Nations Unies A/HRC/39/29*

Assemblée générale

Distr. générale
3 août 2018
Français
Original : anglais

Conseil des droits de l'homme
Trente-neuvième session
Points 2 et 3 de l'ordre du jour
Rapport annuel du Haut-Commissaire des Nations Unies aux droits de l'homme et rapports du Haut-Commissariat et du Secrétaire général

Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Le droit à la vie privée à l'ère du numérique

Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme

Résumé

Le présent rapport est soumis en application de la résolution 34/7 du Conseil des droits de l'homme, dans laquelle le Conseil a prié le Haut-Commissaire des Nations Unies aux droits de l'homme d'établir un rapport ayant pour objet de recenser et de préciser les principes, les normes et les meilleures pratiques concernant la promotion et la protection du droit à la vie privée à l'ère du numérique, ainsi que la responsabilité incombant aux entreprises à cet égard, et de lui soumettre ce rapport à sa trente-neuvième session.

* Nouveau tirage pour raisons techniques (31 août 2018).

GE.18-12799 (F) 200818 290818

1812799

I. Introduction

1. Il est aujourd'hui plus nécessaire que jamais de s'attaquer aux problèmes que le monde numérique suscite en ce qui concerne le droit à la vie privée. Mises au point principalement par le secteur privé, les technologies numériques qui exploitent en permanence des données privées pénètrent progressivement dans le tissu social, culturel, économique et politique des sociétés modernes. Des technologies de plus en plus puissantes faisant un usage intensif de données, telles que les technologies des mégadonnées et l'intelligence artificielle, risquent de favoriser l'émergence d'un environnement numérique intrusif dans lequel les États et les entreprises commerciales seront en mesure de surveiller, d'analyser, de prédire et même de manipuler le comportement des personnes à un degré sans précédent. S'il est indéniable que les technologies axées sur les données peuvent être utilisées à des fins très positives, ces évolutions technologiques comportent toutefois des risques très importants pour la dignité humaine, l'autonomie et la vie privée ainsi que pour l'exercice des droits de l'homme en général si elles ne sont pas gérées avec la plus grande attention.

2. Les acteurs régionaux et internationaux sont de plus en plus conscients de ces problèmes et commencent à agir en conséquence. Le Conseil des droits de l'homme a établi en juillet 2015 un mandat de Rapporteur spécial sur le droit à la vie privée. Dans de nombreuses résolutions, le Conseil des droits de l'homme et l'Assemblée générale se sont déclarés préoccupés par les risques pour la vie privée que suscitent les mesures de surveillance appliquées par les États et certaines pratiques commerciales[1]. Au niveau régional, la protection de la vie privée a été renforcée par plusieurs mesures, dont le Règlement général de l'Union européenne sur la protection des données, qui est entré en vigueur récemment et a des répercussions à l'échelle de la planète, le protocole adopté par le Conseil de l'Europe afin de mettre à jour et de moderniser la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les lignes directrices de la Commission de l'Union africaine relatives à la protection des données à caractère personnel en Afrique. Par contre, de nombreux gouvernements ont adopté des lois ou des projets de loi qui renforcent leurs pouvoirs de surveillance, souvent par des moyens contraires aux normes internationales applicables en matière de droits de l'homme[2].

3. Le présent rapport donne des orientations sur la manière de faire face à certains des problèmes urgents qui menacent le droit à la vie privée à l'ère du numérique. Il donne un bref aperçu du cadre juridique international en la matière et comprend un examen des tendances actuelles les plus significatives. Il aborde ensuite les obligations des États et la responsabilité des entreprises commerciales, et se penche notamment sur les garanties et les moyens de contrôle adéquats. Le dernier chapitre offre un aperçu des moyens d'obtenir réparation en cas de violation de la vie privée ou d'atteinte à ce droit.

4. Le présent rapport s'appuie sur le rapport sur le droit à la vie privée à l'ère du numérique (A/HRC/27/37) établi en 2014 par la Haute-Commissaire ainsi que sur les exposés présentés et les débats tenus au cours d'un atelier d'experts qui a eu lieu à Genève

[1] Voir, par exemple, les résolutions 68/167, 69/166 et 71/199 de l'Assemblée générale ainsi que les résolutions 28/16 et 34/7 et la décision 25/117 du Conseil des droits de l'homme.

[2] Voir, par exemple, Anja Seibert-Fohr, « Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy » (avril 2018), consultable à l'adresse https://ssrn.com/abstract=3168711 ; https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee et www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyin DigitalAge/SR_right_privacy.pdf.

en février 2018[3]. Il s'appuie également sur les 63 communications écrites soumises par un large éventail de parties prenantes[4].

II. Comprendre le droit à la vie privée à l'ère du numérique

5. Le droit à la vie privée est un droit de l'homme fondamental reconnu par la Déclaration universelle des droits de l'homme en son article 12, par le Pacte international relatif aux droits civils et politiques en son article 17, et dans de nombreux autres instruments internationaux et régionaux relatifs aux droits de l'homme[5, 6]. Le respect de la vie privée peut être considéré comme la présomption que tout individu a droit à un espace dans lequel il peut s'épanouir, interagir et jouir d'une liberté en toute autonomie, une « sphère privée » dans laquelle il est libre d'interagir ou non avec d'autres personnes et peut échapper à l'intervention de l'État et à toute intervention excessive non sollicitée d'une tierce partie (voir, par exemple, A/HRC/13/37, par. 11, et A/HRC/23/40, par. 22 et 42). Dans l'environnement numérique, la confidentialité des renseignements personnels, c'est-à-dire de l'information qui existe ou qui peut être extrapolée au sujet d'une personne, de sa vie et des décisions fondées sur cette information, revêt une importance particulière.

6. La notion de protection du droit à la vie privée est large et s'étend non seulement aux informations de fond contenues dans les communications mais aussi aux métadonnées car, lorsqu'elles sont analysées et agrégées, ces données « peuvent donner des indications sur la conduite d'un individu, ses relations sociales, ses préférences privées et son identité qui vont bien au-delà de ce que l'on obtient en accédant au contenu d'une communication privée » (voir A/HRC/27/37, par. 19). La protection du droit à la vie privée ne se limite pas aux espaces privés et délimités, comme le domicile d'une personne, mais s'étend aux espaces publics et aux informations librement accessibles (voir CCPR/C/COL/CO/7, par. 32). Par exemple, le droit à la vie privée entre en jeu lorsque les autorités publiques surveillent un espace public, comme un marché ou une gare ferroviaire, et observent ainsi des particuliers. De même, la collecte et l'analyse des informations concernant une personne accessibles au public sur les médias sociaux menacent aussi le droit à la vie privée[7]. Le fait qu'une information soit échangée publiquement ne signifie pas que sa teneur n'est pas protégée[8].

7. Le droit à la vie privée n'est pas menacé uniquement par des pratiques telles que l'examen ou l'utilisation d'informations concernant une personne par un humain ou un algorithme[9]. Le simple fait de produire ou de collecter des données relatives à l'identité, à la famille ou à la vie privée d'une personne porte déjà atteinte au droit à la vie privée, car de tels actes ont pour effet de faire perdre à la personne concernée une part du contrôle qu'elle exerce sur des informations qui pourraient constituer un risque pour sa vie privée

[3] Voir https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx et la diffusion sur Internet disponible à l'adresse http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2.

[4] Toutes ces communications sont disponibles à l'adresse https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

[5] Voir, par exemple, l'article 16 de la Convention relative aux droits de l'enfant ; l'article 14 de la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille ; et l'article 22 de la Convention relative aux droits des personnes handicapées.

[6] Voir, par exemple, l'article 10 de la Charte africaine des droits et du bien-être de l'enfant ; l'article 11 de la Convention américaine relative aux droits de l'homme et l'article 8 de la Convention européenne des droits de l'homme.

[7] Voir la communication de Privacy International pour le présent rapport.

[8] Anja Seibert-Fohr, « Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy ».

[9] Voir Paul Bernal, « Data gathering, surveillance and human rights: recasting the debate », *Journal of Cyber Policy*, vol. 1, nº 2 (2016).

(voir A/HRC/27/37, par. 20)[10]. En outre, la simple existence d'une surveillance secrète constitue une atteinte au droit à la vie privée (ibid.)[11].

8. Le droit à la vie privée s'applique de manière égale à tous. Toute différence de protection de ce droit fondée sur la nationalité ou tout autre motif est incompatible avec le droit à l'égalité et à la non-discrimination énoncé à l'article 26 du Pacte international relatif aux droits civils et politiques.

