Nations Unies A/HRC/62/45*

Assemblée générale

Distr. générale
21 avril 2026
Français
Original : anglais

Conseil des droits de l'homme
Soixante-deuxième session
15 juin-10 juillet 2026
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Mise en lumière des effets dissuasifs de l'écosystème de la surveillance numérique : l'érosion des droits de réunion pacifique et d'association

Rapport de la Rapporteuse spéciale sur les droits à la liberté de réunion pacifique et à la liberté d'association, Gina Romero**

Résumé

Dans le présent rapport, la Rapporteuse spéciale sur les droits à la liberté de réunion pacifique et à la liberté d'association, Gina Romero, traite les menaces que fait peser la surveillance numérique sur ces droits. Faisant fond sur les travaux précédents menés dans le cadre du mandat, elle explique et révèle, dans le rapport, les effets dissuasifs liés à cette surveillance, décrivant en détail l'ingérence considérable qu'elle représente pour l'exercice effectif des droits de réunion pacifique et d'association. Elle explique comment les effets dissuasifs devraient être pris en compte dans une analyse du droit des droits de l'homme axée sur une reconnaissance des préjudices cumulés et décrit l'écosystème de surveillance actuel.

* Nouveau tirage pour raisons techniques (21 mai 2026).

** Les annexes au présent document sont distribuées telles qu'elles ont été reçues, uniquement dans la langue de l'original.

Merci de recycler

I. Introduction

1. Dans le présent rapport, la Rapporteuse spéciale sur les droits à la liberté de réunion pacifique et à la liberté d'association décrit les effets importants que la surveillance numérique[1] a sur les droits à la liberté de réunion pacifique et à la liberté d'association, en mettant spécialement l'accent sur les effets dissuasifs qu'entraîne une telle surveillance. En détaillant ces effets, elle va au-delà des discours axés sur le droit à la vie privée ou à la liberté d'expression qui dominent les travaux de recherche existants. Ce faisant, elle ne minimise pas les effets sur ces droits ; en revanche, elle analyse la façon dont les effets dissuasifs sur les libertés publiques touchent simultanément toute une série de droits interdépendants et étroitement liés, et causent ainsi un préjudice cumulé. Il est essentiel de mettre en avant les effets particuliers sur la liberté de réunion, d'association et de participation, étant donné leur rôle central dans le bon fonctionnement des sociétés démocratiques[2].

2. Les données utilisées pour le présent rapport proviennent d'une étude menée au niveau mondial[3] sur la base d'entretiens et de consultations avec divers acteurs de contextes et juridictions variés. Au total, 152 militants, défenseurs des droits de l'homme, avocats commis d'office, juristes, journalistes et acteurs de la société civile de toutes les régions[4] ont été interrogés, afin que l'on puisse identifier des expériences communes ou transversales en matière de surveillance numérique. Une consultation a été organisée dans la région du Moyen-Orient et de l'Afrique du Nord, deux en Amérique latine, trois en Asie du Sud-Est et deux en Afrique, ainsi qu'un événement mondial en ligne. Cette méthode visait à produire des données fiables permettant de contrer les opinions sceptiques selon lesquelles les effets dissuasifs seraient trop subjectifs ou difficilement mesurables dans les faits. Pour son rapport, la Rapporteuse spéciale a également exploité 62 contributions écrites − dont 49 émanant de la société civile, d'universitaires, d'organismes internationaux et d'une grande entreprise mondiale de la tech et 13 soumises par des États − et des données recueillies lors de réunions avec la société civile ou des victimes, de visites dans des établissements universitaires et d'une visite de pays officielle. Dans l'ensemble, ces données concernent 84 États et entités, ce qui montre l'ampleur du phénomène des effets dissuasifs.

[1] Sans que cela constitue un inventaire exhaustif des capacités existantes et émergentes, la Rapporteuse spéciale a constaté un emploi croissant des pratiques de surveillance suivantes : a) des appareils compromis − sur lesquels ont été installés des outils commerciaux de cyberintrusion (logiciels espions) tels que Novispy, Pegasus et Predator − ainsi que l'utilisation d'outils d'investigation numérique tels que Cellebrite et d'intercepteurs d'identité internationale d'abonnement mobile pour surveiller les appareils mobiles et les activités de leurs propriétaires ; b) les intrusions via des logiciels ou des réseaux − notamment le piratage et l'infiltration de plateformes de communication telles que WhatsApp et Signal, de comptes de messagerie électronique et de lignes de communication, la surveillance des médias sociaux et la manipulation des réseaux, y compris des ingérences dans le système de noms de domaine (DNS) de Google ; c) les technologies d'identification biométrique, telles que la reconnaissance faciale et l'analyse de la démarche et du comportement, qui sont souvent associées à d'autres ensembles de données pour identifier et surveiller des personnes et des activités ; d) l'adaptation des infrastructures de surveillance existantes, notamment l'extension progressive des réseaux de caméras de surveillance urbaines et la réorientation d'initiatives de « ville intelligente » (qui sont souvent gérées dans le cadre de partenariats public-privé), l'utilisation de véhicules aériens (drones) et de dispositifs de localisation géospatiale, ainsi que l'exploitation de données administratives à des fins de surveillance ; et e) les plateformes numériques gérées par l'État, y compris les applications de prestation de services qui, dans certains cas, facilitent le signalement entre particuliers ou servent de mécanismes de piégeage numérique.

[2] La Rapporteuse spéciale tient à remercier le Queen Mary Centre for International Law à l'Université de Londres pour son soutien, le département de sociologie, de politique sociale et de criminologie de l'université de Southampton et le UK Research and Innovation's Future Leaders Fellowship MR/T042133/2. Elle tient également à remercier les assistants de recherche, les bénévoles et les stagiaires pour leur soutien.

[3] « Pushed into the shadows: evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association », disponible à l'adresse suivante : https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

[4] Pour plus de détails sur la méthode, voir l'annexe II.

3. On trouvera dans l'annexe I au présent rapport une vue d'ensemble des principales activités menées au titre du mandat depuis janvier 2025.

II. Banalisation de la surveillance

4. Les préoccupations accrues en matière de sécurité ont servi à justifier le développement de systèmes de surveillance, y compris ceux à double usage civil et militaire[5]. Parce qu'elles viennent s'ajouter à une sécuritisation et une militarisation croissantes des forces de l'ordre et des services de police à l'échelle mondiale, ces technologies rendent la menace qui pèse sur les libertés publiques plus complexe et plus grave.

5. Des systèmes numériques intrusifs, envahissants et à haut risque, souvent intrinsèquement incompatibles avec les obligations en matière de droits de l'homme, sont souvent inadéquatement justifiés par des arguments liés à la sécurité[6] et à la prévention de la criminalité, à savoir par des déclarations générales concernant la sécurité nationale, la souveraineté, le terrorisme, la sécurité publique, la criminalité transnationale, la cybersécurité, les crimes de haine, les « crimes contre la morale », la désinformation et autres. Le militantisme civique et politique sert de plus en plus souvent de prétexte à l'exercice d'une surveillance. Des associations et des rassemblements sont souvent qualifiés de « menaces pour la sécurité nationale », d'« agents étrangers », de « criminels » ou de « terroristes »[7]. Les autorités emploient un mélange de stratégies de surveillance discrète, cachée et en ligne (dont l'extraction de données), parallèlement à des formes plus ouvertes et visibles (telles que les drones de surveillance).

6. Ainsi, le développement d'infrastructures de surveillance intrusives se banalise (y compris dans les démocraties). Ces infrastructures peuvent facilement être détournées de leur fonction initiale et entraîner une « dérive » de la surveillance.

7. La banalisation de la surveillance numérique est souvent justifiée par des arguments liés à la sécurité et à la prévention de la criminalité alors qu'aucune preuve empirique n'étaye sa nécessité ou son efficacité. Des États ont adopté des mesures bien trop générales qui renforcent la surveillance, sans égard pour la transparence, le contrôle public et les garanties en matière de droits de l'homme. Cette évolution vers un paradigme de la prévention porte gravement atteinte à la présomption d'innocence et au respect des garanties procédurales ; en obligeant les individus à prouver qu'ils ne représentent aucune menace, l'État renverse en fait la charge de la preuve. Un tel cadre facilite la criminalisation à grande échelle des militants et transforme l'espace numérique en un lieu de suspicion permanente.

8. La banalisation d'une surveillance aveugle et omniprésente va à l'encontre des principes fondamentaux de nécessité et de proportionnalité qui s'appliquent aux restrictions de la liberté de réunion pacifique et d'association[8].

9. Les cadres internationaux de lutte contre le terrorisme et la cybercriminalité qui ne sont pas assortis de garanties en matière de droits de l'homme contribuent à l'expansion et à l'utilisation abusive potentielle de la surveillance numérique et facilitent ainsi la répression transnationale[9]. Les tendances en faveur d'une réglementation multilatérale et nationale non contraignante des puissants outils de surveillance (tels que les logiciels espions commerciaux) ne renforcent pas les cadres juridiques respectueux des droits de l'homme mais contribuent à la banalisation de ces outils.

[5] Voir https://shorturl.at/0vEby et https://shorturl.at/68IL2.
[6] Voir A/HRC/52/39.
[7] A/HRC/56/49, par. 23 : « La désignation des groupes LGBT comme extrémistes ou comme une menace pour la sécurité nationale est une autre tendance perceptible ».
[8] Voir A/HRC/55/60.
[9] Voir A/HRC/52/39 et https://tinyurl.com/2fs6frur.

III. Les écosystèmes de surveillance à l'ère du numérique

10. La surveillance généralisée est une menace omniprésente inhérente à l'environnement numérique moderne. Les outils numériques et les processus en ligne occupent désormais une place centrale dans les activités humaines de base, qu'elles soient sociales, professionnelles ou économiques. Dans le même temps, les processus sociaux et économiques reposent sur le traitement de données numériques. De ce fait, la vulnérabilité de chacun face à la surveillance numérique augmente. L'environnement numérique moderne entraîne une évolution radicale des capacités de surveillance des acteurs étatiques et non étatiques, y compris celles d'entités malveillantes, et favorise l'« autoritarisme numérique ».

11. La surveillance numérique s'effectue à distance, est largement invisible, fait appel à de multiples sources et se caractérise par une opacité et un manque de transparence inhérents. Cela signifie que, même si les personnes peuvent être conscientes de la possibilité d'une surveillance, elles ne savent pas − et souvent ne peuvent pas savoir − si, quand et comment cette surveillance est exercée, ni par qui. Il en résulte de nouvelles asymétries de pouvoir, qui compromettent la capacité de contester la surveillance au moyen du contrôle public ou par des moyens politiques ou juridiques.

12. Compte tenu du rôle central que jouent les infrastructures numériques dans la vie moderne, il est impossible de se soustraire à la surveillance ou de l'éviter ; un inévitable état d'enfermement numérique se crée, présenté comme si la surveillance était devenue une nouvelle norme acceptée.

13. Les appareils numériques du quotidien peuvent devenir de puissants outils de surveillance : les bracelets connectés peuvent servir à indiquer la fréquence cardiaque (ou le niveau de stress) d'une personne à un moment donné, les cartes électroniques permettent de retracer les trajets effectués dans les transports en commun, et l'accès aux réseaux Wi-Fi ou de télécommunications permet de localiser précisément une personne à un moment donné.

14. Des infrastructures de surveillance sont présentes dans la plupart des zones urbaines, y compris dans les écoles et sur les lieux de travail. De nombreux outils de surveillance avancés sont basés sur des logiciels et peuvent être intégrés aux infrastructures de surveillance existantes et augmenter la capacité de celles-ci. Si, au départ, ils répondent à des objectifs légitimes, ces outils peuvent facilement être détournés, notamment pour réprimer le militantisme citoyen, les associations et les rassemblements pacifiques.

15. Les outils et les pratiques de surveillance sont de plus en plus interopérables. Ils ne se distinguent plus l'un de l'autre mais agissent de concert pour renforcer les possibilités. Par exemple, l'identification biométrique peut être appliquée à des flux vidéo, être reliée à des architectures de données complexes (notamment des données issues des médias sociaux, des dossiers administratifs et des profils fournis par des courtiers en données commerciales) et être analysée à l'aide de l'intelligence artificielle (IA). C'est un changement déterminant, puisqu'on passe d'une « minimisation des données », où seules les informations strictement nécessaires sont extraites, à la « maximisation des données », où toutes les informations disponibles sont collectées, analysées et exploitées.

