DEFENDRE LES DROITS : UNE ACTIVITE SOUS SURVEILLANCE

SYNTHÈSE DE L'IMPACT DE LA SURVEILLANCE NUMÉRIQUE SUR LES PERSONNES QUI DÉFENDENT LES DROITS HUMAINS

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL REUNISSANT PLUS DE SEPT MILLIONS DE PERSONNES QUI AGISSENT POUR QUE LES DROITS FONDAMENTAUX DE CHAQUE INDIVIDU SOIENT RESPECTES.

AMNESTY INTERNATIONAL

La vision d'Amnesty International est celle d'un monde où chacun peut se prévaloir de tous les droits énoncés dans la Déclaration universelle des droits de l'homme et dans d'autres textes internationaux relatifs aux droits humains.

Essentiellement financée par ses membres et les dons de particuliers, Amnesty International est indépendante de tout gouvernement, de toute tendance politique, de toute puissance économique et de tout groupement religieux.

L'édition originale de ce document a été publiée en 2019 par
Amnesty International Ltd
Peter Benenson House, 1 Easton Street
Londres WC1X 0DW, Royaume-Uni

Index : ACT 30/1385/2019
L'édition originale a été publiée en langue anglaise.

amnesty.org

Photo de couverture : *© Getty Images*

AMNESTY INTERNATIONAL

SOMMAIRE

GLOSSAIRE

TERME	DEFINITION
SURVEILLANCE NUMÉRIQUE DE MASSE	Contrôle de toute une population, ou d'une partie importante de celle-ci, à l'aide d'outils numériques. Cette surveillance prend généralement la forme d'un contrôle des communications électroniques, d'une installation de caméras numériques, d'un recours aux technologies de reconnaissance faciale, d'une collecte d'informations dans des bases de données biométriques, et peut même passer par l'utilisation de drones, entre autres tactiques. Habituellement réalisée par les États, cette surveillance peut aussi être l'œuvre d'entreprises privées agissant pour le compte d'un État ou pour servir leurs propres intérêts.
SURVEILLANCE NUMÉRIQUE CIBLÉE	Contrôle ou espionnage, à l'aide de technologies numériques, de personnes ou organisations spécifiques pouvant intéresser les autorités. La surveillance numérique ciblée peut passer, entre autres, par le piratage des appareils via l'installation de logiciels malveillants ou espions ou par des campagnes d'hameçonnage compromettant les communications numériques.
HAMEÇONNAGE	Forme de cyberattaque consistant à créer et diffuser de fausses pages de connexion à des services reconnus (comme Gmail ou Facebook) afin de recueillir les identifiants et mots de passe des victimes, qui sont généralement ciblées par l'envoi de faux liens.
LOGICIEL MALVEILLANT	Logiciel conçu pour être installé secrètement sur l'ordinateur ou le téléphone de la victime dans le but de lui dérober des informations privées, de commettre d'autres formes d'escroquerie, d'endommager l'appareil ou encore pour perturber la victime.
LOGICIEL ESPION	Logiciel malveillant conçu pour espionner l'ordinateur ou le téléphone de la victime, surveiller ses communications de manière permanente et lui dérober des informations et des fichiers privés.
DÉFENSEUR DES DROITS HUMAINS	Personne, homme ou femme, qui, individuellement ou en association avec d'autres, agit pour défendre et promouvoir les droits humains aux niveaux local, national, régional ou international, sans avoir recours à la haine, la discrimination ou la violence, ni préconiser leur usage.

1. LA SURVEILLANCE NUMÉRIQUE CIBLÉE EN BREF

> **« Partout dans le monde, les conflits et la peur sont de plus en plus utilisés pour répandre la violence et les divisions, ainsi que pour réduire la société civile au silence. Certains pays tournent le dos à la solidarité et à la justice. Il est même des dirigeants qui s'enorgueillissent des violations des droits humains et déclarent une guerre ouverte à tous ceux qui osent défendre la justice. Le mouvement des défenseurs des droits humains se trouve ainsi aujourd'hui confronté à un niveau de persécution et de répression inédit. »**
>
> Sommet mondial des défenseurs des droits humains 2018[1]

Les attaques personnelles telles que les menaces, les campagnes de dénigrement, les poursuites en justice, les violences physiques, les meurtres et les disparitions forcées font parties des tactiques et moyens de répressions utilisés contre les défenseurs des droits humains dans une impunité quasi totale. Des États ont en outre adopté une quantité impressionnante de lois et de pratiques limitant la liberté d'expression, de réunion pacifique et d'association et le droit de circuler librement.

