Nations Unies A/HRC/29/37

Assemblée générale

Distr. générale
24 avril 2015
Français
Original: anglais

Conseil des droits de l'homme
Vingt-neuvième session
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

Rapport du Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires, Christof Heyns

Le recours aux technologies de l'information et de la communication pour garantir le droit à la vie

Résumé

Dans le présent rapport, soumis au Conseil des droits de l'homme en application de sa résolution 26/12, le Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires s'intéresse aux incidences des technologies de l'information et de la communication (TIC) sur la protection du droit à la vie.

Le Rapporteur spécial passe en revue les différentes utilisations qui sont actuellement faites des TIC pour promouvoir et protéger les droits de l'homme et en surveiller le respect. Constatant que les «témoins civils» peuvent changer la donne en contribuant à la collecte d'informations sur les violations des droits de l'homme, mais qu'il existe aussi des obstacles, notamment du point de vue de la vérification, à surmonter pour pouvoir utiliser les éléments de preuve recueillis et communiqués par ces témoins, le Rapporteur spécial examine comment les différents mécanismes internationaux des droits de l'homme peuvent tirer parti de ces éléments. Il formule plusieurs recommandations tendant notamment à ce que le Haut-Commissariat des Nations Unies aux droits de l'homme nomme un spécialiste des éléments de preuve numériques pour l'aider à utiliser au mieux les TIC.

GE.15-08235 (F) 220515 220515
1508235

Table des matières

I. Activités du Rapporteur spécial

1. Le Rapporteur spécial a soumis un rapport à l'Assemblée générale pour la dernière fois en octobre 2014. Dans ce rapport (A/69/265), il examinait quatre questions relatives à la protection du droit à la vie, à savoir: le rôle des systèmes régionaux de protection des droits de l'homme; l'emploi par les forces de l'ordre d'armes moins létales et d'armes télécommandées; la reprise des exécutions; et le rôle des indicateurs statistiques.

2. Le Rapporteur spécial a soumis son précédent rapport au Conseil des droits de l'homme en juin 2014. Ce rapport (A/HRC/26/36) portait sur la protection du droit à la vie dans le contexte des opérations de maintien de l'ordre, ainsi que sur la nécessité d'aligner sur les normes internationales les dispositions législatives internes relatives à l'usage de la force meurtrière par la police. Le Rapporteur spécial y encourageait le Conseil à définir les principaux paramètres d'un cadre juridique pour encadrer l'utilisation des aéronefs téléguidés et des drones armés, ainsi qu'à continuer de s'intéresser de près à la question des systèmes d'armes autonomes.

A. Communications

3. Le Rapporteur spécial a formulé des observations sur les communications adressées entre le 1er mars 2014 et le 28 février 2015, ainsi que sur les réponses reçues entre le 1er mai 2014 et le 30 avril 2015 (A/HRC/29/37/Add.5).

B. Visites

4. Le Rapporteur spécial s'est rendu en Gambie du 3 au 7 novembre 2014 avec le Rapporteur spécial sur la torture et autres peines ou traitements cruels, inhumains ou dégradants, Juan E. Méndez (A/HRC/29/37/Add.2).

5. On trouvera les rapports de suivi sur les visites effectuées par le Rapporteur spécial en Inde et en Turquie dans les documents A/HRC/29/37/Add.3 et 4, et le rapport sur la visite en Papouasie-Nouvelle-Guinée dans le document A/HRC/29/37/Add.1.

6. Depuis la soumission de son précédent rapport au Conseil des droits de l'homme, le Rapporteur spécial a adressé des demandes de visite aux Gouvernements nigérian, rwandais, ukrainien et yéménite. Il remercie les Gouvernements gambien, iraquien et yéménite d'avoir répondu positivement à ses demandes de visite et encourage les Gouvernements de l'Égypte, de l'Érythrée, de l'Iran (République islamique d'), du Nigéria, du Pakistan, du Rwanda et de l'Ukraine à faire de même.

C. Communiqués de presse[1]

7. Entre mars 2014 et mars 2015, le Rapporteur spécial a publié les communiqués de presse et les déclarations ci-après.

8. Le 6 mars 2014, le Rapporteur spécial a publié une déclaration conjointe sur des allégations de recours excessif à la force et à la violence contre des manifestants, des journalistes et des professionnels des médias en République bolivarienne du Venezuela.

[1] Les communiqués de presse du Rapporteur spécial sont consultables à l'adresse suivante: www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx?MID=SR_Summ_Executions.

9. Le 18 mars 2014, il a publié une déclaration conjointe sur les événements qui ont conduit à la mort d'une défenseuse des droits de l'homme chinoise.

10. Le 30 mai 2014, le Rapporteur spécial a publié un communiqué de presse conjoint sur la décision du Conseil de sécurité de ne pas saisir la Cour pénale internationale de la situation en République arabe syrienne.

11. Le 12 juin 2014, il a publié une déclaration appelant le Gouvernement mexicain à faire cesser les violations du droit à la vie dans le pays.

12. Le 2 juillet 2014, le Rapporteur spécial a appelé avec d'autres titulaires de mandat le Gouvernement sri-lankais à mettre un terme à la promotion de la haine raciale et religieuse.

13. Le 4 juillet 2014, il a publié une déclaration conjointe appelant le Gouvernement népalais à modifier les dispositions de sa législation sur la recherche de la vérité autorisant les mesures d'amnistie pour les auteurs de graves atteintes aux droits de l'homme et infractions au droit humanitaire.

14. Le 8 août 2014, le Rapporteur spécial a publié une déclaration conjointe jugeant très préoccupante l'explosion du nombre de personnes arrêtées et condamnées en République islamique d'Iran.

