Nations Unies A/HRC/51/17

Assemblée générale

Distr. générale
4 août 2022
Français
Original : anglais

Conseil des droits de l'homme
Cinquante et unième session
12 septembre-7 octobre 2022
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-Commissariat des Nations Unies aux droits de l'homme*

Résumé

Le présent rapport, soumis en application de la résolution 48/4 du Conseil des droits de l'homme, examine les tendances et les difficultés rencontrées récemment en ce qui concerne le droit à la vie privée. Il s'intéresse en particulier aux questions suivantes : a) l'utilisation abusive d'outils de piratage intrusifs ; b) le rôle clef du chiffrement pour ce qui est d'assurer le respect du droit à la vie privée et des autres droits ; c) la surveillance généralisée des espaces publics. Il met en évidence le risque de créer des systèmes de surveillance et de contrôle omniprésents susceptibles de compromettre le développement de sociétés dynamiques et respectueuses des droits.

* Il a été convenu que le présent rapport serait publié après la date normale de publication en raison de circonstances indépendantes de la volonté du soumetteur.

I. Introduction

1. Le présent rapport est soumis en application de la résolution 48/4 du Conseil des droits de l'homme, dans laquelle le Conseil a demandé au Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) d'établir un rapport présentant les tendances et les difficultés récentes liées au droit à la vie privée afin de mettre en évidence et d'expliciter les principes, les garanties et les meilleures pratiques en matière de droits de l'homme qui s'y rapportent, et de lui soumettre ce rapport à sa cinquante et unième session. Il s'appuie sur les communications reçues en réponse à l'appel lancé par le HCDH à ce sujet[1].

2. Partout dans le monde, on assiste à des avancées technologiques impressionnantes, ainsi qu'à des innovations qui améliorent les conditions de vie et stimulent les économies. Cependant, les outils numériques peuvent aussi se retourner contre les personnes, en les exposant à de nouvelles formes de surveillance, de profilage et de contrôle. Le respect et la protection du droit à la vie privée, reconnu à l'article 12 de la Déclaration universelle des droits de l'homme, à l'article 17 du Pacte international relatif aux droits civils et politiques et dans de nombreux autres instruments internationaux et régionaux relatifs aux droits de l'homme[2], peuvent jouer un rôle central dans la gestion des nouvelles menaces que fait peser le numérique sur les droits de l'homme, qui sont inextricablement liées aux données personnelles sur lesquelles repose le fonctionnement des sociétés à l'heure de la transformation numérique.

3. Faisant fond sur les précédents rapports au Conseil des droits de l'homme consacrés aux obstacles à l'exercice du droit à la vie privée[3], le présent rapport examine plus particulièrement trois grandes problématiques en ce qui concerne le rôle des États dans la protection et la promotion du droit à la vie privée : a) l'utilisation abusive d'outils de piratage intrusifs ; b) le rôle clef du chiffrement pour ce qui est d'assurer le respect du droit à la vie privée et des autres droits ; c) la surveillance généralisée des espaces publics. Il met en évidence le risque très réel et grandissant de créer des systèmes de surveillance et de contrôle omniprésents qui pourraient finir par étouffer le développement de sociétés dynamiques, prospères et respectueuses des droits, et conclut par une série de recommandations visant à éviter un tel résultat.

II. Surveillance des appareils personnels et des communications

A. Piratage

4. En juillet 2021, le réseau de journalistes d'investigation Forbidden Stories, soutenu par Amnesty International, a publié des révélations sur l'utilisation du logiciel Pegasus qui ont attiré l'attention de la communauté internationale sur une crise des droits de l'homme qui prenait de l'ampleur depuis des années − à savoir la prolifération mondiale d'outils de piratage pour la surveillance ciblée et secrète des appareils numériques. Alors qu'ils sont censés avoir pour finalité de lutter contre le terrorisme et la criminalité, ces logiciels espions ont souvent été utilisés pour des raisons illégitimes, notamment pour réprimer les opinions critiques ou dissidentes et museler ceux qui les expriment, y compris les journalistes, les personnalités politiques de l'opposition et les défenseurs des droits de l'homme.

5. L'ampleur des opérations du logiciel espion Pegasus et le nombre de victimes qu'elles ont faites sont stupéfiants. Un rapport de 2021, qui s'appuyait sur une liste de plus de 50 000 numéros de téléphone de cibles de surveillance potentielles et réelles ayant fait l'objet

[1] Voir https://www.ohchr.org/en/calls-for-input/2022/call-inputs-report-right-privacy-digital-age-2022.

[2] Voir art. 16 de la Convention relative aux droits de l'enfant ; art. 14 de la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille ; art. 22 du Protocole facultatif se rapportant à la Convention relative aux droits des personnes handicapées ; art. 10 de la Charte africaine des droits et du bien-être de l'enfant ; art. 11 de la Convention américaine relative aux droits de l'homme ; art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

[3] Voir A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 et A/HRC/48/31.

d'une fuite et sur une analyse médico-légale de nombreux téléphones infectés, a révélé qu'au moins 189 journalistes, 85 défenseurs des droits de l'homme et plus de 600 personnalités politiques et hauts responsables gouvernementaux, y compris des ministres, et des diplomates étaient concernés en tant que cibles[4]. L'enquête a également révélé l'espionnage de juges, d'avocats, de médecins, de dirigeants syndicaux et d'universitaires[5]. La société NSO Group, qui fabrique et vend Pegasus, a admis que ses clients espionnaient 12 000 à 13 000 personnes par an[6].

6. Le logiciel espion Pegasus est l'exemple le plus marquant de l'essor des logiciels espions commercialisés par des entreprises auprès des gouvernements du monde entier[7]. Selon les chercheurs, au moins 65 États ont acquis des outils de surveillance commerciaux[8]. NSO a indiqué qu'elle comptait parmi ses clients 60 organismes publics de 45 pays. Quelques jours avant les révélations concernant Pegasus, Citizen Lab et Microsoft ont publié un rapport qui expliquait comment un autre logiciel, Candiru, avait été utilisé par des gouvernements pour s'en prendre à des défenseurs des droits de l'homme, des dissidents, des journalistes, des militants et des hommes politiques[9]. En novembre 2021, la société de réseaux sociaux Meta a annoncé qu'elle avait désactivé les comptes de sept entités qui s'en étaient prises à des personnes au moyen d'Internet dans plus de 100 pays. Elle a également alerté environ 50 000 personnes qui selon elle avaient été la cible de ces activités[10]. Il a été rapporté que plus de 500 entreprises concevaient, commercialisaient et vendaient de tels outils de surveillance à des États[11].

7. Les capacités des outils et services d'espionnage proposés sur le marché mondial sont redoutables. Pegasus, par exemple, une fois installé, donne un accès complet et illimité à tous les capteurs et à toutes les informations des appareils infectés, transformant de fait la plupart des smartphones en dispositifs de surveillance 24 heures sur 24, pouvant accéder à la caméra et au microphone, aux données de géolocalisation, aux courriers électroniques, aux messages, aux photos et aux vidéos, ainsi qu'à toutes les applications. Il permet à l'infiltré de connaître en détail la vie de ses victimes, leurs pensées, leurs préférences, leurs activités professionnelles, leurs préoccupations politiques, leur état de santé, leur situation financière et leur vie sociale et intime. Alors que de nombreux outils de piratage nécessitent une action de la part de la victime, comme celle de cliquer sur un lien ou d'ouvrir la pièce jointe d'un message, Pegasus est installé de manière furtive, au moyen d'une « attaque sans clic »[12]. Il est presque impossible pour les victimes d'éviter l'infection une fois qu'elles ont été prises pour cible par le logiciel.

8. Les opérations de piratage peuvent prendre de nombreuses formes, plus ou moins intrusives. Si le fait d'obtenir le contrôle total d'un téléphone portable ou d'un ordinateur permet de dresser un tableau détaillé de la vie des personnes visées, diverses autres

[4] Voir https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

[5] Voir https://forbiddenstories.org/ about-the-pegasus-project/ ; https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ ; https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[6] Audition du 21 juin 2022 devant le Parlement européen, Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, disponible sur https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

[7] Voir https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepression Report2022_NEW_0.pdf, p. 29.

[8] Voir https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

[9] Voir https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[10] Voir https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. Pour d'autres exemples, voir https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/ ; https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating ; https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] A/HRC/41/35, par. 6 ; voir également https://data.mendeley.com/datasets/csvhpkt8tm/2 pour un inventaire mondial des logiciels espions commerciaux.