9. Tout État partie doit respecter et garantir à quiconque se trouve sous son pouvoir ou son contrôle effectif les droits reconnus dans le Pacte même s'il ne se trouve pas sur son territoire[12]. Le droit des droits de l'homme s'applique lorsqu'un État exerce son pouvoir ou son contrôle effectif à l'échelle de l'infrastructure des communications numériques, où que cela se produise, par exemple sous la forme d'écoutes directes ou d'une pénétration de l'infrastructure située en dehors du territoire de cet État. De même, dans les cas où l'État exerce une compétence réglementaire sur une tierce partie qui contrôle les informations d'une personne (par exemple, un fournisseur de services en nuage), cet État doit également étendre la protection des droits de l'homme aux personnes dont le droit à la vie privée serait menacé par l'accès à ces informations ou l'utilisation de celles-ci (voir A/HRC/27/37, par. 34).

10. Selon l'article 17 du Pacte, l'immixtion dans la vie privée d'une personne n'est autorisée que si elle n'est ni arbitraire ni illégale. Les mécanismes des droits de l'homme ont toujours interprété ces termes comme faisant référence aux principes fondamentaux de légalité, de nécessité et de proportionnalité (voir A/HRC/27/37, par. 21 à 27)[13]. Conformément à ces principes, les États ne peuvent porter atteinte au droit à la vie privée que dans la mesure prévue par la législation, et une loi pertinente doit préciser dans le détail les circonstances précises dans lesquelles une telle immixtion peut être autorisée[14]. L'immixtion est illégale et arbitraire non seulement lorsqu'elle n'est pas prévue par la loi, mais aussi lorsque le texte de loi ou l'immixtion particulière est contraire aux dispositions, aux buts et aux objectifs du Pacte[15]. Toute limitation de ce droit n'est légale et non arbitraire que si elle sert un but légitime (voir A/HRC/29/32, par. 33). Il faut que la limitation soit nécessaire pour atteindre cet objectif légitime, qu'elle soit proportionnée à cet objectif et qu'elle constitue l'option la moins intrusive possible. En outre, aucune limitation du droit à la vie privée ne peut vider de son sens le principe de ce droit (voir A/69/397, par. 51).

11. Le droit à la vie privée est essentiel à la jouissance et à l'exercice des droits de l'homme en ligne et hors ligne. Il constitue l'un des fondements de toute société démocratique et joue un rôle clef dans la réalisation d'un large éventail de droits de l'homme, allant de la liberté d'expression (voir A/HRC/23/40 et A/HRC/29/32, par. 15) à la liberté d'association et de réunion (voir A/HRC/31/66, par. 73 à 78 et A/72/135, par. 47 à 50) en passant par l'interdiction de la discrimination et d'autres droits[16]. L'immixtion dans la vie privée peut avoir des effets disproportionnés sur certaines personnes et/ou groupes et accentuer de la sorte les inégalités et la discrimination[17]. Des réglementations trop étendues en matière de protection de la vie privée peuvent également donner lieu à des limitations injustifiées d'autres droits, en particulier de la liberté d'expression, par exemple lorsqu'une réglementation aux visées excessives entrave la réalisation légitime de reportages d'actualité, de travaux d'expression artistique ou d'activités de recherche scientifique.

[10] Voir également Cour européenne des droits de l'homme, *Rotaru* c. *Roumanie*, requête nº 28341/95, arrêt du 4 mai 2000, et *Kopp* c. *Suisse*, requête nº 23224/94, arrêt du 25 mars 1998.

[11] Voir aussi Cour européenne des droits de l'homme, *Roman Zakharov* c. *Russie*, requête nº 47143/06, arrêt du 4 décembre 2015.

[12] Voir Comité des droits de l'homme, observation générale nº 31 (2004) sur la nature de l'obligation juridique imposée aux États parties au Pacte, par. 8.

[13] Voir aussi la résolution 34/7 du Conseil des droits de l'homme, par. 2.

[14] Voir Comité des droits de l'homme, observation générale nº 16 (1988) sur le droit au respect de la vie privée, par. 3 et 8.

[15] Ibid., par. 4.

[16] Voir Paul Bernal, « Data gathering, surveillance and human rights: recasting the debate ».

[17] Voir la résolution 71/199 de l'Assemblée générale, par. 5 g) ; la résolution 34/7 du Conseil des droits de l'homme, par. 5 g) ; et la communication du Réseau international des organisations pour les libertés civiles soumise pour le présent rapport.

Faute d'espace, il n'est pas possible d'examiner dans le présent rapport les relations entre le droit à la vie privée et l'ensemble des autres droits de l'homme, l'effet discriminatoire que ce droit peut avoir sur divers groupes et personnes, ainsi que les différentes approches des moyens de protéger ces groupes et personnes.

III. Immixtions dans la vie privée : tendances et sujets de préoccupation

A. Utilisation accrue des données personnelles par les États et les entreprises commerciales

Croissance du nombre d'empreintes numériques

12. Tant les États que les entreprises commerciales collectent et utilisent de plus en plus de données relatives à la vie privée des particuliers. D'énormes flux de données relatives à des milliards d'individus sont collectés par des ordinateurs personnels, des téléphones intelligents, des montres intelligentes, des systèmes de suivi des performances sportives et d'autres systèmes portables. Un nombre croissant d'autres dispositifs et capteurs interconnectés installés dans les maisons et les villes dites « intelligentes » y ajoutent des données supplémentaires. L'éventail et la profondeur des informations recueillies et utilisées sont vastes : éléments d'identification des appareils, adresses électroniques et numéros de téléphone, données biométriques, données sur la santé et les finances, ou encore modèles de comportement. Une grande partie de ces actions se produisent à l'insu des personnes concernées et sans leur consentement éclairé.

Le partage et la fusion des données

13. Les entreprises commerciales et les États échangent et fusionnent en permanence des données personnelles provenant de diverses sources et bases de données, et les courtiers en données occupent dans ce domaine une position clef. En conséquence, les individus se trouvent dans une position d'impuissance, car il leur est presque impossible de savoir qui détient quel type d'information les concernant, et encore moins de contrôler les nombreux usages faits de cette information.

Données biométriques

14. Les États et les entreprises déploient de plus en plus de systèmes reposant sur la collecte et l'utilisation de données biométriques, telles que l'ADN, la géométrie faciale, la voix, les caractéristiques de la rétine ou de l'iris et les empreintes digitales. Certains pays ont créé d'immenses bases de données centralisées stockant ces informations à des fins diverses, allant de la sécurité nationale et des enquêtes pénales à l'identification des personnes à des fins liées à la fourniture de services essentiels, tels que les services sociaux et financiers ou l'éducation. Dans le monde entier, les acteurs étatiques déploient, dans les villes, les gares ferroviaires et les aéroports, des caméras de télévision en circuit fermé qui utilisent la reconnaissance faciale pour identifier et signaler automatiquement des individus. Les technologies biométriques sont de plus en plus utilisées pour contrôler les migrations, tant aux frontières qu'à l'intérieur des pays. La création de bases de données biométriques de masse soulève d'importantes préoccupations touchant aux droits de l'homme. De telles données sont particulièrement sensibles, car elles sont par définition indissociables de la personne et de sa vie, et peuvent faire l'objet de graves abus. Par exemple, l'usurpation d'identité au moyen des données biométriques est un danger extrêmement difficile à traiter et peut porter gravement atteinte aux droits de la personne. En outre, les données biométriques peuvent être utilisées à des fins différentes de celles pour lesquelles elles ont été collectées, notamment pour localiser et surveiller illégalement des personnes. Compte tenu de ces risques, il convient d'accorder une attention particulière aux questions relatives à la nécessité et à la proportionnalité de la collecte de données biométriques. Cela étant, il est inquiétant de constater que certains États se lancent dans de vastes projets fondés sur des données biométriques sans avoir mis en place des garanties juridiques et procédurales adéquates.

Augmentation de la puissance d'analyse

15. La puissance d'analyse des technologies axées sur les données continue d'augmenter de manière exponentielle. L'analyse des mégadonnées et l'intelligence artificielle permettent de plus en plus aux États et aux entreprises d'obtenir des informations détaillées sur la vie des personnes, de tirer des conclusions quant à leurs caractéristiques physiques et mentales, et de créer des profils de personnalité détaillés. De nombreux systèmes utilisés par les États et les entreprises sont conçus dans ce but précis : augmenter autant que possible la quantité d'informations sur les individus afin de les analyser, d'établir leur profil, de les évaluer, de les catégoriser et finalement de prendre des décisions, souvent automatisées, à leur sujet.