Les défenseurs des droits humains les plus exposés aux inégalités, à l'exclusion et à la discrimination, comme les femmes, les personnes LGBTI, les migrants, les Noirs et les Autochtones courent doublement le risque de se faire attaquer, d'une part en raison de

[1] Voir le site du Sommet mondial des défenseurs des droits humains 2018 : https://hrdworldsummit.org/le-sommet/?lang=fr

leurs activités et d'autre part en raison de leur identité. Ces attaques prennent différentes formes et ont des impacts spécifiques, tels que les violences liées au genre. Elles sont en outre souvent aggravées par des inégalités structurelles et par une exclusion systématique du pouvoir et des ressources[2].

Ces tactiques découragent les défenseurs des droits humains d'exprimer leur désaccord, de dénoncer les violations des droits fondamentaux et de militer en faveur d'un changement. Nous observons une tendance croissante des États à se copier mutuellement des techniques et à importer des outils et des technologies pour appliquer une stratégie de contrôle et de répression.

Parmi les tactiques les plus utilisées par les gouvernements aux quatre coins du monde figure celle de la surveillance, numérique ou autre. La surveillance numérique est actuellement employée dans un contexte d'augmentation exponentielle de l'utilisation des technologies dans le maintien de l'ordre et l'application des lois. Sous prétexte de lutter contre le terrorisme ou de faire respecter la loi et l'ordre public, les États utilisent tout un éventail de techniques de surveillance qui empiètent sur la vie privée des personnes partout dans le monde. La surveillance numérique de masse et la surveillance numérique ciblée en font partie. La surveillance numérique de masse prend généralement la forme d'un contrôle des communications électroniques, d'une installation de caméras de surveillance, d'un recours aux technologies de reconnaissance faciale, d'une collecte d'informations dans des bases de données biométriques, et peut même passer par l'utilisation de drones, entre autres tactiques. Des pays comme le **Royaume-Uni**[3], la **Chine**[4] et les **États-Unis**[5] auraient procédé à une surveillance numérique de masse.

La surveillance numérique ciblée utilise quant à elle des technologies permettant de viser spécifiquement certaines personnes. Elle se fait par placement sur écoute ou à l'aide de technologies numériques. Elle peut aussi passer, entre autres, par le piratage des appareils via l'installation de logiciels malveillants ou espions ou par des campagnes d'hameçonnage compromettant les communications numériques. Au **Royaume-Uni**, par exemple, des journalistes auraient fait l'objet d'une surveillance numérique exercée par la police[6]. Aux **Émirats arabes unis**, le gouvernement aurait utilisé un logiciel espion pour suivre des militants[7]. En **Colombie**, la police nationale aurait placé des journalistes radio sous surveillance numérique[8]. Et en **Éthiopie**, l'ancien gouvernement avait recours à la

---

[2] Voir les rapports d'Amnesty International : *Défenseurs des droits humains menacés. Un espace de plus en plus restreint pour la société civile* (index : ACT 30/6011/2017) ; *Attaques mortelles mais évitables. Homicides et disparitions forcées à l'encontre des personnes qui défendent les droits humains* (index : ACT 30/7270/2019) ; *Des lois conçues pour museler. La répression mondiale des organisations de la société civile* (index : ACT 30/9647/2019) ; et *Bousculer les rapports de force, lutter contre la discrimination. Appel à l'action pour la reconnaissance et la protection des femmes défenseures des droits humains et des personnes qui défendent les droits liés au genre* (index : ACT 30/1139/2019)

[3] Voir Amnesty International, *Chiffrement : une question de droits humains* (index : POL 40/3682/2016) ; Amnesty International UK, *Campaigners win vital battle against UK mass surveillance at European Court of Human Rights*, www.amnesty.org.uk/press-releases/campaigners-win-vital-battle-against-uk-mass-surveillance-european-court-human ; *The UK government has been spying on Amnesty – so we're going to court*, www.amnesty.org.uk/blogs/ether/uk-government-spying-amnesty-mass-surveillance-court

[4] Des informations sur différents programmes de surveillance de masse en Chine sont disponibles à l'adresse suivante : www.hrw.org/tag/mass-surveillance-china.