[12] Il convient de noter que le logiciel Pegasus n'est pas le seul outil doté de ces capacités et qu'il existe de plus en plus d'outils de ce genre.

techniques de piratage, comme l'obtention de l'accès à des comptes de courrier électronique, peuvent être moins intrusives mais restent très graves. Le piratage peut également permettre d'accéder à d'autres dispositifs connectés, tels que les accessoires technologiques portables ou la technologie embarquée dans les véhicules, qui peuvent fournir des informations supplémentaires, notamment sur la santé et la localisation. Les appareils équipés de caméras ou de microphones, comme les enceintes intelligentes ou les téléviseurs, peuvent également être transformés en outils de surveillance audiovisuelle. En s'attaquant à l'infrastructure des fournisseurs de services, on peut obtenir une somme considérable d'informations sur des milliers de clients, notamment sur leurs communications, leurs données de navigation et leur localisation[13]. La question examinée dans les paragraphes suivants est celle du piratage des appareils de communication personnels.

9. Le piratage des appareils de communication personnels constitue une grave atteinte au droit à la vie privée et peut être lié à des violations préoccupantes de toute une série d'autres droits. Étant donné que l'intrusion dans les dispositifs de communication numérique permet d'accéder aux brouillons et aux historiques de recherche et de navigation, elle peut également permettre de connaître en profondeur les processus de pensée des individus visés, ainsi que leurs opinions et convictions politiques et religieuses, portant ainsi atteinte aux libertés d'opinion et de pensée[14]. Les opérations de piratage peuvent être profondément traumatisantes pour les victimes et affecter leur santé mentale et celle de leur famille. Le piratage aurait conduit à l'arrestation et à la détention de défenseurs des droits de l'homme et de personnalités politiques, dont certains auraient été soumis à la torture[15]. Le piratage ciblé a également été lié à des exécutions extrajudiciaires[16].

10. En outre, le fait de prendre pour cible des journalistes et des médias au moyen d'outils de piratage porte gravement atteinte à la liberté des médias, du fait notamment que les sources d'information peuvent craindre d'être repérées et de subir des représailles. La simple existence de programmes de piratage peut avoir des effets paralysants sur la liberté d'expression, le travail des médias, le débat public et la participation du public, ce qui peut saper la gouvernance démocratique. Comme l'a déclaré la Cour suprême de l'Inde dans son récent arrêt sur l'utilisation du logiciel Pegasus, l'effet paralysant de la surveillance pourrait empêcher la presse de jouer son rôle vital de chien de garde[17].

11. Le piratage peut également avoir un effet négatif sur les droits à une procédure régulière et à un procès équitable[18]. En infiltrant un appareil, il est possible non seulement d'observer son contenu et ses interactions avec d'autres appareils, mais aussi de le manipuler, notamment en modifiant, supprimant ou ajoutant des fichiers[19]. Cela peut être un moyen de falsifier des preuves afin d'incriminer ou de faire chanter les personnes visées[20].

12. En outre, les logiciels espions peuvent avoir des conséquences non seulement pour les personnes visées par les opérations de piratage, mais aussi pour toute personne avec qui elles

[13] L'enquête sur EncroChat menée par la police française et la police néerlandaise, qui ont réussi à s'introduire dans l'infrastructure des serveurs d'un réseau de communications chiffrées, a permis de recueillir des informations sur plus de 32 000 téléphones dans 121 pays ; voir Cour fédérale de justice allemande, décision du 2 mars 2022, 5 StR 457/21, par. 18.

[14] A/HRC/29/32, par. 20. Pour une analyse complète concernant la liberté de pensée, voir A/76/380.

[15] Voir https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/.

[16] A/HRC/41/35, par. 1 ; voir également le document de séance du Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires, intitulé « Annexe au rapport du Rapporteur spécial : enquête sur la mort illégale de M. Jamal Khashoggi ». Disponible sur le site https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

[17] Cour suprême de l'Inde, *Manohar Lal Sharma v. Union of India*, décision du 27 octobre 2021, par. 39.

[18] A/HRC/23/40, par. 62.

[19] A/HRC/39/29, par. 19.

[20] Voir https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/ pour un exemple d'allégations de ce type.

communiquent ou, si la caméra, le microphone ou la géolocalisation de l'appareil sont activés, toute personne présente dans le même lieu physique[21].

13. Enfin, le piratage s'appuie sur les failles de sécurité des systèmes informatiques, dont il exploite l'existence. En entretenant ces vulnérabilités, voire en les créant, ceux qui se livrent au piratage peuvent contribuer à menacer la sécurité et la vie privée de millions d'utilisateurs et de l'ensemble de l'écosystème de l'information numérique[22].

14. Les organismes et experts des droits de l'homme mettent en garde contre les logiciels espions depuis des années. L'Assemblée générale et le Conseil des droits de l'homme ont déclaré à plusieurs reprises que les États membres devaient s'abstenir de toute surveillance illicite ou arbitraire, y compris au moyen du piratage informatique[23]. Plusieurs rapporteurs spéciaux ont vivement critiqué les pratiques de piratage qui vont bien au-delà de ce qui est nécessaire pour poursuivre des objectifs légitimes, comme la lutte contre le terrorisme et la criminalité[24]. Le Comité des droits de l'homme s'est également déclaré préoccupé par les activités de piratage informatique commanditées par des États, en particulier lorsqu'il n'existe pas de mécanisme de contrôle ni de garanties appropriées[25]. Au niveau régional, l'ancien Rapporteur spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme a condamné les opérations de piratage informatique à des fins illicites et demandé que les contrevenants soient sévèrement punis, notamment pour les actions menées pour des raisons politiques contre des journalistes et les médias indépendants[26].

15. Réagissant aux révélations concernant l'utilisation du logiciel Pegasus, diverses institutions régionales et nationales, dont le Conseil de l'Europe, la Commission interaméricaine des droits de l'homme, le Parlement européen et la Cour suprême de l'Inde, ont exprimé leur inquiétude quant à la prolifération des logiciels espions et ont lancé des auditions et des enquêtes[27]. Des enquêtes criminelles[28] et des poursuites civiles[29] sont également en cours.

16. Il existe un vaste corpus d'analyses relatives à la surveillance et aux droits de l'homme dont il est possible de tirer des orientations concernant les conditions minimales et les garanties nécessaires à toute utilisation de logiciels espions par les pouvoirs publics[30]. Les effets profondément préjudiciables du piratage rendent nécessaire une approche

[21] Voir https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

[22] A/HRC/39/29, par. 19.

[23] Voir la résolution 75/176 de l'Assemblée générale et les résolutions 48/4 et 45/18 du Conseil des droits de l'homme.

[24] A/HRC/17/27 ; A/HRC/20/17 ; A/HRC/23/40, par. 62 ; A/HRC/41/35 ; A/HRC/41/41 ; et A/73/438 ; voir aussi https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[25] Voir CCPR/C/DEU/CO/7, CCPR/C/NLD/CO/5 et CCPR/C/ITA/CO/6.

[26] Voir https://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1.

[27] Voir https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1207&lID=1 ; https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/media_center/PReleases/2022/022.asp ; https://www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing ; https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe ; https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023 ; Cour suprême de l'Inde, *Manohar Lal Sharma v. Union of India*, décision du 27 octobre 2021.

[28] Voir https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali et https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

[29] https://www.glanlaw.org/nso-spyware-hacking ; https://privacyinternational.org/examples/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and ; https://www.washingtonpost.com/technology/2021/11/23/ apple-pegasus-lawsuit-spyware-nso/ ; et https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/ 20-16408.pdf. Pour un aperçu détaillé des actions en justice engagées, voir https://citizenlab.ca/ 2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

[30] Voir A/HRC/27/37, A/HRC/39/29, A/HRC/23/40 et A/HRC/23/40/Corr.1, CCPR/C/UKR/CO/8, CCPR/C/DEU/CO/7, CCPR/C/ARM/CO/3, CCPR/C/BWA/CO/2 et CCPR/C/FIN/CO/7.

particulièrement prudente, qui limite cette pratique aux circonstances les plus exceptionnelles, dans le strict respect du droit international des droits de l'homme.

17. Cependant, de nombreuses juridictions n'ont pas mis en place ces garde-fous juridiques essentiels et ne disposent pas de lois publiques claires et précises qui régissent les activités de piratage. Si certains États ont adopté des cadres juridiques conformes au droit international des droits de l'homme, d'autres s'appuient sur des lois trop générales ou obsolètes, adoptées avant l'avènement des technologies modernes.

18. Comme l'ont montré les révélations sur le logiciel Pegasus et d'autres rapports sur la question, le piratage informatique par différents acteurs étatiques semble souvent poursuivre des objectifs qui ne sont pas légitimes au regard du droit international des droits de l'homme. Si, dans certaines circonstances, les mesures de surveillance intrusives peuvent être autorisées au regard des articles 17 et 19 du Pacte international relatif aux droits civils et politiques pour des raisons de protection de la sécurité nationale ou de l'ordre public, le piratage ne saurait être justifié par des raisons politiques ou commerciales, souvent avancées lorsque des défenseurs des droits de l'homme ou des journalistes sont visés.

