Nations Unies A/HRC/41/35

Assemblée générale

Distr. générale
28 mai 2019
Français
Original : anglais

**Conseil des droits de l'homme**
**Quarante et unième session**
24 juin-12 juillet 2019
Point 3 de l'ordre du jour
**Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement**

# Surveillance et droits de l'homme

## Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*

*Résumé*

Il est établi que la surveillance des personnes privées − en particulier les journalistes, les militants, les personnalités de l'opposition, les critiques du gouvernement et les autres personnes exerçant leur droit à la liberté d'expression − conduit à la détention arbitraire, voire à la torture ou encore aux exécutions extrajudiciaires. L'insuffisance des contrôles exercés sur les exportations et les transferts de technologies vers des États connus pour leurs politiques répressives a permis à ce phénomène de se développer. Dans le présent rapport, le Rapporteur spécial commence par exposer le problème que pose la surveillance ciblée eu égard aux obligations qui incombent aux États en vertu du droit des droits de l'homme et aux responsabilités des entreprises en la matière. Il propose ensuite l'adoption d'un cadre juridique et stratégique permettant de réglementer le secteur privé de la surveillance de sorte que les entreprises respectent les principes de responsabilité et de transparence. Enfin, il recommande de réglementer plus strictement l'exportation et l'utilisation des technologies de surveillance et d'appliquer un moratoire immédiat sur la vente et le transfert internationaux des technologies du secteur privé de la surveillance jusqu'à ce que des mesures solides soient adoptées pour garantir que les États et les autres acteurs utilisent ces technologies en toute légitimité et dans le respect des droits de l'homme.

* Le présent rapport est soumis après la date prévue pour que l'information la plus récente puisse y figurer.

GE.19-08652 (F) 210619 240619

*1908652*

# Table des matières


| | | *Page* |
|---|---|---|
| I. | Introduction | 3 |
| II. | Les États et le secteur privé de la surveillance | 3 |
| III. | Cadre juridique | 8 |
| IV. | Cadre pour la protection des droits fondamentaux contre la surveillance ciblée | 15 |
| V. | Recommandations | 22 |

# I. Introduction

1. L'Assemblée générale a condamné la surveillance et l'interception illicites ou arbitraires des communications, estimant que, compte tenu de leur « caractère éminemment intrusif », elles portaient atteinte aux droits de l'homme fondamentaux (voir les résolutions 68/167 et 71/199). Pourtant, la surveillance illicite continue sans qu'il y soit manifestement fait obstacle. Selon les communications soumises dans le cadre de l'élaboration du présent rapport, de nombreux États utilisent des logiciels de surveillance dont la conception, la commercialisation et la maintenance sont assurées par des entreprises privées. Or, il est établi que la surveillance des personnes privées − en particulier les journalistes, les militants, les personnalités de l'opposition, les critiques des gouvernements et les autres personnes exerçant leur droit à la liberté d'expression − conduit à la détention arbitraire, voire à la torture ou encore aux exécutions extrajudiciaires. Cette surveillance est facilitée par le fait que les exportations et les transferts de technologies vers des États connus pour leurs politiques répressives ne sont pas suffisamment contrôlés. Le marché des technologies de surveillance étant très secret, c'est principalement grâce aux travaux de criminalistique numérique effectués par des chercheurs du secteur privé et aux investigations menées par les organisations de la société civile et les médias que le problème est connu.

2. La gravité de la situation a conduit le Rapporteur spécial à conclure le présent rapport en recommandant non seulement une plus stricte réglementation de l'exportation et de l'utilisation des technologies de surveillance, mais aussi l'application d'un moratoire immédiat sur la vente et le transfert internationaux des technologies du secteur privé jusqu'à ce que des mesures solides soient adoptées pour garantir que les États et les autres acteurs utilisent ces technologies en toute légitimité et dans le respect des droits de l'homme.

3. Le Rapporteur spécial propose l'adoption d'un cadre juridique et stratégique permettant de réglementer le secteur privé de la surveillance et de faire en sorte que les principes de responsabilité et de transparence y soient respectés. Il commence par définir le problème, précisant que ses travaux portent sur la surveillance ciblée et non sur l'interception, la collecte et la conservation à grande échelle de données privées (souvent appelée « surveillance de masse »). Ensuite, il donne un aperçu des obligations mises à la charge des États par le droit des droits de l'homme et des responsabilités qui incombent aux entreprises. Dans la quatrième partie, il propose des mesures visant à améliorer la législation et les politiques existantes pour qu'elles protègent les droits à la liberté d'opinion et d'expression garantis par le droit international des droits de l'homme. Enfin, en conclusion, il formule des recommandations à l'intention des principaux intéressés.

4. Le présent rapport a été élaboré grâce aux renseignements fournis par 11 États parties et 33 organisations de la société civile. En décembre 2018, le Haut-Commissariat aux droits de l'homme a organisé à Bangkok deux journées de consultations avec des experts. Les débats qui ont eu lieu et la documentation qui a été présentée à cette occasion sont résumés dans un additif au présent rapport[1].

# II. Les États et le secteur privé de la surveillance

5. À l'heure actuelle, les technologies de surveillance numérique sont facilement accessibles et aisément utilisables à mauvais escient, d'autant que leur utilisation est difficile à détecter. Dans son rapport phare de 2013 sur la surveillance, le précédent titulaire du mandat, Frank La Rue, a signalé que la faiblesse des cadres réglementaires avait créé un terrain propice aux violations arbitraires et illégales du droit à la vie privée et du droit à la liberté d'opinion et d'expression (A/HRC/23/40, par. 3). L'année suivante, dans son premier rapport sur le droit à la vie privée à l'ère du numérique, la Haute-Commissaire aux droits de l'homme a conclu que les pratiques de nombreux États indiquaient que les

[1] Je tiens à remercier tout particulièrement Amos Toh, Desiree Murray, Cristina Butoiu, Matthew Marcoly et Kyoolee Park de l'International Justice Clinic de la faculté de droit d'Irvine de l'Université de Californie pour m'avoir aidé à élaborer le présent rapport et son additif.

législations nationales n'étaient pas suffisamment étoffées ou suffisamment respectées et que les garanties procédurales étaient insuffisantes et les contrôles inefficaces, autant de facteurs qui permettaient à ceux qui menaient des activités de surveillance numérique illicite de ne pas avoir à rendre compte de leurs actes (A/HRC/27/37, par. 47).

6. Certains États utilisent des technologies de surveillance ciblée conçues par leurs propres services, d'autres adaptent des logiciels criminels, et d'autres encore acquièrent des logiciels espions sophistiqués sur le marché international de la surveillance[2]. Dans le présent rapport, le Rapporteur spécial s'intéresse principalement à cette dernière catégorie. La 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. Selon Privacy International, en 2016, plus de 500 entreprises concevant des technologies de surveillance vendaient leurs produits à des États[3].

## Types de surveillance visés par le présent rapport

7. Dans le présent rapport, le Rapporteur spécial s'intéresse principalement aux outils permettant d'accéder clandestinement aux informations numériques telles que les communications, les recherches et travaux effectués, l'historique de navigation, l'historique des positions et les activités en ligne et hors ligne. Les principales techniques et pratiques de surveillance ciblée sont décrites ci-après.

### Intrusion dans les ordinateurs

8. Les technologies de surveillance peuvent permettre à des intrus d'accéder à un ordinateur ou à un réseau tiers. Les intrusions peuvent atteindre des proportions considérables[4]. En 2017, par exemple, une cour d'appel des États-Unis d'Amérique a été saisie d'une affaire de surveillance menée sur le sol américain à l'initiative d'un État étranger[5]. Un citoyen des États-Unis né en Éthiopie et vivant dans le Maryland avait fourni une assistance technique à des membres de la diaspora éthiopienne. Un document initialement envoyé à un militant par des agents du Gouvernement éthiopien avait infecté son ordinateur avec un type de logiciel malveillant intrusif appelé FinSpy, commercialisé par la société germano-britannique Gamma Group[6]. FinSpy aurait enregistré les appels vidéo, les courriels et d'autres communications échangés entre l'intéressé et sa famille, notamment en enregistrant les touches sur lesquelles il frappait, et aurait envoyé ces données à des serveurs situés en Éthiopie[7].

### Piratage des appareils mobiles

9. Les produits de surveillance commercialisés par les entreprises privées permettent aussi de pirater directement les appareils mobiles. Le logiciel espion Pegasus, conçu par la société NSO Group, aurait été utilisé au Mexique d'une manière qui illustre bien le problème. Dès 2015, plusieurs personnes qui dénonçaient la corruption et le trafic de drogues ont reçu des liens par SMS ou par courriel. Certains messages semblaient provenir de sources dignes de confiance bien informées sur le destinataire. Des journalistes, des personnalités politiques, des enquêteurs de l'Organisation des Nations Unies, des

[2] Citizen Lab, *Communities @ Risk : Targeted Digital Threats Against Civil Society* (Toronto, Monk School of Global Affair, Université de Toronto, 2014), résumé, p. 8 à 11.

[3] Communication de Privacy International, p. 1.

[4] Voir, par exemple, Ronald J. Deibert, *Black Code : Inside the Battle for Cyberspace* (Toronto, Signal, 2013), p. 186 à 190.

[5] *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (Cour d'appel du district de Columbia, 2017).

[6] Pour voir des supports promotionnels de FinSpy, voir WikiLeaks, "The spy files : remote monitoring and infection solutions : FINSPY".

[7] Pour davantage de détails sur ces allégations, voir *first amended complaint, Doe v. Federal Democratic Republic of Ethiopia* (18 juillet 2014).

défenseurs des droits de l'homme et d'autres personnes ont été visés. Une organisation de recherche et de sensibilisation canadienne, Citizen Lab, a découvert que les liens avaient infecté les appareils avec le logiciel espion Pegasus, qui permet de surveiller une cible à distance. Citizen Lab a découvert que Pegasus était utilisé comme outil de surveillance dans 45 pays, dont l'Arabie saoudite, Bahreïn, les États-Unis, le Royaume-Uni et le Togo[8].