[5] Amnesty International, *Chiffrement : une question de droits humains* (index : POL 40/3682/2016)

[6] 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.

[7] Citizen Lab, "The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/).

[8] 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.

surveillance électronique pour espionner les militants de l'opposition, chez eux et à l'étranger[9].

L'apparition de nouvelles technologies de pointe très accessibles, associées à des lois qui limitent la liberté d'expression en ligne et portent atteinte à la confidentialité sur Internet, fait de la surveillance numérique ciblée une menace encore plus pressante. Des pays comme la **Thaïlande**[10] et le **Bangladesh**[11] ont adopté des lois visant à élargir le champ de la surveillance électronique et conférant aux gouvernements le pouvoir d'espionner les communications électroniques.

Fait extrêmement significatif, des gouvernements font depuis peu appel aux services d'entreprises privées du secteur de la surveillance numérique pour mettre au point des technologies de surveillance numérique ciblée. Ces outils sont ensuite utilisés de manière abusive pour cibler illégalement des militants pour les droits humains et les placer sous surveillance. Les entreprises qui interviennent dans ce secteur sont devenues un rouage redoutable de la répression, responsable de la création de nouveaux outils qui accroissent les menaces contre les personnes qui défendent nos droits fondamentaux.

On sait peu de choses de ce secteur, qui intervient dans l'ombre malgré les demandes répétées de plus de transparence. Le peu de contrôle juridique et réglementaire fait que ces entreprises sont libres de vendre leurs technologies à des pays où les droits humains ne sont ni protégés ni respectés, qui les utilisent pour suivre et surveiller les personnes qui défendent les droits fondamentaux.

---

[9] Amnesty International, *Chiffrement : une question de droits humains* (index : POL 40/3682/2016).
[10] Tech Crunch, "Thailand passes controversial cybersecurity law that could enable government surveillance", 28 février 2019, https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/ et
Reuters, "Thailand defends cybersecurity law amid concerns over rights abuse", 1er mars 2019, **WWW.REUTERS.COM/ARTICLE/US-THAILAND-CYBER/THAILAND-DEFENDS-CYBERSECURITY-LAW-AMID-CONCERNS-OVER-RIGHTS-ABUSE-IDUSKCN1QI4KA**.
[11] Amnesty International « Bangladesh. La nouvelle Loi sur la sécurité numérique est une atteinte à la liberté d'expression », novembre 2018, https://www.amnesty.org/fr/latest/news/2018/11/bangladesh-muzzling-dissent-online/.

2. SURVEILLANCE NUMÉRIQUE CIBLÉE ET RESTRICTION DE L'ESPACE ACCORDÉ À L'OPPOSITION

Le droit international relatif aux droits humains interdit sans ambiguïté de cibler des défenseurs des droits humains à l'aide de technologies de surveillance numérique en raison de leurs activités. La surveillance illégale viole le droit au respect de la vie privée et empiète sur les droits à la liberté d'expression, d'opinion, d'association et de réunion. Ces droits sont protégés par la Déclaration universelle des droits de l'homme et par le Pacte international relatif aux droits civils et politiques. Le Pacte garantit le droit de ne pas être inquiété pour ses opinions[12] et protège contre les immixtions arbitraires ou illégales dans la vie privée des personnes[13]. Le droit international et les normes y afférentes interdisent en outre toute ingérence d'un État dans le droit d'une personne au respect de sa vie privée si cette ingérence n'est pas légale, nécessaire, proportionnée et légitime. Les États doivent par ailleurs garantir que toute personne dont les droits ont été violés dispose d'un recours utile[14].