16. La surveillance numérique facilite l'analyse algorithmique (par l'IA) et lui permet d'exploiter pleinement son considérable potentiel. Cette analyse assistée par la surveillance peut servir, par exemple, à suivre ou à surveiller des individus (en nombre quasi infini), à établir des profils de mode de vie, à repérer des activités « suspectes » ou à exercer un contrôle sur des individus et des populations. Ces outils peuvent générer des alertes lorsque des individus pénètrent dans une zone donnée ou en sortent (« géorepérage ») ou lorsqu'ils rencontrent certaines personnes. Ces alertes constituent de nouveaux points de données, qui permettent de faire avancer une enquête ou d'intervenir physiquement en temps réel.

17. Cela augmente le degré d'intrusion et facilite l'extraction d'informations − par exemple sur les opinions politiques des individus, leur appartenance à des associations, leur participation à des activités, leur orientation sexuelle et leur état de santé − ainsi que la localisation et le ciblage d'individus.

18. La surveillance numérique s'étend aussi à la sphère privée. Les logiciels espions en sont un exemple très connu ; d'autres formes de surveillance intrusive viennent de l'accès aux enregistrements des communications Internet ou aux métadonnées de ces communications.

19. Pris ensemble, tous ces éléments transforment la participation légitime à des associations, notamment des groupes de la société civile, ou la présence à des rassemblements, en activités à haut risque, en particulier pour les populations marginalisées.

20. On pourrait s'arrêter sur des pratiques ou des outils particuliers, mais il est plus exact de considérer ces éléments émergents comme formant un écosystème de surveillance.

21. Les écosystèmes de surveillance sont constitués d'infrastructures numériques et de données gérées par des acteurs étatiques et non étatiques. Des acteurs non étatiques, y compris des entités commerciales, possèdent des données détaillées sur des particuliers qui peuvent être utilisées à des fins de surveillance. De plus, les données sont devenues un produit à part entière que l'on peut collecter et vendre. Lorsque l'État a accès aux données de télécommunications et aux données numériques que possèdent les entreprises privées, les pouvoirs et possibilités d'action des autorités s'en trouvent considérablement élargis. Typiquement, un tel accès s'organise dans le cadre d'accords de partage (formels ou informels) ou au moyen d'ordonnances judiciaires, qui tirent parfois parti de lacunes réglementaires ou d'exceptions liées à la sécurité nationale. Cette interaction entre État et acteurs non étatiques manque de transparence, ce qui entraîne un manque de prévisibilité qui porte atteinte au principe de légalité.

22. Les pouvoirs incontrôlés des plateformes numériques et des fournisseurs de services, dont les modèles économiques reposent souvent sur l'extraction massive de données à caractère personnel, favorisent aussi l'expansion de la surveillance numérique. En concevant des architectures qui privilégient la collecte de données, les acteurs privés de la tech ont créé l'infrastructure même que les États exploitent aujourd'hui à des fins de surveillance. Cette convergence entre secteurs public et privé facilite une transition fluide entre la collecte de données commerciales et la surveillance dirigée par l'État. Lorsque ces entreprises privilégient le profit ou le respect des exigences étatiques par rapport à la protection des utilisateurs, elles se rendent complices des effets dissuasifs qui érodent l'espace civique.

IV. Cadre normatif international relatif à la technologie et à la surveillance

23. L'Assemblée générale et le Conseil des droits de l'homme ont constamment exhorté les États à s'abstenir de toute surveillance illégale ou arbitraire[10] et à veiller à ce que les droits de l'homme soient respectés et réalisés tout au long du cycle de vie des technologies numériques, y compris l'intelligence artificielle. Ce cycle comprend la préconception, la conception, le développement, l'évaluation, la mise à l'essai, le déploiement, l'utilisation, la vente, l'achat, l'exploitation et la mise au rebut. Les États doivent appliquer des mesures efficaces pour prévenir, atténuer et réparer les effets néfastes sur les droits de l'homme[11] ou par un contrôle approprié[12]. Ces obligations sont fondées sur le droit international des droits de l'homme, notamment le Pacte international relatif aux droits civils et politiques et les Principes directeurs relatifs aux entreprises et aux droits de l'homme.

24. Le respect strict du droit international des droits de l'homme, y compris des garanties adéquates, est une condition préalable à l'utilisation ou au transfert de technologies numériques. Le Conseil des droits de l'homme a affirmé que des technologies qui ne respectaient pas le droit des droits de l'homme ou présentaient des risques excessifs ne devaient pas être déployées, et que les technologies de reconnaissance biométrique ne devaient pas être employées à des fins de surveillance de masse[13]. Ces exigences reflètent les

[10] Résolution 78/213 de l'Assemblée générale et résolution 59/4 du Conseil des droits de l'homme.
[11] Résolution 78/213 de l'Assemblée générale.
[12] Résolutions 77/211, 78/213 et 80/215 de l'Assemblée générale.
[13] Résolution 58/23 du Conseil des droits de l'homme.

recommandations formulées de longue date par les titulaires du mandat et les instances régionales[14].

25. Toute technologie de surveillance numérique susceptible de porter atteinte à des droits doit respecter les principes de légalité, de nécessité et de proportionnalité. Son utilisation doit être fondée sur un cadre juridique accessible et précis qui définit clairement les finalités autorisées et les catégories de personnes concernées. Une atteinte aux droits à la liberté de réunion pacifique et d'association n'est admissible que dans des cas exceptionnels et limités, lorsqu'elle est strictement justifiée par l'un des objectifs légitimes énoncés aux articles 21 et 22 du Pacte international relatif aux droits civils et politiques. La surveillance doit être limitée dans sa portée et sa durée − y compris lorsqu'elle sert des objectifs de sécurité nationale − et ne doit être exercée que lorsqu'elle est « nécessaire dans une société démocratique ». Toute restriction doit être exceptionnelle et la moins intrusive possible et préserver l'essence même de ces droits. Les mesures de surveillance doivent faire l'objet d'une autorisation préalable, d'un contrôle adéquat et indépendant « de bout en bout » (la nécessité et la proportionnalité doivent être évaluées à chaque étape) et d'un examen a posteriori indépendant[15]. La Rapporteuse spéciale affirme qu'une évaluation globale des préjudices cumulés liés à la surveillance doit être obligatoire.

26. Un contrôle humain efficace des systèmes d'IA est essentiel pour prévenir ou atténuer les risques concernant les droits de l'homme, et pour garantir que ces systèmes restent sûrs, éthiques et responsables[16].

27. Cependant, ces normes sont souvent mises à mal par des mesures générales de lutte contre le terrorisme et la cybercriminalité, par des dérogations au nom de la sécurité nationale que permettent les cadres mondiaux, régionaux et nationaux, et par un manque de volonté politique de réglementer les technologies de surveillance à haut risque, dont certaines peuvent en elles-mêmes être incompatibles avec les obligations des États en matière de droits de l'homme[17]. C'est là le fruit de collaborations opaques entre États et entreprises dans le cadre desquelles les obligations en matière de droits de l'homme ne sont pas prises en compte, et de pressions coercitives que les États et les entreprises exercent pour faire supprimer les garde-fous empêchant les abus ou les détournements[18].

28. Le droit international des droits de l'homme impose aux États de veiller à ce que la surveillance, y compris la surveillance numérique, ne porte pas indûment atteinte à la liberté de réunion pacifique et d'association. Ces obligations juridiques restent applicables dans les situations d'urgence, et les mesures de surveillance ne peuvent en aucun cas porter indûment atteinte aux libertés publiques[19]. De même, la surveillance numérique et la mise au point et l'utilisation des technologies nouvelles et émergentes dans le domaine militaire doivent être compatibles avec le droit international des droits de l'homme tout au long de leur cycle de vie[20].

[14] Voir https://shorturl.at/V0asY.

[15] Cour européenne des droits de l'homme, *Ekimdzhiev et autres c. Bulgarie*, requête n° 70078/12, arrêt du 11 avril 2022 ; *Green Alliance c. Bulgarie*, requête n° 6580/22, arrêt du 17 février 2026 ; *Big Brother Watch et autres c. Royaume-Uni*, requêtes n°s 58170/13, 62322/14 et 24960/15, arrêt du 25 mai 2021 ; et Cour interaméricaine des droits de l'homme, *Members of the José Alvear Restrepo Lawyers' Collective v. Colombia*, arrêt du 18 octobre 2023.

[16] Résolutions 79/175 et 78/265 de l'Assemblée générale ; et Règlement sur l'intelligence artificielle de l'Union européenne.

[17] Fionnuala Ní Aoláin, « One step forward? Agreement on spyware regulation in the Pall Mall Process », 9 mai 2025.

[18] Voir https://tinyurl.com/4jmf86aa, https://tinyurl.com/ycxxhkjm, https://tinyurl.com/e6mu9x9u et https://tinyurl.com/rtch62xu.

[19] Voir A/HRC/50/42 et https://shorturl.at/BYrPy.

[20] Résolution 79/239 de l'Assemblée générale et A/C.1/80/L.46.

V. Éléments fondamentaux des droits de réunion pacifique et d'association concernés par la surveillance numérique

29. L'importance cruciale de la liberté d'association et du droit de réunion pacifique pour une démocratie dynamique est largement reconnue[21]. La société civile[22] – et les médias[23] – jouent le rôle de « gardiens publics » essentiels au bon fonctionnement des processus démocratiques, et, de ce fait, toute atteinte à ces droits touche aussi directement le droit de participer aux affaires publiques[24]. Étant donné que les droits à la liberté de réunion pacifique et d'association sont interdépendants et favorisent l'exercice d'autres droits, toute ingérence indue réduit la capacité de plaider en faveur de tous les droits de l'homme. Elle touche à la dignité humaine, étouffe l'action démocratique et entrave la construction de sociétés justes et pacifiques, et donc, en fin de compte, freine les progrès dans des domaines essentiels tels que le développement durable, la justice climatique, la sécurité et la paix[25].

30. Dans le présent rapport, la Rapporteuse spéciale traite les éléments fondamentaux des droits à la liberté de réunion pacifique et d'association, mettant l'accent sur leur protection effective dans la pratique. Elle se penche sur les éléments qui permettent aux individus, aux associations, aux mouvements sociaux et aux rassemblements d'agir librement pour atteindre les objectifs qu'ils se sont fixés. Plus précisément, elle met l'accent sur la capacité d'organiser, de mobiliser, d'obtenir et de gérer des ressources (y compris des financements étrangers), et sur d'autres activités essentielles légitimes, telles que la planification, le choix de la stratégie ou des objectifs, la diffusion de l'information, la communication et l'expression, la libre circulation et l'accès à la solidarité[26].

31. L'organisation et la mobilisation d'un militantisme civique ou politique nécessitent un engagement durable de la part d'individus ou de groupes[27]. Une communication aisée est essentielle lorsque l'on veut diffuser des informations, accéder à des ressources, mobiliser des participants et des partisans et assurer la protection et la justice. À cet égard, la résilience et la confiance sont fondamentales[28]. Toute atteinte à la résilience nuit à la capacité d'élaborer et de pérenniser une action collective, de générer et partager des connaissances ou de préserver la mémoire collective et la solidarité. De même, l'érosion de la confiance interpersonnelle entraîne une désocialisation et limite la capacité des individus et des groupes de communiquer librement et d'agir efficacement[29]. Elle renforce l'isolement et augmente la vulnérabilité face à la stigmatisation, à la répression ou à une fermeture injustifiée[30]. La confiance et le tissu social sont également profondément atteints lorsque des applications de

[21] Comité des droits de l'homme, observation générale nº 37 (2020), par. 1 et 12 ; A/HRC/20/27, par. 24 et 51 ; A/77/171, par. 5, 8 et 36 ; A/HRC/31/66, par. 5 ; Principes sur l'application de la législation internationale des droits humains en matière d'orientation sexuelle et d'identité de genre, principe 20. Comité des droits de l'enfant, observation générale nº 25 (2021), par. 64 ; et Cour européenne des droits de l'homme, *Gorzelik et autres c. Pologne*, requête nº 44158/98, arrêt du 17 février 2004, par. 93.

[22] Cour européenne des droits de l'homme, *Magyar Helsinki Bizottság c. Hongrie*, requête nº 18030/11, arrêt du 8 novembre 2016, par. 167 ; et *Szabó et Vissy c. Hongrie*, requête nº 37138/14, arrêt du 6 juin 2016, par. 38.

[23] Cour européenne des droits de l'homme, *Jersild c. Danemark*, requête nº 15890/89, arrêt du 23 septembre 1994, par. 31.

[24] A/HRC/59/44, par. 1 ; et Comité des droits de l'homme, observation générale nº 25 (1996).

[25] Voir A/HRC/59/44 et A/78/246.

[26] Comité des droits de l'homme, observation générale nº 37 (2020), par. 33. A/HRC/53/38/Add.4, par. 7 ; et A/77/171, par. 4.

[27] Comité des droits de l'homme, observation générale nº 37 (2020), par. 33.