**Ingénierie sociale**

10. Nombre des technologies susmentionnées s'accompagnent de stratégies destinées à manipuler la cible pour qu'elle télécharge à son insu un logiciel malveillant, par exemple en lui faisant croire que le courriel contenant le lien malveillant provient d'un de ses contacts ou qu'elle clique sur un lien sûr qui concerne son travail, ses activités de militant ou sa vie privée. Un membre du personnel d'Amnesty International a ainsi reçu un message WhatsApp dans lequel il lui était demandé de couvrir une manifestation et qui contenait un lien vers des « informations supplémentaires ». Selon des chercheurs, si l'intéressé avait cliqué sur ce lien, il aurait probablement installé le logiciel espion Pegasus sur son portable[9].

**Surveillance des réseaux**

11. La surveillance ciblée peut aussi être exercée grâce à des programmes installés sur un réseau. Par exemple, le système russe SORM (« système pour activités d'enquêtes opératoires ») permet d'intercepter les communications grâce à un appareil installé sur les réseaux de télécommunications. Ce système, conçu et commercialisé par une entreprise privée, est largement utilisé en Fédération de Russie et ailleurs en Asie centrale. La société Protei fabrique du matériel grâce auquel les outils qui permettent d'écouter les appels téléphoniques et d'intercepter les communications sur Internet fonctionnent dans des pays tels que l'Ouzbékistan et le Kazakhstan[10].

**Reconnaissance faciale et reconnaissance des expressions faciales émotionnelles**

12. La reconnaissance faciale permet d'enregistrer les traits du visage d'une personne afin de la reconnaître, ce qui peut conduire à un profilage fondé sur l'appartenance ethnique ou raciale, l'origine nationale, le sexe ou d'autres caractéristiques qui sont dans bien des cas des motifs de discrimination illégale[11]. La reconnaissance des expressions faciales émotionnelles permet de reconnaître les sentiments, les émotions ou les intentions d'une personne à partir de ses expressions faciales en utilisant des techniques de classification très contestables[12]. La Chine est peut-être le pays qui illustre le mieux à quel point ces outils sont intrusifs. D'après des informations fiables, le Gouvernement chinois a installé dans l'ensemble du pays des caméras de surveillance qui fonctionnent avec un programme de reconnaissance faciale dans le but de surveiller les Ouïghours et de consigner leurs déplacements à des fins de recherche et de contrôle[13]. La plupart des technologies employées par le Gouvernement semblent être produites en Chine par des entreprises publiques et des entreprises privées[14].

**Intercepteurs d'identité internationale d'abonnement mobile (Stingray)**

13. Les intercepteurs d'identité internationale d'abonnement mobile simulent le fonctionnement d'une antenne-relais afin d'intercepter les communications et les données de localisation transmises par les appareils de communication personnels. Ils sont

[8] Voir Bill Marczak et autres, "Hide and seek : tracking NSO Group's Pegasus spyware to operations in 45 countries", Citizen Lab, 18 septembre 2018.

[9] Voir Bill Marczak, John Scott-Railton et Ron Deibert, "NSO Group infrastructure linked to targeting of Amnesty International and Saudi dissident", Citizen Lab, 31 juillet 2018.

[10] Andrei Soldatov et Irina Borogan, *The Red Web : The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York, PublicAffairs, 2015), p. 190 et 191.

[11] Voir, par exemple, la communication de Internet Lab, p. 6 ; et celle du Center for Internet and Society, p. 12.

[12] AI Now Institute, *AI Now Report 2018* (New York, New York University, 2018), p. 13 et 14.

[13] Voir Paul Mozur, "One month, 500,000 face scans : how China is using A.I. to profile a minority", *New York Times*, 14 avril 2019.

[14] Communication de Human Rights in China, 2016, p. 2 et 3. Voir aussi A/HRC/39/29, par. 14.

largement utilisés dans le monde entier, surtout par les forces de l'ordre et les services de renseignements. Une entreprise privée du Royaume-Uni aurait vendu ce type d'intercepteurs aux Philippines, ainsi que des logiciels espions, et beaucoup craignent que ces appareils aient servi à identifier et à surveiller les consommateurs de drogues dans le cadre de la guerre contre la drogue menée par le Gouvernement, qui a été très critiquée[15].

**Contrôle approfondi des paquets**

14. Le contrôle approfondi des paquets permet la surveillance, l'analyse et la redirection des flux des réseaux Internet et des autres réseaux de communications. Il peut aussi servir à rediriger des utilisateurs vers des sites infectés par des logiciels malveillants et à les empêcher d'accéder à certains sites Web. Des dispositifs de contrôle de ce type auraient été installés sur le réseau Türk Telekom pour que les utilisateurs se trouvant en Turquie et en République arabe syrienne qui tentaient de télécharger des applications légitimes soient redirigés vers des logiciels espions[16].

## Coopération entre le secteur public et le secteur privé

15. Le secteur public et le secteur privé collaborent étroitement en ce qui concerne les outils de surveillance numérique. Il arrive que les États aient des exigences auxquelles les services et organismes publics ne peuvent pas répondre tandis que des entreprises privées disposent de l'expertise et des ressources nécessaires pour le faire et y aient tout intérêt. Des salons professionnels régionaux ou internationaux fonctionnant comme des services de rencontre réunissent les acteurs des différents secteurs[17], à charge pour eux de décider s'ils veulent collaborer ou non. Il reste à savoir si les entreprises prennent les précautions qui s'imposent pour vérifier le bilan de leurs clients en matière de droits de l'homme.

16. Les intentions des vendeurs peuvent être légitimes. Il se peut qu'une entreprise croit en toute bonne foi que ses produits sont utilisés par les pouvoirs publics avec l'autorisation de l'appareil judiciaire ou d'acteurs indépendants pour intercepter légalement les communications de cibles légitimes. Toutefois, on ne peut l'affirmer avec certitude étant donné que le contrôle et la transparence sont généralement insuffisants à toutes les étapes de la collaboration, que ce soit avant, pendant ou après la vente. En fait, presque toutes les informations disponibles sur le secteur privé de la surveillance proviennent de recherches menées par des organisations non gouvernementales ou des établissements universitaires, comme Citizen Lab, et de reportages d'investigation[18].

17. Le fonctionnement du « marché des vulnérabilités » est particulièrement opaque. Il est de notoriété publique que les États et les acteurs du secteur privé achètent à des experts en sécurité informatique des informations sur les vulnérabilités des logiciels courants dans l'objectif de mener des « exploits zero day » afin d'accéder aux appareils et aux communications de particuliers[19]. Tant que le fabricant du logiciel ou de l'appareil n'a pas connaissance de telle ou telle vulnérabilité, celle-ci peut être utilisée à des fins de surveillance. La non-divulgation d'une vulnérabilité par un État ou une entreprise met donc en danger les utilisateurs finaux, y compris les États et les clients du secteur privé qui stockent des données sensibles concernant plusieurs domaines (finance, santé, emploi, police et justice) dans des bases de données commerciales. À ce jour, la question de savoir

[15] Voir Sofia Tomacruz, "You think your data, communication devices are safe? Think again", Rappler, 17 mars 2018.

[16] Voir Bill Marczak et autres, "Bad traffic : Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?", Citizen Lab, 9 mars 2018.

[17] Voir, par exemple, www.issworldtraining.com ; et Patrick Howell O'Neill, "ISS World : the traveling spyware roadshow for dictatorships and democracies", Cyberscoop, 20 juin 2017.

[18] Les recherches sur la surveillance privée font ressortir l'importance de la liberté et de l'indépendance des médias et des chercheurs. En effet, leurs auteurs se sont eux-mêmes exposés à la surveillance. Voir, par exemple, Raphael Satter, "Undercover agents target cybersecurity watchdog", Associated Press, 26 janvier 2019.

[19] Voir Privacy International, "Exploiting privacy : surveillance companies pushing zero-day exploits", 7 février 2018.

si les États et les entreprises ont la responsabilité de divulguer les vulnérabilités qu'ils ont découvertes ne fait pas consensus et la vente d'informations sur les vulnérabilités n'est pas réglementée. Outre qu'elle a stimulé le marché des vulnérabilités, cette situation a incité nombre d'États et d'entreprises à garder jalousement pour eux les vulnérabilités qu'ils ont découvertes dans l'espoir de pouvoir les utiliser pour mener des attaques informatiques[20].

18. La collaboration entre le secteur public et le secteur privé ne prend certainement pas fin avec la vente ou le transfert du produit. Selon des documents divulgués par des sources secrètes, les entreprises de surveillance privées assurent un service après-vente. En 2014, par exemple, FinFisher aurait conclu avec des clients étatiques des contrats annuels de maintenance dans le cadre desquels elle s'engageait à fournir des mises à niveau techniques et des mises à jour de produits, ainsi que d'autres services après-vente[21]. En outre, les entreprises dispensent des formations pour apprendre aux clients comment tirer le meilleur parti de leurs logiciels malveillants pour pirater les communications, les ordinateurs et les réseaux wi-fi de leurs cibles[22].

19. Les entreprises entretiennent des relations étroites non seulement avec leurs clients, mais aussi avec les gouvernements des pays dans lesquels elles sont basées. Certaines ont une influence considérable sur la réglementation nationale du contrôle des exportations et ont sapé les efforts visant à renforcer ces contrôles. Ainsi, selon des informations crédibles, en 2016, l'influence exercée par les groupes de pression a conduit à ce que certains types de technologies de surveillance ne soient finalement pas ajoutés à la liste des biens et technologies à double usage soumis à un contrôle à l'exportation par l'Union européenne[23]. Au cours de récentes négociations sur la réglementation du contrôle des exportations de l'Union, des intérêts commerciaux auraient pesé sur la décision de restreindre considérablement les garanties en matière de droits de l'homme qu'il était prévu d'introduire dans la réglementation et dont l'adoption avait pourtant recueilli une large adhésion au Parlement européen.[24]

20. Par ailleurs, selon de récentes informations, de nombreux experts ayant une solide expérience dans les domaines du renseignement ou de l'application des lois passent du secteur public au secteur privé, et inversement. À cause de ces « vases communicants », il se peut que d'anciens experts du secteur public travaillent pour des acteurs du secteur privé dont les produits sont utilisés pour commettre des violations des droits de l'homme[25]. Dans un rapport de 2019, Reuters a révélé que plusieurs anciens employés de l'Agence nationale de sécurité des États-Unis avaient été recrutés par une entreprise privée pour développer des programmes d'interception des communications dans le cadre d'un projet mené par les Émirats arabes unis connu sous le nom de code « Project Raven »[26]. Ces personnes auraient utilisé leurs connaissances pour surveiller des opposants au Gouvernement des Émirats arabes unis et s'en prendre à des citoyens des États-Unis. Dans bon nombre de pays, voire dans la plupart d'entre eux, la législation est muette ou presque à ce sujet.