Il est souvent pratiquement impossible pour les défenseurs des droits humains de prouver l'existence d'une surveillance, soit en raison de problèmes techniques, soit parce que ces pratiques sont clandestines.[15] Or, même quand le ciblage ou la présence d'une infection

[12] Article 19 du Pacte international relatif aux droits civils et politiques.
[13] Article 17 du Pacte international relatif aux droits civils et politiques.
[14] Article 2(3) du Pacte international relatif aux droits civils et politiques.
[15] Amnesty International, *Défenseurs des droits humains menacés. Un espace de plus en plus restreint pour la société civile* (index : ACT 30/6011/2017).

active ne peuvent être prouvés[16], le fait de vivre sous la menace constante d'une *éventuelle* surveillance peut suffire à constituer une violation des droits humains[17].

Que la tentative de surveillance aboutisse ou non, le ciblage instille la peur et empêche les militants pour les droits humains de continuer sereinement leurs activités par crainte d'une ingérence injustifiée[18]. Dans de nombreux cas, cela conduit les personnes qui défendent les droits humains à se censurer et à renoncer à exercer leurs droits à la liberté d'expression, d'association et de réunion pacifique. À cela s'ajoutent les poursuites abusives fondées sur les informations obtenues, qui sont manipulées et utilisées à mauvais escient contre les défenseurs des droits humains, lesquels voient leur énergie et leurs ressources accaparées par les procédures judiciaires dont ils font l'objet[19]. La menace de la surveillance peut être préjudiciable à la santé mentale des défenseurs des droits humains et les informations obtenues peuvent être divulguées dans la sphère publique et les exposer à des attaques personnelles et des campagnes de dénigrement. Tout cela a des répercussions sur les populations dont les droits sont défendus par ces militants.

En **Azerbaïdjan**, par exemple, des militants pour les droits humains qui se trouvent sous la menace constante de la surveillance et doivent partir par peur d'être attaqués ont du mal à communiquer avec leurs proches, car ils craignent qu'ils soient eux aussi pris pour cible[20]. En **Ouzbékistan**, les personnes ciblées par des cyberattaques qui sont parties de chez elles sont toujours visées par des campagnes de surveillance numérique[21]. Les défenseurs des droits humains vivent ainsi dans un état de peur constant, regardent sans cesse par-dessus leur épaule et, où qu'ils aillent, ils ont le sentiment d'être exposés à un danger imminent. La surveillance est une manière très efficace de décourager ou d'empêcher les personnes qui défendent les droits fondamentaux d'exprimer leur opposition ou de dénoncer les atteintes à ces droits[22].

[16] Le « ciblage » désigne la tentative de mettre une personne sous surveillance. Cela peut se faire, par exemple, en envoyant des liens malveillants contenant un logiciel espion. Le ciblage peut aboutir ou non. Lorsqu'il aboutit, les appareils de l'utilisateur peuvent être infectés et compromis.

[17] Amnesty International, *A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work* (blog, 16 août 2019).

[18] Global Justice Clinic, NYU School of Law, *Attempted digital surveillance as a completed human rights violation: Why targeting human rights defenders infringes on rights. Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 1er mars 2019, https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf.

[19] Voir Amnesty International, *Des lois conçues pour museler. La répression mondiale des organisations de la société civile* (index : ACT 30/9647/2019).

[20] Amnesty International, "False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan" (blog, 9 mars 2017).

[21] Amnesty International, "*We Will Find You Anywhere" : The Global Shadow of Uzbekistani Surveillance* (index : EUR 62/5974/2017).

[22] Amnesty International, *Défenseurs des droits humains menacés. Un espace de plus en plus restreint pour la société civile* (index : ACT 30/6011/2017).

3. ÉTUDE DE CAS : CYBERATTAQUES CONTRE LA DÉFENSEURE DES DROITS HUMAINS PAKISTANAISE DIEP SAEEDA

> **« Désormais, à chaque fois que j'ouvre un courriel, j'ai peur. À tel point que je ne suis même plus capable de faire mon travail – et mon travail social en souffre. »**
>
> Diep Saeeda[23]

En 2018, Diep Saeeda, défenseure des droits humains bien connue au Pakistan, faisait activement campagne pour que la responsabilité de la disparition forcée de Raza Khan, un autre défenseur pakistanais, soit établie. Elle a alors été ciblée par une cyberattaque concertée. Sur Facebook, une utilisatrice qui s'est fait passer pour une Afghane du nom de Sana Halimi, habitant à Dubaï et travaillant pour l'ONU, l'a contactée à plusieurs reprises via Messenger, assurant qu'elle avait des informations sur Raza Khan. La personne gérant le profil a envoyé à Diep Saeeda des liens vers des fichiers contenant un logiciel malveillant, StealthAgent. Si elle avait ouvert ces fichiers, le logiciel aurait infecté ses appareils mobiles.