[28] A/77/171, par. 52 ; et Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki et Amy Stevens, « The chilling effects of surveillance and human rights: insights from qualitative research in Zimbabwe and Uganda », *Journal of Human Rights Practice*, vol. 16, nº 1 (février 2024).

[29] A/77/171, par. 52.

[30] A/80/219, par. 86.

prestation de services encouragent le signalement entre particuliers, comme c'est le cas en Chine et au Venezuela (République bolivarienne du)[31].

32. Les droits à la liberté d'association et de réunion pacifique s'appliquent sans discrimination à quiconque − citoyen, non-citoyen[32] ou enfant[33] − et les obligations qui incombent à l'État de faciliter l'exercice de ces droits sont « neutres sur le fond »[34]. L'indépendance des associations doit être protégée.

33. Le droit des droits de l'homme reconnaît clairement l'importance d'un espace civique libre de toute entrave − physique ou numérique − pour l'exercice de ces droits[35]. Dans cet espace, le fait de pouvoir agir anonymement ou de ne révéler que certains aspects de son identité est essentiel pour que chacun puisse participer à la vie publique et poursuivre les objectifs qu'il s'est fixés[36]. Par ailleurs, l'importance de la spontanéité lorsqu'il s'agit de répondre aux besoins urgents de la communauté, et le caractère intrinsèquement perturbateur des rassemblements pacifiques, sont également reconnus et protégés[37].

34. L'accès à la justice est indispensable à l'exercice effectif de ces libertés. Le manque de transparence en matière de surveillance numérique et l'insuffisance des garanties juridiques empêchent tout établissement de responsabilités, ce qui entrave l'exercice effectif de ces droits[38].

A. Préjudices intersectionnels

35. La surveillance numérique et ses effets dissuasifs entraînent des préjudices intersectionnels manifestes. Ces effets accentuent des vulnérabilités sociopolitiques préexistantes et la discrimination historique.

36. Comme il a été signalé dans le cadre du mandat, la stigmatisation[39] vise généralement des femmes et des militants marginalisés par des techniques de surveillance numérique, dont des logiciels espions, la surveillance des médias sociaux ou le « doxxing ». Ces manœuvres, destinées à nuire à la réputation des personnes concernées et à les pousser à se retirer, prennent souvent la forme d'attaques à caractère sexuel, notamment au moyen de deepfakes, ou obligent des militants LGBTQI+ à révéler contre leur gré leur orientation sexuelle. Ces tactiques utilisent la technologie comme une arme pour faire taire les voix diverses au sein de l'espace civique.

37. La surveillance des espaces publics érode la vie socioculturelle. La crainte d'être qualifiées d'« agents étrangers », de « criminels », de « terroristes » ou de « fauteurs de troubles » ou d'autres choses encore, dissuade des personnes de se montrer en public. Ces effets sont exacerbés dans des contextes répressifs, en particulier pour les associations criminalisées, les groupes contestataires et les personnes dont le statut migratoire est incertain. En outre, la surveillance exercée à proximité des prestataires de services restreint l'accès aux services sociaux, y compris aux soins de santé, tandis que la surveillance dans les établissements d'enseignement porte préjudice aux enfants et aux jeunes, et nuisent à leur éducation, à leur estime de soi, à leur identité et à leur évolution professionnelle. De même, les effets dissuasifs engendrés par la surveillance portent préjudice de manière disproportionnée aux communautés marginalisées et racisées, et aux personnes ou groupes qui remettent en cause le statu quo, parlent vrai face au pouvoir, exigent que justice soit faite

[31] Voir https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29302.
[32] Comité des droits de l'homme, observation générale nº 37 (2020), par. 5.
[33] Convention relative aux droits de l'enfant, art. 15.
[34] Comité des droits de l'homme, observation générale nº 37 (2020), par. 21.
[35] Ibid., par. 1 et 53 ; CCPR/C/108/D/1948/2010 et CCPR/C/108/D/1948/2010/Corr.1, par.7.4 ; et A/77/171, par. 53.
[36] Comité des droits de l'homme, observation générale nº 37 (2020), par. 60. et A/HRC/44/24, par. 24.
[37] Comité des droits de l'homme, observation générale nº 37 (2020), par. 47.
[38] Voir A/HRC/47/24 et A/HRC/53/38/Add.4.
[39] Voir A/79/263.

et que les responsabilités soient établies en cas de violation des droits de l'homme, ou encore luttent contre la corruption.

38. Les effets discriminatoires des outils de surveillance basés sur l'IA, notamment la reconnaissance faciale et les algorithmes prédictifs, sont largement documentés[40]. C'est ce qu'ont corroboré des contributions montrant comment des systèmes d'IA biaisés touchaient de manière disproportionnée, entre autres, les personnes d'ascendance africaine, les minorités ethniques et religieuses, et les enfants.

B. Diligence raisonnable en matière de droits de l'homme et technologies de surveillance numérique

39. Pour respecter leurs obligations en matière de droits de l'homme, les États et les entreprises doivent rigoureusement faire preuve de diligence raisonnable et évaluer les effets de la surveillance numérique. Une solide analyse du critère de « nécessité » exige une évaluation globale de l'utilité par rapport aux préjudices. Cette approche globale axée sur les « préjudices cumulés » est essentielle, car les évaluations se limitent trop souvent à la vie privée ou à la liberté d'expression ; or, bien qu'essentiels, ces éléments ne sont qu'une partie de la réalité. Toute étude d'impact complète sur les droits de l'homme doit expressément inclure la liberté de réunion pacifique et d'association et tout autre droit concerné. Une évaluation utilité − préjudice doit être fondée sur des données factuelles, et il faut tenir compte du contexte et/ou des outils utilisés, prendre en considération les préjudices intersectionnels et adopter des méthodes interdisciplinaires[41].

40. Les études d'impact sur les droits de l'homme sont essentielles en ce qui concerne les technologies émergentes, dont les conséquences sur les droits de l'homme ne sont souvent pas immédiatement prévisibles dans leur intégralité et tendent à s'aggraver avec le temps.

VI. Introduction aux effets dissuasifs

41. Les effets dissuasifs découlant de la surveillance apparaissent lorsque des individus modifient leur comportement par crainte des conséquences d'une surveillance réelle, supposée ou perçue. Les effets dissuasifs sont variés et influencent l'engagement sur les médias sociaux, la fréquentation de sites Web, les requêtes de recherche et la participation à des réunions (y compris en ligne). Ils influencent notamment le choix des interlocuteurs auxquels une personne s'adresse, ce qu'elle dit, ses activités sociales publiques ou privées, et sa participation (le cas échéant) aux processus démocratiques et aux activités politiques, entre autres choses. Les effets dissuasifs peuvent empêcher des individus ou des groupes d'organiser des rassemblements ou d'y participer, d'entrer en contact ou de collaborer avec certains acteurs (autorités, donateurs, partenaires, communautés, victimes, journalistes, avocats ou autres) ou de mener certaines activités.

42. Les effets dissuasifs ne sont pas uniquement binaires. Ils comportent des nuances et leur intensité et leur influence varient. Ils vont au-delà des pratiques courantes destinées à préserver la confidentialité et l'anonymat, telles que l'utilisation de réseaux privés virtuels ou l'élaboration de systèmes de sécurité solides au sein des organisations. Ils peuvent entraîner des modifications de l'activité prévue. Par exemple, des rassemblements ou des associations peuvent adopter une approche de communication plus « modérée » ou plus « acceptable », ou choisir d'agir de manière moins visible.

43. Dans le présent rapport, la Rapporteuse spéciale expose en détail comment les personnes soumises à la surveillance ou menacées de l'être sont souvent confrontées à de graves conséquences et à une répression intense, notamment la stigmatisation, l'intimidation, la criminalisation, la détention arbitraire, des menaces de mort, entre autres.

[40] Voir, par exemple, Simone Browne, Dark Matters: On the Surveillance of Blackness (Duke University Press, 2015).

[41] A/HRC/55/60, par. 24.

44. Les effets dissuasifs touchent bien plus que les seules cibles de la surveillance (réelle ou supposée), notamment les membres de la famille, les communautés, les mouvements sociaux et la société. Les effets dissuasifs générés par la surveillance sont durables et s'étendent bien au-delà de l'activité de surveillance réelle ou supposée, parfois sur plusieurs générations.

45. Les effets dissuasifs émanent de nombreuses sources et sont inspirés par les conséquences supposées des manifestations directes et visibles de la surveillance, et des signes plus indirects et ambigus de celle-ci.

46. Dans certains cas, les activités de surveillance numérique sont clandestines, tandis que dans d'autres, elles sont menées au grand jour et employées dans le but explicite de dissuader et brider l'activisme et la dissidence. Dans les deux cas, l'effet dissuasif est très important.

47. Parce qu'elle est invisible et se pratique à distance, la surveillance numérique génère un doute constant quant à l'existence même d'une surveillance. À cela s'ajoutent un manque de transparence concernant les activités de surveillance, le traitement et la conservation des données, des restrictions d'accès opaques concernant les informations collectées, et la nature complexe (et souvent non déclarée) des entités qui détiennent, exploitent et gèrent les systèmes de surveillance et collectent les données. Les lois existantes sont souvent inadéquates, en ce qu'elles accordent des pouvoirs trop larges et ne prévoient suffisamment ni protections ni établissement des responsabilités. Les individus n'ont souvent d'autre choix que de vivre en supposant qu'ils sont constamment surveillés.

48. Si les effets dissuasifs constituent un phénomène bien documenté dans les rapports des organismes chargés des droits de l'homme et la jurisprudence[42], aucune véritable analyse du droit des droits de l'homme n'a encore pris en compte ceux découlant de la surveillance numérique actuelle. À ce jour, la jurisprudence en matière de droits de l'homme fait principalement référence aux formes de surveillance existant depuis longtemps[43] ou à leurs effets dissuasifs[44]. En ne tenant pas compte du caractère particulier de la surveillance numérique, les cadres juridiques actuels peinent à prendre pleinement en compte le préjudice global qu'elle représente pour les droits de l'homme et les libertés.

VII. Atteintes aux droits à la liberté de réunion pacifique et d'association liées à des effets dissuasifs

49. Les tendances décrites ici reflètent l'expérience de personnes ayant apporté leur témoignage pour le présent rapport (152 acteurs divers à travers le monde ; 62 contributions écrites[45]) − leurs propos sont représentatifs d'un vécu largement partagé qui ressort des données. Chaque référence ne constitue donc pas une liste exhaustive des personnes concernées par un point précis. En fonction du consentement des participants et pour des raisons de sécurité, pour certaines contributions ou citations, seuls un pays ou une région sont mentionnés et non l'organisation ou un autre élément d'identification direct, afin de préserver l'anonymat[46].

[42] Comité des droits de l'homme, observation générale n°s 37 (2020) et 34 (2011). A/HRC/27/37 ; A/HRC/56/50 ; A/HRC/23/40 ; Cour interaméricaine des droits de l'homme, *Members of the José Alvear Restrepo Lawyers' Collective v. Colombia*, arrêt du 18 octobre 2023. Cour européenne des droits de l'homme, *Glukhin c. Russie*, requête n° 11519/20, arrêt du 4 juillet 2023.

[43] Pete Fussey et Daragh Murray, F*acial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence*, (Oxford University Press, 2025) ; et Cour européenne des droits de l'homme, *Catt c. Royaume-Uni*, requête n° 43514/15, arrêt du 24 avril 2019, par. 123.

[44] Cour européenne des droits de l'homme, *Navalnyy c. Russie*, requêtes n°s 29580/12, 36847/12, 11252/13, 12317/13 et 43746/14, arrêt du 15 novembre 2018, par. 103 ; et *Baka c. Hongrie*, requête n° 37138/14, arrêt du 23 juin 2016, par. 173.

[45] Voir annexe 2.

[46] Voir l'étude globale, disponible à l'adresse suivante : https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

50. La surveillance numérique a bouleversé la possibilité de rester anonyme en public. Les technologies, en particulier celles de reconnaissance faciale, permettent l'identification et le suivi rapides et précis des personnes participant à des rassemblements publics et aux activités d'associations. Des militants de toutes les régions consultées ont montré que la surveillance de foules en temps réel et l'identification a posteriori d'individus à partir d'images enregistrées renforçaient l'effet dissuasif, portaient atteinte à l'anonymat, conduisaient à des arrestations arbitraires préventives en masse et réduisaient la participation du public aux rassemblements[47]. Le renforcement des capacités de surveillance influence de manière très importante la capacité de participer à la vie civique, notamment dans le cadre d'actions en faveur des droits du travail, puisque la surveillance numérique a servi à cibler des syndicalistes et des organisations syndicales.

