risques énormes pour la sécurité physique et le bien-être mental des journalistes. Elle met également en danger leurs sources, leurs collègues, leurs amis et leur famille. Elle peut entraîner de lourdes conséquences sur la vie quotidienne des personnes visées ou infectées.

En 2017, Amnesty International a recueilli des informations sur la surveillance ciblée illégale dont a fait l'objet Galima Bukharbaeva, une journaliste d'Ouzbékistan, par le biais d'une attaque de phishing sur sa messagerie électronique. Peu après l'attaque, des articles sont apparus sur des sites Web généralement perçus comme étant proches du gouvernement de l'Ouzbékistan, pour ne pas dire sous son contrôle, avec des informations tirées de ses courriels privés. Aussi, lorsque Gulasal Kamolova et Vasiliy Markov, deux journalistes ouzbeks, ont vu leurs noms commencer à apparaître dans ces articles, ils ont compris qu'ils pourraient être en danger.

---

[11] Amnesty International, « Monde. L'ampleur de la cybersurveillance secrète constitue "une crise internationale des droits humains" dont NSO Group est complice », juillet 2021 https://www.amnesty.org/fr/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/ (communiqué de presse)

[12] Amnesty International, « Le Projet Pegasus : des fuites massives de données révèlent que le logiciel espion israélien de NSO Group est utilisé contre des militant·e·s, des journalistes et des dirigeant·e·s politiques partout dans le monde », juillet 2021, https://www.amnesty.org/fr/latest/news/2021/07/the-pegasus-project/ (communiqué de presse)

[13] Phineas Rueckert, Pegasus: "The new global weapon for silencing journalists", juillet 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon- for-silencing-journalists/

[14] Amnesty International, « Le Projet Pegasus : des fuites massives de données révèlent que le logiciel espion israélien de NSO Group est utilisé contre des militant·e·s, des journalistes et des dirigeant·e·s politiques partout dans le monde », juillet 2021, https://www.amnesty.org/fr/latest/news/2021/07/the-pegasus-project/ (communiqué de presse)

[15] Omer Benjakob, "The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware", janvier 2022, https://www.haaretz.com/israel-news/MAGAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510

[16] Amnesty International, *Forensic Methodology Report: Pegasus Forensic Traces per Target*, juillet 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/

[17] Phineas Rueckert, "Pegasus: The new global weapon for silencing journalists", juillet 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon- for-silencing-journalists/

Ils ont ressenti une anxiété et une peur extrêmes. Moins de six mois après l'attaque du compte de messagerie de Galima Bukharbaeva, Vasiliy Markov et Gulasal Kamolova ont été contraints de fuir de manière permanente l'Ouzbékistan, où ils vivaient, et de se réfugier à l'étranger[18].

Les attaques ciblées par le logiciel espion Pegasus contre la famille, les amis et les associés du journaliste assassiné Jamal Khashoggi ont été menées avant et après son meurtre, bien que l'entreprise NSO Group ait toujours nié toute implication. Les analyses techniques d'Amnesty International ont confirmé que l'iPhone de la fiancée turque de Jamal Khashoggi, Hatice Cengiz, avait été ciblé et infecté avec succès quatre jours après son assassinat, puis à plusieurs reprises les jours suivants. Les vérifications techniques ont également confirmé que son épouse Hanan Elatr a été prise pour cible par le logiciel espion, tout comme son ami et ancien directeur général d'Al Jazira, Wadah Khanfar, dont le téléphone a été piraté[19].

Ces cas illustrent la façon dont la surveillance peut toucher des réseaux entiers de personnes et être liée à de graves atteintes aux droits humains. En effet, de nombreux journalistes dont on sait qu'ils ont été pris pour cibles ou dont les téléphones ont été infectés par Pegasus ont déjà été victimes de répression de la part de gouvernements, notamment des actes de harcèlement, des campagnes de dénigrement et de l'emprisonnement. Pour les femmes journalistes, la menace de la surveillance est encore plus grave.

Les informations obtenues par le biais d'une surveillance illégale peuvent être utilisées contre toutes ces personnes par le biais de campagnes de dénigrement, de « doxing » (qui consiste à mettre en ligne des informations personnelles d'un tiers pour lui porter préjudice) et d'autres attaques numériques. Ainsi, la surveillance constitue une forme de violence à l'égard des femmes[20]. En outre, comme nous l'avons vu dans de nombreux cas révélés par le projet Pegasus, les journalistes continuent d'être surveillés même s'ils choisissent de quitter leur pays d'origine. Cela fait de la surveillance ciblée illégale un outil de répression transnationale, suscitant le sentiment de ne plus être en sécurité nulle part.

Les divulgations qui ont débuté avec le projet Pegasus ont fait boule de neige et se sont transformées en une année de révélation sur le secteur des logiciels espions, grâce au travail de chercheurs de la société civile et de géants du numérique. En raison de nouvelles découvertes, la liste des clients potentiels de NSO Group comprend désormais la Pologne, la Thaïlande, le Salvador, le Ghana et l'Ouganda[21]. Tout récemment, en janvier 2022, Citizen Lab et Access Now ont mené une enquête conjointe sur le piratage à l'aide de Pegasus au Salvador, en collaboration avec Frontline Defenders, SocialTIC et Fundación Acceso. Ils ont confirmé l'existence de 35 cas de journalistes et de membres de la société civile dont les téléphones ont été infectés avec succès par le logiciel espion Pegasus de NSO Group entre juillet 2020 et novembre 2021. Les cibles étaient des journalistes de *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy*, ainsi que deux journalistes indépendants[22].