16. L'environnement qui en résulte entraîne des risques pour les particuliers et pour les sociétés qu'il ne faudrait pas sous-estimer. Par exemple, on a assisté ces dernières années à des atteintes à la protection des données d'une ampleur considérable, qui ont exposé les personnes concernées à l'usurpation d'identité et à la divulgation d'informations relevant de la sphère privée. Des opérations de collecte et d'analyse illégitimes de données ont été effectuées pour cibler les électeurs. Le profil, la « notation » et le « classement » des individus peuvent être utilisés pour évaluer l'admissibilité à une assurance médicale, à d'autres types d'assurance, à des services financiers et autres. Dans les affaires dont l'enjeu est important, par exemple dans les procédures de détermination de la peine et les évaluations de récidive, les décisions fondées sur des données opaques peuvent menacer les garanties d'une procédure régulière. Les tentatives de définir certains individus comme des menaces potentielles pour la sécurité dans le cadre des services de police prédictifs soulèvent des préoccupations en raison des questions liées à la transparence, à la portée excessive des systèmes, au principe de responsabilité et au risque d'obtenir des résultats discriminatoires[18].

B. Surveillance de l'État et interception des communications

Surveillance de masse

17. De nombreux États continuent d'exercer une surveillance secrète, de procéder à des interceptions de masse des communications et de recueillir, conserver et analyser les données de tous les utilisateurs d'un large éventail de moyens de communication (par exemple, les courriels, les appels téléphoniques et vidéo, les messages texte et les sites Web visités). Même si certains États affirment qu'une telle surveillance de masse indifférenciée est nécessaire pour protéger la sécurité nationale, « le droit international des droits de l'homme n'autorise pas [cette pratique], puisqu'une analyse de la nécessité et de la proportionnalité d'une mesure par rapport à un individu donné ne serait pas possible dans le contexte de telles mesures » (voir A/HRC/33/29, par. 58)[19]. Comme l'a souligné la Cour européenne des droits de l'homme, « un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre »[20].

Accès aux données des utilisateurs des entreprises commerciales

18. Les États s'appuient souvent sur des entreprises commerciales pour procéder à la collecte et à l'interception des données personnelles. Par exemple, certains États obligent les fournisseurs de services de télécommunications et d'accès à Internet à leur donner un accès direct aux flux de données circulant sur leurs réseaux. Ces systèmes d'accès direct sont très préoccupants, car ils sont particulièrement susceptibles de donner lieu à des abus et tendent à contourner les principales garanties procédurales[21]. Certains États exigent également d'avoir accès aux quantités massives d'informations recueillies et conservées par

[18] Voir Ajay Sandhu, « Data driven policing: highlighting some risks associated with predicting crime », Human Rights Centre, Université de l'Essex.

[19] Voir aussi A/HRC/27/37, par. 25.

[20] Voir *Roman Zakharov* c. *Russie*, par. 232.

[21] Voir *Roman Zakharov* c. *Russie*, par. 270.

les fournisseurs de services de télécommunications et d'accès à Internet. Des États continuent d'imposer aux entreprises de télécommunications et aux fournisseurs d'accès à Internet l'obligation de conserver les données relatives aux communications pendant de longues périodes[22]. Nombre de ces lois exigent des entreprises qu'elles collectent et conservent de manière indifférenciée l'ensemble des données relatives au trafic de tous les abonnés et utilisateurs concernant tous les moyens de communication électronique. Elles limitent les possibilités qu'ont les particuliers de communiquer de façon anonyme, engendrent des risques d'abus et peuvent faciliter la divulgation d'informations à des tiers, y compris des criminels, des opposants politiques ou des concurrents commerciaux, au moyen de piratages informatiques ou d'autres atteintes à la protection des données. Ces lois dépassent les limites de ce qui peut être considéré comme nécessaire et proportionné[23].

Piratage informatique

19. Apparemment, les États s'appuient de plus en plus sur des logiciels d'intrusion offensive qui infiltrent les appareils numériques des individus. Ce type de piratage permet l'interception et la collecte indifférenciées de toutes formes de communications et de données, chiffrées ou non, ainsi que l'accès à distance et secret aux appareils personnels et aux données qui y sont conservées, ce qui permet de procéder à une surveillance en temps réel et de manipuler les données stockées dans ces appareils[24]. Cela pose des risques non seulement pour le droit à la protection de la vie privée, mais aussi pour le droit à l'équité procédurale en cas d'utilisation de ce type de preuve dans les procès (voir A/HRC/23/40, par. 62). Le piratage informatique soulève également d'importantes préoccupations en matière d'extraterritorialité, car il peut toucher des personnes dans de nombreuses juridictions[25]. De plus, il repose sur l'exploitation des vulnérabilités des systèmes de technologies de l'information et des communications (TIC), et contribue ainsi aux menaces pour la sécurité de millions d'utilisateurs.

Tentatives d'affaiblissement du chiffrement et de l'anonymat

20. Les tentatives répétées des États d'affaiblir les technologies de chiffrement et de limiter l'accès aux outils d'anonymat menacent également la sécurité et la confidentialité des communications et d'autres activités en ligne. Certains États exigent l'intégration de « portes dérobées » dans les communications chiffrées, imposent aux fournisseurs de services de communications chiffrées qu'ils leur remettent les clefs de chiffrement (voir A/HRC/29/32, par. 38 à 45), ou vont jusqu'à interdire ou bloquer certaines applications de communications sécurisées, notamment les messageries chiffrées, les réseaux virtuels privés et les réseaux d'anonymisation. Le chiffrement et l'anonymat offrent aux individus et aux groupes une zone de confidentialité en ligne où ils peuvent exprimer leurs opinions et exercer leur liberté d'expression sans immixtion ou attaque arbitraire et illégale (A/HRC/29/32)[26]. Les outils de chiffrement et d'anonymat sont largement utilisés dans le monde entier, notamment par les défenseurs des droits de l'homme, la société civile, les journalistes, les lanceurs d'alerte et les dissidents politiques qui doivent faire face à la persécution et au harcèlement. Leur affaiblissement compromet la vie privée de tous les utilisateurs et les expose à des immixtions illégales non seulement de la part des États, mais aussi de la part d'acteurs non étatiques, y compris des réseaux criminels[27]. Des effets aussi

[22] Voir CCPR/C/ZAF/CO/1, par. 42 et 43, et CCPR/C/PAK/CO/1, par. 35 et 36.

[23] Voir, par exemple, Cour de justice européenne, affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB* c. *Autorité suédoise des postes et télécommunications*, et *Secretary of State for the Home Department* c. *Watson*, arrêt du 21 décembre 2016, par. 107 ; CCPR/C/ZAF/CO/1, par. 42 et 43 ; CCPR/C/CMR/CO/5, par. 39 et 40.

[24] Voir Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « Encryption and anonymity follow-up report » (juin 2018).

[25] Voir la communication de Privacy International.

[26] Voir aussi Faculté de droit d'Irvine de l'Université de Californie (Justice internationale), « Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression » ; Amnesty International, « Encryption. A matter of human rights » (mars 2016) ; et Wolfgang Schulz et Joris van Hoboken, « Human Rights and Encryption », Organisation des Nations Unies pour l'éducation, la science et la culture (2016).

[27] Voir https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138.

généralisés et indifférenciés ne sont pas compatibles avec le principe de proportionnalité (voir A/HRC/29/32, par. 36).

Échange de renseignements

21. Partout dans le monde, les États échangent régulièrement des renseignements sur des individus en dehors de tout cadre légal et sans contrôle adéquat [28]. L'échange de renseignements pose le risque sérieux qu'un État utilise cette méthode pour contourner les contraintes juridiques qui lui sont imposées au niveau national en s'appuyant sur d'autres pays pour obtenir et ensuite échanger des informations. Une telle pratique ne remplit pas les conditions voulues pour être légale et est susceptible de porter atteinte à l'essence du droit à la vie privée (voir A/HRC/27/37, par. 30). La menace qui pèse sur la protection des droits de l'homme est particulièrement grave lorsque les renseignements sont partagés avec des pays où l'état de droit est fragile ou qui violent systématiquement les droits de l'homme. Les renseignements reçus par un État d'un autre État peuvent avoir été obtenus en violation du droit international, notamment par la torture et d'autres traitements cruels, inhumains ou dégradants. Les risques qu'entraîne l'échange de renseignements s'agissant du respect des droits de l'homme sont aggravés par le manque actuel de transparence, de responsabilisation et de contrôle en ce qui concerne les accords d'échange de renseignements (voir A/69/397, par. 44, CCPR/C/GBR/CO/7, par. 24, et CCPR/C/SWE/CO/7, par. 36). À de très rares exceptions près, la législation n'encadre pas l'échange de renseignements au moyen d'une base légale appropriée et conforme au principe de légalité défini par le droit international des droits de l'homme[29].