[20] Voir l'analyse figurant dans la communication de Sarah McKune, p. 2 à 4 ; Centre d'études des politiques européennes, *Software Vulnerability Disclosure in Europe : Technology, Policies and Legal Challenges* (Bruxelles, juin 2018) ; et Sven Herpig et Ari Schwartz, "The future of vulnerabilities equities processes around the world", Lawfare, 4 janvier 2019.

[21] Voir Privacy International, "Six things we know from the latest FinFisher documents", 15 août 2014.

[22] Ibid.

[23] Voir Reporters sans frontières International, "International regulations : broken or blocked by lobbies", 14 mars 2017.

[24] Voir Daniel Moßbrucker, "Surveillance exports : how EU Member States are compromising new human rights standards", netzpolitik.org, 29 octobre 2018.

[25] Voir Privacy International, "Switching hats : why South Africa's surveillance industry needs scrutiny", 14 décembre 2016 ; et Alex Kane, "How Israel became a hub for surveillance technology", The Intercept, 17 octobre 2016.

[26] Voir Christopher Bing et Joel Schectman, "Inside the UAE's secret hacking team of American mercenaries", Reuters, 30 janvier 2019 ; Robert Chesney, "Project Raven : what happens when U.S. personnel serve a foreign intelligence agency", Lawfare, 11 février 2019 ; et la communication de Sarah McKune, p. 7 et 8.

# III. Cadre juridique

## A. Obligations des États

21. Que les activités de surveillance aboutissent ou non, le droit à la vie privée et à la liberté d'opinion et d'expression des personnes visées est bafoué[27]. Même si ces personnes n'ont pas connaissance de l'immixtion ou de la tentative d'immixtion dans leur vie privée, leur droit à la vie privée est foulé aux pieds. Dans la pratique, les États s'efforcent généralement d'utiliser des technologies non détectables par leur cibles. Il faut toutefois retenir que l'immixtion participe d'un objectif plus large qui est d'agir sur la personne visée. La surveillance, ou tentative de surveillance, peut viser à atteindre des fins illicites comme bâillonner l'opposition, sanctionner les critiques ou punir ceux qui publient des informations non officielles (et leurs sources)[28]. Dans certains cas, les sanctions visent non la cible, mais son réseau de contacts. Dans les environnements où la surveillance illicite est chose courante, les groupes visés savent ou soupçonnent qu'ils font l'objet de tentatives de surveillance, ce qui restreint leur capacité à exercer leurs droits, notamment les droits à la liberté d'expression, d'association, de religion et de culture. Bref, l'immixtion dans la vie privée d'autrui au moyen d'une surveillance ciblée est conçue pour réprimer l'exercice du droit à la liberté d'expression.

22. Il n'est pas nécessaire de refaire le travail d'information approfondi fait par les précédents rapporteurs spéciaux, les titulaires d'autres mandats au titre des procédures spéciales, la Haute-Commissaire, le Conseil des droits de l'homme, le Comité des droits de l'homme et d'autres entités, qui ont déjà mis en lumière les principales caractéristiques du cadre juridique des droits de l'homme destiné à protéger les particuliers contre la surveillance ciblée, énoncées ci-après.

23. Premièrement, le droit à la vie privée et la liberté d'opinion et d'expression de toutes les personnes est consacré par le Pacte international relatif aux droits civils et politiques et la Déclaration universelle des droits de l'homme. Selon l'article 19 de ces deux instruments, nul ne peut être inquiété pour ses opinions et toute personne a le droit de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières et par tout moyen de son choix. En écho à l'article 12 de la Déclaration, le paragraphe 1 de l'article 17 du Pacte dispose que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance ».

24. À l'ère du numérique, droit à la vie privée et droit à la liberté d'expression sont étroitement liés, et le respect du premier est un préalable à l'exercice en toute sécurité du deuxième, ainsi que du droit à la liberté d'opinion (A/HRC/29/32, et A/HRC/23/40, par. 24). Les mesures constituant une immixtion dans la vie privée ne sont compatibles avec les dispositions de l'article 17 que si elles « sont autorisées par le droit interne, qui doit être accessible, précis et conforme aux prescriptions du Pacte », « poursuivent un but légitime » et « répondent à une nécessité et à la notion de proportionnalité » (A/69/397, par. 30). Il découle des dispositions de l'article 19 que les restrictions doivent obligatoirement remplir trois conditions, à savoir être fixées par la loi, être nécessaires au respect des droits ou de la réputation d'autrui, et être nécessaires à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques[29]. Le Comité des droits de l'homme a souligné que ces conditions signifiaient au minimum ce qui suit :

a) Les restrictions doivent être fixées par la loi : toute restriction doit être exprimée avec suffisamment de précision pour permettre aux personnes d'adapter leur comportement selon qu'il convient et doit être accessible pour le public. Les restrictions

[27] Voir la communication de la Global Justice Clinic de la Faculté de droit de New York University, p. 6.

[28] Voir la communication de la Human Rights Foundation.

[29] Les trois conditions fixées à l'article 19 sont exposées en détail dans l'observation générale n° 34 (2011) du Comité des droits de l'homme sur la liberté d'opinion et la liberté d'expression, par. 5 à 9 et 22 à 36, ainsi que dans le document paru sous la cote A/HRC/38/35.

doivent répondre à des critères précis et ne doivent pas avoir une portée trop large ni conférer des pouvoirs illimités aux agents de l'État[30] ;

b) Les restrictions doivent répondre aux principes de nécessité et de proportionnalité : l'État doit établir l'existence d'un lien direct et immédiat entre la liberté d'expression et la menace et démontrer que la restriction qu'il souhaite imposer est le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir la protection recherchée[31] ;

c) Les restrictions doivent être légitimes : selon les dispositions du paragraphe 3 de l'article 19, seuls certains motifs peuvent justifier l'imposition de restrictions. Si les États invoquent souvent la sécurité nationale pour justifier des restrictions, en particulier des mesures de surveillance ciblée, le Rapporteur spécial a estimé que ce motif devrait néanmoins être réservé aux cas dans lesquels l'intérêt de la nation tout entière est en jeu, ce qui exclurait donc les limitations instaurées au seul bénéfice d'un gouvernement, d'un régime ou d'un groupe d'influence (A/71/373, par. 18).

25. Le Comité des droits de l'homme a appliqué les principes susmentionnés dans les observations finales qu'il a formulées en 2017 à l'issue de l'examen du sixième rapport périodique soumis par l'Italie au titre du Pacte (CCPR/C/ITA/CO/6, par. 36). Il a estimé que le respect du droit à la vie privée supposait que de solides systèmes indépendants de contrôle des activités de surveillance, d'interception et de piratage soient établis, notamment que ces activités soient toujours soumises à l'autorisation du pouvoir judiciaire et que les victimes de surveillance abusive aient accès à une réparation effective et, si possible, qu'elles soient informées a posteriori qu'elles ont fait l'objet d'une surveillance ou que leurs données ont été piratées (ibid., par. 37). Dans sa résolution 73/179, l'Assemblée générale a fait écho aux conclusions du Comité, soulignant que la surveillance des communications numériques devait être conforme aux obligations internationales relatives aux droits de l'homme et s'inscrire dans un cadre juridique accessible à tous, clair, précis, complet et non discriminatoire.

26. Ces principes, qui valent pour tous les cas de surveillance ciblée, sont encore plus importants lorsque la liberté d'expression sert l'intérêt général. La surveillance ciblée incite à l'autocensure et limite directement les moyens dont disposent les journalistes et les défenseurs des droits de l'homme pour mener des enquêtes et établir des relations viables avec des sources (A/HRC/38/35/Add.2, par. 53). Le Comité a souligné que les restrictions énoncées au paragraphe 3 de l'article 19 ne pouvaient en aucun cas légitimer des mesures visant à faire taire ceux qui défendent la démocratie multipartite, les valeurs démocratiques et les droits de l'homme[32], ni justifier que l'on prenne une personne pour cible parce qu'elle a exercé sa liberté d'opinion ou d'expression[33]. Le Comité a également estimé qu'il importait de protéger les journalistes et les personnes qui recueillent et analysent des informations sur la situation des droits de l'homme ou ont publié des informations à ce sujet, y compris les juges et les avocats[34]. Dans ce contexte, il faut aussi que la loi protège la confidentialité des sources, comme l'ont souligné les mécanismes internationaux et régionaux (africains, européens et interaméricains) de défense des droits de l'homme (A/70/361, par. 5).

27. Outre qu'ils sont tenus au premier chef de ne pas s'immiscer dans la vie privée des particuliers et de ne pas restreindre l'exercice de la liberté d'expression, les États ont l'obligation de protéger les particuliers contre les ingérences de tiers. Aux termes de l'article 2 du Pacte international relatif aux droits civils et politiques, où sont énoncés les devoirs fondamentaux des États, ceux-ci doivent s'engager à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus dans cet instrument[35]. Aux termes du paragraphe 2 de l'article 17, toute personne

[30] Observation générale nº 34, par. 25.

[31] Ibid., par. 34 et 35.

[32] Observation générale nº 34, par. 23.

[33] Ibid.

[34] Ibid.

[35] Voir aussi l'observation générale nº 31 (2004) du Comité des droits de l'homme sur la nature de l'obligation juridique générale imposée aux États parties au Pacte. Selon cette observation générale,

a droit à la protection de la loi contre les immixtions illégales dans sa vie privée. Toutefois, il est difficile de déterminer si, de manière générale, les législations nationales protègent les personnes contre la surveillance ciblée. Par contre, il est certain qu'elles ne les protègent pas contre la surveillance transnationale, y compris la surveillance exercée sur leurs propres nationaux par des entités étrangères[36]. Après que des allégations de surveillance ciblée ont été formulées contre le Mexique, le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression et le Rapporteur spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme (CIDH) ont effectué une mission conjointe dans ce pays, à l'issue de laquelle ils ont soulevé la question de l'utilisation par le Gouvernement du logiciel espion Pegasus. Ils ont instamment prié les autorités mexicaines d'autoriser une enquête indépendante sur les allégations selon lesquelles ce logiciel avait été utilisé contre des journalistes (A/HRC/38/35/Add.2, par. 52 à 55). À ce jour, et bien que l'Institut national de la transparence, de l'accès à l'information publique et de la protection des données à caractère personnel ait demandé au Gouvernement de révéler la teneur des contrats conclus en vue de l'achat de Pegasus[37], l'enquête n'a pas permis de faire la lumière sur la situation.