Alors que des affaires continuent de faire surface, il est important de noter que NSO Group n'est pas la seule entreprise à vendre ces outils. Citizen Lab a révélé que des outils conçus par l'entreprise Cytrox ont ciblé un journaliste égyptien en exil[23]. Il est inquiétant de constater que le manque de transparence dans un secteur qui continue à opérer dans l'ombre implique que les cas énumérés dans cette communication ne représentent probablement qu'une partie de la réalité et ne permettent pas de dresser un tableau exhaustif.

---

[18] Amnesty International, *"We will find you, anywhere": The global shadow of Uzbekistani surveillance*, mars 2017, (EUR 62/5974/2017), https://www.amnesty.org/en/documents/eur62/5974/2017/en/

[19] Amnesty International, *Forensic Methodology Report: Pegasus Forensic Traces per Target*, juillet 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/

[20] Access Now and Frontline Defenders, "Unsafe anywhere: women human rights defenders speak out about Pegasus attacks", janvier 2022 https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/

[21] Voir: https://www.amnesty.org/fr/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/ et, https://techcrunch.com/2021/11/24/apple-nso-hacking-notify/, et https://www.primenewsghana.com/politics/stan-dogbe-alleges-state-sponsored-attack-on-his-phone.html

[22] Railton et. al, *Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*, janvier 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

[23] Marczak, et. al, *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, décembre 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

PISTES DE RÉFLEXION

Comme nous l'avions déjà noté dans la communication adressée à l'ancien rapporteur spécial en 2019, les cadres réglementaires et les mécanismes de recours existants étaient inefficaces et inadéquats[24]. Et c'est toujours le cas aujourd'hui. Nous avons déjà montré comment les lois nationales régissant la surveillance dans de nombreuses juridictions, les cadres nationaux et régionaux de contrôle des exportations et d'autres mécanismes tels que l'arrangement de Wassenaar ne sont pas adaptés dans leur forme actuelle à la lutte contre la menace de la surveillance ciblée illégale[25]. Même là où les mécanismes réglementaires ont été mis à jour, comme dans le cas du nouveau règlement de l'UE en ce qui concerne les exportations de biens à double usage, ils ne vont pas assez loin[26] et ne seront efficaces que s'ils sont mis en œuvre dans une totale transparence[27]. En effet, l'ancien rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression indiquait dans son rapport : « 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[28]. »

Les entreprises qui exercent dans cette sphère le font dans l'opacité totale et en toute impunité. En effet, nous avons constaté à plusieurs reprises que les affirmations de NSO Group selon lesquelles il respecte les droits humains sont sans fondement, et que ses politiques et pratiques sont inefficaces. Il ressort de nos nombreux contacts avec l'entreprise que l'on ne peut pas faire confiance aux fournisseurs de cybersurveillance pour s'autoréguler. En outre, les investisseurs ont un rôle à jouer pour garantir qu'ils ne contribuent pas ou ne sont pas directement liés aux atteintes aux droits humains du fait de leurs investissements dans ces entreprises[29].

Amnesty International réitère sa demande aux États d'instaurer un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies de surveillance, jusqu'à ce qu'un cadre réglementaire solide et respectueux des droits humains soit mis en place. Nous avons également, avec d'autres, demandé à l'Union européenne de procéder à des sanctions ciblées contre NSO Group[30]. Pour combattre cette crise, il faut agir à différents niveaux. Ainsi, nous rappelons les recommandations faites aux différents acteurs dans notre rapport intitulé *La partie immergée de l'iceberg : La responsabilité des États et du secteur privé dans la crise de la surveillance numérique*[31].

Une culture de l'impunité spécifique à la surveillance numérique ciblée s'est développée et doit être combattue de toute urgence. Les informations présentées dans cette communication montrent à quel point l'utilisation par les États des outils de surveillance numérique ciblée fournis par des entreprises privées est hors de contrôle et déstabilise et menace les droits des personnes, y compris leur sécurité physique. Ces révélations mettent en lumière un secteur et des États qui font appel à ses services, lesquels restent dispensés de rendre des comptes de leurs actes en la matière. Il faut mettre un terme aux pratiques sous leur forme actuelle. Les droits des journalistes à s'exprimer librement, à mener leur travail sans crainte et en toute sécurité, et la sécurité de l'ensemble de l'écosystème numérique en dépendent.

---

[24] Amnesty International, *The Surveillance Industry and Human Rights. Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression* (22 février 2019, Index : TIGO IOR 40/9868/2019) https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf

[25] Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure*, mai 2021, DOC 10/4182/2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/

[26] Amnesty International, « Le nouveau règlement de l'Union européenne sur les exportations de biens à double usage représente une « occasion manquée » en vue de mettre fin à l'exportation d'instruments de surveillance destinés à des régimes répressifs », mars 2021, https://www.amnesty.org/fr/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/ (communiqué de presse)

[27] Access Now et.al, "Human Rights Organizations Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states' role in Pegasus affair", septembre 2021, https://www.accessnow.org/cms/assets/uploads/2021/09/Pegasus_Export_Control_Rules_Statement.pdf

[28] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, doc. ONU A/HCR/41/35, § 46, https://undocs.org/A/HRC/41/35

[29] Amnesty International, *Operating in the shadows: Investor risk from the private surveillance industry*, octobre 2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/ (DOC 10/4359/2021)

[30] Voir : Lettre conjointe réclamant des sanctions ciblées de l'UE contre le groupe NSO | Human Rights Watch (hrw.org)

[31] Amnesty International, *La partie immergée de l'iceberg. La responsabilité des États et du secteur privé dans la crise de la surveillance numérique*, juillet 2021, https://www.amnesty.org/fr/documents/doc10/4491/2021/fr/ (DOC 10/4491/2021)