Accès transfrontalier aux données détenues par des entreprises commerciales

22. Récemment, des efforts ont été faits pour créer des mécanismes juridiques destinés à faciliter l'accès des États aux données personnelles conservées sur les serveurs des entreprises commerciales à l'étranger. L'obtention de preuves dans le cadre d'une enquête pénale est sans aucun doute un objectif important et légitime. Toutefois, un tel accès peut affaiblir les garanties d'une procédure régulière ou permettre de les contourner ; c'est notamment le cas pour ce qui concerne l'obligation d'obtenir l'autorisation d'un organisme indépendant et la mise en place de mécanismes de contrôle adéquats. Les demandes d'accès transfrontalier aux données peuvent également avoir une incidence négative sur la possibilité pour les citoyens de recourir aux mécanismes d'appel et de recours. Il est particulièrement préoccupant de constater que des pays dans lesquels l'état de droit est fragile ou qui ont des antécédents problématiques en matière de droits de l'homme peuvent avoir accès à des informations sensibles sur des individus sans que des mesures de protection adéquates contre les violations des droits de l'homme aient été mises en place.

IV. Responsabilités des États

A. Responsabilité de l'État de respecter le droit à la vie privée à l'ère du numérique et devoir de protéger ce droit

23. L'article 2 1) du Pacte international relatif aux droits civils et politiques impose aux États de 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 le Pacte, sans distinction aucune. Les États parties doivent s'abstenir de violer les droits reconnus par le Pacte, et toute restriction à leur exercice doit être autorisée par les dispositions pertinentes du Pacte[30]. Toutefois, les obligations des États vont au-delà de l'obligation de respecter ces droits et comprennent également l'adoption de mesures « positives » visant à en protéger l'exercice. Pour ce qui concerne le droit à la vie privée, cela implique l'obligation d'adopter

[28] Voir Privacy International, « Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards » (avril 2018) et https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

[29] Voir la communication de Privacy International.

[30] Voir Comité des droits de l'homme, observation générale n° 31, par. 6.

des mesures législatives et autres pour donner effet à l'interdiction des immixtions et des atteintes illégales ou arbitraires, et à la protection contre celles-ci, qu'elles émanent des pouvoirs publics ou de personnes physiques ou morales[31].

24. L'obligation de protéger est prise en considération dans le premier pilier des Principes directeurs relatifs aux entreprises et aux droits de l'homme, intitulé « Obligation de protéger les droits de l'homme incombant à l'État », qui donne des précisions sur les incidences de l'obligation qu'ont les États de protéger les citoyens contre les atteintes aux droits de l'homme auxquelles participent des entreprises. Le premier des Principes directeurs exige l'adoption de mesures appropriées pour empêcher ces atteintes, et lorsqu'elles se produisent, enquêter à leur sujet, en punir les auteurs, et les réparer par le biais de politiques, de lois, de règles et de procédures judiciaires. Les principes qui suivent décrivent les différents domaines législatifs et de politique générale dans lesquels les États devraient adopter un ensemble judicieux de mesures − nationales et internationales, obligatoires et volontaires − propres à promouvoir le respect des droits de l'homme par les entreprises[32]. Parmi les exemples d'application de l'approche adoptée dans les Principes directeurs en ce qui concerne le secteur des TIC, on peut citer les orientations sectorielles élaborées au niveau de l'Union européenne, qui sont axées sur la manière dont les entreprises des TIC devraient gérer tout effet préjudiciable de leurs activités.

25. Le devoir des États de protéger les personnes contre les violations du droit à la vie privée par les entreprises et d'autres tierces parties établies ou domiciliées dans leur juridiction a des effets extraterritoriaux. Par exemple, les États devraient mettre en place des régimes de contrôle des exportations applicables aux technologies de surveillance de manière à pouvoir évaluer le cadre juridique régissant l'utilisation de ces technologies dans le pays de destination, le bilan de l'utilisateur final proposé en matière de droits de l'homme, et les garanties et procédures de contrôle en place concernant l'application des pouvoirs de surveillance. Les garanties en matière de droits de l'homme doivent être intégrées dans les accords de licence d'exportation. En outre, les États ont le devoir de protéger les personnes relevant de leur juridiction contre toute atteinte extraterritoriale à leur droit à la vie privée, telle que l'interception de communications ou le piratage informatique.

B. Responsabilité incombant à l'État de mettre en place des garanties suffisantes et un contrôle efficace

26. L'exercice du droit à la vie privée est largement tributaire de la qualité et de l'efficacité des garanties et des mécanismes de contrôle que prévoit le cadre juridique, réglementaire et institutionnel. À une époque où les États et les entreprises ont accès à une grande quantité de données personnelles et où les particuliers ont peu d'indications et guère de moyens de contrôler l'usage qui est fait des données concernant leur personne ou leur vie, il est essentiel que l'attention soit portée sur les mesures qui atténuent l'incidence de ces asymétries, en ce qui concerne le pouvoir et d'information, sur les droits de l'homme.

1. Cadre général de protection contre les immixtions injustifiées

27. Le cadre public de la protection de la vie privée devrait notamment reposer sur des lois établissant les normes relatives au traitement des renseignements personnels par les États et par les acteurs privés[33]. Les États ont certes toute latitude pour définir un ensemble judicieux de mesures régissant l'utilisation des renseignements personnels par les entreprises mais, à l'alinéa 2 de son article 17, le Pacte international relatif aux droits civils

[31] Voir Comité des droits de l'homme, observations générales nº 16, par. 1 et 9, et nº 31, par. 8.

[32] Voir le Principe directeur 2 et son commentaire.

[33] Voir l'observation générale nº 16 du Comité des droits de l'homme, par. 9, le document A/HRC/13/37, par. 61 et le document A/HRC/17/27, par. 56. Pour un aperçu de la législation relative à la confidentialité des données, voir Graham Greenleaf, University of New South Wales, communication aux fins du présent rapport. Dans le cadre du présent rapport, on entend par « traitement » toute opération effectuée sur des données à caractère personnel, notamment la collecte, la conservation, l'utilisation, la modification, la suppression, la divulgation, le transfert et la combinaison.

et politiques énonce la nécessité de protéger les personnes au moyen de la loi. L'imbrication toujours plus grande du traitement des données publiques et du traitement des données privées et le bilan à ce jour, qui montre un usage abusif, généralisé et récurrent de renseignements personnels par certaines entreprises, confirment que des mesures législatives sont nécessaires pour atteindre un niveau adéquat de protection de la vie privée[34].

28. Il existe un consensus croissant au niveau mondial au sujet des normes minimales qui devraient régir le traitement des données personnelles par les États, les entreprises et d'autres acteurs privés. Parmi les directives et les instruments internationaux tenant compte de cette évolution, on peut citer les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (1990), la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981) et sa version actualisée, qui fixe un niveau élevé de protection au niveau mondial[35], les Lignes directrices régissant la protection de la vie privée que l'Organisation de coopération et de développement économiques a établies en 1980 et qu'elle a révisées en 2013, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo, 2014), la résolution de Madrid de la Conférence internationale annuelle des commissaires à la protection des données et à la vie privée et, enfin, le cadre de protection de la vie privée « Privacy Framework » de 2015 de la Coopération économique Asie-Pacifique. Ces normes, en particulier la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, sont à l'origine des cadres de protection des données personnelles de nombreux États et peuvent orienter la conception d'instruments de politique adéquats[36].

29. Les instruments et directives mentionnés ci-dessus définissent un ensemble de principes clefs, de droits et d'obligations qui garantissent un niveau minimum de protection des données personnelles. Premièrement, le traitement des données personnelles doit être équitable, légal et transparent. Les particuliers dont les données personnelles sont traitées devraient être informés de ce traitement, des conditions dans lesquelles il a lieu, de sa nature et de son ampleur, notamment dans le cadre de politiques transparentes en matière de confidentialité des données. Pour prévenir l'utilisation arbitraire des renseignements personnels, il faut que le traitement des données personnelles s'appuie sur le consentement libre, exprès, éclairé et sans équivoque des particuliers concernés ou sur un autre fondement légitime prévu par la loi[37]. Le traitement des données personnelles doit répondre à une nécessité et être proportionné par rapport à un objectif légitime que l'entité responsable du traitement devrait préciser. Par conséquent, la quantité et le type de données, ainsi que la période de conservation de ces données doivent être limités ; les données doivent être exactes et les techniques d'anonymisation et de pseudonymisation utilisées chaque fois que possible. Il faut éviter de changer l'objectif de départ sans le consentement préalable de la personne concernée mais, si le changement a lieu, il doit être limité de telle sorte que les nouveaux objectifs soient compatibles avec celui défini au départ. Comme les données personnelles risquent d'être divulguées, modifiées ou supprimées sans autorisation, il est primordial de prendre des mesures de sécurité appropriées. De plus, les entités qui traitent des données à caractère personnel devraient être responsables de leur conformité au cadre juridique et politique applicable à ce domaine. Enfin, les données sensibles devraient bénéficier d'un niveau de protection particulièrement élevé[38].