28. Il ressort clairement des Principes directeurs relatifs aux entreprises et aux droits de l'homme concernant la mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, adoptés en 2011, que l'obligation de protéger incombant à l'État comprend celle de prendre les dispositions voulues pour prévenir les atteintes aux droits de l'homme de la part de tierces parties, enquêter sur les atteintes commises, punir les auteurs et offrir réparation aux victimes (A/HRC/17/31). Les Principes directeurs engagent les États à exercer le contrôle nécessaire pour s'assurer que les marchés qu'ils passent avec des entreprises fournissant des services susceptibles d'avoir une incidence sur l'exercice des droits de l'homme et les lois qu'ils adoptent pour régir ce type de marchés ne les empêchent pas de s'acquitter de leurs obligations internationales en matière de droits de l'homme (Ibid. p. 10).

## B. Responsabilité des entreprises

29. Les activités des entreprises privées du secteur de la surveillance étant tenues secrètes, le public n'a accès à aucune information sur la manière dont ces entreprises tiennent compte des incidences de leurs produits sur les droits de l'homme − si tant est qu'elles en tiennent compte. Compte tenu de la nature de leurs activités et du fait que leurs produits sont généralement utilisés à des fins incompatibles avec le droit international des droits de l'homme, on peut difficilement imaginer que ce soit le cas. En d'autres termes, étant donné qu'il est de notoriété publique qu'un grand nombre de leurs clients exercent des mesures de répression, elles ne peuvent pas sérieusement feindre d'ignorer cette situation.

30. Les Principes directeurs établissent un cadre permettant de déterminer si les entreprises de surveillance respectent les droits des personnes visées par leurs produits et services. Ces principes mettent l'accent sur la nécessité de prendre des mesures aux fins du respect des droits de l'homme, de prendre les précautions qui s'imposent en vue de repérer et de prévenir les incidences négatives des activités de surveillance sur les droits de l'homme, d'en atténuer les effets et d'en tenir compte, de consulter les groupes concernés, de vérifier régulièrement l'efficacité des mesures de politique générale prises pour défendre les droits de l'homme et d'établir des mécanismes de plainte efficaces à l'intention les titulaires de droits touchés par les activités des entreprises de surveillance (A/HRC/17/31, par. 15 à 25).

l'article 17, qui garantit le respect de la vie privée, fait partie des articles dont les dispositions visent des domaines dans lesquels les États parties ont l'obligation positive de réglementer les activités des personnes privées, physiques et morales.

[36] Voir Nate Cardozo, "D.C. circuit court issues dangerous decision for cybersecurity : Ethiopia is free to spy on Americans in their own homes", Electronic Frontier Foundation, 14 mars 2017.

[37] Voir Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Fiscalía general de la República tiene oportunidad histórica para acabar con la impunidad en caso Pegasus : Salas Suárez", 27 mars 2019, et Juan Arvizu, "Ordena Inai a PGR abrir contrato de compra de Pegasus", *El Universal*, 17 avril 2018.

31. Les entreprises de surveillance ne remplissent semble-t-il même pas ces exigences de base. Les conditions générales de vente que quelques rares d'entre elles ont publiées se contentent de faire vaguement référence à l'obligation de respecter les droits de l'homme. La société Hacking Team, par exemple, déclare vérifier avant toute vente s'il existe des éléments objectifs et crédibles permettant de penser que le client éventuel utilisera les technologies qu'elle commercialise pour faciliter des atteintes aux droits de l'homme. Toutefois, elle ne précise pas ce qu'elle fait de ces informations, ni quels droits de l'homme pourraient être menacés par ses produits[38]. NSO Group affirme se conformer aux avis d'un comité d'éthique commerciale composé d'experts externes spécialistes de différentes disciplines, dont le droit et les relations internationales, et laisse entendre qu'un projet peut être annulé si ses produits sont utilisés à mauvais escient[39]. Cette société indique en outre sur son site Web qu'elle enquêtera sur toute allégation crédible d'« utilisation abusive » de ses produits, sans toutefois préciser si cette expression recouvre les violations des droits de l'homme[40].

32. En résumé, les entreprises n'ont pas donné d'exemples de véritables mesures de précaution qu'elles auraient prises pour repérer et prévenir les incidences négatives sur les droits de l'homme que leurs activités causent ou auxquelles elles contribuent, ou pour prévenir et atténuer les incidences négatives sur les droits de l'homme qui sont directement liées aux activités qu'elles ont menées pour leurs relations commerciales ou aux produits et services qu'elles ont fournis à celles-ci (A/HRC/17/31, annexe, principe 13). À titre d'exemple, il n'existe pas de données publiques permettant de penser que l'évaluation de l'impact de tel ou tel produit ou activité sur les droits de l'homme fait partie des précautions à prendre avant de conclure une vente et a une importance décisive, ni que d'autres évaluations sont menées tout au long du cycle de vie du produit et dans le cadre du service après-vente. Au contraire, de plus en plus d'éléments montrent que les entreprises du secteur de la surveillance jouent un rôle de premier plan dans la facilitation de violations flagrantes des droits de l'homme. Étant donné que, de surcroît, ces entreprises continuent de refuser d'expliquer les précautions qu'elles prennent, force est de conclure que le système d'autoréglementation laisse à désirer.

33. Dans ses directives sur la mise en œuvre des Principes directeurs dans le secteur des technologies de l'information et des communications (ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights), la Commission européenne souligne l'importance qui doit être accordée aux droits de l'homme dès la conception d'un outil[41]. Le risque que les produits de surveillance soient utilisés à mauvais escient étant immense, les entreprises devraient anticiper l'utilisation illicite de leurs logiciels et commencer à concevoir des solutions permettant de remédier à ses effets négatifs. En partenariat avec une association du secteur des technologies, le Gouvernement du Royaume-Uni a élaboré un ensemble de directives à l'intention des entreprises de cybersécurité, dans lesquelles il souligne l'importance de prévenir et d'atténuer les atteintes aux droits de l'homme en introduisant des garde-fous dans les produits dès les premières étapes de la conception.

## C. Contrôle des exportations aux niveaux national et international

34. Le contrôle des exportations joue un grand rôle dans l'action menée pour réduire les risques causés par les activités des entreprises de surveillance privées et l'utilisation répressive de leurs produits. Toutefois, l'efficacité des mesures de contrôle des exportations

[38] Hacking Team, "Customer Policy".

[39] Voir la déclaration de NSO datée du 17 septembre 2018, à l'adresse https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf. Ainsi qu'il est dit sur le site de Citizen Lab, les déclarations de NSO concernant un comité d'éthique commerciale rappellent l'exemple du « panel extérieur d'experts techniques et de conseillers juridiques examinant les projets de vente » de Hacking Team. Il est apparu que ce « panel extérieur » était un cabinet d'avocats, dont les recommandations n'étaient pas toujours appliquées par Hacking Team » (Marczak et al., "Hide and seek").

[40] Voir www.nsogroup.com/about.

[41] Voir Commission européenne, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Luxembourg, 2013).

est limitée. Premièrement, le régime de contrôle des exportations internationales (l'Arrangement de Wassenaar sur le contrôle des exportations d'armes classiques et de biens et technologies à double usage), qui compte 42 États parties, n'est pas contraignant et a été conçu pour réduire les menaces pesant sur la sécurité régionale et internationale. Bien qu'il poursuive un objectif louable et nécessaire, il n'est pas adapté à la lutte contre les menaces que les outils de surveillance ciblée font peser sur les droits de l'homme ; d'ailleurs, il ne dit rien sur les mesures à prendre en cas de violations des droits de l'homme provoquées par l'utilisation de technologies de surveillance. Deuxièmement, ce régime est axé sur le contrôle des exportations, et non sur le problème principal qui nous occupe, à savoir l'utilisation des technologies de surveillance contre des personnes qui, en toute légitimité, expriment leurs opinions ou leur opposition au gouvernement, communiquent desinformations ou mènent d'autres activités participant de l'exercice de leurs droits de l'homme.

35. Néanmoins, l'Arrangement de Wassenaar promeut des objectifs importants, à savoir la transparence et une plus grande responsabilité dans les transferts d'armes conventionnelles et de biens et technologies à double usage. Les États parties s'engagent à contrôler l'exportation de tous les biens figurant sur la Liste des biens et technologies à double usage[42]. Les dispositions de l'Arrangement de Wassenaar ont été (ou devraient être) prises en compte dans les lois et les politiques des États parties et des États non parties ; malheureusement, aucun mécanisme ne permet de garantir leur adoption ni leur application.

36. En 2013, les États parties ont mis à jour la Liste des biens et technologies à double usage, y ajoutant les logiciels d'intrusion et les systèmes de surveillance des communications par Internet. D'après la liste, un logiciel d'intrusion est un logiciel spécialement conçu ou modifié pour échapper à la détection par les outils de veille ou déjouer les contre-mesures de protection et qui extrait des données d'un ordinateur ou d'un réseau ou modifie le chemin d'exécution standard d'un programme afin de permettre l'exécution d'instructions lancées de l'extérieur[43].

37. Les rapports détaillés qui font état de cas d'utilisation abusive des technologies de surveillance montrent que le régime de contrôle des exportations issu de l'Arrangement de Wassenaar n'a pas véritablement limité la propagation de ces technologies ni leur utilisation à des fins répressives. Le fait que le projet de renforcer la protection des droits de l'homme dans les lois et les politiques européennes en matière d'exportation proposé au Parlement européen se trouve au point mort illustre à quel point la réforme est difficile. Il s'agissait d'élargir la liste des biens à double usage et de mettre en place des contrôles « attrape-tout », et de prendre en compte du respect des droits de l'homme dans le pays de destination finale des technologies de cybersurveillance[44]. En janvier 2018, à l'issue de la première lecture, le Parlement était en faveur de l'application de contrôles renforcés sur les exportations de technologies à double usage[45]. Toutefois, la proposition a depuis fait l'objet de critiques de la part d'au moins neuf États membres, qui ont plaidé en faveur de mesures de protection des droits de l'homme moins strictes[46]. Actuellement, l'avenir de cette proposition est incertain[47].