[23] Amnesty International, *Pakistan: Human Rights Under Surveillance* (index : ASA 33/8366/2018).

Le profil, qui selon Amnesty International était un faux, a aussi été utilisé pour la piéger afin qu'elle divulgue son adresse électronique, sur laquelle elle a commencé à recevoir des courriels infectés par un logiciel espion fonctionnant sous Windows, connu sous le nom de « Crimson RAT ».

Diep Saeeda a aussi reçu des courriels émanant prétendument du bureau du Premier ministre de la province du Pendjab, qui contenaient de fausses informations quant à une réunion entre le ministère provincial de l'Éducation et l'organisation de Diep, l'Institut pour la paix et les études séculières. Dans d'autres cas, les hackers se sont fait passer pour des étudiants demandant des conseils. Amnesty International a pu établir que d'autres défenseurs des droits humains avaient été pris pour cible de manière similaire au Pakistan.

Du fait de cette cyberattaque, il est devenu difficile pour Diep Saeeda d'exercer son travail et la défenseure vit dans la peur. Elle a commencé à se méfier des courriels et pièces jointes qu'elle reçoit, même lorsqu'ils proviennent de membres de sa propre famille, car elle craint que quelqu'un se fasse passer pour eux.

4. LE SECTEUR PRIVÉ DE LA SURVEILLANCE NUMÉRIQUE

Un certain nombre d'États achètent des outils de surveillance numérique – notamment des logiciels espions – à des sociétés commerciales. Ils les utilisent ensuite pour suivre, contrôler et intimider des défenseurs des droits humains et d'autres personnes qui expriment des opinions divergentes. Les États comme les entreprises qui leur vendent ces technologies affirment que celles-ci ne sont employées qu'à des fins licites, par exemple pour repérer et surveiller des terroristes ou des criminels. Les éléments de plus en plus nombreux qui attestent de leur utilisation abusive brossent toutefois un tout autre portrait de la situation. Des organisations de la société civile, dont Amnesty International, ont découvert que des campagnes avaient été menées contre des personnes qui défendent les droits humains à l'aide de technologies commercialisées par ces sociétés de surveillance.

Contrairement à ceux produits par des États, les logiciels espions commerciaux sont relativement nouveaux, mais ils sont tout aussi invasifs et perfectionnés[24]. NSO Group, en **Israël** et au **Luxembourg**[25] et Finfisher au **Royaume-Uni** et en **Allemagne**[26] ne sont que deux des principaux acteurs de ce secteur extrêmement discret et fort rentable.

D'après Citizen Lab, NSO Group semble être à l'origine de ciblages à des fins de surveillance dans au moins 45 pays[27]. En juin 2018, un membre du personnel d'Amnesty International a reçu un message WhatsApp malveillant contenant un message lié à l'**Arabie saoudite** visant à l'inciter à cliquer sur des liens qui auraient pu installer un logiciel espion conçu par NSO Group sur son portable[28]. Nombre des pays qui ont acheté des technologies de surveillance à ces entreprises ont un bilan désastreux en matière de droits humains. Un

[24] Just Security, "CTRL+HALT+Defeat: State-sponsored Surveillance and the suppression of Dissent", par Julie Bloch, Sukti Dhital, Rashmika Nedungadi et Nikki Reisch, 15 mai 2019, www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/.
[25] Centre de Ressources sur les Entreprises et les Droits de l'Homme, "Amnesty backs legal action against Israel firm NSO group over spyware used against human rights defenders", mai 2019, www.business-humanrights.org/en/amnesty-backs-legal-action-against-israeli-firm-nso-group-over-spyware-use-against-human-rights-defenders.
[26] Amnesty International, "New tool for spy victims to detect government surveillance" (nouvelles, 20 novembre 2014).
[27] Citizen Lab, "HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", septembre 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[28] Amnesty International, *"Amnesty International among targets of NSO-powered campaign"*, 1er août 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

logiciel de NSO Group a par exemple été utilisé contre des défenseurs des droits humains au **Maroc**[29], au **Mexique, en Arabie saoudite** et aux **Émirats arabes unis**[30]**.**

En vertu des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, les sociétés comme NSO Group sont tenues de faire preuve de la diligence requise pour éviter que l'utilisation de leurs produits porte atteinte aux droits humains, et elles doivent limiter et réparer ces atteintes lorsqu'elles se produisent.[31] Les États ont quant à eux l'obligation d'empêcher les entités privées de porter atteinte aux droits humains, que ce soit à l'intérieur de leurs frontières ou à l'extérieur.