[34] Voir les résolutions du Conseil des droits de l'homme n[os] 34/7 (par. 5 f)) et 38/7 (par. 17).

[35] Outre les 47 États membres du Conseil de l'Europe, Maurice, le Sénégal, la Tunisie et l'Uruguay ont ratifié la Convention et plusieurs autres États sont en passe d'y adhérer.

[36] Pour des orientations plus précises, voir https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection et Access Now, « Creating a data protection framework: a do's and don'ts guide for lawmakers. Lessons from the EU general data protection regulation » (2018).

[37] Voir l'article 5 2) de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans sa version actualisée, l'article 13 1) de la Convention de Malabo et le principe 12 de la résolution de Madrid.

[38] Voir l'article 6 de la version actualisée de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

30. Dans tous les instruments et directives mentionnés ci-dessus, il est reconnu que certains droits doivent être garantis aux personnes dont les données sont traitées. Au minimum, il s'agit du droit de savoir si leurs données sont conservées et traitées, du droit d'accès aux données stockées, du droit de rectifier les données inexactes ou anciennes et du droit de supprimer ou rectifier les données stockées illégalement ou inutilement. Les instruments plus récents ont établi des droits complémentaires importants, notamment le droit de s'opposer au traitement des données à caractère personnel, au moins dans les cas où l'entité ne démontre pas qu'il existe des motifs légitimes et impérieux de traiter des données[39]. Les États devraient s'attacher en particulier à mettre en place une protection solide contre les immixtions dans la vie privée par le biais du profilage et de la prise de décisions automatisée. Les droits décrits plus haut devraient également s'appliquer aux informations obtenues, déduites et prédites par des moyens automatisés, dans la mesure où ces informations sont considérées comme des données à caractère personnel. Il est important que le cadre juridique garantisse que ces droits ne limitent pas indûment le droit à la liberté d'expression, notamment par le traitement des données personnelles à des fins journalistiques, artistiques et académiques.

31. Les cadres de protection des données personnelles devraient également établir certaines obligations pour les entités responsables du traitement des données personnelles. Ces obligations englobent des aspects organisationnels, comme la mise en place d'un mécanisme de contrôle interne, mais aussi des mesures impératives, comme les notifications de violation de données et les évaluations de l'incidence sur la vie privée. Dans un environnement technologique de plus en plus complexe, les évaluations de ce type jouent un rôle essentiel dans la prévention et l'atténuation des atteintes à la vie privée[40]. Par ailleurs, les prescriptions relatives à la conception des produits et des services, telles que la protection des données dès la conception[41] et la protection des données par défaut[42], sont des outils essentiels permettant de protéger le droit à la vie privée.

32. Dans un monde globalisé, les transferts de données, notamment de grandes quantités de données personnelles, sont monnaie courante et sont nécessaires au fonctionnement de nombreux services. Les États doivent veiller à ce que ces transferts ne constituent pas une immixtion injustifiée dans la vie privée et à ce qu'ils ne favorisent pas non plus une telle immixtion. Il convient en même temps d'éviter les exigences strictes de localisation des données, qui obligent toutes les entités de traitement des données à stocker toutes les données personnelles à l'intérieur d'un pays donné (voir A/HRC/32/38, par. 61). Les États devraient plutôt porter leur attention sur les moyens de s'assurer que les données personnelles transférées à un autre État soient protégées au moins au niveau exigé par le droit international des droits de l'homme.

33. Les États devraient établir des organes de contrôle indépendants pour le traitement des données à caractère personnel. Ces organes sont essentiels pour protéger les droits fondamentaux de chacun contre les pratiques abusives en matière de traitement des données personnelles. Toute autorité de surveillance doit pouvoir s'appuyer sur une base légale établissant clairement son mandat, ses pouvoirs et son indépendance. Ces organes de contrôle doivent être dotés des ressources techniques, financières et humaines nécessaires pour contrôler efficacement les activités de traitement des données menées par les États et les entreprises et faire respecter les règles à cet égard. De plus, ces organes doivent avoir un pouvoir légal suffisant pour exercer leurs fonctions, notamment pour imposer des sanctions proportionnées aux violations ou atteintes commises[43].

[39] Ibid., art. 9 1) d). Voir aussi l'article 21 du Règlement général sur la protection des données et l'article 18 1) de la Convention de Malabo.

[40] Pour une analyse approfondie des approches des évaluations de l'incidence sur la vie privée, voir David Wright et Paul de Hert, eds., *Privacy Impact Assessment* (New York, Springer, 2012).

[41] Ce qui signifie que la protection de la vie privée doit être intégrée dès la conception de tout système.

[42] Qui exige que les systèmes appliquent par défaut des paramètres de respect de la vie privée.

[43] Voir par exemple https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

2. Garanties de procédure et contrôle des activités de surveillance et d'interception des communications

Garanties

34. Le Rapporteur spécial sur le droit à la vie privée a constaté que, alors que toutes les activités de l'État concernant la surveillance doivent être menées en vertu d'une loi (voir A/HRC/27/37, par. 28), dans de nombreux cas, ladite loi fait défaut. Il convient de noter que dans nombre de pays, les services de renseignements et des forces de l'ordre sont exclus des dispositions de la législation sur la protection des données personnelles. Pareilles exceptions devraient être limitées et fondées sur les principes de nécessité et de proportionnalité, de façon à garantir un niveau adéquat de confidentialité des données dans tous les services de l'État. La législation sur la surveillance devrait respecter les normes minimales décrites ci-après.

35. La loi doit être accessible au public. Les règles et interprétations secrètes de la loi n'ont pas les qualités nécessaires pour constituer de tels « textes législatifs » (ibid., par. 29). Les lois doivent être suffisamment précises. Le pouvoir discrétionnaire accordé à l'exécutif et la manière dont ce pouvoir peut être exercé doivent être définis avec suffisamment de clarté (voir A/69/397, par. 35)[44]. À cette fin, la nature de l'infraction et la catégorie de personnes qui peuvent faire l'objet d'une surveillance doivent être décrites. Les justifications vagues et excessivement générales, comme les références imprécises à la « sécurité nationale », ne constituent pas des lois acceptables. La surveillance ne peut être justifiée que par un « soupçon raisonnable » et toute décision qui l'autorise doit être suffisamment ciblée[45]. La loi doit attribuer strictement les compétences concernant la surveillance et l'accès au produit de la surveillance à des autorités précises.

36. En ce qui concerne son champ d'application, le cadre juridique de la surveillance devrait englober les demandes faites par les États aux entreprises. Il devrait également comporter l'accès aux renseignements détenus en dehors du territoire ou l'échange de renseignements avec d'autres États. La loi doit expressément prévoir une structure visant à garantir la responsabilité et la transparence des institutions de l'État chargées de la surveillance.

37. Les pouvoirs de surveillance secrète ne peuvent être justifiés que s'ils sont strictement nécessaires pour parvenir à un objectif légitime et qu'ils satisfont la condition de la proportionnalité (voir A/HRC/23/40, par. 83 b))[46]. Pareilles mesures ne doivent être utilisées que pour prévenir les infractions ou contrer les menaces les plus graves, ou pour enquêter à leur sujet. La durée d'exécution de la mesure doit être limitée au strict minimum nécessaire pour atteindre l'objectif défini. L'utilisation et le stockage des données obtenues doivent obéir à des règles strictes et les circonstances dans lesquelles les données recueillies et stockées doivent être effacées doivent être clairement définies en fonction des critères de nécessité et de proportionnalité[47]. Le partage du renseignement doit suivre les mêmes principes de légalité, de nécessité et de proportionnalité.