[42] Voir Arrangement de Wassenaar, Liste des biens et technologies à double usage et Liste des munitions.

[43] Ibid., p. 221.

[44] Voir Commission européenne, "Proposition de règlement du Parlement européen et du Conseil instituant un régime de l'union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte)", 28 septembre 2016, et Lucie Krahulcova, "The European Parliament is fighting to strengthen the rules for surveillance trade", Access Now, 8 décembre 2017.

[45] Pour un aperçu de l'historique de la proposition de règlement, voir https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52016PC0616&from=DE.

[46] Document soumis au nom des délégations de Chypre, de l'Estonie, de la Finlande, de l'Irlande, de l'Italie, de la Pologne, de la République tchèque, du Royaume-Uni et de la Suède, "For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law globally", WK 5755/2018 INIT (15 mai 2018), et Access Now, "EU : States push to relax rules on exporting surveillance technology to human rights abusers", 11 juin 2018.

[47] Voir Catherine Stupp, "Nine countries united against EU export controls on surveillance software", Euractiv, 11 juin 2018, et Moßbrucker, "Surveillance exports".

38. La mise en application des contrôles à l'exportation varie d'un pays à l'autre, même entre les États parties à l'Arrangement de Wassenaar. Ainsi, les États-Unis d'Amérique n'ont pas encore intégré les mises à jour de 2013 concernant les logiciels d'intrusion et les systèmes de surveillance électronique des communications par Internet[48]. Toutefois, le Département du commerce procède actuellement à un examen approfondi du cadre en vigueur et a été chargé de créer un dispositif interinstitutions qui aura pour mission d'établir de nouvelles procédures de contrôle applicables aux technologies émergentes et aux technologies de base, dans le cadre de la loi de 2018 sur la réforme du contrôle des exportations[49]. Israël, État non-partie, a instauré des procédures de contrôle à l'exportation sur les biens à double usage régis par l'Arrangement de Wassenaar, mais l'application de ces procédures est entourée du plus grand secret[50].

## D. Absence de recours utiles en cas de surveillance ciblée

39. Le paragraphe 3 a) de l'article 2 du Pacte international relatif aux droits civils et politiques prévoit que, dans le cadre de l'obligation qui leur est faite de respecter et de garantir l'exercice des droits de l'homme, les États sont tenus d'assurer aux victimes de violations l'accès à un recours utile. Il dispose que les recours concernant des allégations de violation des droits garantis par le Pacte doivent être tranchés par l'autorité compétente, judiciaire, administrative ou législative, ou toute autre autorité compétente selon la législation de l'État. Le Comité des droits de l'homme a souligné que des organes indépendants et impartiaux relevant des services de police et de justice devaient procéder à des enquêtes rapides, approfondies et efficaces sur les allégations de violation[51]. L'obligation de fournir un recours utile emporte l'obligation de protéger les particuliers contre les actions d'entreprises privées qui entraînent des violations, et donc de prendre toutes les précautions nécessaires pour prévenir les violations, enquêter à leur sujet, punir les personnes ou entités qui les commettent et fournir réparation pour le préjudice qui en résulte[52].

40. Rares sont les victimes de surveillance ciblée qui ont réussi à faire reconnaître le préjudice qu'elles avaient subi, même si la Cour européenne des droits de l'homme et la Haute-Commissaire aux droits de l'homme ont estimé que la seule existence de mesures de surveillance, fut elle secrète, suffisait en l'absence de recours à constituer une violation du droit à la vie privée[53].

41. Les poursuites judiciaires engagées contre les entreprises privées qui fabriquent et commercialisent des technologies de surveillance et contre les États qui utilisent ce type de technologies ne sont pas forcément un recours efficace. En l'absence de moyens d'action et de réparations prévues, la possibilité d'amener ces entreprises à répondre de violations des droits de l'homme semble très faible. Dans au moins huit pays, des victimes présumées ont intenté un procès ou déposé une plainte contre des sociétés de surveillance privées ou contre l'État[54]. Toutefois, le succès de ce type d'action est compromis à cause d'obstacles majeurs, notamment l'absence de tout contrôle judiciaire, le fait que les actes reprochés sont rarement qualifiés par la loi, l'absence de voies de recours disponibles et de moyens de faire appliquer les décisions rendues, et la non-conservation des données.

42. Il arrive que des organisations de la société civile demandent à un État d'enquêter sur des activités de surveillance illicite, mais, en général, elles n'obtiennent pas gain de cause. Au Royaume-Uni, Privacy International a déposé une plainte pénale contre Gamma Group auprès de l'agence de lutte contre la criminalité organisée (National Crime Agency),

[48] Contribution de Privacy International, p. 5.

[49] John S. McCain National Defense Authorization Act for Fiscal Year 2019, nº 115–232 (2018) (loi sur les autorisations de dépenses en matière de défense nationale pour l'exercice 2019).

[50] Voir "Israel-U.S. export controls", export.gov, 20 juillet 2018. Voir aussi le par. 43.

[51] Observation générale nº 31, par. 15.

[52] Ibid., par. 8.

[53] Cour européenne des droits de l'homme, *Roman Zakharov c. Russie* (requête 47143/06), arrêt du 4 décembre 2015, par. 171, et A/HRC/27/37, par. 20.

[54] Voir Siena Anstis, "Litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry", Citizen Lab, 12 décembre 2018.

alléguant que l'entreprise avait enfreint de nombreuses dispositions de la législation interne lorsque sa filiale, FinFisher, avait vendu des technologies de surveillance et fourni une assistance au Gouvernement bahreïnien[55]. Le Centre européen des droits constitutionnels et des droits de l'homme (European Centre for Constitutional and Human Rights) et Privacy International ont déposé plainte contre Gamma Group devant la justice pénale allemande, à Munich, mais le ministère public a décidé qu'il n'y avait pas lieu d'engager des poursuites[56]. Même lorsque les États enquêtent pour déterminer si la surveillance exercée par les autorités enfreint le droit des droits de l'homme ou les lois nationales, les investigations sont parfois arbitraires ou mal organisées.

43. De toute évidence, il n'existe pas non plus de solution non judiciaire permettant d'obtenir une réparation conforme au droit international des droits de l'homme. Après qu'un de ses employés a reçu par WhatsApp un message suspect dont elle soupçonnait qu'il avait été envoyé par Pegasus, Amnesty International a écrit au Ministère israélien de la défense pour demander l'annulation de la licence d'exportation octroyée à l'entreprise NSO Group[57]. L'agence israélienne chargée du contrôle des exportations de défense lui a répondu qu'elle ne communiquait aucune information sur la politique d'octroi de licences ni sur les licences elles-mêmes[58]. Sans confirmer ni infirmer si NSO Group bénéficiait d'une licence lui permettant d'exporter le logiciel en question, elle a indiqué que le Ministère israélien de la défense respectait ses obligations internationales en ce qui concernait l'octroi à cette entreprise de licences l'autorisant à passer des marchés avec des gouvernements[59]. Le fait que ni les organisations régionales ni la communauté internationale ne fassent pression et que les États se dotent de politiques de confidentialité qu'ils justifient par la nécessité de protéger la sécurité nationale sont des obstacles de taille à la mise en place de recours efficaces.

44. Privacy International a déposé plainte contre Gamma et Trovicor en Allemagne et au Royaume-Uni, auprès des points de contact nationaux de l'Organisation de coopération et de développement économiques (OCDE), alléguant que ces entreprises avaient aidé le Gouvernement bahreïnien à surveiller des opposants politiques[60]. Dans sa plainte contre Trovicor, Privacy International a demandé au point de contact national de l'Allemagne de vérifier si l'entreprise avait enfreint les Principes directeurs de l'OCDE à l'intention des entreprises multinationales en exportant des produits de surveillance à Bahreïn, où les autorités utilisaient ce type de produits pour porter atteinte aux droits de l'homme, notamment arrêter, emprisonner et torturer des opposants et des dissidents[61]. Le point de contact national a toutefois rejeté la plainte, estimant qu'il disposait de trop peu d'éléments pour établir la présence de Trovicor à Bahreïn. Au Royaume-Uni, de multiples organisations de la société civile ont saisi le point de contact national d'allégations similaires concernant la société Gamma[62]. Le point de contact national a jugé la plainte recevable et, dans l'évaluation initiale qu'il a publiée en juin 2013, il a conclu que, si aucune des parties n'avait apporté la preuve directe que Gamma avait fourni des produits à Bahreïn, il ressortait néanmoins des éléments présentés que les produits de cette entreprise pouvaient avoir été utilisés contre des militants bahreïniens, ce qui démontrait que Gamma

[55] Voir Privacy International, "Criminal complaint to national cyber crime unit on behalf of Bahraini activists", 13 octobre 2014. Lawsuits against the NSO Group have also been filed in Israel and Cyprus : voir David D. Kirkpatrick et Azam Ahmed, "Hacking a prince, an emir and a journalist to impress a client", *New York Times*, 31 août 2018.

[56] Voir European Centre for Constitutional and Human Rights, "FinFisher : no investigation into German-British software company", 12 décembre 2014.

[57] Contribution d'Amnesty International, p. 8.

[58] Ibid.

[59] Ibid.

[60] Selon le site Web de l'organisation, le rôle principal d'un point de contact national est d'améliorer l'efficacité des Principes directeurs en entreprenant des activités de promotion, en traitant les demandes de renseignements et en contribuant à la résolution des problèmes qui peuvent surgir du non-respect des Principes directeurs.

[61] Voir Privacy International, "OECD complaint : Trovicor exporting surveillance technology to Bahrain", 1er février 2013.

[62] Voir Privacy International, "German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain", 20 décembre 2013.

ne s'acquittait pas des obligations qui lui incombent de faire preuve de la diligence voulue et de remédier aux incidences négatives de ses produits[63].

45. Bien que le rapport final du point de contact national contienne plusieurs recommandations fondées sur les normes relatives aux droits de l'homme, rien n'indique que Gamma ait appliqué ces recommandations, ni même pris connaissance du rapport[64].

# IV. Cadre pour la protection des droits fondamentaux contre la surveillance ciblée

46. 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 juridique visant à protéger les droits de l'homme, mais pas de cadre permettant de garantir le respect des restrictions imposées. Il est donc impératif et urgent que les États se limitent à employer les technologies à des fins licites, établissent de rigoureuses procédures de contrôle et d'autorisation, et autorisent les entreprises du secteur privé des technologies de surveillance à mener leurs activités (recherche et développement, commercialisation, vente, transfert et maintenance) uniquement si elles respectent certaines mesures de précaution en matière de droits de l'homme et peuvent prouver qu'elles l'ont toujours fait.