19. Même si des objectifs légitimes, liés notamment à la sécurité nationale ou à la protection des droits d'autrui, sont poursuivis, l'évaluation de la nécessité et de la proportionnalité de l'utilisation de logiciels espions limite considérablement les cas dans lesquels cette pratique pourrait être autorisée[31]. Il existe des arguments solides donnant à penser que des outils tels que Pegasus, qui permettent des ingérences sans entrave dans la vie des personnes voire dans leurs pensées intimes, pourraient altérer l'essence du droit à la vie privée[32] et porter atteinte au droit absolu à la liberté de pensée et d'opinion. Compte tenu des effets négatifs importants de l'utilisation des logiciels espions, dont la portée va bien au-delà de la cible visée, cette utilisation devrait se limiter aux cas où l'objectif est de prévenir une infraction grave ou un acte constituant une menace grave pour la sécurité nationale ou d'enquêter à ce sujet. Elle devrait aussi être étroitement circonscrite à l'enquête concernant la ou les personnes soupçonnées de commettre ou d'avoir commis de tels actes. Il doit s'agir d'une mesure de dernier ressort − ce qui veut dire que toutes les mesures moins intrusives doivent avoir été épuisées ou s'être révélées inutiles − d'une portée et d'une durée strictement limitées. Seules les données pertinentes devraient être consultées et collectées[33]. Toute mesure de ce type devrait également faire l'objet d'un contrôle indépendant rigoureux, et être soumise à l'approbation préalable d'un organe judiciaire[34]. En outre, des contrôles à l'exportation stricts et transparents prenant expressément en compte les risques pour les droits de l'homme peuvent constituer un moyen efficace de prévenir les violations et les atteintes aux droits[35]. Le HCDH renouvelle son récent appel, ainsi que ceux des experts et des organes des droits de l'homme, en faveur d'un moratoire sur la vente, le transfert et l'utilisation des outils de piratage jusqu'à ce qu'un régime de garanties fondé sur les droits de l'homme soit mis en place[36].

B. Restrictions au chiffrement

20. Ces dernières années, plusieurs gouvernements ont pris des mesures qui, intentionnellement ou non, risquent de compromettre la sécurité et la confidentialité des

[31] Voir Cour constitutionnelle fédérale d'Allemagne, arrêt du 27 février 2008 (1 BvR 370, 595/07), p. 247 aa).

[32] Contrôleur européen de la protection des données, voir https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

[33] Voir https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

[34] Voir A/HRC/39/29 sur les garanties minimales concernant les mesures de surveillance secrète.

[35] A/HRC/39/29, par. 25 ; A/HRC/44/24, par. 40 ; A/HRC/48/31, par. 46 ; A/HRC/41/35, par. 34 et 66. L'Union européenne a récemment fait un pas vers un renforcement de la prise en compte des droits de l'homme en adoptant un nouveau règlement sur le contrôle des exportations.

[36] Voir https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe ; https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening ; https://www.amnesty.org/en/documents/doc10/4516/2021/en/ ; https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

communications chiffrées, ce qui peut avoir des incidences préoccupantes sur l'exercice du droit à la vie privée et d'autres droits de l'homme.

21. Le chiffrement est un élément clef de la protection de la vie privée et de la sécurité en ligne et il est essentiel à la sauvegarde des droits, notamment des droits à la liberté d'opinion et d'expression, à la liberté d'association et de réunion pacifique, à la sécurité, à la santé et à la non-discrimination. Il permet aux personnes de partager des informations librement, sans craindre que des tiers, qu'il s'agisse d'autorités publiques ou de cybercriminels, puissent en prendre connaissance. Il est essentiel pour que toute personne se sente en sécurité lorsqu'elle échange librement des informations avec d'autres sur diverses expériences, pensées et identités, y compris des informations sensibles sur la santé ou des données financières, des éléments relatifs à l'identité de genre et à l'orientation sexuelle, des formes d'expression artistique et des informations en lien avec le l'appartenance à une minorité. Dans les contextes où la censure est omniprésente, le chiffrement permet aux individus de préserver un espace pour la formation, l'expression et l'échange d'opinions. Dans certains cas, les journalistes et les défenseurs des droits de l'homme ne peuvent pas faire leur travail sans la protection d'un chiffrement solide, qui protège leurs sources et les met à l'abri des acteurs puissants visés par une enquête. Le chiffrement offre aux femmes, qui sont particulièrement exposées à la surveillance, au harcèlement et à la violence en ligne, un niveau de protection important contre la divulgation involontaire d'informations[37]. Dans les conflits armés, les systèmes de messagerie avec chiffrement sont indispensables pour assurer une communication sécurisée entre les civils. Il convient de noter qu'au cours des deux mois qui ont suivi le début du conflit armé en Ukraine le 24 février 2022, le nombre de téléchargements de l'application de messagerie chiffrée Signal a augmenté en Ukraine de plus de 1 000 % par rapport aux mois précédents[38].

22. Le rôle vital du chiffrement en tant que moyen de protection de la vie privée et des droits de l'homme a été largement reconnu, notamment par les États, les organismes des Nations Unies, le Haut-Commissaire des Nations Unies aux droits de l'homme et les experts des droits de l'homme[39]. L'Assemblée générale et le Conseil des droits de l'homme ont également souligné l'importance du chiffrement pour la sauvegarde des droits de l'homme dans plusieurs résolutions, demandant aux États de ne pas s'ingérer dans l'utilisation des techniques de chiffrement[40] et encourageant les entreprises à favoriser la mise en place de solutions qui permettent de garantir et de préserver la confidentialité des communications et des transactions numériques, notamment par des mesures de chiffrement, de pseudonymisation et d'anonymisation[41]. Les rapporteurs spéciaux et les experts régionaux se sont déclarés favorables à un chiffrement fort comme outil de promotion des droits, recommandant d'encourager et de protéger le chiffrement fort et mettant en garde contre les mesures qui restreindraient arbitrairement ou illégalement l'utilisation de cette technologie clef[42]. Le Comité des droits de l'enfant a souligné que toute mesure visant à détecter des contenus exploitant sexuellement des enfants ou montrant des atteintes sexuelles sur enfant dans des communications chiffrées doit être strictement limitée selon les principes de légalité, de nécessité et de proportionnalité[43]. Le Conseil des droits de l'homme, l'ONU et les experts régionaux des droits de l'homme ont souligné que le chiffrement était vital pour le travail

[37] A/HRC/35/9, par. 18.

[38] Voir https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

[39] Voir https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid.

[40] Résolution 75/176 de l'Assemblée générale et résolutions 39/6, 44/12, 45/18 et 48/4 du Conseil des droits de l'homme.

[41] Résolution 75/176 de l'Assemblée générale et la résolution 48/4 du Conseil des droits de l'homme.

[42] Voir A/HRC/29/32 ; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf ; A/HRC/41/41 ; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf ; https://www.osce.org/representative-on-freedom-of-media/379351 ; et https://www.oas.org/en/iachr/expression/reports/ENGIA2020.pdf.

[43] Comité des droits de l'enfant, observation générale nº 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique, par. 70.

journalistique et la protection des sources[44]. Les Indicateurs sur l'universalité de l'Internet publiés par l'Organisation des Nations Unies pour l'éducation, la science et la culture soulignent l'importance du chiffrement pour la confiance et la sécurité en ligne[45].

23. Les pouvoirs publics restreignent parfois l'utilisation du chiffrement, malgré ses avantages, par exemple pour protéger la sécurité nationale et lutter contre la criminalité, en particulier pour détecter les contenus montrant des violences sexuelles sur enfant. Les mesures prises à cet effet comprennent l'interdiction des communications chiffrées et la criminalisation de l'offre ou de l'utilisation d'outils de chiffrement[46], ou encore l'enregistrement obligatoire et l'octroi de licences pour les outils de chiffrement[47]. De même, dans certains cas, il a été demandé aux fournisseurs de ce type d'outils de faire en sorte que les services de police ou d'autres organes publics aient accès à toutes les communications sur demande, ce qui de fait revient à imposer une restriction générale rendant nécessaire, ou tout au moins encourageant, la création de portes dérobées (qui sont un moyen intégré de contourner le chiffrement, permettant d'avoir secrètement accès aux données en texte clair)[48]. Une autre forme de restriction est l'obligation de créer et d'entretenir des systèmes de dépôt de clefs, exigeant que toutes les clefs de chiffrement privées soient confiées aux autorités ou à une tierce partie approuvée[49]. Les exigences de traçabilité, selon lesquelles les fournisseurs doivent être en mesure de remonter jusqu'à l'expéditeur supposé de tout message, pourraient également nécessiter un affaiblissement des normes de chiffrement[50]. Récemment, plusieurs États ont commencé à imposer ou à envisager des obligations générales de surveillance pour les fournisseurs de communications numériques, y compris ceux qui offrent des services de communication chiffrée[51]. De telles obligations pourraient effectivement contraindre ces fournisseurs à renoncer à un chiffrement fort de bout en bout ou à trouver des solutions de contournement très problématiques (voir plus bas, par. 27 et 28).