38. Lorsqu'ils envisagent des mesures de piratage ciblées, les gouvernements devraient adopter une approche extrêmement prudente en ne recourant à de telles mesures que dans des circonstances exceptionnelles, à des fins d'enquête sur les infractions ou menaces les plus graves ou de prévention de telles menaces, et en y associant le pouvoir judiciaire (voir CCPR/C/ITA/CO/6, par. 37)[48]. Les opérations de piratage devraient être conçues avec rigueur et, dans leur cadre, l'accès à l'information devrait être limité à certains types de renseignements correspondant à des objectifs précis. Les États devraient s'abstenir d'obliger des entités privées à participer aux opérations de piratage pour qu'il n'y ait pas d'incidence sur la sécurité de leurs propres produits et services. Le décryptage obligatoire

[44] Voir également *Roman Zakharov* c. *Russie*, par. 230.

[45] Ibid., par. 248 et 260.

[46] Voir également *Szabo and Vissy* c. *Hongrie*, par. 73.

[47] Voir *Roman Zakharov* c. *Russie*, par. 231.

[48] Voir également Access Now, « A human rights response to government hacking » (septembre 2016) et Privacy International, « Government hacking and surveillance: 10 necessary safeguards ».

ne peut être autorisé que de manière ciblée, au cas par cas, et sous réserve d'un mandat judiciaire et de la protection du droit à une procédure régulière (voir A/HRC/29/32, par. 60).

Indépendance du dispositif d'autorisation et de contrôle[49]

39. Les mesures de surveillance, en ce comprises les demandes de communication de données adressées aux entreprises et l'échange de renseignements, devraient être autorisées, examinées et supervisées par des organes indépendants à chaque étape, notamment lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé (voir CCPR/C/FRA/CO/5, par. 5)[50]. L'organe indépendant qui autorise des mesures de surveillance particulières, de préférence une autorité judiciaire, doit s'assurer qu'il existe des éléments de preuve évidents d'une menace suffisamment importante et que la surveillance proposée est ciblée, strictement nécessaire et proportionnée, et il doit autoriser (ou rejeter) *ex ante* les mesures de surveillance.

40. Les cadres de contrôle peuvent intégrer des mesures de contrôle administratif, judiciaire et/ou parlementaire[51]. Les organes de contrôle ne peuvent dépendre des autorités chargées de la surveillance et doivent être dotés d'une expérience, de compétences et de ressources appropriées et adéquates. L'autorisation et le contrôle devraient être séparés sur le plan institutionnel. Les organes de contrôle indépendants devraient enquêter de manière proactive, surveiller les activités de ceux qui exercent la surveillance et avoir accès aux produits de la surveillance ; ils devraient également procéder périodiquement à l'examen des capacités de surveillance et des progrès technologiques accomplis. Les organismes chargés de la surveillance devraient être tenus de fournir toutes les informations nécessaires à un contrôle efficace sur demande, de faire régulièrement rapport aux organes de contrôle et de tenir des registres de toutes les mesures de surveillance prises[52]. Les processus de contrôle doivent également être transparents et soumis à un examen public approprié, et les décisions des organes de contrôle doivent pouvoir faire l'objet d'un appel ou d'un examen indépendant. En l'absence d'un processus contradictoire, il est particulièrement important d'exposer les organes de contrôle à des points de vue divergents, par exemple dans le cadre de consultations d'experts et de consultations multipartites (voir par exemple A/HRC/36/40, par. 36) : il est essentiel que les « points de friction », autrement dit le questionnement permanent des choix et des visions retenus, soient intégrés[53].

Principe de transparence

41. Il faut aussi que les autorités de l'État et les organes de contrôle expliquent à la population les lois, politiques et pratiques existantes en matière de surveillance et d'interception des communications, et les autres formes de traitement des données à caractère personnel, un débat ouvert et un examen approfondi étant essentiels pour faire comprendre les avantages et les limites des techniques de surveillance (voir A/HRC/13/37, par. 55). Il convient que les personnes qui ont fait l'objet de mesures de surveillance en soient informées et il faut leur expliquer a posteriori les raisons de l'ingérence dans leur vie privée. Elles devraient également avoir le droit de faire modifier ou supprimer les renseignements personnels non pertinents les concernant, pour autant que ces renseignements ne soient plus nécessaires à l'enquête en cours ou à venir (voir A/HRC/34/60, par. 38).

[49] Voir A/HRC/34/60 et Agence des droits fondamentaux de l'Union européenne, *Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne. Volume II : évolution juridique et situation sur le terrain* (Luxembourg, Office des publications de l'Union européenne, 2017).

[50] Voir également *Roman Zakharov* c. *Russie*, par. 233.

[51] Voir la résolution 71/199 de l'Assemblée générale, par. 5 d).

[52] Voir Cour européenne des droits de l'homme, *Kennedy* c. *Royaume-Uni*, requête nº 26839/05, arrêt du 18 mai 2010, par. 165 et *Roman Zakharov* c. *Russie*, par. 272.

[53] Voir Human Rights, Big Data and Technology Project, Human Rights Centre, University of Essex, communication aux fins du présent rapport.

V. Responsabilités des entreprises

42. Le deuxième pilier des Principes directeurs relatifs aux entreprises et aux droits de l'homme offre un plan détaillé et rigoureux à toutes les entreprises, indépendamment de leur taille, de leur secteur, de leur cadre de fonctionnement, de leur régime de propriété et de leur structure, sur la prévention des incidences négatives sur les droits de l'homme, notamment sur le droit à la vie privée, et sur la réparation de celles qui ont été causées[54]. Il énonce la responsabilité incombant aux entreprises de respecter tous les droits de l'homme reconnus internationalement ; il s'agit pour les entreprises d'éviter de porter atteinte aux droits de l'homme d'autrui et de remédier aux incidences négatives sur les droits de l'homme d'activités auxquelles elles participent[55]. Cette responsabilité s'applique à l'ensemble des activités et des relations commerciales des entreprises. Dans l'espace numérique, il est particulièrement important que la responsabilité de respecter les droits de l'homme s'applique, où que se trouvent les personnes concernées. Cette responsabilité existe indépendamment du fait que l'État remplit ou non ses propres obligations relatives aux droits de l'homme.

43. Pour assumer leur responsabilité de respecter les droits de l'homme, les entreprises doivent : a) s'abstenir de toute activité aux incidences négatives sur les droits de l'homme ; b) s'abstenir de contribuer aux incidences négatives sur les droits de l'homme par leurs propres activités, que ce soit directement ou par l'intermédiaire d'une entité extérieure (État, entreprise ou autre) ; c) s'efforcer de prévenir ou d'atténuer les incidences négatives sur les droits de l'homme qui sont directement liées à leurs activités, produits ou services par leurs relations commerciales, même si elles n'ont pas contribué à ces incidences[56]. Par exemple, l'entreprise qui fournit des données sur les utilisateurs à un État qui utilise ensuite ces données pour retrouver et poursuivre des dissidents politiques aura contribué à de telles atteintes aux droits de l'homme, y compris à l'atteinte au droit à la vie privée. Les entreprises qui fabriquent et vendent des technologies utilisées pour des intrusions illégales ou arbitraires contribuent également à créer des incidences négatives sur les droits de l'homme.

44. S'il existe des exigences contradictoires entre le respect du droit international des droits de l'homme et les obligations découlant du droit interne, les entreprises doivent s'efforcer de respecter le droit international des droits de l'homme dans toute la mesure possible et d'atténuer autant que faire se peut toute incidence négative, par exemple, en interprétant les demandes des autorités nationales de la manière la plus restrictive qui soit[57].

45. La responsabilité en matière de respect des droits de l'homme exige des entreprises qu'elles mettent en place des politiques et des procédures en rapport avec leur taille et leurs particularités, y compris :

a) Qu'elles prennent, à leur plus haut niveau, un engagement politique public et qu'elles ancrent leur responsabilité quant au respect des droits de l'homme dans les politiques et procédures opérationnelles[58] ;

b) Qu'elles fassent preuve de diligence raisonnable en matière de droits de l'homme, ce qui suppose :

i) De procéder à des études des incidences sur les droits de l'homme pour identifier et évaluer toutes les incidences négatives effectives ou potentielles sur les droits de l'homme ;

[54] Les Principes directeurs ont été approuvés à l'unanimité par le Conseil des droits de l'homme dans sa résolution 17/4.

[55] Principe directeur 11.

[56] Principe directeur 13. Voir aussi HCDH, « The corporate responsibility to respect human rights: an interpretive guide » (2012).

[57] Principe directeur 23.