47. Le précédent titulaire du mandat a insisté pour que les États prennent des mesures en vue d'éviter la commercialisation des technologies de surveillance, en se penchant en particulier sur la recherche, le développement, la vente, l'exportation et l'utilisation de ces technologies, sachant qu'elles peuvent faciliter les violations systématiques des droits de l'homme (A/HRC/23/40, par. 97). Cette recommandation reste d'actualité. Dans la présente section, le Rapporteur spécial passe en revue les principaux éléments que doit comporter un cadre visant à protéger les particuliers contre toute utilisation des technologies de surveillance entravant l'exercice des droits fondamentaux. L'adoption et l'application des mesures proposées ci-après nécessitent l'intervention des acteurs suivants : les États utilisateurs et exportateurs de ces technologies ; les entreprises, qui sont tenues de respecter les Principes directeurs relatifs aux entreprises et aux droits de l'homme ; les États et les entreprises travaillant en collaboration avec la société civile ; et le Conseil des droits de l'homme.

## A. Moratoire sur l'exportation et l'utilisation de technologies de surveillance ciblée

48. La manière dont les entreprises privées conçoivent et transfèrent les technologies de surveillance et en assurent le service après-vente est préoccupante, de même que la manière dont les États se procurent et utilisent ces technologies. Selon des allégations dignes de foi, certaines entreprises vendent ce type de technologies à des gouvernements qui les utilisent contre des journalistes, des militants, des personnalités de l'opposition et d'autres personnes qui jouent un rôle fondamental dans une société démocratique. Certaines entreprises contestent ces allégations et soutiennent qu'elles ne permettent pas que leurs produits soient utilisés à des fins illicites, qu'elles disposent de mécanismes permettant de savoir qui sont les acheteurs et utilisateurs finals « sensibles » et qu'elles se conforment aux lois nationales sur le contrôle des exportations. Il est possible que des entreprises s'efforcent véritablement de prendre les mesures qui s'imposent face aux accusations de

[63] Ministère des entreprises, de l'innovation et des compétences du Royaume-Uni, "Initial assessment by the UK National Contact Point for the OECD Guidelines for Multinational Enterprises : complaint from Privacy International and others against Gamma International UK Limited, June 2013" (Londres, 2013), par. 25.

[64] Voir Amitpal Singh, "OECD finds actions of Gamma International to be in violation of human rights", Citizen Lab, 3 mars 2015, et "UK National Contact Point for the OECD Guidelines for Multinational Enterprises − Privacy International and Gamma International UK Ltd : final statement after examination of complaint", décembre 2014.

complicité dans l'utilisation de technologies de surveillance à des fins illicites ou répressives. Il n'y a toutefois aucune raison particulière de croire les entreprises sur parole sans les soumettre à des obligations de communication ni les tenir responsables de leurs actes. Compte tenu de la gravité des allégations, il est indispensable d'exiger la transparence dans les relations commerciales et les procédures des entreprises, ainsi que de prendre plusieurs autres mesures, décrites ci-après.

49. L'application des mesures proposées dans le présent rapport prendra un certain temps. Dans l'intervalle, de nombreux journalistes, militants, défenseurs des droits de l'homme et opposants politiques seront à la merci des gouvernements enhardis par l'éventail des technologies de surveillance extrêmement intrusives mises à leur disposition. Par conséquent, il faut immédiatement faire en sorte que les entreprises cessent de vendre et de transférer ce type de technologies et d'en assurer la maintenance jusqu'à ce qu'elles aient démontré de manière convaincante qu'elles ont adopté des mesures suffisantes (voir ci-après) en ce qui concerne le devoir de diligence, la transparence et l'application du principe de responsabilité pour empêcher ou limiter l'utilisation de ces technologies dans le but de porter atteinte aux droits de l'homme. Les États devraient en outre imposer un moratoire immédiat sur l'octroi de licences d'exportation pour les technologies de surveillance, et le lever uniquement lorsqu'il aura été démontré de manière convaincante que, sur le plan pratique, ces technologies ne peuvent être utilisées qu'à des fins licites et conformément aux normes relatives aux droits de l'homme et ne sont exportées que vers des pays dans lesquels leur utilisation sera soumise à une procédure d'autorisation par un organe judiciaire indépendant et impartial et respectera les principes de légalité, de nécessité et de légitimité. Pour l'heure, étant donné qu'il apparaît de plus en plus évident que les technologies de surveillance conçues par le secteur privé sont utilisées à des fins manifestement illicites, l'instauration d'un moratoire sur les transferts semble tout à fait justifiée.

## B. Obligations incombant aux États en tant qu'utilisateurs de technologies de surveillance

### 1. Renforcer la législation nationale visant à limiter la surveillance de manière à respecter les obligations découlant du droit international des droits de l'homme

50. En premier lieu, les États utilisant des technologies de surveillance doivent se conformer à un cadre juridique national répondant aux règles du droit international des droits de l'homme. La législation ne devrait autoriser la surveillance que lorsque les infractions pénales les plus graves ont été commises. Partant, le droit interne doit :

a) Insister sur le fait que toute personne a le droit de ne pas faire l'objet d'immixtion illicite ou arbitraire dans sa vie privée et de ne pas être inquiétée pour ses opinions ainsi que de rechercher, de recevoir et de répandre des informations et des idées sans considération de frontières et par tout moyen de son choix ;

b) Exiger que toute loi régissant la surveillance soit clairement formulée et accessible au public et ne soit appliquée que lorsque cela est nécessaire et proportionné à la réalisation de l'un des objectifs énoncés au paragraphe 3 de l'article 19 du Pacte international relatif aux droits civils et politiques ;

c) Garantir que les opérations de surveillance ciblée ne soient approuvées que si elles sont conformes au droit international des droits de l'homme et ont été autorisées par un organe judiciaire compétent, indépendant et impartial et si leur durée, leurs modalités, leur objet et leur portée ont été dûment délimités ;

d) Exiger, compte tenu des risques extrêmement élevés d'utilisation abusive des technologies de surveillance ciblée, que les opérations autorisées soient soumises au respect de formalités strictes. Il faudrait en outre que les demandes de surveillance soient dûment motivées et approuvées par un juge. Les personnes visées devraient être informées de la

décision d'autoriser leur mise sous surveillance, pour autant que cela ne compromette pas sérieusement le but de l'opération[65].

51. En général, les règles d'administration de la preuve limitent très strictement le droit d'accéder au travail des journalistes à des fins d'enquête pénale (A/70/361, par. 24). Les technologies de surveillance sont souvent utilisées pour cibler les personnes qui jouent un rôle de premier plan dans la promotion des valeurs démocratiques. Le Rapporteur spécial est conscient que certains États allèguent que les journalistes, entre autres personnes, se servent parfois de leur profession pour commettre de graves infractions pénales. Il sait par expérience que les allégations à ce propos sont presque toujours fausses ou exagérées. Dans bien des cas, les États en tirent prétexte pour saper la crédibilité des journalistes et des dissidents, voire pour surveiller certains journalistes, même des journalistes qui ne font pas l'objet d'une enquête criminelle, ce qui a une incidence disproportionnée sur la liberté de la presse. Dans un tel contexte, la loi devrait par défaut interdire l'utilisation de technologies de surveillance numérique contre les membres des médias. Bien entendu, il ne s'agit pas de protéger les journalistes contre d'autres mesures juridiques légitimes, y compris la surveillance non numérique. Simplement, comme les technologies de surveillance numérique sont intrusives, le risque d'utilisation abusive ou de « fuite » dans le cadre d'enquêtes criminelles légitimes sur des faits couverts par des journalistes est réel et extrêmement difficile, voire impossible, à contenir. Ce seul risque est susceptible de dissuader les journalistes de travailler sur les sujets les plus sensibles et de décourager les sources et les lanceurs d'alerte de se manifester.

### 2. Établir des mécanismes publics chargés d'approuver et de contrôler l'utilisation des technologies de surveillance

52. Exiger que l'État obtienne l'autorisation d'un juge pour utiliser des technologies de surveillance est une condition nécessaire, mais insuffisante. L'achat de ce type de technologies devrait aussi être surveillé et contrôlé et donner lieu à des consultations publiques. Ces dernières années, aux États-Unis, les forces de l'ordre ont de plus en plus souvent eu recours aux technologies de surveillance, ce qui a conduit plusieurs collectivités à établir des organes de contrôle chargés de réglementer l'utilisation et l'achat de ces technologies. Par exemple, la municipalité d'Oakland, en Californie, a pris un décret comportant plusieurs dispositions relatives à l'acquisition de technologies de surveillance dont les États pourraient s'inspirer[66]. Ces dispositions prévoient notamment :

a) La mise en place d'une procédure d'approbation par les services compétents, qui doivent tenir compte des obligations de l'État en matière de droits de l'homme ;

b) La divulgation de l'acquisition de pareilles technologies suivant les procédures habituelles de notification du public et la tenue de consultations publiques sur des questions telles que les incidences de ces technologies sur les droits de l'homme et leur efficacité pour ce qui est de la réalisation des objectifs visés ;

c) La publication régulière de rapports sur les cas dans lesquels l'achat et l'utilisation de ces technologies ont été autorisés et l'utilisation qui a été faite de celles-ci.

53. C'est surtout dans les États dans lesquels les organes infranationaux sont dotés d'une certaine autonomie en ce qui concerne l'achat d'outils de surveillance qu'il faudrait faire en sorte que ce type d'achat soit véritablement contrôlé. Étant donné qu'il est manifestement de l'intérêt public de préserver la confidentialité et la sécurité des logiciels commerciaux largement accessibles, les mécanismes publics de contrôle devraient en outre être habilités à établir des politiques concernant l'accumulation de vulnérabilités et la conception d'exploits.

65

[65] Voir le document intitulé « Nécessaires et proportionnés : Principes internationaux sur l'application des droits de l'homme à la surveillance des communications » (mai 2014).

[66] Voir American Civil Liberties Union of Northern Carolina, « Oakland becomes latest municipality to reclaim local control over surveillance technologies used by local law enforcement », 2 mai 2018.