24. Il ne fait aucun doute que les capacités de chiffrement communément utilisées, que le public a exigées face à la surveillance de masse et à la cybercriminalité, créent un dilemme pour les pouvoirs publics qui cherchent à protéger les populations, en particulier leurs membres les plus vulnérables, contre les infractions graves et les menaces pour la sécurité. Toutefois, comme l'a souligné le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, la réglementation du chiffrement risque de porter atteinte aux droits de l'homme[52]. Les États qui cherchent à limiter le chiffrement n'ont souvent pas réussi à démontrer que les restrictions qu'ils entendent imposer sont nécessaires pour répondre à un intérêt légitime particulier, étant donné qu'il existe divers autres outils et approches permettant d'obtenir les informations nécessaires à l'application de la loi ou à d'autres fins légitimes[53]. Ces autres mesures comprennent l'amélioration des services de police traditionnels et l'augmentation des ressources qui leur sont allouées, les opérations d'infiltration, l'analyse des métadonnées et le renforcement de la coopération policière internationale.

[44] Résolution 45/18 du Conseil des droits de l'homme ; A/HRC/29/32 ; https://www.osce.org/representative-on-freedom-of-media/379351.

[45] Voir https://en.unesco.org/internet-universality-indicators, indicateur D.5.

[46] Voir PSE 2/2017 et LBY 3/2022. Toutes les communications mentionnées dans le présent rapport peuvent être consultées à l'adresse suivante : https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[47] Voir https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf (LBY 3/2022).

[48] Voir GBR 4/2015, MYS 2/2018, AUS 5/2018 et AUS 6/2018.

[49] Voir RUS 7/2016 et RUS 7/2018.

[50] Voir IND 31/2018, IND 3/2019, BRA 6/2020 et BRA 7/2020.

[51] Par exemple, la loi « EARN IT » adoptée aux États-Unis d'Amérique en 2020 (voir USA 4/2020) ; le projet de loi sur la sécurité en ligne au Royaume-Uni (voir GBR 5/2022) ; la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, soumise par la Commission européenne le 11 mai 2022 (COM(2022) 209) ; et le règlement adopté par le Gouvernement indien intitulé Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (voir IND 8/2021).

[52] Voir A/HRC/29/32.

[53] Ibid., par. 39.

25. En outre, la plupart des restrictions au chiffrement ont des effets disproportionnés sur le droit à la vie privée et les droits connexes, qui touchent souvent non seulement les personnes visées, mais aussi l'ensemble de la population. L'interdiction pure et simple ou la criminalisation du chiffrement par les États, en particulier, ne peut être justifiée car elle empêcherait tous les utilisateurs relevant de leur juridiction de disposer d'un moyen de communication sûr. Les systèmes de dépôt de clefs présentent des vulnérabilités importantes, étant donné qu'ils dépendent de l'intégrité de l'installation de stockage et exposent les clefs stockées au risque de cyberattaques. En outre, les portes dérobées obligatoires dans les outils de chiffrement créent des responsabilités qui dépassent largement leur utilité en ce qui concerne les usagers soupçonnés d'avoir commis une infraction ou identifiés comme présentant une menace pour la sécurité. Elles mettent en péril la vie privée et la sécurité de tous les utilisateurs et exposent ceux-ci à des ingérences illicites, de la part non seulement des pouvoirs publics, mais aussi d'acteurs non étatiques, y compris des réseaux criminels[54]. Les conditions imposées en matière de licence et d'enregistrement ont aussi des effets disproportionnés, car elles reposent sur l'existence de faiblesses exploitables dans les logiciels de chiffrement[55]. Ces effets négatifs ne se limitent pas nécessairement à la juridiction de l'État qui impose la restriction ; il est en effet probable que les portes dérobées, une fois établies sous la juridiction d'un État, deviennent partie intégrante des logiciels utilisés dans d'autres parties du monde.

26. Des techniques dites d'analyse côté client, conçues pour détecter certaines formes de contenu répréhensible, ont été récemment mises au point pour éviter une grande partie des problèmes susmentionnés. L'analyse côté client déplace l'étape de détection du contenu, qui ne se déroule plus au niveau des serveurs par lesquels les communications sont envoyées mais directement sur les appareils personnels eux-mêmes. De cette façon, le contenu en question est examiné avant d'être chiffré pour la transmission. En août 2021, Apple a annoncé son intention d'introduire un tel système pour ses services iMessage et iCloud, mais le projet a été suspendu après avoir essuyé de vives critiques d'un large éventail d'experts en sécurité informatique, de cryptographes et de groupes de défense des droits de l'homme[56]. Cependant, diverses mesures législatives[57] pourraient, au moins indirectement, contraindre les services de communications Internet à mettre en place de tels systèmes en imposant de larges obligations de surveillance pour toutes les communications, y compris celles qui sont chiffrées. Étant donné que le contenu des messages, une fois chiffré, ne peut être consulté par personne d'autre que l'expéditeur et le destinataire, toute obligation générale de surveillance contraindrait les fournisseurs de services soit à renoncer au chiffrement de la transmission, soit à chercher à accéder aux messages avant qu'ils ne soient chiffrés.

27. La généralisation de l'analyse côté client constituerait un changement de paradigme soulevant une série de problèmes graves, avec des conséquences potentiellement désastreuses pour l'exercice du droit à la vie privée et d'autres droits. À la différence d'autres mesures, celle-ci, si elle devenait obligatoire, aurait inévitablement des conséquences pour toute personne utilisant les moyens modernes de communication, et pas seulement les personnes se livrant à des activités criminelles ou représentant une grave menace grave pour la sécurité. L'analyse côté client modifie la capacité qu'ont les personnes de contrôler pleinement les dispositifs de communication qui sont intrinsèquement liés à toutes les facettes de leur vie et de limiter les informations que ces dispositifs partagent[58]. En outre, lorsqu'elle est générale, il est impossible d'éviter des faux positifs fréquents, en dépit de taux de précision élevés, ce qui a des retombées sur de nombreuses personnes innocentes[59]. Compte tenu de la possibilité de telles conséquences, la surveillance indifférenciée est susceptible d'avoir un effet dissuasif

[54] A/HRC/39/29, par. 20.

[55] A/HRC/29/32, par. 41.

[56] Voir https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.

[57] Commission européenne, proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, 11 mai 2022 (COM(2022) 209) ; voir également le projet de loi sur la sécurité en ligne au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, disponible à l'adresse https://www.gov.uk/government/publications/draft-online-safety-bill.

[58] Documents soumis par le Comité directeur de la Global Encryption Coalition et par Privacy International.

[59] Voir https://doi.org/10.48550/arXiv.2110.07450.

important sur la liberté d'expression et d'association, poussant les personnes à limiter leurs modes de communication et d'interaction avec les autres et à pratiquer l'autocensure[60].

28. L'analyse côté client pose également de nouveaux défis en matière de sécurité, rendant les failles de sécurité plus probables[61]. Le processus de filtrage peut en outre être manipulé de façon à créer artificiellement des profils de faux positifs ou de faux négatifs[62]. Même si, en l'état actuel des choses, le filtrage côté client est étroitement ciblé, le fait de rendre les appareils accessibles à ce type d'intervention décidée par les autorités risque d'entraîner des tentatives d'élargir le champ des contenus visés[63]. En particulier, dans les situations où l'état de droit est faible et où les droits de l'homme sont menacés, l'analyse côté client pourrait avoir des conséquences beaucoup plus étendues, en étant par exemple utilisée pour étouffer le débat politique ou pour s'en prendre aux figures de l'opposition, aux journalistes et aux défenseurs des droits de l'homme[64]. Compte tenu de l'ampleur de la menace que ferait peser l'application généralisée de ce processus sur la protection des droits de l'homme, une telle obligation ne devraient pas être imposée sans un examen approfondi de ses effets potentiels sur les droits de l'homme et des mesures pouvant permettre de les atténuer. Sans enquête et analyse approfondies, il semble peu probable que de telles restrictions puissent être considérées comme proportionnées au regard du droit international des droits de l'homme, même lorsqu'elles visent des objectifs légitimes, compte tenu de la gravité des conséquences qu'elles peuvent avoir[65].

III. Surveillance du public

29. Le Haut-Commissaire a fait part à plusieurs reprises de ses préoccupations concernant la surveillance de masse, en particulier l'interception des communications à grande échelle[66]. Si certains États ont amélioré les garanties contre la surveillance, la pratique profondément troublante consistant à surveiller les activités en ligne d'une grande partie de la population, voire de populations entières, n'a pas cessé. Les rapports précédents ayant porté principalement sur la surveillance des communications privées, la question des répercussions de la surveillance des lieux publics sur la vie privée, qui a moins été traitée, est abordée ci-après.