51. Le fait que des acteurs étatiques et non étatiques surveillent de plus en plus souvent secrètement les rassemblements pacifiques remet fondamentalement en cause la présomption d'innocence et la possibilité de participer sans entrave. Des participants aux mouvements de solidarité avec la Palestine, qui sont apparus dans des universités partout dans le monde, ont fait état d'une intensification de la surveillance sur les campus, notamment avec l'installation de nouvelles caméras, de systèmes de reconnaissance faciale et d'un suivi renforcé des médias sociaux[48]. Un universitaire qui a fait l'objet d'une surveillance discrète avant de donner une conférence dans une université du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord a expliqué : « Vous êtes censé être innocent jusqu'à ce que votre culpabilité soit établie… Mais ils ont commencé à enquêter sur moi … à cause de ma bourse. Je suis un chercheur palestinien. Que suis-je censé étudier et enseigner pour éviter cette surveillance et ce contrôle injustifiés, injustes et abusifs ? »[49]. Son expérience correspond à une pratique plus générale au sein des universités britanniques et de leurs homologues américaines, qui font appel à des sociétés de renseignement privées pour enquêter sur des militants pro-palestiniens avant des manifestations, souvent sous la pression de ces entreprises[50].

52. La surveillance accrue de lieux physiques a contribué à l'attrait des rassemblements en ligne, qui sont devenus une bouée de sauvetage essentielle, en particulier pour les militants en exil. Cependant, cette transition génère un autre dilemme : dans certains cas, le fait de se réfugier en ligne peut réduire l'effet de la surveillance exercée dans la rue, mais augmente la vulnérabilité, la visibilité et l'exposition parce que la surveillance numérique est moins perceptible. Les participants sont exposés à une censure généralisée, une surveillance intrusive, des actes de harcèlement ciblés et des arrestations. Les autorités utilisent les espaces numériques comme outils de surveillance et de contrôle, suivant les activités en ligne afin d'identifier, de localiser et d'arrêter des militants. Une militante afghane a expliqué comment « les autorités utilisaient l'espace numérique comme une arme contre elle et ses semblables ; les responsables taliban repèrent les militants via leur activité en ligne et les arrêtent »[51].

53. Les associations et les rassemblements en ligne sont aussi davantage exposés au risque de coupures générales d'Internet. Celles-ci se produisent dans des phases bien précises des mouvements de contestations, comme on a pu le constater tout au long de l'année 2026 en République islamique d'Iran, et lors d'événements marquants, dont la Journée des droits de l'homme, le Cinco de Mayo et d'autres[52].

[47] Deuxième, troisième et quatorzième entretiens, première consultation en Asie du Sud-Est, première consultation en Afrique et contributions écrites de la société civile du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, de Serbie et de Géorgie.

[48] Voir https://tinyurl.com/mrbdx9ku.

[49] Contribution de Liberty Investigates.

[50] Voir https://tinyurl.com/5ayc7yz7 et https://tinyurl.com/mrbdx9ku.

[51] Contribution écrite de la société civile d'Afghanistan ; seizième entretien (Nigéria) ; et première consultation en Afrique.

[52] Première consultation en Amérique latine (Cuba). Voir aussi A/HRC/47/24/Add.2.

A. Participation restreinte et « désocialisation »

54. La surveillance numérique entraîne une limitation des contacts entre personnes et organisations. Diverses mesures prises en réaction ont été rapportées, comme le fait d'éviter les réunions faisant appel aux technologies numériques ; le fait de limiter les communications concernant la stratégie, l'organisation ou le plaidoyer ; et un isolement général par rapport à l'entourage personnel et professionnel. Ces pratiques touchent les personnes visées par une surveillance et, par ricochet, celles qui craignent d'être accusées par association ou de faire l'objet d'une surveillance accrue en raison de leurs liens avec ces personnes. Un tel auto-isolement limite nécessairement l'accès aux canaux de plaidoyer, aux financements et aux mesures de protection, ce qui aggrave l'isolement et réduit la capacité de réaliser des objectifs stratégiques.

55. La surveillance exerce un effet dissuasif évident, qui entrave la mobilisation des participants et des sympathisants (y compris bénévoles), le recrutement de personnel et, entre autres, dissuade les gens de rejoindre des groupes sociopolitiques ou de poursuivre leur engagement au sein de ceux-ci[53]. Il en résulte une désocialisation et une réduction de l'activité collective, puisque les effets dissuasifs « constituent une dissolution de facto des espaces organisationnels »[54] et une disparition de l'engagement politique[55].

56. Les effets dissuasifs de la surveillance poussent des mouvements à la décentralisation afin de limiter l'exposition et d'éviter de mettre en danger des partenaires, ce qui rend toute action collective unie moins viable[56]. De nombreuses organisations se sont dites réticentes à communiquer avec des personnes ou des organisations dont la sécurité numérique était insuffisante[57], tandis que d'autres ont dit avoir suspendu leur adhésion à des mouvements de solidarité étroitement surveillés par les autorités[58]. Les effets dissuasifs imposent des contraintes aux organisations ; ces contraintes nuisent à un élément essentiel de la construction d'un mouvement[59].

57. Les effets dissuasifs de la surveillance sont durables et persistent longtemps après la fin des activités de surveillance proprement dites. Cet effet durable est particulièrement manifeste chez les victimes d'attaques par des logiciels espions. Des journalistes des Balkans ont raconté comment un de leurs collègues, dont l'appareil avait été « infecté par Pegasus », s'était retrouvé ostracisé et considéré comme s'il était « littéralement infecté »[60]. En général, les victimes de logiciels espions ont décrit des effets dissuasifs à plusieurs niveaux, dont une exclusion à long terme, la ruine professionnelle et l'autocensure volontaire destinée à protéger d'autres personnes, y compris des bénéficiaires[61].

B. Atteinte à la fonction de « surveillant public »

58. Les effets dissuasifs de la surveillance limitent l'accès aux sources nécessaires pour dénoncer les violations des droits de l'homme, ce qui modifie profondément les relations avec les lanceurs d'alerte[62], les défenseurs des communautés marginalisées[63], les

[53] Contributions écrites de la société civile provenant d'Italie, du Pakistan, d'Espagne et des États-Unis d'Amérique ; première consultation en Afrique ; deuxième consultation en Asie du Sud-Est ; deuxième et troisième consultations en Amérique latine.

[54] Contribution écrite de la société civile provenant du Centre pour les droits de l'homme et la justice, République bolivarienne du Venezuela.

[55] Première et troisième consultations en Asie du Sud-Est.

[56] Deuxième consultation en Amérique latine (République bolivarienne du Venezuela) ; et neuvième entretien (États-Unis).

[57] Douzième et treizième entretiens.

[58] Neuvième entretien (États-Unis) évoquant les mouvements de soutien à la Palestine ; et dixième entretien.

[59] Première consultation en Asie du Sud-Est.

[60] Huitième entretien.

[61] Sixième et huitième entretiens

[62] Quatrième entretien (Serbie).

[63] Première consultation en Amérique latine.

mouvements syndicaux[64] et les journalistes qui cherchent à mettre en lumière les atteintes aux droits de l'homme[65]. Couvrir des événements dans un contexte de surveillance est devenu beaucoup plus complexe[66], le nombre de sources est réduit[67] et certains journalistes et observateurs de manifestations choisissent de ne pas couvrir celles-ci[68].

C. Crainte de mettre d'autres personnes en danger

59. La dissociation professionnelle destinée à protéger autrui est une conséquence directe de la surveillance numérique. Des militants de la société civile en Algérie ont fait part de leur crainte d'exposer des collègues à une surveillance étatique relevant de la sécurité nationale[69]. Des militants au Myanmar ont expliqué comment les effets dissuasifs de la surveillance les avaient contraints à ne communiquer entre eux que de façon limitée, clandestine et extrêmement dangereuse[70]. Des militants en Australie, au Brésil et aux États-Unis, en Europe et dans toute l'Afrique ont expliqué qu'ils filtraient constamment les informations afin de limiter les risques de préjudice et de poursuites judiciaires pour d'autres personnes[71]. Comme l'a décrit un militant pour les droits des peuples autochtones : « C'est devenu plus difficile, et moins éthique, de convaincre les communautés de s'exprimer. »[72].

60. Des inquiétudes concernant les membres de la famille ont été constamment citées dans toutes les régions consultées et dans plusieurs pays, ce qui montre que les effets dissuasifs dépassent systématiquement les personnes directement visées par la surveillance pour toucher aussi des personnes sans lien avec elles. Les effets dissuasifs collatéraux touchant la famille ont découragé de nombreux militants de participer à des rassemblements pacifiques[73], en particulier après la saisie d'appareils électroniques et la divulgation qui s'en est suivie de leurs réseaux personnels[74].

61. Des inquiétudes concernant la famille illustrent la dimension transnationale des effets dissuasifs. Cette dimension a été constatée partout dans le monde, par exemple chez les militants tibétains en exil qui réduisent systématiquement leurs activités dans le pays d'accueil en raison des menaces pesant sur leur famille restée au Tibet[75]. À mesure que la surveillance numérique s'est développée, l'effet qu'elle produit s'est également accru. De nombreux témoignages de première main concernent une répression transnationale à l'encontre de Chinois en exil et de communautés de la diaspora à l'étranger, qui influence les rassemblements pacifiques dans des pays tiers, quelles que soient les protections en matière de droits de l'homme en vigueur dans ces pays[76]. Des militants de Bahreïn, d'Éthiopie, de Géorgie, d'Ouganda, du Bélarus, de Russie et de la République-Unie de Tanzanie, entre autres, ont décrit des expériences similaires vécues personnellement[77]. Un militant afghan a déclaré que cette expérience avait « tout brisé dans [sa] vie »[78], tandis que des militants de la région du Moyen-Orient et de l'Afrique du Nord ont déclaré que des parents, des proches et

[64] Deuxième et troisième consultations en Amérique latine.
[65] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord ; et quatrième consultation en Amérique latine.
[66] Quatrième consultation en Amérique latine.
[67] Septième entretien ; et deuxième consultation en Afrique.
[68] Deuxième consultation en Amérique latine (Argentine).
[69] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord.
[70] Première consultation en Asie du Sud-Est.
[71] Deuxième consultation en Amérique latine ; quatrième consultation en Asie du Sud-Est (Australie) ; troisième entretien (Allemagne) ; neuvième entretien ; et première consultation en Afrique.
[72] Première consultation en Amérique latine.
[73] Neuvième entretien ; première et troisième consultations en Asie du Sud-Est ; première consultation en Afrique ; consultation dans la région du Moyen-Orient et de l'Afrique du Nord ; et deuxième consultation en Amérique latine.
[74] Onzième entretien.
[75] Deuxième et troisième consultations en Asie du Sud-Est.
[76] Deuxième consultation en Asie du Sud-Est ; et voir les sites https://shorturl.at/fZD5X et https://shorturl.at/OuZ85.
[77] Cinquième, quatorzième, seizième et dix-septième entretiens. Contributions écrites de la société civile.
[78] Contribution écrite de la société civile d'Afghanistan, récits 31 et 32.

des amis de personnes exilées étaient arrêtés ou disparaissaient si celles-ci participaient à des actions de plaidoyer à l'étranger[79].

62. Des effets dissuasifs qui touchent la famille affectent profondément les personnes concernées. Celles-ci peuvent s'isoler et rompre volontairement les liens avec leurs proches − y compris les enfants − pour les protéger[80], et s'abstenir de contacts même en cas de maladie ou de deuil[81].

D. Méfiance et stigmatisation

63. La surveillance engendre un climat de méfiance et sape la solidarité. Le processus mental de réévaluation de la confiance est constant. Un acteur de la société civile l'a exprimé en ces termes : « La confiance n'est plus automatique. Elle doit se négocier chaque jour. »[82]. La surveillance numérique a transformé la culture de la sécurité au sein de la société civile, jetant un soupçon injustifié sur certains groupes[83] et obligeant d'autres à recourir à des modes de communication plus complexes et nécessitant davantage de ressources pour prouver leur fiabilité[84].

64. La méfiance engendrée par les effets dissuasifs de la surveillance a un impact considérable sur les relations personnelles[85] et « a brisé la capacité de socialiser et d'entretenir des relations humaines normales, parce qu'on ne peut pas vraiment être soi-même »[86]. Dans les cas les plus extrêmes, la confiance est soumise à des conditions très exigeantes, par exemple le fait d'être également prêts à accepter le risque de la prison[87]. La méfiance engendrée par les effets dissuasifs perturbe aussi les relations avec les partenaires intimes[88].