[58] Principe directeur 16.

ii) De tenir compte de ces évaluations et de prendre les mesures qui s'imposent pour prévenir et atténuer les incidences négatives sur les droits de l'homme qui ont été recensées ;

iii) De contrôler l'efficacité de leurs mesures ;

iv) De faire connaître officiellement la manière dont elles font face aux incidences sur les droits de l'homme[59] ;

c) Qu'elles prévoient des mesures de réparation ou qu'elles collaborent à leur mise en œuvre lorsqu'elles déterminent qu'elles ont eu des incidences négatives, ou y ont contribué[60].

46. Selon les Principes directeurs, toutes les entreprises ont la responsabilité de faire preuve de diligence raisonnable en matière de droits de l'homme afin de repérer toute incidence sur les droits de l'homme de leurs activités et d'y remédier. Pour prendre un exemple concret, les entreprises qui vendent des technologies de surveillance devraient, dans le cadre de leur diligence raisonnable, procéder, avant toute transaction potentielle, à une évaluation approfondie de l'incidence sur les droits de l'homme. L'atténuation des risques devrait passer par des garanties claires d'utilisation finale stipulées dans les accords contractuels assorties de garanties solides en matière de droits de l'homme, qui empêchent l'utilisation arbitraire ou illégale de ces technologies, ainsi que par des examens périodiques de l'utilisation de ces technologies par les États[61]. Les entreprises qui collectent et conservent des données d'utilisateurs doivent évaluer les risques pour le droit à la vie privée liés à d'éventuelles demandes de ces données par les États, y compris l'environnement juridique et institutionnel des États concernés. Elles doivent prévoir des procédures et des garanties adéquates pour prévenir et atténuer les atteintes potentielles à la vie privée et aux autres droits de l'homme. Des évaluations de l'incidence sur les droits de l'homme doivent aussi être réalisées dans le cadre de l'adoption des conditions d'utilisation, du choix des caractéristiques et des techniques en matière de sécurité et de vie privée, et des décisions relatives à la fourniture ou à la cessation de services dans un contexte donné (voir A/HRC/32/38, par. 11).

47. Dans le cadre de la procédure de diligence raisonnable en matière de droits de l'homme, les Principes directeurs préconisent que les entreprises rendent compte de la façon dont elles remédient à leurs incidences sur les droits de l'homme et soient prêtes à communiquer l'information en externe, en particulier lorsque des préoccupations sont exprimées par les acteurs concernés ou en leur nom[62]. Dans l'environnement numérique, cela veut dire révéler quelles données à caractère personnel sont collectées, pendant combien de temps elles sont conservées, dans quel but, comment elles sont utilisées et avec qui et dans quelles circonstances elles sont échangées. Cela inclut les demandes d'accès aux données des utilisateurs reçues par les États. Dans les cas où les lois et réglementations nationales font obstacle à la communication de ces informations, les entreprises devraient user dans toute la mesure possible de l'influence qu'elles peuvent avoir ; elles sont également encouragées à défendre la possibilité de divulguer ces informations.

48. Dans le cadre de ses engagements politiques au titre des Principes directeurs, le secteur des technologies de l'information et des communications (TIC) a établi des directives sur les moyens à employer pour mettre en œuvre les politiques relatives aux droits de l'homme. Parmi ces initiatives, on peut citer les Principes sur la liberté d'expression et le respect de la vie privée de Global Network Initiative (les Principes GNI)[63] et les Principes directeurs de Telecommunications Industry Dialogue[64]. Par exemple,

[59] Principes directeurs 17 à 21.

[60] Principe directeur 22 et partie VI du présent rapport.

[61] Voir la communication de Privacy International au Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression (janvier 2016), disponible à l'adresse https://www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf.

[62] Principe directeur 21.

[63] Disponibles à l'adresse suivante : https://globalnetworkinitiative.org/gni-principles/. Voir aussi la communication de Global Network Initiative aux fins du présent rapport.

[64] Disponibles à l'adresse suivante : http://www.telecomindustrydialogue.org/about/guiding-principles/.

les Principes GNI disposent expressément que les entreprises participantes « mettront en place des protections en matière d'informations à caractère personnel dans tous les pays où elles opèrent et elles respecteront et œuvreront à protéger le droit au respect de la vie privée de leurs utilisateurs soumis à des exigences des autorités, des lois et des règlements nationaux, susceptibles de compromettre le respect de la vie privée d'une manière incompatible avec les lois et normes internationalement reconnues ».

49. Le Ranking Digital Rights Corporate Accountability Index note un certain nombre d'entreprises de télécommunications, Internet et téléphonie mobile en fonction de leurs engagements et de leurs politiques en matière de liberté d'expression et de protection de la vie privée[65]. Cette notation peut être s'avérer utile, pour ce qui est de tenir les entreprises responsables de leur incidence sur les droits des utilisateurs.

VI. Voies de recours

50. Les victimes de violations du droit à la vie privée ou d'atteintes à ce droit commises par des États ou des entreprises doivent avoir accès à un recours effectif. Les États ont non seulement l'obligation d'établir les responsabilités et d'offrir des voies de recours en cas d'atteintes aux droits de l'homme commises par des acteurs étatiques, mais ils doivent aussi prendre des mesures appropriées pour que les victimes d'atteintes aux droits de l'homme commises par des entreprises aient accès à un recours effectif (voir le troisième pilier des Principes directeurs relatifs aux entreprises et aux droits de l'homme). En fonction de la nature d'une affaire ou d'une situation donnée, les victimes devraient être en mesure d'obtenir réparation grâce à des mécanismes de réclamation judiciaires ou non judiciaires efficaces relevant de l'État (A/HRC/32/19, Corr.1 et Add.1 et A/HRC/38/20 et Add.1). Parmi les mécanismes non judiciaires relevant de l'État dans le contexte des TIC, on compte les autorités indépendantes chargées de surveiller les pratiques de l'État et du secteur privé en matière de confidentialité des données, comme les organismes de protection de la vie privée et des données.

51. Selon les Principes directeurs, lorsque les entreprises déterminent qu'elles ont eu des incidences négatives sur les droits de l'homme, ou qu'elles y ont contribué, elles devraient prévoir des mesures de réparation ou collaborer à leur mise en œuvre suivant des procédures légitimes[66]. Pour qu'un mécanisme non judiciaire soit efficace, il doit être légitime, accessible, prévisible, équitable, compatible avec les droits, transparent, source d'apprentissage permanent et, en ce qui les concerne, les mécanismes de réclamation de niveau opérationnel doivent être fondés sur le dialogue et la participation[67].

52. Le principe directeur 19 décrit ce que doit faire l'entreprise dont l'activité n'a pas eu d'incidence négative ou qui n'y a pas contribué, mais dont pareille incidence est directement liée à son exploitation, ses produits ou ses services en raison d'une relation commerciale, l'action appropriée. Il peut s'agir pour l'entreprise d'utiliser le pouvoir qu'elle peut avoir sur son partenaire commercial ou son client pour l'influencer et l'inciter à remédier aux incidences négatives[68].

53. Les Principes directeurs soulignent également le rôle que peuvent jouer les mécanismes de réclamation de niveau opérationnel dans le traitement direct des réclamations. Ces mécanismes peuvent revêtir diverses formes, qui dépendront du type d'entreprise concernée, des besoins de ses parties prenantes et du tableau des risques qu'entraîne l'activité de l'entreprise en matière de droits de l'homme. Pour déterminer comment ces mécanismes peuvent être conçus et fonctionner concrètement dans le secteur des TIC, il faudra poursuivre les discussions internes de ce secteur et les discussions avec les parties prenantes.

[65] Voir https://rankingdigitalrights.org/index2018/.

[66] Principe directeur 22.

[67] Principe directeur 31.

[68] Principe directeur 19 et son commentaire. Voir aussi HCDH, « The corporate responsibility to respect human rights: an interpretive guide », p. 48 à 52.

54. Dans la pratique, il est souvent très malaisé de fournir un accès à des voies de recours en cas d'atteinte à la vie privée. La nature et les effets transnationaux de la surveillance, les interceptions des communications et les nombreuses formes de traitement des données à caractère personnel posent des problèmes juridiques et pratiques (voir A/HRC/34/60, par. 34). De plus, l'ignorance des victimes ou l'absence d'éléments de preuve établissant une immixtion injustifiée est un obstacle fréquent à l'accès aux recours (voir A/HRC/27/37, par. 40). Par exemple, les demandes d'accès aux données que les États adressent aux entreprises s'accompagnent souvent de « consignes de silence », qui interdisent aux entreprises d'informer les personnes concernées. Souvent, les États n'avertissent pas non plus les personnes touchées par d'autres mesures de surveillance, en particulier dans les cas de surveillance de masse. Il est vrai qu'une notification préalable ou concomitante pourrait compromettre l'efficacité de mesures de surveillance légitimes ; les particuliers devraient néanmoins être informés une fois la surveillance achevée (voir A/HRC/23/40, par. 82). Si cela n'est pas possible, la loi devrait accorder généreusement la qualité pour agir à toutes les personnes qui, en principe, ont pu être touchées par ces mesures (voir A/HRC/13/37, par. 38). De même, les entreprises devraient aviser leurs clients lorsqu'elles ont connaissance de violations de données personnelles susceptibles d'avoir porté atteinte à leurs droits.