A. Surveillance des lieux publics

30. Les caméras de surveillance installées dans les rues, les parkings, les pôles de transport et d'autres lieux publics sont devenues courantes dans de nombreux pays. On estime que le nombre de caméras de surveillance utilisées dans le monde a dépassé un milliard en

[60] Pour plus d'informations sur les effets dissuasifs de la surveillance, voir plus bas, par. 47.

[61] À la différence des attaques sur les serveurs d'entreprise, celles qui ciblent les appareils personnels peuvent être exécutées par un plus grand nombre d'acteurs et sur des infrastructures moins sécurisées. Les adversaires peuvent utiliser leur accès à l'appareil pour reproduire le mécanisme au moyen de l'ingénierie inversée, voir https://doi.org/10.48550/arXiv.2110.07450.

[62] https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha ; https://openreview.net/forum?id=CQbqeGAM_Ki.

[63] https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/ ; https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha ; https://doi.org/10.48550/arXiv.2110.07450.

[64] Ibid.

[65] A/HRC/39/29, par. 20 ; A/HRC/29/32, par. 43. Les avis de la Cour de justice de l'Union européenne rejoignent cette conclusion. La Cour a récemment statué que l'analyse automatisée des données de trafic et de localisation, effectuée de manière généralisée et indifférenciée, devait être limitée à ce qui était strictement nécessaire pour répondre à une menace grave, réelle, actuelle ou prévisible pour la sécurité nationale. Elle a rejeté toute autre justification. Voir *La Quadrature du Net et autres c. Premier ministre et autres*, arrêt du 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), par. 177. En outre, sa jurisprudence dénote un scepticisme encore plus fort à l'égard du filtrage de contenu, Cour de justice de l'Union européenne, *Maximillan Schrems c. Data Protection Commissioner*, arrêt du 6 octobre 2015 (C-362/14), par. 94.

[66] Voir A/HRC/27/37, A/HRC/39/29, et https://www.ohchr.org/en/press-releases/2013/07/mass-surveillance-pillay-urges-respect-right-privacy-and-protection.

2021[67]. Dans les 10 villes du monde ayant la plus forte densité de vidéosurveillance, le nombre de caméras de surveillance va de 39 environ à plus de 115 pour 1 000 habitants[68].

31. Outre les systèmes de surveillance gérés par l'État, certaines entreprises ont adopté des outils de surveillance à usage privé, dotés de fonctionnalités dédiées permettant de signaler les incidents aux autorités, voire d'accorder à celles-ci un accès direct aux flux de données[69]. Cela vient considérablement élargir l'espace public sous surveillance, tout en affaiblissant la transparence, le contrôle et le principe de responsabilité.

32. Ces dernières années, les capacités des caméras de surveillance se sont considérablement accrues grâce à l'ajout de fonctions d'analyse vidéo sophistiquées. On estime qu'en 2010, moins de 2 % des caméras réseau vendues comportaient une fonction d'analyse vidéo intégrée, mais cette proportion était passée à plus de 40 % en 2016 et devrait continuer à augmenter[70]. Les fonctions d'analyse font de plus en plus appel à l'intelligence artificielle. Les capacités accrues de reconnaissance faciale et de repérage des comportements suspects sont parmi les caractéristiques les plus problématiques des systèmes de vidéosurveillance sophistiqués[71]. En outre, l'utilisation de drones à des fins de surveillance a été normalisée dans de nombreux pays, qui y ont recours pour surveiller les manifestations et autres rassemblements[72].

33. La notion générique de « villes intelligentes » recouvre un nombre croissant d'initiatives axées sur les données, qui visent à remodeler les espaces urbains. Les projets de villes intelligentes mettent l'accent sur la collecte et le traitement des données aux fins de la gestion des installations de la ville, grâce à des systèmes de capteurs toujours plus performants. Si la plupart des données collectées et traitées dans ce contexte concernent des questions telles que les flux de circulation, la pollution ou le bruit, qui ne relèvent pas du domaine des données personnelles, certaines autres, comme les plaques d'immatriculation et les données des compteurs intelligents, peuvent facilement être rattachées à des individus. En outre, il est souvent possible de faire perdre aux données leur caractère anonyme[73] et des dispositifs tels que les caméras installées pour surveiller les flux de circulation peuvent être utilisés pour suivre des individus[74].

34. Ces changements se doublent souvent de l'adoption de nouveaux systèmes d'identité et d'un élargissement des bases de données biométriques. Dans de nombreux pays, les systèmes d'identité sont liés à un stockage centralisé des données personnelles, notamment d'informations biométriques comme les empreintes digitales, la géométrie faciale, les images de l'iris et les données ADN. Qui plus est, les bases de données sont souvent reliées entre elles et peuvent être consultées par d'autres organismes. Par conséquent, l'identification des individus, où qu'ils se trouvent, est devenue de plus en plus facile.

B. Surveillance en ligne

35. Parallèlement, la surveillance des propos tenus en ligne s'est généralisée. Dans le monde entier, de nombreuses autorités collectent et analysent les publications sur les médias sociaux et les réseaux privés et professionnels utilisant les plateformes de communication accessibles au public. Ces activités de renseignement relatives aux médias sociaux vont de l'enquête sur des utilisateurs précis à la collecte, au stockage et à l'analyse de vastes quantités

[67] Voir https://venturebeat.com/2022/06/18/how-ml-powered-video-surveillance-could-improve-security/.

[68] Voir https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ et https://surfshark.com/surveillance-cities.

[69] Voir https://www.accessnow.org/amazon-ring-privacy-review/.

[70] Voir https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf.

[71] Voir les communications reçues de Derechos Digitales et International Network of Civil Liberties Organizations.

[72] Voir les communications reçues de Amnesty International et CIVICUS.

[73] Voir https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

[74] Pour en savoir plus sur les conséquences des villes intelligentes pour les droits de l'homme, voir https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/ et https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

de données. Les données obtenues peuvent être les suivantes : noms ; âges; photos et modèles numériques connexes ; adresses ; publications et réactions aux publications d'autres personnes ; contacts personnels et professionnels et réseaux associés ; données de localisation ; centres d'intérêt ; orientation sexuelle ; identité de genre ; affiliation et activités politiques ; croyances religieuses ; informations sur la santé.

36. Souvent, les pratiques de surveillance des médias sociaux comprennent différents types d'analyse prédictive, visant notamment à localiser les principales zones de criminalité. Cependant, ces activités peuvent également servir à évaluer le comportement passé, présent et futur des individus et à établir des probabilités concernant les risques de délinquance ou de menace pour la sécurité[75]. Elles sont également utilisées pour prévoir les éventuels épisodes d'agitation sociale[76].

37. Ces activités peuvent servir de multiples objectifs légitimes et illégitimes, allant des enquêtes criminelles et de la prévention du crime au contrôle des demandeurs de prestations sociales, en passant par la surveillance des manifestations, la mesure de l'opinion publique ou le profilage du comportement social des personnes[77].

C. Incidences sur les droits de l'homme

38. Les technologies modernes axées sur les données modifient radicalement l'équilibre des forces entre l'entité chargée de la surveillance et les personnes surveillées. Avant l'avènement de la surveillance automatisée à grande échelle et des outils d'analyse des données, il existait des limites pratiques à la surveillance qui assuraient un certain niveau de protection des individus, même en public[78]. Les outils numériques sophistiqués font disparaître ces anciennes protections « naturelles ». Aujourd'hui, un seul agent peut surveiller les comptes de médias sociaux de dizaines de personnes et, grâce à des logiciels de pointe et à l'analyse des mégadonnées, de petites équipes peuvent observer des milliers de comptes et en établir le profil[79].

39. Les tendances sont les mêmes en ce qui concerne l'efficacité et la portée des autres mesures de surveillance des espaces publics. Par exemple, l'essor des techniques de reconnaissance faciale et autres techniques de reconnaissance biométrique a fondamentalement transformé les pratiques traditionnelles de surveillance audiovisuelle en augmentant considérablement la capacité d'identifier les individus, y compris les participants à des rassemblements, dans les espaces publics. La reconnaissance faciale en direct permet l'identification en temps réel des personnes, ainsi que leur surveillance et leur suivi ciblés. L'identification rétrospective des personnes peut éventuellement élargir l'éventail des sources de données, ce qui peut avoir des effets tout aussi intrusifs[80] si elle n'est pas utilisée avec la plus grande retenue.