65. Les tentatives de stigmatisation sapent la capacité de s'organiser et de mobiliser[89]. La surveillance remplit une double fonction : elle permet de recueillir des informations qui alimentent la stigmatisation initiale, puis d'exploiter le fait qu'une personne est stigmatisée pour justifier une surveillance accrue. La divulgation d'informations privées recueillies par une surveillance illégale − y compris la surveillance d'espaces privés intimes − est l'une des tactiques employées et sert à menacer et discréditer des militants par des campagnes de diffamation[90].

66. Des victimes de violences policières ont été spécialement visées dans le cadre de campagnes de stigmatisation[91]. De telles tactiques visent à discréditer de futures manifestations et ont un effet dissuasif manifeste sur quiconque envisage d'organiser ou de rejoindre un mouvement[92].

67. La stigmatisation en ligne contient souvent une dimension de genre, les militantes étant la cible d'insultes et de menaces de violence sexuelle. Les médias sociaux sont souvent employés de manière à ternir la réputation d'acteurs de premier plan de la société civile[93].

[79] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord.
[80] Contribution écrite de la société civile d'Afghanistan ; première et troisième consultations en Asie du Sud-Est ; quinzième entretien (Afrique de l'Ouest) ; et première consultation en Afrique.
[81] Contribution écrite de la société civile d'Afghanistan ; et première consultation en Afrique.
[82] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord.
[83] Quatorzième entretien.
[84] Quatrième et quinzième entretiens ; et deuxième consultation en Amérique latine.
[85] Quinzième entretien ; et première consultation en Asie du Sud-Est.
[86] Neuvième et quatorzième entretiens.
[87] Quatorzième entretien.
[88] Premier, onzième et quatorzième entretiens.
[89] Quatrième consultation en Asie du Sud-Est ; sixième consultation en Amérique latine ; et première consultation en Afrique.
[90] Amy Stevens, Pete Fussey, Daragh Murray *et al.*, « 'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe », *Big Data and Society*, vol. 10, nº 1 (2023).
[91] Première et deuxième consultations en Amérique latine.
[92] Ibid.
[93] Deuxième consultation en Asie du Sud-Est ; seizième entretien ; et deuxième et sixième consultations en Amérique latine.

Les préjudices peuvent être plus graves dans des contextes profondément conservateurs et discriminatoires. En Afghanistan, des acteurs de la société civile ont rapporté que les militantes arrêtées sont souvent menacées, pour le cas où elles continueraient à s'exprimer, de voir diffuser sur Internet des photos ou des vidéos montrant les mauvais traitements et les humiliations subis pendant leur détention[94].

68. Une infiltration effective ou une tentative d'infiltration des réseaux professionnels ou sociaux ou des associations provoque souvent des effets dissuasifs. Dans de nombreux pays, la coercition physique et la coercition numérique vont de pair, la confiscation physique des téléphones facilitant l'infiltration des réseaux numériques via des appareils piratés. La confiance entre militants en pâtit, ce qui entrave leur capacité de communiquer librement et de s'organiser[95].

69. Des militants au Soudan du Sud ont fait état d'une infiltration généralisée et délibérée, aux fins expresses d'intimidation. Celle-ci a nui à leur capacité de s'organiser, de mobiliser et d'agir. En Asie du Sud-Est, les groupes de discussion en ligne ont été si couramment infiltrés que les militants ont qualifié les conversations privées de « sphère semi-publique », l'infiltration étant considérée comme un moyen de faire cesser le débat − un « acte de perturbation »[96]. Des pratiques analogues sont signalées au Togo.

70. Parfois, l'infiltration est effectuée entièrement en ligne, souvent via une usurpation d'identité ou de coordonnées[97]. Plusieurs organisations africaines de la société civile ont soupçonné une complicité entre l'État et les entreprises, qui aurait permis la réattribution de numéros de téléphone portable et l'accès ultérieur à ceux-ci, et le clonage de cartes SIM, rendant possibles la surveillance et l'envoi de messages menaçants ou suspects[98]. Par exemple, des activistes kenyans ont fait état de l'utilisation de cartes SIM clonées pour l'envoi de messages destinés à semer la méfiance entre personnes proches ou à diriger des personnes vers des lieux où elles seraient victimes de harcèlement policier[99]. Les victimes de piratage informatique et d'usurpation d'identité décrivent des conséquences similaires à celles subies par les personnes touchées par des logiciels espions, notamment une ostracisation durable et l'impossibilité de maintenir les réseaux professionnels[100]. Les tactiques d'intimidation délibérées montrent que ceux qui exercent cette surveillance sont conscients des effets dissuasifs qu'elle entraîne et de leur effet dévastateur sur les personnes visées.

71. Certains services de forces de l'ordre, notamment en Argentine, au Bangladesh et en Thaïlande, ont recours à la cybersurveillance pour surveiller les médias sociaux et s'ingérer de manière arbitraire dans des rassemblements, y compris ceux qui se tiennent à titre privé.

E. Restrictions concernant la conservation et le partage d'informations

72. La crainte d'être surveillé entrave considérablement la circulation de l'information. Des militants originaires de zones de conflit ou de zones militarisées, telles que le Darfour (Soudan) et le Soudan du Sud, ont expliqué comment les fouilles, le harcèlement et les contrôles ciblés effectués à de nombreux postes de contrôle physiques avaient un effet dissuasif sur leur engagement et sur leur capacité de partager des informations[101].

[94] Contributions écrites de la société civile d'Afghanistan.

[95] Première consultation en Afrique ; Amy Stevens, Pete Fussey, Daragh Murray *et al.*, « 'I started seeing shadows everywhere' : the diverse chilling effects of surveillance in Zimbabwe » ; et deuxième consultation en Amérique latine.

[96] Première consultation en Asie du Sud-Est.

[97] Première consultation en Afrique.

[98] Ibid.

[99] Deuxième consultation en Afrique.

[100] Première consultation en Afrique ; et contribution écrite de la société civile du Pakistan.

[101] Première consultation en Afrique.

73. Au Soudan, en cas de transport physique de matériel, les appareils risquent d'être saisis, en particulier aux postes de contrôle, où les personnes sont souvent contraintes de les déverrouiller pour qu'ils soient inspectés. Les journalistes et les défenseurs des droits de l'homme seraient particulièrement visés[102].

74. Des militants tibétains ont expliqué comment les effets dissuasifs de la surveillance avaient ralenti la circulation de l'information au-delà des frontières nationales, et ainsi considérablement limité la capacité d'action des organisations de la société civile en exil et de la diaspora[103]. Dans des cas extrêmes, les effets dissuasifs de la surveillance les avaient poussés à se limiter aux outils de communication de base. Par exemple, des militants cessaient d'utiliser leur téléphone après leur arrestation[104], ou nombre d'entre eux bloquaient tous leurs contacts après la saisie d'un appareil mobile[105].

75. Ces restrictions de la capacité de communiquer, induites par des effets dissuasifs, ont des répercussions à long terme en ce qu'elles sapent la mémoire collective nécessaire à l'existence continue des organisations et mouvements.

76. Les solutions à forte intensité de main-d'œuvre − comme se déplacer pour assister à des réunions plutôt que de communiquer en ligne, ou recourir au transport physique plutôt qu'à l'envoi de données − entraînent une diminution du partage d'informations et une diminution de l'opportunité et de la pertinence des informations partagées[106]. Davantage d'efforts doivent aussi être consacrés à la reconstitution d'informations fragmentées, souvent au détriment de l'exactitude. Dans les zones de conflit telles que le Darfour, où l'information peut être une question de vie ou de mort et où, la vérifier revient à décider de mettre des personnes en danger, les organisations de la société civile ont expliqué que l'accès à l'information était complexe mais nécessaire pour écarter les personnes en situation de déplacement du danger, et que la diffusion de fragments d'informations pouvait entraîner des risques supplémentaires[107].

F. Visibilité réduite et effets

77. Une surveillance et une stigmatisation accrues ont des effets sur la visibilité publique des acteurs de la société civile, des associations, des rassemblements et des journalistes, et limitent directement leur capacité de se rencontrer, d'agir et de communiquer librement. De nombreux acteurs ont réduit leur présence sur les médias sociaux et en public, ce qui a eu des conséquences importantes sur leur capacité de communiquer et de mobiliser et leur accès aux ressources et, partant, sur leur impact et la réalisation de leurs objectifs[108]. Des représentants de la société civile d'Amérique latine et d'Afrique l'ont bien formulé : « Qui va financer une organisation qui n'est pas visible ? »[109]. En Tunisie, des acteurs de la société civile ont parlé de la « nécessité d'agir plus discrètement », faisant état de difficultés similaires pour accéder aux financements. Ces effets dissuasifs ont un double inconvénient : d'une part, ils réduisent l'utilité des outils numériques et l'espace civique, et d'autre part, ils font naître le sentiment qu'il faut s'autocensurer pour éviter la criminalisation : « La visibilité pose un risque énorme. Nous communiquons moins ouvertement, davantage dans l'ombre. »[110].

[102] Ibid.
[103] Troisième consultation en Asie du Sud-Est.
[104] Première consultation en Afrique ; et contribution écrite de la société civile d'Afghanistan.
[105] Premier entretien.
[106] Deuxième et troisième consultations en Amérique latine.
[107] Première consultation en Afrique.
[108] Contributions écrites de la société civile provenant d'Argentine, d'Inde, d'Indonésie, d'Italie, du Myanmar, d'Espagne, d'Ouganda, de la République-Unie de Tanzanie, des États-Unis et du Venezuela (République bolivarienne du).
[109] Troisième consultation en Amérique latine ; et deuxième consultation en Afrique.
[110] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord.

78. Au Kenya et au Venezuela (République bolivarienne du), certaines organisations se sont senties contraintes de déménager à plusieurs reprises afin de s'éloigner le plus possible de l'attention des pouvoirs publics, ce qui a aussi accru leur éloignement de leurs réseaux professionnels[111].

79. De nombreuses organisations ont supprimé leurs profils publics et se sont retirées des médias sociaux. Au Venezuela, certaines, face au harcèlement du Gouvernement, ont supprimé leur propre site Web et leurs propres archives en ligne, une mesure d'autoprotection qui cause la perte de la mémoire institutionnelle du secteur[112]. En Argentine, de nombreux collaborateurs d'organisations non gouvernementales de défense des droits de l'homme ont choisi de garder secrète leur action en la matière[113]. Les suppressions forcées de comptes de médias sociaux, qui entraînent parfois la perte de centaines de milliers d'abonnés acquis sur des années, ne sont pas rares[114].

G. Conséquences sur les ressources et les activités

80. Les effets dissuasifs de la surveillance numérique entraînent une diminution des ressources financières, et donc des capacités d'action, des organisations de la société civile. Dans ce secteur en proie à des difficultés financières[115], le fait de réaffecter des ressources pour atténuer la menace et les effets de la surveillance limite nécessairement la capacité des individus, des mouvements et des organisations (y compris les donateurs) à poursuivre librement leurs objectifs stratégiques.

81. Les propos qui suivent décrivent des expériences couramment vécues : « L'effet dissuasif a des répercussions […] sur toutes les mesures de protection. Beaucoup d'efforts, de temps, de ressources et d'argent sont nécessaires. »[116]. « Ce niveau de surveillance n'est pas normal… Il a influencé notre façon de travailler, tant sur le plan stratégique qu'opérationnel. Beaucoup de ressources, de temps et d'énergie sont consacrés à l'atténuation des effets de la surveillance. »[117].

82. La nécessaire mise en place d'autres moyens de transfert de fonds et de formes clandestines de paiement du personnel sous surveillance, qui permettent de rester discret et moins vulnérable, constitue une autre incidence financière directe[118].

83. Il faut souvent employer des moyens de transport et des arrangements logistiques plus coûteux pour instaurer un climat de confiance et échapper à la surveillance[119]. Un militant pour les droits des peuples autochtones a fait remarquer qu'en Amazonie, « en raison de la politique de la peur, 50 % de notre budget doit aujourd'hui être consacré à la mobilisation ; nous devons voyager pour convaincre les gens que c'est sans danger »[120].

84. Cette réallocation problématique des ressources aux fins d'une atténuation des vulnérabilités à la surveillance numérique, qui entrave considérablement la capacité d'agir pour atteindre les objectifs stratégiques, a été signalée dans toutes les régions. Au niveau organisationnel, le renforcement de la sécurité face à la surveillance numérique suppose un investissement stratégique majeur[121]. Ce détournement de fonds nécessite des efforts supplémentaires pour justifier ce changement de priorités auprès des donateurs.

[111] Troisième consultation en Amérique latine ; et deuxième consultation en Afrique.
[112] Troisième consultation en Amérique latine.
[113] Deuxième consultation en Amérique latine (Argentine).
[114] Premier entretien.
[115] Voir A/80/219.
[116] Troisième consultation en Asie du Sud-Est.
[117] Sixième entretien.
[118] Deuxième consultation en Amérique latine.
[119] Quatrième entretien.
[120] Première consultation en Amérique latine (Brésil).
[121] Quatrième entretien.