Il est particulièrement difficile d'amener ces entreprises à rendre des comptes, car elles s'entourent du plus grand secret. Très souvent, elles se cachent derrière des « raisons de sécurité » ou des « clauses de confidentialité » pour ne rendre publique aucune information relative à leurs activités. On sait peu de choses sur ces entreprises ou leur structure. Nombre d'entre elles ne révèlent aucune donnée relative à leurs contrats de licence d'exportation, et leurs dispositions en matière de diligence requise relative aux droits humains et de réparation des atteintes sont soit inexistantes soit totalement insuffisantes. À cela s'ajoute l'absence de contrôle réglementaire et d'encadrement solide de l'octroi de licences d'exportation à l'échelle nationale et internationale, qui fait qu'il est encore plus difficile de s'attaquer à ce secteur.

Des instruments comme l'Arrangement de Wassenaar, un accord multilatéral sur le contrôle des exportations, ont par exemple été mis en place pour harmoniser les règles d'exportation entre les États signataires en ce qui concerne les articles militaires et les biens et technologies à double usage contribuant aux capacités militaires[32]. Cet arrangement peut être utile, mais il n'est pas conçu pour limiter les problèmes relatifs aux droits humains.

Certains régimes nationaux de licence d'exportation, comme celui d'Israël[33], sont connus pour accorder des licences d'exportation en dépit des risques qu'elles posent pour les droits fondamentaux, car les considérations stratégiques ont souvent plus de poids que les inquiétudes en matière de droits humains. L'Union européenne dispose d'un cadre de protection des droits humains plus clair, mais cela n'empêche pas les États membres de continuer à accorder des licences pour des technologies de surveillance pouvant porter atteinte aux droits humains ou dont des éléments attestent que de telles atteintes ont déjà été causées par leur utilisation, ce qui devrait pourtant conduire à un refus de licence[34]. Les dispositions relatives à la confidentialité nuisent en outre à la capacité des entreprises à respecter les obligations qui leur incombent en matière de droits humains dans d'autres territoires.

---

[29] Amnesty International, « Maroc. Des défenseurs des droits humains ciblés par un logiciel espion de NSO Group », 2019, https://www.amnesty.org/fr/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/.
[30] Citizen Lab, "HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", septembre 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[31] Principes directeurs relatifs aux entreprises et aux droits de l'homme, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf.
[32] https://www.wassenaar.org/fr/about-us/.
[33] Amnesty International, *Amnesty International affidavit in support of Israeli petition* (index : ACT 10/0332/2019) et « Israël. Amnesty International engage une action judiciaire pour mettre fin au système de surveillance créé par NSO Group » (nouvelles, 13 mai 2019).
[34] Amnesty International, « Union européenne. Des États font pression pour obtenir un assouplissement des règles sur l'exportation d'équipements de surveillance vers des pays portant atteinte aux droits humains » (nouvelles, 11 juin 2018).

Il en résulte un vide juridique et réglementaire qui permet de vendre et de transférer des technologies de surveillance numérique sans disposer de garanties suffisantes. Plus longtemps ces entreprises et les États qui leur achètent ces technologies échapperont aux contrôles, plus les possibilités d'opposition et de défense des droits humains se réduiront dangereusement. Il est urgent de mettre fin à ces tentatives de surveillance menées par des États qui utilisent en toute illégalité des outils de surveillance produits par des entreprises privées pour cibler les personnes qui militent pour les droits humains.