40. Les répercussions de la surveillance publique sur les droits de l'homme sont encore aggravées par le fait que les sources de données sont de plus en plus fusionnées, comme par exemple dans le cas des données issues de la vidéosurveillance avec reconnaissance faciale conjuguées aux informations provenant des médias sociaux[81] et des bases de données gouvernementales, y compris les informations sur la sécurité sociale, les flux migratoires, les personnes soupçonnées de terrorisme, les arrestations ou même les listes de personnes faisant l'objet d'un suivi pour des raisons politiques.

41. En outre, les États s'appuient sur de vastes ensembles de données amassées par diverses entreprises privées. Dans de précédents rapports, le (la) Haut(e)-Commissaire et les rapporteurs spéciaux ont appelé l'attention sur la pratique des États consistant à demander l'accès aux données collectées par les fournisseurs de services de télécommunication et

[75] Voir https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, p. 152.
[76] Voir https://dx.doi.org/10.2139/ssrn.2702426, p. 1.
[77] Voir https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[78] A/HRC/44/24, par. 34.
[79] Voir https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[80] Voir la communication reçue de Amnesty International.
[81] Voir communication de l'International Network of Civil Liberties Organizations.

d'accès à Internet, souvent en s'appuyant sur des lois relatives à l'obligation de conservation des données[82]. Le nombre d'entreprises recevant de telles demandes ne cesse d'augmenter. Certains États obligent les entreprises 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[83].

42. En outre, les États s'appuient de plus en plus sur les services de surveillance proposés par des entreprises, par exemple en acquérant des données auprès de courtiers en données et d'autres sociétés collectant et vendant des données personnelles[84]. Ces pratiques peuvent les amener à contourner des restrictions et des garanties procédurales cruciales, en leur permettant d'accéder indirectement à des outils qu'ils n'auraient pas pu déployer eux-mêmes sans contrevenir à leurs obligations en matière de droits de l'homme. Par exemple, l'outil de reconnaissance faciale développé par la société Clearview AI a été utilisé par des milliers d'organismes chargés du maintien de l'ordre, alors qu'il avait été mis au point à partir de milliards de photographies récupérées sur Internet, ce qui constituait une atteinte massive au droit à la vie privée[85].

43. La surveillance systématique des personnes dans l'espace public en ligne et hors ligne, en particulier lorsqu'elle est associée à des moyens supplémentaires d'analyser les informations obtenues et de les recouper avec d'autres sources de données, constitue une atteinte au droit à la vie privée et peut avoir des effets hautement préjudiciables sur l'exercice d'autres droits de l'homme[86]. Elle peut constituer une menace pour la liberté d'expression et la liberté de réunion pacifique, la participation et la démocratie et doit donc être envisagée avec la plus grande prudence et uniquement dans le strict respect des normes relatives aux droits de l'homme. C'est le cas même si les activités qui font l'objet d'une surveillance se déroulent en public, ou sur des plateformes de médias sociaux ouvertes, car chacun devrait disposer d'un espace dans lequel il échappe à toute observation et toute ingérence systématiques, en particulier de la part d'entités publiques. Comme l'a déjà noté le Haut-Commissaire, la protection du droit à la vie privée s'étend aux espaces publics et aux informations accessibles au public[87]. Le Comité des droits de l'homme a rejeté l'idée selon laquelle les données recueillies dans les espaces publics relèvent automatiquement du domaine public et peuvent être librement accessibles[88]. La Cour européenne des droits de l'homme a reconnu que les informations disponibles publiquement ou perceptibles par le

[82] A/HRC/27/37, par. 26 ; A/HRC/39/29, par. 18 ; A/HRC/23/40 et A/HRC/23/40/Corr.1, par. 65 à 67 ; A/69/397, par. 53 à 55.

[83] A/HRC/39/29, par. 19.

[84] Voir, par exemple, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances ; et https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, p. 25.

[85] Plusieurs autorités de protection des données, ayant établi que Clearview AI avait violé la législation pertinente en vigueur, lui ont imposé des amendes élevées et ont obtenu que les données personnelles recueillies soient effacées, voir https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ ; voir aussi https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy, https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en et https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Les autorités de protection des données ont estimé qu'en utilisant cet outil, les forces de police avaient violé la législation relative à la protection des données, voir https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en et https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[86] Voir CCPR/C/NGA/CO/2, observations finales dans lesquelles le Comité des droits de l'homme s'est déclaré préoccupé par la surveillance des médias sociaux, par. 40.

[87] A/HRC/39/29, par. 6.

[88] CCPR/C/COL/CO/7, par. 32.

public peuvent tout à fait relever du droit à la vie privée, en particulier lorsque les données personnelles sont enregistrées de manière systématique ou permanente[89].

44. L'enregistrement des images photographiques constitue un sujet de préoccupation particulier en ce qui concerne la surveillance publique. L'image d'une personne incarne des attributs clefs de sa personnalité et révèle des caractéristiques uniques qui la distinguent d'autres personnes. L'enregistrement, l'analyse et la conservation des images faciales des personnes sans leur consentement constituent une atteinte à leur droit à la vie privée. Le déploiement de systèmes de reconnaissance faciale dans les espaces publics, qui suppose la collecte et le traitement des images faciales de toutes les personnes filmées, représente une immixtion massive et indifférenciée[90].

45. De plus, la surveillance publique peut conduire, et conduit souvent, à l'adoption de mesures qui affectent directement les individus et les communautés, y compris des mesures coercitives. Ces mesures comprennent le renforcement de la surveillance et du maintien de l'ordre dans certains quartiers et à l'égard de certains groupes ou individus, qui débouche parfois sur des interrogatoires, des arrestations et des mises en détention. Certains groupes et individus peuvent aussi être signalés comme présentant une menace ou un risque, par exemple comme étant des terroristes ou des criminels potentiels, souvent sans fondement solide. Plusieurs États utilisent les résultats de diverses mesures de surveillance publique pour identifier leurs détracteurs ou les personnes qui ne se conforment pas aux attentes sociales, ce qui conduit parfois à des actes de harcèlement, des détentions ou un refus de services essentiels[91].

46. Les opérations de surveillance ont tendance à viser de manière disproportionnée les minorités et les communautés marginalisées[92]. L'utilisation de l'intelligence artificielle, notamment des techniques de reconnaissance faciale pour le profilage racial et ethnique[93], risque de perpétuer ces schémas de discrimination[94]. Il a été démontré que les systèmes prédictifs pour le maintien de l'ordre et l'administration de la justice touchaient de façon disproportionnée les minorités[95].

47. En outre, la surveillance a des effets paralysants très marqués sur la façon dont les personnes exercent leurs droits, en particulier le droit à la liberté d'expression et le droit de réunion pacifique[96]. Diverses études illustrent l'ampleur de ces effets. Une enquête de 2015

[89] Voir Cour européenne des droits de l'homme, *Rotaru c. Roumanie*, arrêt du 4 mai 2000, par. 43 ; *Peck v. the United Kingdom*, arrêt du 28 janvier 2003, par. 59 ; *Perry c. Royaume_Uni*, arrêt du 17 juillet 2003, par. 38 ; *Vukota-Bojić c. Suisse*, arrêt du 18 janvier 2017, par. 55.

[90] A/HRC/44/24, par. 33.

[91] Voir https://privacyinternational.org/explainer/55/social-media-intelligence.

[92] Voir CERD/C/CHN/CO/14-17 et https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.

[93] Voir le document de séance de la Haute-Commissaire intitulé « Promotion et protection des droits de l'homme et des libertés fondamentales des Africains et des personnes d'ascendance africaine face au recours excessif à la force et aux autres violations des droits de l'homme dont se rendent coupables des membres des forces de l'ordre », par. 93 et 94. Disponible à l'adresse https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

[94] A/HRC/41/35, par. 12, et A/HRC/44/57, par. 39.

[95] Comité pour l'élimination de la discrimination raciale, recommandation générale n° 36 (2020) sur la prévention et l'élimination du recours au profilage racial par les représentants de la loi, par. 33 et 34 ; A/HRC/44/57, par. 43 ; document de séance de la Haute-Commissaire intitulé « Promotion et protection des droits de l'homme et des libertés fondamentales des Africains et des personnes d'ascendance africaine face au recours excessif à la force et aux autres violations des droits de l'homme dont se rendent coupables des membres des forces de l'ordre », par. 93 ; A/HRC/48/31, par. 24 ; https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/ ; https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf ; https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[96] A/HRC/27/37, par. 20 ; en ce qui concerne les manifestations, voir : A/HRC/44/24, par. 29, 35 et 52 ; Cour européenne des droits de l'homme, *Big Brother Watch and Others v. the United Kingdom*, arrêt du 25 mai 2021 (58170/13, 62322/14 et 24960/15), par. 495 ; http://dx.doi.org/10.15779/Z38SS13 ; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf ; https://pen.org/research-resources/global-chilling/.

a révélé que 25 % des participants qui connaissaient l'affaire Edward Snowden avaient modifié leur utilisation de diverses plateformes technologiques[97]. Une autre étude a révélé qu'entre 34 % et 61 % des écrivains (selon le pays concerné) avaient évité ou au moins envisagé d'éviter certains sujets dans leur travail par crainte de la surveillance exercée par l'État[98]. Dans une enquête menée par le Conseil norvégien de la technologie, 39 % des personnes interrogées ont déclaré qu'elles éviteraient d'utiliser des mots et des phrases relevant de la surveillance de la police[99]. Comme l'a déjà souligné le Haut-Commissaire, ces effets paralysants s'étendent aux rassemblements, y compris aux manifestations pacifiques[100].