85. Il faut également puiser dans les ressources organisationnelles pour réagir à une attaque par un logiciel espion. Il faut minutieusement recenser les réseaux et les contacts des victimes afin de découvrir les « dommages collatéraux de la surveillance »[122] liés à ces attaques, notamment en identifiant précisément qui pourrait courir un risque du fait de ces piratages[123].

86. Des acteurs de la société civile en Afrique et en Asie du Sud-Est ont fait remarquer que la taille d'une organisation déterminait sa capacité d'investir dans des mesures de sécurité numérique, et que les groupes locaux et de petite taille faisaient face aux choix les plus difficiles et à la plus grande vulnérabilité[124], un état de fait aggravé par l'évolution de l'écosystème financier, notamment la suppression des financements accordés par le Gouvernement des États-Unis[125].

87. Toutes les organisations de la société civile ne sont donc pas égales en ce qui concerne la sécurité numérique. Par exemple, des organisations isolées et de petite taille sont souvent plus exposées et doivent consacrer une part plus importante de leur budget à cette activité que les grandes organisations internationales de la société civile[126].

H. Conséquences des effets dissuasifs sur l'individu

88. Les effets dissuasifs générés par la surveillance, qui touchent à la liberté d'association et de réunion, touchent aussi profondément les personnes. Ils touchent de plusieurs façons, souvent déterminantes, les aspects les plus intimes de la vie. Au-delà des conséquences économiques, culturelles et sociales, ils influencent la capacité des personnes de s'intégrer dans la société et d'accéder aux services essentiels.

89. De nombreux acteurs de la société civile ont expliqué comment la conviction d'être surveillé sapait la confiance entre les personnes et les relations sociales[127]. La méfiance, l'isolement et la rupture des liens sociaux engendrent un stress psychologique profond qui affecte « tous les aspects de la vie d'un militant ». Une telle intrusion « transforme fondamentalement la vie des militants : chaque conversation devient suspecte, chaque relation est potentiellement compromise et chaque moment d'intimité est soumis à une surveillance inconnue »[128].

1. Psychologie individuelle et hypervigilance

90. Les personnes consultées ont communément décrit un état d'hypervigilance constante face à une surveillance présumée. La résilience et la capacité de maintenir un engagement à long terme en sont considérablement affaiblies.

91. De nombreux participants avaient de sérieuses raisons d'être en état d'alerte. Au Soudan du Sud, des militants pensent que la surveillance biométrique a permis d'identifier et d'assassiner des personnes ayant participé à des manifestations[129]. En Éthiopie, une hypervigilance a succédé à des actes d'intimidation directs, notamment des cambriolages survenus à l'arrivée dans des refuges tenus secrets[130]. Le poids psychologique lié au fait d'être physiquement suivi, aggravé par la surveillance numérique, est un ressenti qui a été rapporté

[122] Daragh Murray et Pete Fussey, « Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data », *Israel Law Review*, vol. 52, nº 1 (2019).
[123] Troisième consultation en Asie du Sud-Est.
[124] Deuxième consultation en Asie du Sud-Est.
[125] Première consultation en Afrique.
[126] Quatrième entretien.
[127] Contributions écrites de la société civile provenant de Thaïlande, d'Ouganda et des États-Unis. Ce constat concorde avec les travaux universitaires consacrés à l'impact des effets dissuasifs de la surveillance sur la confiance entre personnes : voir Amy Stevens, Pete Fussey, Daragh Murray et al., « "I started seeing shadows everywhere": the diverse chilling effects of surveillance in Zimbabwe ».
[128] Contribution écrite de la société civile du Pakistan.
[129] Première consultation en Afrique.
[130] Douzième et quatorzième entretiens.

dans toutes les régions du monde. Le niveau de vigilance augmente également lorsque des pressions sont exercées pour qu'extérieurement l'on se comporte « normalement ».

92. De nombreux militants avaient le sentiment que la surveillance était constante et omniprésente : « Tout le monde a l'impression d'être surveillé, d'être suivi. »[131].

93. L'hypervigilance envahissante constante est un phénomène courant dans l'état d'esprit des militants. Les témoignages suivants sont représentatifs : « Je suis devenu un peu paranoïaque, mais je pense que c'est une bonne paranoïa. »[132] ou « C'était très bizarre… Je ne suis pas paranoïaque, mais j'avais juste ce sentiment très fort que quelque chose n'allait pas. »[133], et montrent que certains en viennent à douter de leur propre santé mentale : « Vous êtes toujours à vous demander si vous êtes seul ou non… Est-ce juste de la paranoïa ? »[134]. Un militant éthiopien a expliqué comment cette hypervigilance s'était transformée en un état d'anxiété chronique : « Je ne peux pas sortir en public … parce qu'on est tout le temps paranoïaque, surtout quand on a des enfants … on est toujours paranoïaque. »[135]. D'autres ont évoqué l'absence de répit à la maison : « J'essaie de les maîtriser dans une certaine mesure, mais ces pensées envahissantes, ces sentiments négatifs, vous savez, cette peur que quelque chose pourrait arriver, sont toujours là, donc c'est difficile à gérer. »[136].

94. Plusieurs raisons expliquent le caractère persistant de l'hypervigilance, notamment la conviction que vous serez surveillé, quelles que soient les mesures que vous prenez pour y échapper. Commentant l'essor rapide de la technologie de reconnaissance faciale au Brésil, des participants ont fait observer que « São Paulo était une ville marquée par l'angoisse et l'hypervigilance »[137]. On a le sentiment que la surveillance est omniprésente et que l'on ne peut s'y soustraire, et l'on ne sait jamais vraiment si l'on est visé. C'est particulièrement vrai dans les réseaux dont certains membres ont été victimes de logiciels espions : « Ça vous fait remettre en question tout ce que vous faites. »[138].

2. Santé et santé mentale

95. Les effets de la surveillance permanente sur la santé mentale sont largement documentés en psychologie, en épidémiologie et dans d'autres domaines de la médecine[139]. Si nombre de ces études portent sur l'impact des formes visibles et manifestes de surveillance, comme une présence policière excessive, l'ère des technologies numériques et le développement d'outils intrusifs à peine perceptibles de surveillance à distance augmentent les effets de la surveillance sur la santé mentale.

96. L'épuisement mental et le burnout ont été systématiquement constatés dans toutes les régions étudiées, comme en témoignent les témoignages des militants eux-mêmes et les observations des professionnels des services de santé mentale. Une organisation a dit que plus de 60 % des militants souffraient de dépression, de burnout et d'autres problèmes, ajoutant que « bien sûr, d'autres facteurs contribuent également à ces problèmes de santé mentale, mais la répression est un facteur majeur »[140]. De nombreux autres facteurs auxquels la société civile est régulièrement confrontée influencent aussi la santé mentale, notamment le fait d'être constamment visé, « jour après jour, par des campagnes de diffamation. Le fait d'être surveillé 24 heures sur 24, en ligne comme hors ligne, vous épuise sur le plan mental, physique et social », et de nombreuses personnes ont abandonné le militantisme[141].

[131] Cinquième entretien.
[132] Premier entretien.
[133] Huitième entretien.
[134] Quatrième entretien.
[135] Quatorzième entretien.
[136] Deuxième entretien.
[137] Première consultation en Amérique latine.
[138] Deuxième entretien.
[139] Voir https://shorturl.at/25MEV.
[140] Première consultation en Asie du Sud-Est.
[141] Ibid. ; et quatrième entretien.

97. Presque tous les militants de la région du Moyen-Orient et de l'Afrique du Nord ont évoqué un épuisement psychologique et émotionnel[142], systématiquement associé à un sentiment de défaite face à la surveillance autoritaire[143]. Une victime de logiciels espions a décrit « un sentiment de perte totale, d'impuissance »[144], tandis que des militants en Afghanistan ont expliqué que « l'on ne saurait trop insister sur le sentiment de désespoir que la surveillance en ligne […] avait engendré. Elle avait vraiment un effet dissuasif »[145].

98. D'autres ont décrit une incapacité de trouver refuge[146], le sentiment qu'aucun endroit n'est sûr, car les effets dissuasifs envahissent les sphères les plus intimes de la vie[147]. Des remarques spontanées peuvent donner lieu à des heures de remise en question[148]. Dans ce cas, les effets dissuasifs vont au-delà de l'autocensure ; ils entraînent un stress permanent dû à une remise en question de soi-même[149].

99. De nombreuses techniques sophistiquées de surveillance ont des effets psychologiques arbitraires de grande ampleur et accentuent aussi des vulnérabilités intersectionnelles. Par exemple, du fait de l'état d'urgence constitutionnel en vigueur en Araucanie (Chili), les communautés mapuche sont soumises à une surveillance intensive depuis 2021. La surveillance constante exercée par des aéronefs avec ou sans pilote a entraîné une augmentation alarmante « des cas d'anxiété, d'insomnie, de dépression et de stress post-traumatique » chez les membres de la communauté, en particulier les enfants[150]. On a recensé des cas d'enfants perdant leur concentration, manifestant de l'anxiété et cherchant à se réfugier à l'intérieur dès qu'ils entendent un drone, des comportements similaires à ceux observés chez des écoliers dans les zones des favelas brésiliennes soumises à une surveillance aérienne[151].

100. Le fait d'être surveillé est souvent décrit comme un véritable traumatisme grave[152], et chez de nombreuses personnes concernées, un diagnostic médical de troubles liés à un traumatisme est posé[153]. Nombre d'entre elles consacrent une part importante de leurs revenus à atténuer ces effets dans le cadre d'une thérapie[154]. Le phénomène est si répandu que les thérapies spécialement élaborées pour soigner ces troubles constituent désormais un domaine à part entière en pleine expansion[155].

101. Partout dans le monde, les manifestants jeunes ont difficilement accès à la justice en cas de violation de leurs droits, ce qui renforce un traumatisme déjà grave. La surveillance omniprésente exploite encore ce stress, afin qu'ils abandonnent leur soutien aux victimes et leur quête légitime en faveur de l'établissement des responsabilités.

VIII. Effets dissuasifs et écosystème de surveillance

102. Pour les personnes faisant l'objet d'une surveillance, les mesures de surveillance ne sont pas des actions ponctuelles isolées. Par exemple, l'utilisation de la reconnaissance faciale lors de rassemblements, les logiciels espions ciblant des militants, les caméras de surveillance publiques, le déploiement de systèmes de reconnaissance automatique des plaques d'immatriculation, la présence policière aux abords d'un événement, l'infiltration de groupes WhatsApp, etc., ne sont pas considérés comme des faits isolés, même s'ils visent des

[142] Consultation dans la région du Moyen-Orient et de l'Afrique du Nord.
[143] Quatrième entretien.
[144] Quatrième et treizième entretiens.
[145] Contribution écrite de la société civile d'Afghanistan.
[146] Première consultation en Asie du Sud-Est ; et consultation dans la région du Moyen-Orient et de l'Afrique du Nord.
[147] Quatrième consultation en Asie du Sud-Est.
[148] Première consultation en Afrique.
[149] Onzième entretien.
[150] Voir A/HRC/62/45/Add.1.
[151] Deuxième consultation en Amérique latine.
[152] Troisième consultation en Amérique latine.
[153] Premier entretien ; et troisième consultation en Amérique latine.
[154] Première consultation en Afrique.
[155] Treizième entretien.

groupes différents. Au contraire, ils forment un écosystème de surveillance. Les incertitudes quant aux liens entre acteurs étatiques et non étatiques, en particulier en ce qui concerne le partage des données, aggravent encore les conséquences liées à l'environnement de surveillance interconnecté.

103. Les activités de surveillance, même si elles sont discrètes, s'inscrivent dans un continuum et dans la durée, et laissent des traces profondes et durables sur l'ensemble de la société. Elles détruisent la confiance indispensable dans les institutions démocratiques, dont la gouvernance et la police de proximité − pour lesquelles cette confiance est essentielle − et renforcent les effets dissuasifs. Ces traces liées à l'écosystème sont déterminantes du ressenti plus ou moins marqué des effets dissuasifs chez différents individus et groupes. Elles sont plus prononcées pour les communautés marginalisées et vulnérables, et pour celles qui mènent des activités sociopolitiques remettant en cause le statu quo.