5. OBLIGATIONS DES ÉTATS ET DES ENTREPRISES EN MATIERE DE DROITS HUMAINS

Un certain nombre d'instruments internationaux, régionaux et nationaux énoncent l'obligation de respecter et de protéger les défenseurs des droits humains. Les États ont l'obligation de veiller au respect de ces normes afin de garantir un environnement sûr et favorable permettant aux défenseurs des droits humains de travailler librement, sans avoir à craindre les attaques, et de mener à bien leurs activités essentielles de protection et de promotion de tous les droits humains[35].

La **Déclaration des Nations unies sur les défenseurs des droits de l'homme**[36] (1998) s'appuie sur les instruments internationaux juridiquement contraignants déjà existants. Elle réaffirme le droit de défendre les droits humains et expose les obligations des États concernant le rôle et la situation spécifiques des défenseurs des droits humains. Elle énonce les responsabilités et les devoirs qui en découlent pour les États et affirme clairement que c'est à eux que revient la responsabilité ultime de protéger les personnes qui défendent les droits humains, d'empêcher les atteintes à leurs droits fondamentaux, de traiter efficacement les accusations de telles atteintes et de veiller à ce que ces personnes puissent mener à bien leur travail dans un environnement sûr et favorable. Par ailleurs, elle souligne que les défenseurs des droits humains sont indispensables pour faire des droits humains une réalité et pour élaborer de nouveaux principes et idées dans le domaine des droits humains, pour en discuter et pour en promouvoir la reconnaissance.

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. Les

[35] Amnesty International, *Amnesty International Comments on the European Commission Dual-Use Export Proposal* (index : POL 10/1558/2017).
[36] Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus, 1998, doc. ONU A/RES/53/144.

États ont ainsi l'obligation de réguler la conduite des acteurs non étatiques qui se trouvent sous leur autorité, afin de les empêcher de causer des atteintes aux droits humains ou d'y contribuer, même dans d'autres pays.

Comme l'indiquent les **Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme**[37], 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 de la capacité et de la volonté des États de respecter 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 relatifs aux entreprises et aux droits de l'homme précise que l'on peut considérer qu'une entreprise contribue 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[38]. »

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 relativement 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. Ce groupe d'experts a estimé que le lien pourrait s'établir relativement facilement en droit si la conduite de l'entreprise permettait, aggravait ou facilitait ces atteintes aux droits humains et si celle-ci savait, ou aurait raisonnablement dû savoir, que de telles atteintes seraient perpétrées. Il a surtout précisé qu'une entreprise pouvait permettre, aggraver ou faciliter des atteintes aux droits humains notamment par la fourniture de biens ou de services[39].

[37] Principes directeurs relatifs aux entreprises et aux droits de l'homme, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf.

[38] HCDH, *La responsabilité des entreprises de respecter les droits de l'homme : Guide interprétatif*, 2012, p. 19, https://www.ohchr.org/Documents/Publications/HR_PUB_12_2_fr.pdf.

[39] Commission internationale de juristes, *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 2008, www.icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes/.

6. RECOMMANDATIONS

> **« Les États devraient imposer un moratoire immédiat sur l'exportation, la vente, le transfert, l'utilisation et la maintenance des technologies de surveillance conçues par le secteur privé et le lever uniquement lorsqu'un régime de garanties conforme aux droits de l'homme aura été établi. »**
>
> David Kaye, rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression[40]

C'est aux États que revient la responsabilité ultime de protéger les défenseurs des droits humains, d'empêcher les atteintes à leurs droits fondamentaux ou à leurs activités, de traiter efficacement les accusations de telles atteintes et de veiller à ce que ces personnes puissent mener à bien leur travail dans un environnement sûr et favorable. Beaucoup reste à faire pour reconnaître et protéger toutes celles et tous ceux qui dénoncent et combattent l'injustice et pour les protéger contre la surveillance numérique ciblée.