D. Exigences en matière de droits de l'homme

48. La surveillance publique comporte indubitablement des risques importants pour les droits de l'homme et peut porter gravement atteinte au droit à la vie privée. Il est donc essentiel que les États qui y ont recours évaluent les effets potentiels de leurs actions sur les droits de l'homme et veillent strictement au respect du droit international des droits de l'homme, qui exige que toute immixtion ou restriction de ce type soit fondée en droit, nécessaire pour atteindre un objectif légitime et proportionnelle. Les mesures actuelles de surveillance publique ne répondent souvent pas à ces critères.

49. Légalité : malgré les répercussions considérables des diverses formes de surveillance publique, de nombreux pays ne disposent d'aucun cadre juridique adéquat. Les lois sur la protection des données sont souvent inexistantes ou inadéquates ou prévoient de larges exceptions pour les services de police et de renseignement[101]. En outre, il arrive souvent que les lois générales sur la protection des données ne donnent pas d'orientations détaillées ou ne prévoient pas de restrictions adéquates à l'utilisation de certains outils de surveillance. Des instruments juridiques ciblés sont donc nécessaires, en particulier pour la surveillance aux fins du maintien de l'ordre et de la sécurité nationale[102]. Les lois et réglementations doivent prévoir des restrictions claires et strictes concernant l'accès aux bases de données gouvernementales et leur fusion. Malheureusement, peu d'éléments laissent à penser que les États s'orientent vers une réglementation de l'utilisation des techniques, technologies et outils de renseignement sur les médias sociaux. Bien que les autorités de réglementation et les législateurs aux niveaux local, national et régional déploient de plus en plus d'efforts pour réglementer la reconnaissance faciale et d'autres outils de surveillance biométrique[103], la plupart des autorités continuent à exploiter des systèmes de surveillance biométrique malgré l'absence de fondement juridique pour cette activité.

50. Objectifs légitimes : il ne fait aucun doute que la surveillance publique peut servir un large éventail d'objectifs légitimes, comme la protection de la vie ou de l'intégrité corporelle des personnes et la sécurité des infrastructures critiques. Malheureusement, la surveillance publique est couramment utilisée à des fins qui ne sont pas autorisées par le droit international des droits de l'homme. Elle a ainsi été utilisée, entre autres, pour identifier et suivre des dissidents politiques, établir des profils raciaux et ethniques, cibler les communautés de

[97] Voir https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

[98] Voir https://pen.org/research-resources/global-chilling/.

[99] Voir https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Online-with-the-public.pdf.

[100] A/HRC/44/24, par. 35 et 53.

[101] A/HRC/39/29, par. 34.

[102] Les prescriptions légales minimales concernant la surveillance ont été précédemment exposées par le Haut-Commissaire, voir A/HRC/27/37 et A/HRC/39/29.

[103] Voir proposition de loi de l'Union européenne sur l'intelligence artificielle ; Lignes directrices 05/2022 du Conseil européen de la protection des données sur l'utilisation de la reconnaissance faciale par les autorités de répression, version 1.0, disponible à l'adresse https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en ; voir également la loi de l'État de Washington (États-Unis d'Amérique) relative à l'utilisation de la reconnaissance faciale, disponible à l'adresse https://www.securityindustry.org/report/washington-facial-recognition-law-faq/ et les interdictions et moratoires adoptés par les législatures locales et régionales.

personnes lesbiennes, gays, bisexuelles, transgenres et intersexes et évaluer le respect des normes sociales.

51. Nécessité et proportionnalité : si la surveillance publique peut être autorisée, les États doivent démontrer que les mesures sont à la fois nécessaires et proportionnées. Or, l'efficacité des mesures de surveillance est souvent douteuse, ce qui soulève de sérieuses questions quant à leur nécessité ou leur proportionnalité. Les preuves de l'effet de la vidéosurveillance sur la sécurité et la prévention de la criminalité sont mitigées. La plupart des études font état, tout au plus, d'un léger recul de certains types d'infractions (notamment des infractions liées aux véhicules et aux biens) dans les zones surveillées par des caméras, tandis que, de manière générale, la présence de caméras ne semble pas avoir d'incidence sur les crimes violents[104]. En outre, une comparaison entre de nombreuses municipalités de diverses juridictions montre qu'il n'y a que peu ou pas de corrélation entre le nombre de caméras de surveillance publique et la criminalité ou la sécurité dans l'ensemble d'une municipalité[105]. En ce qui concerne la détection automatique des menaces, largement utilisée par les forces de police pour détecter les coups de feu afin de repérer les possibles scènes de crime, il a été démontré que ce système assimilait à tort les sons détectés à des coups de feu dans 89 % des cas[106]. Enfin, de nombreux services de police qui avaient fait appel à des dispositifs de police prédictive ont depuis mis fin à ces collaborations, invoquant une utilité limitée[107].

52. La surveillance générale des personnes dans les espaces publics est presque toujours disproportionnée. Les mesures de surveillance dans les espaces publics devraient être ciblées et répondre à un objectif légitime concret, tel que la prévention d'une menace précise pour la sûreté ou la sécurité publique, d'une gravité suffisante pour compenser les effets négatifs de ces mesures sur les droits de l'homme. Elles devraient aussi être circonscrites à des lieux et des moments précis, par exemple lorsque des éléments indiquent qu'une infraction est susceptible de se produire ou que des menaces pour la sûreté et la sécurité publiques peuvent apparaître. Aucune autre solution empiétant moins sur la vie privée ne doit être disponible. Il est essentiel d'imposer des limites strictes à la durée de stockage des données recueillies et aux fins pour lesquelles ces données sont utilisées. Les systèmes de télésurveillance biométrique, en particulier, soulèvent de sérieuses inquiétudes quant à leur proportionnalité, étant donné leur nature hautement intrusive et leurs vastes répercussions pour un grand nombre de personnes[108]. Dans ce contexte, la Haute-Commissaire a salué les efforts récents visant à limiter ou à interdire l'utilisation des systèmes de reconnaissance biométrique à distance et a appelé à un moratoire sur leur utilisation dans les espaces publics, au moins jusqu'à ce que des garanties essentielles soient en place[109]. S'ils sont utilisés, ces systèmes ne devraient être déployés que pour répondre à certaines situations, notamment pour faire face à des infractions graves ou des menaces sérieuses pour la sécurité publique, s'ils ne risquent pas d'avoir des effets discriminatoires et s'ils sont soumis à une surveillance adéquate et efficace, y compris une autorisation indépendante et des audits indépendants réguliers concernant les droits de l'homme.

IV. Conclusions et recommandations

53. **Le présent rapport donne un aperçu de plusieurs des domaines clefs dans lesquels le numérique fait peser une menace sur le droit à la vie privée. L'adoption rapide des technologies numériques soulève toute une série de problèmes supplémentaires qui ne sont pas abordés dans le présent rapport, mais qui mériteraient une attention particulière. Par exemple, la surveillance de masse secrète, évoquée dans**

[104] Voir https://academicworks.cuny.edu/jj_pubs/256/ et https://doi.org/10.1080/01924036.2021.1879885.

[105] Voir https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[106] Voir https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/ et https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

[107] Voir https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[108] A/HRC/48/31, par. 26 et 27 ; et A/HRC/44/24, par. 33 à 38.

[109] A/HRC/48/31, par. 27 et 59 d).

de précédents rapports du Haut-Commissaire[110], reste un grave sujet de préoccupation. De même, les répercussions des systèmes d'identité numérique sur les droits de l'homme et les différents cas d'utilisation de la biométrie sont peu compris, malgré leur déploiement à l'échelle mondiale. Le suivi constant des utilisateurs d'Internet par d'innombrables acteurs, parmi lesquels les annonceurs, les institutions financières et les courtiers en données, devrait recevoir une attention bien plus grande dans les forums internationaux consacrés aux droits de l'homme. La pandémie de maladie à coronavirus (COVID-19) et l'éventail vertigineux des mesures qui ont été prises dans le domaine numérique pour y faire face pourraient faire l'objet d'un rapport à part entière. La façon dont les violations du droit à la vie privée et les atteintes à la vie privée affectent les personnes marginalisées et les personnes en situation de vulnérabilité doit être analysée de manière plus approfondie et mieux comprise. Les phénomènes émergents, tels que la propagation de l'adoption des chaînes de blocs, l'expansion de la réalité virtuelle et augmentée et le développement de neurotechnologies de plus en plus puissantes, devraient être suivis de très près.