104. Ce constat remet en question l'analyse traditionnelle du droit des droits de l'homme, car les effets dissuasifs liés à l'existence d'un écosystème ne sont pas des préjudices classiques de type « cause et effet », dans lesquels un incident précis entraîne un préjudice bien défini. Si l'on ne s'attaque pas à l'écosystème de surveillance, ses effets sur l'espace civique au sens large seront ignorés ou sous-estimés, ce qui faussera l'analyse du critère de « nécessité dans une société démocratique » lorsque les restrictions seront évaluées. Un biais favorable aux activités et outils de surveillance préjudiciables en résultera, qui ne fera qu'aggraver davantage les effets dissuasifs.

IX. Préjudice cumulé

105. Les effets dissuasifs portent atteinte au droit à la vie privée *et* au droit à la liberté d'expression *et* au droit à la liberté de réunion pacifique *et* au droit à la liberté d'association *et* au droit à la non-discrimination *et* à d'autres droits connexes[156]. Ils portent atteinte simultanément à ces droits et entravent l'exercice de ces droits interdépendants et interconnectés. En ce sens, ils causent un préjudice cumulé aux droits de l'homme. À ce jour, les effets dissuasifs ne sont pas pris en compte[157], ou sont examinés de manière restrictive, droit par droit ; par exemple, les effets sur la liberté d'expression sont examinés indépendamment des effets sur d'autres droits[158].

106. Il est important de noter que la notion de préjudice multiple ne se limite pas à un préjudice simultané à plusieurs droits de l'homme. En portant atteinte au caractère interconnecté et interdépendant des droits concernés, le préjudice lui-même est amplifié et intensifié. Par exemple, ensemble, la liberté de réunion pacifique, la liberté d'association, la liberté d'expression et le droit à la vie privée protègent le développement de l'identité des individus ainsi que le bon fonctionnement de la société démocratique[159]. De ce fait, les effets dissuasifs ne portent pas seulement atteinte aux droits sous-jacents, mais aussi à la capacité des individus et des collectivités de développer et d'exprimer librement leur identité et de participer à la vie sociale, culturelle et politique. L'ampleur du préjudice est d'autant plus grave qu'il faut tenir compte du « rôle catalyseur » que jouent la liberté de réunion pacifique et la liberté d'association. Les effets dissuasifs compromettent donc la capacité même de promouvoir et de défendre les droits. Le préjudice cumulé s'entend de ce préjudice global découlant des effets dissuasifs de la surveillance.

107. Ces préjudices cumulés doivent être pris en compte dans toute étude d'impact en matière de diligence raisonnable et de droits de l'homme.

[156] Voir https://committees.parliament.uk/writtenevidence/148179/pdf.

[157] Cour européenne des droits de l'homme, *Glukhin c. Russie*, requête nº 11519/20, arrêt du 4 juillet 2023, par. 88.

[158] Cour européenne des droits de l'homme, *Catt c. Royaume-Uni*, requête nº 43514/15, arrêt du 24 avril 2019, par. 123.

[159] Ronit Matar et Daragh Murray, « Rethinking international human rights law's approach to identity in light of surveillance and AI », *Human Rights Law Review*, vol. 25, nº 3 (juin 2025).

X. Conclusion

108. **Dans le présent rapport, la Rapporteuse spéciale met en lumière les effets dissuasifs complexes et multiformes de la surveillance numérique, démontrant que ces effets existent bel et bien et sont communément ressentis, quel que soit le pays ou le contexte. Les effets dissuasifs ont des conséquences sociopolitiques profondes et entravent directement la capacité des individus, des groupes, des associations et des rassemblements à exercer effectivement leurs libertés fondamentales, à agir sur le plan politique et à participer à la vie publique. La surveillance omniprésente aggrave les effets dissuasifs de la stigmatisation et de la criminalisation.**

109. **Les effets dissuasifs ont des conséquences concrètes sur la vie quotidienne des personnes directement ou indirectement concernées. Lorsque les espaces publics se vident ou que les actions sont « édulcorées » pour des raisons de sécurité, lorsque les mots disparaissent des campagnes de plaidoyer, des rapports et des projets des donateurs, lorsque le travail en faveur des droits humains est requalifié d'« aide », lorsque des ressources sont consacrées à la sécurité numérique plutôt qu'au plaidoyer − tout cela pour échapper à la surveillance et aux répercussions qui pourraient en découler −, les conséquences sont graves. Ces éléments sapent la résilience et la possibilité de s'engager durablement civiquement et politiquement. La banalisation de la surveillance conduit à des violations institutionnelles des libertés fondamentales. En réalité, elle freine l'activisme et la participation démocratique inclusive.**

110. **La gravité et le caractère systématique des effets dissuasifs mis en évidence, qui sont amplifiés par des techniques de surveillance facilitées par le numérique et alimentées par l'intelligence artificielle, constituent un signal d'alarme qui appelle de toute urgence à une action mondiale concertée. Il n'est plus permis d'ignorer les conséquences sur l'espace civique des effets dissuasifs découlant de ces techniques de surveillance. Les États ont la responsabilité d'assurer la sécurité nationale et la sécurité publique, mais ils doivent le faire en protégeant et en favorisant les libertés fondamentales. De ce fait, les effets dissuasifs et les préjudices qu'ils représentent pour les droits à la liberté de réunion pacifique et à la liberté d'association doivent devenir un élément central des analyses en matière de droits de l'homme, des procédures judiciaires, du droit et de l'élaboration des politiques. Ils doivent aussi être pris en compte dans la conception, le déploiement et la commercialisation d'outils numériques.**

111. **La sécurité ainsi que la prévention et l'atténuation des effets dissuasifs doivent être intégrées dès la conception afin de prévenir toute utilisation abusive ou détournée visant à restreindre ou à museler la participation démocratique, le contrôle public et l'activisme politique. Une participation citoyenne sans entrave, tant en ligne que hors ligne, est vitale pour le développement démocratique et une participation inclusive, dans lesquels tous les membres de la société sont valorisés, y compris les enfants.**

XI. Recommandations

112. **Les États, les Nations Unies et toutes les parties prenantes devraient veiller à la mise en place d'un environnement propice au respect des droits et protéger l'espace civique contre les effets dissuasifs. Ils devraient :**

a) S'abstenir de stigmatiser et de criminaliser l'activisme civique légitime et d'utiliser la surveillance et les technologies numériques pour réprimer la dissidence politique et les actions de la société civile. L'utilisation des technologies numériques à ces fins doit être interdite ;

b) Protéger l'espace civique par la promotion et la protection d'un chiffrement fort, notamment l'intégrité du chiffrement de bout en bout, et s'abstenir de criminaliser les mesures légitimes destinées à préserver l'anonymat ;

c) Veiller à la mise en place d'un cadre juridique respectueux des droits de l'homme pour réglementer toutes les activités de surveillance facilitées par les technologies numériques, conformément aux principes de légalité, de nécessité, de

proportionnalité et de non-discrimination. Les effets dissuasifs devraient être pris en compte dans l'analyse de la nécessité. Toute exception, y compris celles liées à la sécurité nationale, doit être interprétée de manière restrictive et strictement limitée. Compte tenu du rythme de l'évolution technologique, toute législation devrait restreindre les pouvoirs de surveillance plutôt que de les autoriser, et devrait faire l'objet d'un réexamen régulier. La vente, le transfert et le courtage d'outils de surveillance numérique, et l'assistance technique qui s'y rapporte, devraient être soumis à un cadre juridique similaire ;

d) Veiller à ce que les mesures de surveillance, y compris celles qui sont fondées sur des outils numériques et l'intelligence artificielle, soient assorties de garanties solides en matière de droits de l'homme, en exigeant que toute mesure de surveillance soit strictement limitée dans le temps et subordonnée à une autorisation judiciaire préalable obligatoire et à un contrôle indépendant et efficace et comprenne une possibilité de recours ;

e) Imposer obligatoirement la réalisation d'études d'impact en matière de diligence raisonnable et de droits de l'homme pour toutes les activités de surveillance numérique. Ces études doivent être fondées sur des données factuelles, tenir compte des effets dissuasifs potentiels et analyser les préjudices cumulés, compte tenu de l'importance des éléments intersectionnels. La diligence raisonnable doit nécessairement être un processus continu ;

f) Mettre en place un processus de diligence raisonnable distinct et institutionnalisé, axé sur l'évaluation de l'écosystème de surveillance. Évaluer régulièrement la « nécessité » de l'ensemble des activités de surveillance menées par l'État, en tenant compte des divers risques et impacts intersectionnels et cumulés. Ce processus doit être obligatoire, en particulier avant le déploiement de nouvelles technologies de surveillance, lorsque le contexte évolue et avant des échéances démocratiques (telles que les élections) ;

g) Veiller à ce qu'un contrôle humain soit effectué et que les responsabilités puissent être établies ;

i) Veiller à la transparence et à une large consultation inclusive concernant l'acquisition, le transfert et le déploiement de systèmes de surveillance, y compris les collaborations avec des entreprises ;

ii) Établir un mécanisme de contrôle indépendant, efficace et doté des ressources nécessaires, habilité à contrôler les systèmes de surveillance, leur ingérence dans les droits et libertés et leurs effets dissuasifs intersectionnels, à enquêter sur les plaintes et à suspendre ou sanctionner les acteurs étatiques ou non étatiques en cas de non-respect ;

iii) Veiller à ce que les forces de l'ordre et le système judiciaire soient en mesure d'enquêter et de poursuivre tous les responsables, à tous les niveaux de la prise de décisions, en cas de surveillance illégale, y compris lorsqu'elle est liée à des violations de la liberté de réunion pacifique et de la liberté d'association, et aux effets dissuasifs connexes ;

iv) Mettre en place des mécanismes de plainte et de recours spécifiques, centrés sur les victimes et leurs besoins, permettant à toute personne, y compris les enfants et les groupes marginalisés, de signaler en toute sécurité des abus en matière de surveillance, et d'obtenir et contester les informations détenues à son sujet, y compris par des acteurs non étatiques ;

v) Prévoir des mesures correctives appropriées, en tenant compte des préjudices intersectionnels, y compris la destruction des données collectées illégalement ;

h) Veiller à l'élaboration de politiques tenant compte des questions de genre et de l'intersectionnalité, en tenant compte des effets différenciés de la surveillance numérique et des technologies numériques. Il conviendra d'accorder une attention particulière à l'utilisation abusive des données à caractère personnel, y compris celles

relatives à la santé reproductive, et à la violence fondée sur le genre qui s'exerce en ligne ;

i) Interdire formellement ce qui suit :

i) L'utilisation et le transfert d'outils numériques intrusifs qui ne respectent pas les garanties en matière de droits de l'homme, notamment les logiciels espions hautement intrusifs (dont les fonctionnalités ne peuvent être limitées ou dont l'utilisation ne peut faire l'objet d'un contrôle indépendant) ;

ii) La surveillance arbitraire, aveugle et de masse à des fins répressives, y compris les applications biométriques et d'intelligence artificielle, telles que la technologie de reconnaissance faciale, les systèmes d'intelligence artificielle qui créent ou enrichissent des bases de données de reconnaissance faciale par la collecte non ciblée d'images faciales sur Internet ou à partir d'enregistrements de vidéosurveillance, et les systèmes d'intelligence artificielle destinés à l'évaluation sociale ;

iii) L'utilisation de technologies de surveillance et de collecte de données à des fins prédictives et de profilage arbitraires et discriminatoires, y compris dans le cadre de la prévision policière, et à des fins non justifiées ;

iv) L'utilisation de technologies et de techniques de surveillance militarisées à des fins de maintien de l'ordre, spécialement dans le cadre de l'exercice des droits à la liberté de réunion pacifique et d'association, et l'utilisation de données concernant l'activisme civil à des fins militaires ;

v) Le transfert et l'utilisation de technologies et de produits facilitant la commission de violations graves des droits de l'homme, y compris lorsqu'il existe un risque qu'ils soient utilisés à de telles fins ;

vi) L'emploi de la surveillance numérique dans les établissements scolaires et sur les lieux de travail ;

vii) D'une manière générale, les technologies présentant un potentiel coercitif plus élevé, y compris celles pouvant être utilisées à des fins militaires, doivent être soumises à des critères d'autorisation et d'utilisation plus stricts afin d'éviter des préjudices cumulés.

113. **Les Nations Unies et la communauté internationale devraient :**

a) Adopter des normes juridiques contraignantes et des mécanismes de gouvernance mondiale axés sur les droits de l'homme et chargés de régir les technologies de surveillance numérique et l'intelligence artificielle, en tenant compte des effets dissuasifs potentiels ;

b) Veiller à ce que les cadres mondiaux de prévention de la criminalité, y compris en matière de lutte contre le terrorisme et la cybercriminalité, n'aient pas d'effet dissuasif sur l'exercice des libertés publiques. Traiter d'urgence ces questions dans le cadre de l'actualisation en cours du cadre des Nations Unies chargé de la lutte contre le terrorisme ;

c) Soutenir la création d'une commission mondiale pour la vérité et la justice chargée d'examiner les conséquences systémiques et généralisées de la surveillance numérique, y compris ses effets dissuasifs intersectionnels ;

d) Interdire la vente, le transfert et l'utilisation de technologies commerciales facilitant la surveillance illégale et des restrictions graves et injustifiées des libertés publiques, et sanctionner efficacement les violations ;

e) Tenir les entreprises responsables des violations des droits de l'homme découlant du transfert et de l'utilisation de leurs produits, y compris des effets dissuasifs.