### 3. Assurer l'accès des victimes à des recours juridiques internes

54. Pour les raisons décrites précédemment, il est difficile pour les cibles d'une surveillance illégale ou arbitraire d'intenter une action contre l'État. Certains des obstacles sont d'ordre structurel ; par exemple, dans bon nombre d'États, la législation ne prévoit pas la possibilité de poursuivre les acteurs publics en justice. Il se peut qu'il ne soit pas possible d'engager des poursuites parce que les autorités législatives ou judiciaires accordent une importance excessive au respect de ce qu'elles perçoivent comme des intérêts liés à la sécurité nationale et l'ordre public. Il se peut aussi qu'il soit difficile et onéreux de prouver que la surveillance a bien eu lieu et a été le fait de l'État, voire d'une autorité particulière, sachant que l'État ou l'autorité en question s'exposerait alors à un procès. Dans bien des cas, les personnes surveillées ne savent pas qu'elles le sont, ou, si elles le savent, le délai de prescription a expiré[67]. En d'autres termes, il est extrêmement rare qu'une personne qui saisit la justice d'une plainte pour surveillance illicite obtienne gain de cause.

55. Les États qui entendent sérieusement lutter contre l'utilisation abusive des technologies de surveillance devraient prendre des mesures pour permettre aux particuliers de déposer plainte contre des acteurs étatiques et des acteurs non étatiques. À cette fin, certains États devront prendre les mesures nécessaires pour que les règles relatives à la compétence des juridictions, à l'administration de la preuve, à la prescription et à d'autres aspects fondamentaux d'une action en justice soient adaptées à l'ère du numérique. Ils devraient faire en sorte que les tribunaux puissent déclarer recevables et apprécier les analyses scientifiques réalisées par des experts techniques. Il faudrait aussi que les législations nationales donnent aux particuliers les moyens d'engager une action contre les entités privées, même lorsque celles-ci changent de propriétaire (dans le cadre de procédures connues sous le nom de « disposals » (cessions) ou « makeovers » (refontes)), ce qui complique souvent la tâche des victimes qui veulent que les responsables soient amenés à répondre de leurs actes et à leur offrir réparation[68]. Il faudrait enfin envisager d'autres voies de recours, telles que la création de commissions pour la vérité chargées d'entendre les témoignages des victimes de violations flagrantes des droits de l'homme facilitées par la surveillance numérique et d'examiner la complicité des entreprises dans ces violations.

56. Cela étant, la surveillance ciblée n'est pas toujours interne à un État. Il peut s'avérer difficile de porter plainte contre un État qui surveille une personne située en dehors de son territoire. En outre, il se peut que l'intéressé se trouve face aux mêmes contraintes que celles qu'il rencontrerait dans l'État en question − en ce qui concerne la preuve, par exemple. Il se peut également que, comme dans l'affaire *Doe* susmentionnée, les tribunaux soient réticents à juger un État étranger souverain. Bien que les règles applicables à ce type de procédure varient, les États parties devraient interpréter les normes relatives à l'immunité de l'État souverain de manière à ce que leurs tribunaux puissent juger un État étranger.

## C. Obligations incombant aux gouvernements délivrant des licences d'exportation de technologies de surveillance

57. L'adoption de l'Arrangement de Wassenaar ne garantit pas à elle seule le contrôle effectif des exportations de technologies de surveillance ; le respect des listes de contrôle dépend de l'application de l'Arrangement au niveau des États. En outre, les principaux pays exportateurs ne sont pas tous parties à l'Arrangement. Par exemple, Israël, qui est un acteur clef du marché des technologies de surveillance, affirme qu'il respecte pleinement les dispositions de l'Arrangement, mais n'y est pas encore partie[69]. De surcroît, la portée de l'Arrangement est limitée en ce que, bien qu'il vise à réaliser des objectifs importants liés à la paix et à la sécurité régionales et internationales, cet instrument n'est pas axé sur les droits de l'homme. Néanmoins, étant donné qu'il établit des normes censées être largement appliquées et respectées, les États parties devraient en tirer parti pour soumettre le transfert des technologies de surveillance à des restrictions fondées sur les droits.

[67] Voir *Roman Zakharov c. Russie*.

[68] Communication d'Access Now, p. 8.

[69] Voir « IL − Israel cybersecurity export control policy » (présentation PowerPoint), juin 2016, disponible sur la page Web de l'Arrangement de Wassenaar.

58. Afin de contribuer davantage à l'élaboration de normes mondiales en matière d'exportation, les États parties pourraient établir un groupe de travail sur les droits de l'homme chargé de proposer et d'envisager des normes favorisant la prise en compte des questions relatives aux droits de l'homme dans les transferts de technologie. En tout état de cause, qu'ils créent un groupe de travail ou un autre mécanisme, les États parties devraient se doter d'un cadre prévoyant que l'octroi d'une licence pour une technologie quelle qu'elle soit sera soumis à un examen du respect des droits de l'homme dans le pays de destination et à un examen du respect des Principes directeurs sur les entreprises et les droits de l'homme par l'entreprise fabricante, ainsi qu'il est exposé ci-après. Comme l'a indiqué Privacy International, les États parties et les autres États exportateurs devraient refuser d'octroyer une licence lorsqu'il existe un risque important que le produit exporté serve à commettre des violations des droits de l'homme, lorsque le pays de destination n'est doté d'aucun cadre juridique régissant l'utilisation des technologies de surveillance ou lorsque le cadre juridique existant ne garantit pas le respect du droit international des droits de l'homme ou des normes connexes[70]. En cas de refus d'octroyer une licence d'exportation pour l'une de ces raisons, il faudrait que les technologies de surveillance concernées soient ajoutées à la liste des biens visés par les régimes de sanctions[71].

59. De tels cadres viendraient utilement compléter l'Arrangement de Wassenaar, mais la capacité du public et de certaines organisations de la société civile à surveiller leur application dépendra de l'adoption de règles de transparence plus strictes aux niveaux national et international. L'Arrangement lui-même devrait d'ailleurs promouvoir la transparence en fixant des lignes directrices claires et applicables pour le partage d'informations entre États et la divulgation d'informations concernant les normes applicables en ce qui concerne les licences, les décisions d'accorder, de modifier ou de refuser une licence, les cas isolés ou répétés d'utilisation abusive de technologies de surveillance et les violations des droits de l'homme qui en découlent, ainsi que le traitement des vulnérabilités numériques. Les lois nationales relatives aux exportations devraient prévoir l'allocation de ressources permettant de consigner dans des registres publics accessibles les décisions concernant l'octroi de licences d'exportation et donner pour mandat aux organismes publics compétents de demander l'avis du public et de mener des consultations multipartites dans le cadre de l'examen des demandes de licences d'exportation. Enfin, les États devraient prendre des mesures destinées à protéger les recherches qui touchent à la sécurité et exempter les outils de cryptage des restrictions applicables aux exportations[72].

## D. Application des Principes directeurs relatifs aux entreprises et aux droits de l'homme par les entreprises

60. Le risque d'utilisation abusive des technologies de surveillance est tel que l'octroi de licences d'exportation devrait être interdit par les législations nationales sauf si l'entreprise démontre régulièrement qu'elle s'acquitte rigoureusement des responsabilités mises à sa charge par les Principes directeurs en ce qui concerne la conception, la vente, le transfert ou la maintenance de ces technologies. Cela permettrait de poser l'application des Principes directeurs comme une condition préalable à la participation des entreprises au marché de la surveillance. Dans de précédents rapports, le Rapporteur spécial a expliqué ce que le secteur des technologies de l'information et de la communication devait faire pour s'acquitter de ses responsabilités en matière de respect des droits de l'homme (A/HRC/35/22, par. 45 à 75). Pour que les entreprises de surveillance privées s'acquittent elles aussi de leurs responsabilités, elles doivent au minimum prendre les mesures suivantes[73] :

a) Adopter des politiques commerciales qui consacrent l'obligation des entreprises de respecter le droit à la liberté d'expression, le droit à la vie privée et les droits de l'homme connexes dans toutes leurs activités, et qui subordonnent l'approbation et la

[70] Communication de Privacy International, p. 8.

[71] Ibid., p. 3 et 4.

[72] Ibid., p. 5.

[73] La plupart de ces mesures sont inspirées des communications présentées par la société civile qui figurent dans l'additif au présent rapport et sur le site Web du Rapporteur spécial.

conclusion d'une vente, d'un transfert ou d'un contrat de service après-vente au respect du droit international des droits de l'homme par le client ;

b) Prendre des mesures de précaution en matière de droits de l'homme (par exemple faire des études d'impact) lorsqu'elles mènent des activités ayant une incidence sur la liberté d'expression et le respect de la vie privée, notamment la conception, la vente, le transfert et la maintenance de produits et services de surveillance ;

c) Se doter de politiques internes et de clauses contractuelles types interdisant expressément la personnalisation de produits afin qu'ils puissent être utilisés pour exercer une surveillance ciblée constituant une violation du droit international des droits de l'homme et la maintenance de produits et la fourniture d'un service après-vente ;

d) Se doter de procédures internes garantissant que la nécessité de protéger les droits de l'homme est prise en considération dans la conception et le développement technique des produits, et notamment de systèmes permettant de détecter les utilisations abusives et de déclencher des coupe-circuits pour y mettre fin ;

e) Contrôler et vérifier régulièrement le respect des droits de l'homme afin de garantir que leurs produits et services sont utilisés dans le respect des dispositions du droit international des droits de l'homme et s'engager à rendre publiques les conclusions de ces contrôles et vérifications ;

f) Établir des procédures permettant de signaler rapidement toute utilisation abusive de leurs technologies aux organismes de contrôle gouvernementaux compétents (par exemple les institutions nationales pour la promotion des droits de l'homme) ou aux organes intergouvernementaux (tels que les mécanismes de plaintes relevant des procédures spéciales) ;

g) Communiquer des informations à des fins de transparence, notamment des informations sur les capacités de leurs produits, les utilisations qui peuvent en être faites, les différents types de services après-vente fournis, les cas d'utilisation abusive, et le nombre et le type de ventes conclues avec des services de police et de renseignements, d'autres services de l'État ou leurs agents ;

h) Organiser régulièrement des consultations avec les titulaires de droits et les groupes de la société civile concernés et les organisations spécialisées dans le droit numérique au sujet des effets réels ou potentiels de leurs produits et services et des garanties concernant les droits de l'homme devant être mises en place pour prévenir ou atténuer ces effets, en attachant une importance particulière à la participation des personnes susceptibles d'être surveillées pour des motifs discriminatoires ou à des fins répressives, comme les membres des minorités raciales et ethniques et des groupes traditionnellement marginalisés ;

i) Établir des mécanismes chargés de recueillir les plaintes de particuliers qui allèguent avoir été victimes de violations des droits de l'homme facilitées par leurs produits et services, d'apprécier ces plaintes en toute indépendante et de s'assurer qu'il y est donné suite comme il se doit ;

j) Établir des mécanismes de recours qui permettent aux plaignants de demander une indemnisation, des excuses et d'autres formes de réparation, selon qu'il convient, une fois qu'un mécanisme indépendant a déterminé le bien-fondé de la plainte.