55. Les victimes se heurtent également à des difficultés nouvelles et croissantes face aux décisions algorithmiques, où les particuliers peuvent ne pas être en mesure d'accéder aux données d'entrée ou de contester les résultats obtenus par l'algorithme proprement dit ou la façon dont ces résultats ont été utilisés dans la décision prise[69]. En collaboration avec d'autres parties prenantes, les États et les entreprises devraient envisager d'éventuels mécanismes pour traiter cette question, tels que la création d'organes d'experts en matière d'audit dotés de ressources suffisantes.

56. La nature du préjudice causé par les atteintes à la vie privée est à l'origine de difficultés supplémentaires. Les effets des atteintes à la vie privée sont difficiles à effacer et peuvent entraîner des conséquences permanentes et d'autres répercussions sur les droits de la personne. La facilité avec laquelle les données et les profils peuvent être conservés, échangés, réutilisés et fusionnés influe sur la permanence des données numériques, ce qui signifie que la personne peut encourir des risques nouveaux et permanents pour ses droits à l'avenir[70].

57. Les atteintes à la vie privée causent des préjudices considérables, même lorsqu'il n'y a pas d'impact économique ou autre quantifiable ; la nature du préjudice ne devrait pas empêcher les victimes de demander réparation. Par exemple, les organisations de protection des consommateurs pourraient être habilitées à demander réparation au nom des victimes d'atteintes à la vie privée commises par des entreprises.

VII. Conclusions et recommandations

58. **Le cadre international des droits de l'homme fournit une base solide pour élaborer des réponses aux multiples défis associés à l'ère du numérique. Il est urgent que les États s'acquittent pleinement de leur obligation de respecter le droit à la vie privée et de leur devoir de protéger ce droit, y compris à l'égard des atteintes commises par les entreprises. Pour atteindre cet objectif, ils doivent établir un cadre juridique et politique approprié, y compris une législation et une réglementation adéquates en matière de protection de la vie privée qui intègrent les principes de légalité, de proportionnalité et de nécessité, et mettre en place des garanties, un contrôle et des voies de recours.**

59. **De nombreuses questions qui n'ont pas pu être traitées dans le présent rapport nécessitent une étude plus approfondie, notamment sur les liens entre le droit à la vie privée et les autres droits de l'homme, en particulier les droits économiques, sociaux et culturels, sur les incidences disproportionnées ou discriminatoires des atteintes à la**

[69] Voir la communication de University of Essex, Human Rights, Big Data and Technology Project, par. 33.

[70] Ibid., par. 7.

vie privée sur les particuliers ou les groupes à risque, sur l'incidence des mégadonnées et de l'apprentissage machine, y compris à des fins prévisionnelles et préventives, sur l'exercice du droit à la vie privée et d'autres droits de l'homme et, enfin, sur la réglementation des marchés des technologies de surveillance.

60. **La nature et les formes de recours efficaces dans les situations où le droit à la vie privée a été violé est un autre point qui requiert plus d'attention. Dans un premier temps, il faudrait déterminer de façon systématique les types de mesures correctives à apporter selon les situations. Cela pourrait servir à l'élaboration d'autres directives. Dans le cadre de cette analyse, il convient de tenir dûment compte des orientations et des recommandations élaborées dans le cadre du projet sur la responsabilité et les voies de recours du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH). De manière plus générale, il conviendrait de mettre au point des outils d'orientation sectoriels concernant la responsabilité des entreprises de respecter le droit à la vie privée.**

61. **Le Haut-Commissaire recommande aux États :**

a) De reconnaître toutes les incidences des nouvelles technologies, en particulier des technologies axées sur les données, sur le droit à la vie privée, mais aussi sur tous les autres droits de l'homme ;

b) D'adopter une législation solide et complète en matière de protection de la vie privée, y compris en ce qui concerne la confidentialité des données, qui soit conforme au droit international des droits de l'homme pour ce qui est des garanties, du contrôle et des recours pour protéger efficacement le droit à la vie privée ;

c) De veiller à ce que les systèmes à forte intensité de données, y compris ceux qui impliquent la collecte et la conservation de données biométriques, ne soient instaurés que lorsque les États peuvent démontrer qu'ils sont nécessaires et proportionnés pour atteindre un objectif légitime ;

d) De mettre en place des autorités indépendantes ayant le pouvoir de surveiller les pratiques du secteur public et du secteur privé en matière de protection des données personnelles, d'enquêter sur les atteintes, de recevoir des plaintes de particuliers et d'organisations, et d'imposer des amendes et d'autres sanctions effectives pour le traitement illégal de données à caractère personnel par des organismes privés et publics ;

e) De veiller, par une législation appropriée et par d'autres moyens, à ce que toute immixtion dans la vie privée, y compris par la surveillance des communications et l'échange de renseignements, soit conforme au droit international des droits de l'homme, notamment aux principes de légalité, de finalité légitime, de nécessité et de proportionnalité, indépendamment de la nationalité des personnes concernées ou du lieu où ces personnes se trouvent, et de préciser que, pour autoriser l'adoption de mesures de surveillance, il faut qu'il y ait un soupçon raisonnable selon lequel une personne en particulier a commis ou commet une infraction pénale ou se livre à des actes constituant une menace précise à la sécurité nationale ;

f) De renforcer les mécanismes pour l'autorisation et le contrôle indépendants de la surveillance exercée par l'État et de veiller à ce que ces mécanismes soient compétents et dotés de ressources suffisantes pour contrôler et faire respecter la légalité, la nécessité et la proportionnalité des mesures de surveillance ;

g) De réviser les lois pour s'assurer qu'elles n'imposent pas d'obligations de conservation générale et systématique des données de communications aux entreprises de télécommunications et autres ;

h) De prendre des mesures pour accroître la transparence et la responsabilité dans l'acquisition de technologies de surveillance par les États ;

i) De s'acquitter pleinement de leur devoir de protéger le droit à la vie privée contre les atteintes commises par les entreprises de tous les secteurs concernés, y compris le secteur des TIC, en prenant les mesures voulues pour prévenir, examiner,

sanctionner et réparer ces atteintes grâce à des politiques, des lois, des règlements et des décisions efficaces ;

j) De veiller à ce que toutes les victimes de violations du droit à la vie privée aient accès à des recours utiles, même dans les affaires transfrontalières.

62. **Le Haut-Commissaire recommande aux entreprises :**

a) De s'employer à assumer leur responsabilité de respecter le droit à la vie privée et tous les autres droits de la personne. Au minimum, les entreprises devraient rendre pleinement opérationnels les Principes directeurs relatifs aux entreprises et aux droits de l'homme, et donc faire preuve d'une diligence raisonnable en matière de droits de l'homme dans toutes leurs activités et en ce qui concerne tous les droits de l'homme, y compris le droit à la vie privée, et de prendre des mesures appropriées pour prévenir et atténuer les incidences réelles et potentielles ou y remédier ;

b) De s'employer à assurer un niveau de sécurité et de confidentialité élevé pour chacune des communications transmises ou des données personnelles recueillies, stockées ou traitées. Faire régulièrement le point sur la meilleure façon de concevoir et de mettre à jour la sécurité des produits et des services ;

c) De respecter les principes clefs de protection de la vie privée mentionnés aux paragraphes 29 à 31 du présent rapport et d'assurer la plus grande transparence possible dans leurs politiques et pratiques internes qui mettent en jeu le droit à la vie privée de leurs utilisateurs et clients ;

d) De prévoir des mesures de réparation ou de collaborer à leur mise en œuvre dans le cadre de processus légitimes lorsqu'elles ont eu des incidences négatives ou qu'elles y ont contribué, notamment grâce à des mécanismes de réclamation efficaces au niveau opérationnel ;

e) De contribuer, dans le cadre du projet du HCDH sur la responsabilité et les voies de recours, aux travaux qui concernent l'élaboration d'orientations et de recommandations visant à améliorer l'efficacité des mécanismes de réclamation non étatiques en cas d'atteinte au droit à la vie privée dans l'espace numérique.