114. **Le secteur privé (développeurs, médias sociaux, prestataires de services, plateformes numériques, opérateurs de télécommunications et autres acteurs impliqués dans la surveillance, y compris les géants de la tech) doit strictement faire preuve de**

diligence raisonnable en matière de droits de l'homme tout au long du cycle de vie des technologies de surveillance. Aux fins de l'évaluation de la diligence raisonnable, il convient de tenir compte des effets dissuasifs et d'associer véritablement divers acteurs de la société civile. Les entreprises devraient :

a) Veiller à ce que la conception inclusive et les fonctionnalités numériques ne permettent pas une surveillance illégale (notamment disproportionnée, aveugle et discriminatoire) ;

b) Refuser de se plier aux demandes de l'État aux fins de l'obtention des données de surveillance, sauf en cas de décision judiciaire, et publier régulièrement des rapports de transparence détaillés rendant compte des demandes des autorités ;

c) Veiller à ce que les contrats conclus avec des États prévoient des obligations claires en matière de droits de l'homme, des droits de contrôle et des procédures de diligence raisonnable ;

d) S'abstenir de vendre des technologies de surveillance lorsqu'il existe un risque qu'elles aient des conséquences négatives sur les droits de l'homme.

115. **Les donateurs devraient apporter un soutien financier durable aux militants et aux associations afin de renforcer la sécurité, d'atténuer les effets de la surveillance et de lutter contre celle-ci au moyen de procédures judiciaires, d'un soutien psychosocial, de signalements établis par la communauté et d'un renforcement des capacités en matière de défense juridique.**

Annex I

I. Key activities conducted from 1 January 2025 to 31 May 2026

1. The period from 2025 through the first quarter of 2026 has been a pivotal era for the defence of the freedoms of association and peaceful assembly. Throughout this timeframe, the mandate faced significant global challenges, yet also witnessed important advances fuelled by the tireless action of civil society, social movements, community leaders, and international actors.

2. The Special Rapporteur expresses her sincere gratitude to : i) her supporting staff at the OHCHR ; ii) her external advisors, specially Sonya Merkova, Felipe Caicedo and Luz Avendaño ; iii) interns from the Master of Advanced Studies International Humanitarian Law and Human Rights, at the Geneva Academy ; iv) all the volunteers that have supported her mandate extensively ; v) Prof. Pete Fussey and Dr. Daragh Murray, for their generosity and wisdom ; vi) and all the other individuals, associations, including pro-bono groups, governments, international bodies and donors, among others, that have engaged with the mandate.

3. The Special Rapporteur shares a warm recognition in solidarity with : i) all civil society colleagues and friends who have experienced one of the toughest years on record, due to the deadly combination of funding cuts, a shifting financial landscape, the accelerated closing of civic space worldwide, a deep crisis in multilateralism, and the rise of conflicts, wars and genocides ; and to ii) the victims of the violations of the right to freedom of peaceful assembly and of association worldwide, especially the youth that have been at the forefront of the defence of human dignity. For their courage, these two groups have been stigmatized, vilified, harassed, surveyed, detained, punished, harmed and even killed. My heart is with you, and my actions are for you.

4. The Special Rapporteur also wishes to acknowledge most of her fellow Special Procedures mandate holders, who even in the mist of reforms (including the disappearance of the Special Procedures Branch at the OHCHR), defunding, a lack of appropriate support, and constant attacks, remain deeply committed to advancing their mandates and protecting human rights. A special acknowledgment to Francesca Albanese, Special Rapporteur on the Occupied Palestinian Territories, who has been subjected to the most outrageous attacks and profound lack of protection from the organization and member States, despite her privileges and immunities.

5. The Special Rapporteur also expresses her appreciation to those Member States that supported the mandate – including its core group – and those that have actively engaged with and provided information in response to requests. She highlights that a global debate is most fruitful when all parties participate actively. For this new cycle, she expresses her hope that all governments will increase their commitments to human rights by transforming words into real actions, including the genuine protection of multilateralism. In a world that is losing its strongest advocates for human rights, we need new leadership – one deeply rooted in respect for human dignity and our shared human values.

6. The Special Rapporteur also expresses her appreciation to Switzerland for the provision of a Junior Professional Officer to support the mandate ; and reiterates that greater contributions are required from member States to fulfil the objectives of her mandate.

II. On-the-ground activities and country visits

7. During this reporting period, the Special Rapporteur emphasized face-to-face connections and the prioritization of local realities in her actions. She conducted a total of 249 engagements, meeting with more than 1,753 people in person out of approximately 3,503 people reached across both physical and digital spaces.

8. The Rapporteur's mobility was central to the mandate's effectiveness, spending more than 100 days on the road across 17 different countries and 19 cities. These visits encompassed 1 official visit (to Chile), as well as 2 travels to present reports (New York and Geneva) and to 17 different countries to attend meetings and events organised by civil society organizations or within educational and research environments.

9. A significant focus of these engagements remained on victims and civil society, who constituted 73% of all interactions. Through over 100 dedicated meetings, the Rapporteur engaged with over 2,200 individuals from these groups to ensure their voices remained the primary focus of the mandate's work. These efforts were balanced with over 80 high-level meetings with government representatives and international organizations to share information, advocate for legislative and policy reforms, and to ask for accountability, justice and reparation.

III. Reports

10. The Special Rapporteur presented two thematic reports : one to the Human Rights Council addressing the lessons learned from the "super election" cycle and the resulting impact on civic space (A/HRC/59/44), and one to the General Assembly focused on the existential threats currently facing the rights to freedom of peaceful assembly and of association and the critical role of human solidarity in the current global context (A/80/219).

IV. Communications

11. Between 1 January 2025 and 31 March 2026, the Special Rapporteur joined or led over 300 communications. In terms of regional distribution, Asia accounted for the largest share with 73 communications. Africa and the Americas followed with a similar volume of 51 and 45 communications, respectively. Europe accounted for 35 communications, while Oceania recorded the lowest number with 2 communications. The Special Rapporteur led 37 of these communications. These interventions were primarily driven by a systematic pattern of repression against peaceful protesters, civil society activists, and human rights defenders. Key reasons for these communications included the excessive and disproportionate use of force by security forces, frequently leading to extrajudicial killings, widespread injuries, and the detention of peaceful demonstrators. A persistent pattern of arbitrary arrests and detentions used to criminalize dissent, which in some instances resulted in enforced disappearances. Finally, the implementation of restrictive laws and police and officials actions, such as internet shutdowns, the acquisition and deployment of "less lethal weapons" for crowd control or of surveillance tools and strategies, used to curtail the rights to assembly and expression.

12. The Special Rapporteur also sent letters to around 15 other stakeholders including universities, social media and tech companies.

13. The Special Rapporteur issued two special statements : i) Civic space must be protected and expanded in anti-corruption efforts : Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism[160], and ii) Streets must be spaces of freedom, not of fear : A call to protect women's right to protest this March 8th[161].

14. The Special Rapporteur published four newsletters with information of her action : May 2024 and January 2025–February–Apr 2025–May–July 2025–August–October 2025 – 2025 summary.

[160] United Nations, "Joint statement by a group of Special Procedures mandate holders :* Civic space must be protected and expanded in anti-corruption efforts : Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism" (22 August 2025), available at www.ohchr.org/sites/default/files/statements/20250822-stm-uncac-cop-sr-assembly.pdf.

[161] See https://us10.campaign-archive.com/?u=92a2c63767a801e0d97cf1568&id=a46cb60268.

V. Technical assistance and cooperations

15. The Special Rapporteur has been providing ongoing technical assistance to different actors involved in the mutual evaluations and other activities held in relation with the Financial Action Task Force (FATF). This collaboration, that includes governments and civil society, aims to ensure that the country recommendations provided by the Task Force are fully aligned with international human rights standards and do not inadvertently jeopardize citizens' rights to freedom of peaceful assembly and of association.

16. The Special Rapporteur provided comments in the following processes :

a) Corte Interamericana de Derechos Humanos, Caso Ramos Durand y otros vs. Perú. – May 2025 ;

b) Comisión Interamericana de Derechos Humanos, Peritaje caso Diego Lamagna y familia, Marcelo Gastón Riva y familia vs Argentina ;

c) United Kingdom of Great Britain and Northern Ireland Parliament's inquiry on Human rights and the regulation of AI.

17. The special Rapporteur coordinated different actions with regional bodies such as :

a) Joint declaration about the prolonged detention of human rights defenders with the UN Special Rapporteur on the situation of human rights defenders ; the UN Special Rapporteur on Environmental Defenders under the Aarhus Convention ; the African Commission on Human and Peoples' Rights, Special Rapporteur on Human Rights Defenders, Focal Point on Reprisals and Focal Point on the Independence of the Judiciary in Africa ; and the Inter-American Commission on Human Rights and Rapporteur on Human Rights Defenders and Justice Operators.

b) Joint Declaration on Protecting the rights to freedom of peaceful assembly and of association from criminalization amid intensified existential threats, with the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), the Commissioner Rapporteur for Human Rights Defenders of the IACHR, and the Special Rapporteur on Human Rights Defenders and focal point for reprisals in Africa of the African Commission on Human and Peoples Rights (ACHPR).

c) Joint Statement on the Recognition of the Right to Care and the Freedom of Association of Women Workers, 01 May 2025, with the Rapporteur on the Rights of Women of the Inter-American Commission on Human Rights (IACHR) ; and the Special Rapporteur on Economic, Social, Cultural and Environmental Rights (REDESCA) of the IACHR.

d) Peer review of ODIHR opinions on :

i) Cyprus : Urgent Opinion on the Law 151(I) of 2025 on Public Gatherings and Parades ;

ii) Urgent opinion on the amendments to the law on assemblies and demonstrations, the code of administrative offences and the criminal code of Georgia (as adopted on 6 February 2025) ;

iii) Opinion on the draft act on the registration of foreign agents in Bulgaria (as of 11 November 2024).

Annex II

Methodology and sources

1. Evidence for this report was drawn from a global study[162], that included interviews, consultations and focus groups with 152 activists, human rights defenders, public defenders and other lawyers, journalists and civil society actors across all regions of the world. Diverse participants, across distinct contexts and jurisdictions were interviewed to identify common and/or cross-cutting experiences of digital surveillance. These participants advocated across the spectrum of issues including indigenous rights, environmental activism, gender equality, LGBTQIA+ rights, racial justice and the range of concerns related to democratic participation. One consultation was convened in the MENA region, two in Latin America (composed by six different meetings), three in Southeast Asia, two in Africa and a further global event hosted online. This methodology was aimed at countering sceptical views that claim chilling effects are overly subjective, or difficult to measure effectively. Further informing the report are 63 written submissions : 49 from civil society, academics, international bodies, a major global tech company, and 13 State submissions. In addition, the Rapporteur included information she received during her term in victims' sub-missions, meetings with civil society, academic visits and an official country visits. Collectively, this data concerns 84 States and other entities, demonstrating the widespread nature of the chilling effects phenomenon.

2. Participants contributing to this report were from the following States and other entities : Afghanistan, Algeria, Argentina, Armenia, Australia, Azerbaijan, Bahrain, Bangladesh, Belarus, Bhutan, Brazil, Cambodia, Canada, Chile, China, Colombia, Côte d'Ivoire, Cuba, Czechia, Denmark, Ecuador, Egypt, El Salvador, Eritrea, Eswatini, Ethiopia, France, Georgia, Hungary, Honduras, India, Indonesia, Iran (Islamic Republic of), Iraq, Ireland, Israel, Italy, Jordan, Kenya, Kuwait, Lebanon, Libya, Malaysia, Mexico, Morocco, Myanmar, Nepal, Nicaragua, Niger, Nigeria, Oman, Pakistan, Paraguay, Peru, Philippines, Poland, Russian Federation, Saudi Arabia, Serbia, South Africa, South Sudan, Spain, Sri Lanka, Sudan, State of Palestine, Switzerland, Syrian Arab Republic, United Republic of Tanzania, Thailand, Tunisia, Türkiye, Uganda, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan, Venezuela (Bolivarian Republic of), Viet Nam, Yemen, Zambia, Zimbabwe.

[162] See the Global Study, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.