54. **Cependant, même en n'abordant que quelques questions clefs, le présent rapport dépeint une image troublante de la manière dont le droit à la vie privée est régulièrement mis à mal à l'ère numérique. Il ne s'agit pas par ce constat de nier les bienfaits considérables que les technologies numériques apportent aux sociétés. Au contraire, les sociétés devraient adhérer pleinement au progrès technologique qui donne des moyens d'action aux personnes, améliore les conditions de vie, renforce la justice et stimule la productivité. Cela étant, on ne peut que s'alarmer des multiples façons dont la surveillance omniprésente menace les droits de l'homme et l'état de droit et peut saper des démocraties dynamiques et pluralistes. Les caractéristiques des technologies numériques modernes en réseau peuvent en faire de formidables outils de contrôle et d'oppression : chaque action dans l'espace numérique laisse une trace ; l'informatique en nuage facilite la fusion et l'analyse de sources de données disparates ; l'automatisation accroît la portée et l'efficacité possibles de la surveillance ; la surveillance numérique est difficile à déceler par ceux qui en font l'objet. En outre, la surveillance numérique est intimement liée à un manque de transparence plus général. Le public sait généralement très peu de choses sur les diverses pratiques de surveillance qui s'immiscent dans de nombreux aspects de la vie. Trop souvent, les autorités ne publient pas d'informations fiables sur le type de systèmes de surveillance qu'elles utilisent et à quelles fins − et négligent souvent de présenter des preuves de l'efficacité de ces systèmes.**

55. **Les mesures de surveillance qui sont incompatibles avec le droit international des droits de l'homme sont déjà très répandues. Même lorsque la surveillance sert des objectifs légitimes, l'infrastructure sous-jacente peut facilement être utilisée à des fins qui ne sont pas celles d'origine (on parle alors de « détournement d'usage »), ou être réaffectée à la suite de changements dans le paysage politique. Les décideurs devraient garder cela à l'esprit lorsqu'ils envisagent de nouveaux projets tendant à renforcer les capacités de collecte et d'analyse des données personnelles. Il est urgent d'organiser des débats publics sur les limites de la surveillance. Sans un débat public actif, les sociétés risquent de basculer imperceptiblement vers des systèmes de surveillance qui permettent aux personnes au pouvoir d'exercer un contrôle sans précédent sur la vie quotidienne.**

56. **Compte tenu de ce qui précède, le HCDH recommande aux États :**

a) De veiller à ce que toute ingérence dans la vie privée, notamment par le piratage informatique, les restrictions d'accès, l'utilisation de technologies de chiffrement et la surveillance du public, soit conforme au droit international des droits de l'homme, notamment aux principes de légalité, de but légitime, de nécessité, de proportionnalité et de non-discrimination, et ne porte pas atteinte à l'essence de ce droit ;

[110] Voir A/HRC/27/37 et A/HRC/39/29.

b) De faire systématiquement preuve de diligence raisonnable en matière de droits de l'homme, notamment en procédant régulièrement à des évaluations complètes des incidences sur les droits de l'homme, lors de la conception, de l'élaboration, de l'acquisition, du déploiement et de l'exploitation des systèmes de surveillance ;

c) De prendre en compte, lorsqu'ils exercent leur devoir de diligence raisonnable en matière de droits de l'homme et évaluent la nécessité et la proportionnalité des nouveaux systèmes et pouvoirs de surveillance, l'ensemble de l'environnement juridique et technologique dans lequel ces systèmes ou pouvoirs s'inscrivent ou s'inscriraient ; les États devraient également prendre en compte les risques d'abus et de détournement d'usage, y compris les risques découlant de changements politiques futurs ;

d) D'adopter et d'appliquer effectivement, par l'intermédiaire d'autorités indépendantes et impartiales dotées de ressources suffisantes, une législation sur la confidentialité des données pour les secteurs public et privé qui soit conforme au droit international des droits de l'homme et prévoie notamment des garanties, une surveillance et des recours visant à protéger efficacement le droit à la vie privée ;

e) De prendre immédiatement des mesures pour accroître la transparence de l'utilisation des technologies de surveillance, notamment en informant de manière appropriée le public et les personnes et communautés concernées et en fournissant régulièrement des données pertinentes pour que le public puisse évaluer l'efficacité et les répercussions de ces technologies sur les droits de l'homme ;

f) D'encourager le débat public sur l'utilisation des technologies de surveillance et de veiller à ce que toutes les parties prenantes participent véritablement aux décisions concernant l'acquisition, le transfert, la vente, le développement, le déploiement et l'utilisation des technologies de surveillance, y compris l'élaboration et la mise en œuvre des politiques publiques ;

g) D'appliquer des moratoires sur la vente et l'utilisation de systèmes de surveillance aux niveaux national et transnational, notamment pour ce qui est des outils de piratage et des systèmes biométriques qui peuvent être utilisés pour l'identification ou la classification des individus dans les lieux publics, jusqu'à ce que des garanties adéquates de protection des droits de l'homme soient en place ; ces garanties devraient inclure des mesures de contrôle internes et à l'exportation, conformément aux recommandations formulées dans le présent rapport et dans les précédents rapports au Conseil des droits de l'homme[111] ;

h) De veiller à ce que les victimes de violations des droits de l'homme et d'atteintes à ceux-ci liées à l'utilisation de systèmes de surveillance aient accès à des recours utiles.

57. **En ce qui concerne les points précis abordés dans le présent rapport, le HCDH adresse aux États les recommandations suivantes :**

Piratage

a) Veiller à ce que le piratage des dispositifs personnels ne soit utilisé par les autorités qu'en dernier recours, uniquement pour prévenir un acte précis constituant une menace grave pour la sécurité nationale ou une infraction grave ou pour enquêter sur un tel acte, et ne vise que la personne soupçonnée d'en être l'auteur ; toute mesure de ce type devrait faire l'objet d'un contrôle indépendant strict et être soumise à l'approbation préalable d'un organe judiciaire ;

Chiffrement

b) Promouvoir et protéger le chiffrement fort et éviter toutes les restrictions directes ou indirectes, générales et indifférenciées, à l'utilisation du chiffrement, telles que les interdictions, la criminalisation, l'imposition de normes de chiffrement faibles

[111] Voir A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 et A/HRC/48/31.

ou l'analyse côté client généralisée et obligatoire ; l'ingérence dans le chiffrement des communications privées ne devrait être possible que lorsqu'elle est autorisée par un organe judiciaire indépendant et au cas par cas, et ne cibler des individus que si cela est strictement nécessaire pour enquêter sur des infractions graves ou prévenir de telles infractions ou des menaces sérieuses pour la sécurité publique ou la sécurité nationale ;

Surveillance des espaces publics et contrôle des exportations de technologies de surveillance

c) Adopter des cadres juridiques adéquats régissant la collecte, l'analyse et le partage des renseignements tirés des médias sociaux, qui définissent clairement les motifs recevables, les conditions préalables, les procédures d'autorisation et les mécanismes de contrôle appropriés ;

d) Éviter toute surveillance générale des espaces publics constituant une immixtion dans la vie privée et veiller à ce que toutes les mesures de surveillance publique soient strictement nécessaires et proportionnées à la réalisation d'objectifs légitimes importants, notamment en limitant strictement leur portée géographique et leur durée, ainsi que la durée de stockage des données, la finalité de leur utilisation et l'accès aux données ; les systèmes de reconnaissance biométrique ne devraient être utilisés dans les espaces publics que pour prévenir des infractions graves ou des menaces sérieuses pour la sécurité publique ou enquêter sur celles-ci, et seulement si toutes les prescriptions du droit international des droits de l'homme sont respectées en ce qui concerne les espaces publics[112] ;

e) Établir des régimes de contrôle des exportations solides et adaptés, applicables aux technologies de surveillance dont l'utilisation menace gravement l'exercice des droits de l'homme ; les États devraient exiger des évaluations transparentes des incidences sur les droits de l'homme, qui tiennent compte des capacités des technologies en cause ainsi que de la situation dans l'État destinataire, notamment du respect des droits de l'homme et de l'état de droit, de l'existence de lois régissant les activités de surveillance et de leur application effective, et de l'existence de mécanismes de contrôle indépendants ;

f) Veiller à ce que, dans le cadre de la fourniture et de l'utilisation des technologies de surveillance, les partenariats public-privé respectent et intègrent expressément les normes relatives aux droits de l'homme et n'entraînent pas, de la part des États, une abdication de leur responsabilité en matière de droits de l'homme.

---

[112] Y compris les prescriptions énoncées dans les documents A/HRC/44/24, par. 53 j) (i à v), et A/HRC/48/31, par. 59 d).