6.1 RECOMMANDATIONS AUX ÉTATS

Amnesty International exhorte tous les États à :

- mettre en place un moratoire sur la vente et le transfert d'équipements de surveillance jusqu'à ce qu'un cadre réglementaire approprié en matière de droits humains soit mis en œuvre ;
- informer sur les contrats qui ont été, sont ou seront passés avec des sociétés privées de surveillance, soit en répondant aux demandes d'informations, soit de leur propre initiative ;
- refuser de délivrer des autorisations d'exportation lorsqu'il existe un risque substantiel que le produit en question soit utilisé pour porter atteinte aux droits humains, soit par une surveillance illégale, soit lorsque le pays de destination ne dispose pas de garanties juridiques, procédurales et techniques suffisantes pour prévenir les atteintes aux droits humains ;

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

- veiller à ce que toutes les technologies concernées soient minutieusement examinées avant transfert ;
- faire preuve de transparence en ce qui concerne le volume, la nature, la valeur et la destination des transferts de technologies de surveillance ;
- faire en sorte que les outils de chiffrement et les outils de sécurité numérique légitimes ne soient pas soumis à des contrôles à l'exportation ;
- mettre en œuvre des lois nationales imposant des limites à la surveillance numérique, en veillant à ce que :
    - la surveillance soit soumise à des lois précises et accessibles au public ;
    - la surveillance ne cible que certaines personnes, sur autorisation d'un organe judiciaire compétent, indépendant et impartial et que des limites de temps, de manière, de lieu et de portée de la surveillance soient imposées ;
    - la surveillance numérique autorisée soit soumise à la tenue de registres détaillés, dûment mandatée conformément aux procédures judiciaires applicables, et que les cibles en soient informées dès que cela s'avère possible sans compromettre l'objectif de la surveillance ;
- veiller à ce que toute surveillance numérique soit soumise à des mécanismes de contrôle public, notamment :
    - un processus d'approbation ;
    - la notification et la consultation de la population avant tout nouvel achat de technologies de surveillance ;
    - des comptes rendus publics réguliers ;
- mettre en place des mécanismes appropriés permettant de demander réparation devant les tribunaux nationaux en cas de surveillance numérique ciblée illégale ou abusive.

6.2 RECOMMANDATIONS AUX ENTREPRISES

Amnesty International exhorte les entreprises à :

- s'engager publiquement à respecter les droits humains, ainsi que le travail et la sécurité des personnes qui défendent ces droits ;
- mettre en œuvre des procédures leur permettant de faire preuve de la diligence requise en ce qui concerne les droits humains, conformément aux instruments internationaux relatifs à la responsabilité des entreprises en matière de droits humains, tels que 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 à l'intention des entreprises multinationales, afin que leurs activités et celles de leurs filiales, sous-traitants et fournisseurs respectent les droits des défenseurs des droits humains et ne gênent pas leur travail légitime ;
- procéder à une évaluation rigoureuse des risques en matière de droits humains pour tous les transferts proposés, conformément à leur responsabilité de diligence raisonnable. Cette évaluation doit ensuite être soumise à l'examen des autorités de contrôle des exportations et rendue publique ;
- veiller à la transparence des ventes et des contrats ;
- consulter les détenteurs de droits avant de signer des contrats dans leur pays ;
- mettre en œuvre des protections contractuelles contre les atteintes aux droits humains ;
- faire des choix en matière de conception et d'ingénierie qui intègrent les normes relatives aux droits humains ;
- veiller à ce que les processus de vérification soient soumis à des audits réguliers, dont les résultats doivent être rendus publics ;

- disposer de mécanismes de réclamation et d'un processus de notification approprié pour signaler les utilisations abusives de leurs technologies ;
- mettre en œuvre de solides mécanismes d'indemnisation des cibles de surveillance illégale ou d'autres formes de réparation.

6.3 RECOMMANDATIONS AUX INVESTISSEURS

Amnesty International demande à tous les investisseurs de :

- veiller à ne pas contribuer aux violations des droits humains par la détention de participations dans des sociétés de surveillance. Les investisseurs doivent pour cela exiger aux sociétés de surveillance d'appliquer une transparence rigoureuse et la diligence requise en matière de droits humains ;
- communiquer les recommandations susmentionnées pertinentes aux sociétés de surveillance dont ils détiennent des participations et demander qu'elles soient appliquées.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DÉFENSE DES DROITS HUMAINS. LORSQU'UNE PERSONNE EST VICTIME D'UNE INJUSTICE, NOUS SOMMES TOUS CONCERNÉS.

NOUS CONTACTER

info@amnesty.org

+44 (0)20 7413 5500

PRENEZ PART A LA CONVERSATION

www.facebook.com/AmnestyGlobal

@Amnesty