## E. Mesures de corégulation

61. Les mesures adoptées par les États et les entreprises décrites dans le présent document peuvent s'avérer insuffisantes pour résoudre le problème que la surveillance ciblée pose au niveau mondial. De surcroît, elles ne tiennent pas compte de l'opinion d'acteurs importants, à savoir les membres de la société civile (militants, spécialistes des technologies, universitaires, victimes ou personnes appartenant à plusieurs de ces catégories). La gouvernance corégulatoire, qui implique une participation significative de l'État, des entreprises et des acteurs de la société civile, peut servir de base à l'application du principe de responsabilité en ce qui concerne le respect des droits de l'homme dans le secteur de la surveillance privée. Les mesures de corégulation prises en vue de promouvoir

l'application du principe de responsabilité et le contrôle mutuel dans le secteur des entreprises de sécurité privées sont particulièrement révélatrices. Comme les entreprises de surveillance privées, les entreprises de sécurité privées mènent des activités qui comportent des risques liés au fait qu'elles touchent aux fonctions de l'État, et en particulier à la sécurité nationale. Par conséquent, la corégulation des entreprises de sécurité privées suppose une sensibilisation de ces entreprises aux questions relatives aux droits de l'homme et la coopération avec les différentes parties prenantes (par exemple, la certification est basée sur des procédures d'audit et de contrôle auxquelles participe la société civile), ce qui pourrait facilement être aussi fait dans le secteur des entreprises de surveillance privées.

62. Deux instruments faisant partie du cadre réglementaire des entreprises de sécurité privées méritent d'être mentionnés dans le contexte de l'examen des activités des entreprises de surveillance privées. Le Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les États en ce qui concerne les opérations des entreprises militaires et de sécurité privées opérant pendant les conflits armés[74] n'est pas contraignant, mais reprend les obligations découlant du droit international qui incombent aux entreprises de sécurité privées et comprend des recommandations présentées sous la forme de meilleures pratiques à l'intention des États contractants, des États territoriaux et des États d'origine. Les principes qui y sont énoncés en ce qui concerne la divulgation et la diligence raisonnable sont antérieurs aux Principes directeurs, auxquels ils sont néanmoins conformes.

63. Le Code de conduite international des entreprises de sécurité privées peut aussi être un modèle à suivre. Établi avec l'appui de la société civile, du secteur privé et du Gouvernement suisse, c'est l'un des rares instruments qui suit une approche fondée sur la participation des entreprises de sécurité privées. L'Association du Code de conduite international des entreprises de sécurité privées comprend des représentants des États, des représentants des entreprises de sécurité privées et des représentants des organisations de la société civile. Le code, qui a un caractère non contraignant, vise à renforcer le contrôle et la supervision des activités des entreprises, à énoncer les obligations mises à la charge de celles-ci par le droit international et à jeter les bases de l'établissement d'un cadre de responsabilité vis-à-vis de l'association. Celle-ci comprend une Assemblée générale et un Comité directeur composé de 12 membres élus, et ces deux instances comprennent des représentants des trois groupes de parties prenantes. Pour adhérer à l'Association, les entreprises doivent respecter le code, y compris pour ce qui est des processus de certification, d'audit et de vérification.

64. Comme il est indiqué dans les statuts de l'association, le but principal du code est d'encourager l'utilisation responsable des services de sécurité ainsi que le respect des droits de l'homme et du droit national et international. Le code énonce, d'une part, les engagements d'ordre général pris par les États, les entreprises de sécurité privées et les autres prestataires de services de sécurité privés et, d'autre part, les règles de conduite applicables en ce qui concerne le recours à la force, l'arrestation et la détention, la torture et les traitements qui y sont assimilés, la violence sexiste, la traite des êtres humains, l'esclavage et le travail forcé, la discrimination, et l'identification et l'enregistrement du personnel de sécurité privé[75].

## F. Nouvelle approche adoptée par l'Organisation des Nations Unies concernant les pratiques de surveillance

65. Le Conseil des droits de l'homme a créé plusieurs groupes de travail chargés d'examiner les principales questions liées à l'application des normes internationales relatives aux droits de l'homme, et les travaux de ces groupes se sont avérés fort utiles. Le Conseil ou ses procédures spéciales pourraient néanmoins envisager de créer un autre

[74] Voir Département fédéral des affaires étrangères de la Suisse, et Comité international de la Croix-Rouge, « Le Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les États en ce qui concerne les opérations des entreprises militaires et de sécurité privées opérant pendant les conflits armés » (Berne, 2008).

[75] Voir également la communication de Sarah McKune, p. 10.

mécanisme capable de se pencher comme il se doit sur certains cas que les titulaires de mandat peuvent ne pas être en mesure d'examiner. La création d'un groupe de travail supplémentaire ou d'une équipe spéciale plurisectorielle ou l'élaboration d'un plan d'action pourraient permettre de se pencher sur les allégations selon lesquelles les activités de surveillance menées par les États − qui relèvent de nombreux domaines du droit international des droits de l'homme et, par conséquent, ont des répercussions sur le mandat de nombreuses procédures spéciales − portent atteinte aux droits de l'homme fondamentaux.

# V. Recommandations

66. **À l'intention des États :**

a) **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 ;**

b) **Les États qui acquièrent ou utilisent des technologies de surveillance (les « États acquéreurs ») devraient veiller à ce que leur législation subordonne l'utilisation de ces technologies au respect des principes de légalité, de nécessité et de légitimité qui participent des normes relatives aux droits de l'homme, et devraient également se doter de mécanismes juridiques de réparation leur permettant de s'acquitter de l'obligation qui leur incombe d'offrir des voies de recours effectives aux victimes d'utilisation abusive des technologies de surveillance ;**

c) **Les États acquéreurs devraient établir des mécanismes dans le cadre desquels l'achat de technologies de surveillance sera soumis à une procédure d'approbation, de supervision et de contrôle publique ou collective ;**

d) **Les États qui exportent des technologies de surveillance ou en autorisent l'exportation (« États exportateurs ») devraient veiller à ce que les organismes gouvernementaux compétents sollicitent l'avis du public et mènent des consultations multipartites lorsqu'ils examinent les demandes d'octroi de licences d'exportation. Tous les documents relatifs à ces licences devraient être conservés et mis à la disposition du plus large public possible. Les États devraient également protéger les recherches en matière de sécurité et exempter les outils de cryptage des restrictions appliquées aux exportations ;**

e) **Les États exportateurs devraient adhérer à l'Arrangement de Wassenaar et appliquer les règles et les normes définies dans cet instrument dans la mesure où elles sont conformes au droit international des droits de l'homme ;**

f) **Les États parties à l'Arrangement de Wassenaar devraient soumettre l'octroi de licences pour toutes les technologies à un examen de la situation des droits de l'homme dans le pays de destination et exiger que les entreprises exportatrices appliquent les Principes directeurs sur les entreprises et les droits de l'homme. Ils pourraient créer un groupe de travail sur les droits de l'homme spécialement chargé de créer un mécanisme à cet effet. En outre, les États devraient expressément définir et faire appliquer des lignes directrices concernant les obligations de transparence et d'application du principe de responsabilité pour ce qui est de l'octroi de licences, des violations des droits de l'homme liées à la surveillance et du traitement des vulnérabilités numériques.**

67. **À l'intention des entreprises :**

a) **Les entreprises de surveillance privées devraient reconnaître publiquement qu'elles sont tenues de respecter le droit à la liberté d'expression, le droit à la vie privée et les droits fondamentaux connexes et prendre des mesures de diligence raisonnable pour garantir le respect des droits de l'homme dès les premières étapes de la conception des produits et dans toutes leurs activités. Elles devraient à cette fin concevoir leurs produits dans l'optique même de respecter les droits de l'homme, mener des consultations régulières avec la société civile (en particulier les groupes susceptibles de faire l'objet d'une surveillance) et communiquer à des fins de transparence toutes les informations voulues sur les activités qu'elles mènent et qui ont une incidence sur les droits de l'homme ;**

b) **Les entreprises devraient prendre des mesures permettant véritablement de garantir que l'utilisation de leurs produits ou services sera conforme aux normes relatives aux droits de l'homme. À cette fin, elles devraient notamment introduire dans leurs contrats des clauses interdisant la personnalisation, le ciblage, la maintenance ou toute autre manipulation de leurs technologies destinée à entraîner une violation du droit international des droits de l'homme ; doter leurs produits de fonctionnalités visant à signaler, empêcher ou limiter l'utilisation abusive de leurs technologies ; et établir des procédures d'audit et de vérification destinées à contrôler le respect des droits de l'homme ;**

c) **Les entreprises qui constatent une utilisation de leurs produits et services constitutive de violations des droits de l'homme devraient signaler rapidement l'abus aux organismes de contrôle nationaux, régionaux ou internationaux compétents. En outre, les entreprises devraient se doter de mécanismes permettant aux victimes de violations des droits de l'homme liées à la surveillance de porter plainte et de demander réparation.**

68. **À l'intention de l'Organisation des Nations Unies : l'Organisation, en particulier le Conseil des droits de l'homme, devrait créer un groupe de travail ou une équipe spéciale plurisectorielle chargé de surveiller les violations ponctuelles ou généralisées des droits de l'homme facilitées par l'utilisation d'outils de surveillance numérique et de formuler des recommandations à ce sujet.**

69. **À l'intention de l'ensemble des parties prenantes : les États, le secteur privé, la société civile et les autres parties prenantes concernées devraient prendre des mesures de corégulation, notamment élaborer des codes de conduite fondés sur les droits à l'intention des entreprises privées du secteur de la surveillance et faire appliquer ces instruments en procédant à des audits indépendants et en menant des activités de formation et d'information.**