15. Le 12 août 2014, il a publié une déclaration conjointe exprimant son inquiétude face au danger imminent de massacre qui menaçait la population yézidie et d'autres communautés minoritaires exposées aux attaques du Groupe islamique d'Iraq et du Cham en Iraq.

16. Le 29 septembre 2014, le Rapporteur spécial a publié une déclaration conjointe sur l'adoption possible du projet de loi n° 85 de 2013 visant à revoir et à étendre la compétence des juridictions militaires en Colombie.

17. Le 29 septembre 2014 également, il a publié une déclaration exhortant le Gouvernement mexicain à enquêter sur la mort de 22 personnes.

18. Le 10 octobre 2014, il a publié une déclaration conjointe appelant le Gouvernement mexicain à enquêter sur la disparition de 43 étudiants dans l'État de Guerrero.

19. Le 26 novembre 2014, il a publié une déclaration conjointe exhortant le Président des États-Unis d'Amérique à donner son aval à la publication dans une forme la plus complète possible d'un rapport sur les méthodes d'interrogatoire de la Central Intelligence Agency.

20. Le 5 décembre 2014, le Rapporteur spécial a publié une déclaration conjointe sur les décisions prises par des grands jurys américains de ne pas porter en justice deux homicides très médiatisés dans lesquels étaient impliqués des policiers.

21. Le 27 mars 2015, il a publié un communiqué de presse conjoint appelant l'Espagne à extrader ou à poursuivre les auteurs de violations des droits de l'homme.

22. Durant la période considérée, le Rapport spécial a également publié des déclarations conjointes sur la peine de mort en Arabie saoudite, au Bangladesh, en Égypte, aux États-Unis d'Amérique, en Inde, en Indonésie, en Iran (République islamique d'), au Pakistan et au Soudan.

D. Rencontres internationales et nationales

23. Les activités qu'a menées le Rapporteur spécial entre le 26 mars et le 22 juillet 2014 sont présentées dans le rapport qu'il a soumis à l'Assemblée générale à sa soixante-neuvième session (A/69/265).

24. Le 2 septembre 2014, le Rapporteur spécial a prononcé un discours sur la peine de mort devant le Comité sur la dimension humaine de l'Organisation pour la sécurité et la coopération en Europe, réuni à Vienne.

25. Le 15 septembre 2014, il a donné une conférence sur les systèmes d'armes autonomes à la Stellenbosch Institute for Advanced Studies (Afrique du Sud).

26. Les 18 et 19 septembre 2014, au King's College de Cambridge (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord), le Rapporteur spécial a participé à la Conférence 2014 de l'Organisation mondiale de la Santé et de l'Université de Cambridge sur la réduction de la violence dans le monde.

27. Le 22 septembre 2014, il a pris part à une réunion-débat organisée par le Conseil des droits de l'homme à Genève sur le thème «Veiller à ce que l'utilisation d'aéronefs téléguidés ou de drones armés dans les opérations antiterroristes et militaires soit conforme au droit international, y compris au droit international des droits de l'homme et au droit international humanitaire».

28. Le 25 septembre 2014, le Rapporteur spécial a prononcé un discours dans le cadre du séminaire parlementaire sur les drones organisé par le Parlement norvégien à Oslo.

29. Du 29 septembre au 3 octobre 2014, le Rapporteur spécial a participé à Genève à la vingt et unième réunion annuelle des titulaires de mandat au titre des procédures spéciales.

30. Les 8 et 9 octobre 2014, il a pris part à l'atelier international sur le renforcement de la coopération entre l'Organisation des Nations Unies et les mécanismes régionaux de promotion et de protection des droits de l'homme organisé à Genève par le Haut-Commissariat des Nations Unies aux droits de l'homme.

31. Le 20 octobre 2014, à l'Université Columbia de New York, le Rapporteur spécial a participé à un débat coparrainé par l'Institut des droits de l'homme de la faculté de droit de l'Université Columbia, Rightlink, l'Institut d'études sur les droits de l'homme, l'unité de recherche sur les droits de l'homme et les questions humanitaires de l'École des affaires internationales et publiques et la Human Rights Law Review.

32. Les 10 et 11 novembre 2014, il a pris part au troisième Dialogue de Jakarta sur les droits de l'homme, consacré au droit à la vie et à l'instauration d'un moratoire sur la peine de mort dans les pays de l'Association des nations de l'Asie du Sud-Est (ASEAN), organisé à Jakarta par le Haut-Commissariat aux droits de l'homme, l'Union européenne et le représentant de l'Indonésie auprès de la Commission intergouvernementale des droits de l'homme de l'ASEAN.

33. Le 10 décembre 2014, le Rapporteur spécial a pris la parole à l'occasion de la publication à Genève de *The War Report 2013: Armed Conflicts and their Consequences*, organisé par l'Académie de droit international humanitaire et de droits humains à Genève.

34. Le 6 février 2015, il a pris la parole dans le cadre de la neuvième édition du Forum sur la sécurité («Des drones aux robots tueurs»), organisée à Genève par l'Université Webster en collaboration avec l'Institut des Nations Unies pour la recherche sur le désarmement.

II. Le recours aux technologies de l'information et de la communication pour garantir le droit à la vie

A. Contexte général[2]

35. De nombreuses normes de droit international relatives au droit à la vie ayant été définies dans les grandes lignes, le problème qui se pose bien souvent dans les efforts de protection est que les faits sont parfois contestés, si ce n'est leur existence même ignorée. Des personnes commettent des violations du droit à la vie non pas parce qu'elles jugent légitime de le faire, mais parce qu'elles pensent qu'elles n'auront pas de comptes à rendre, d'où l'importance d'établir les faits et de collecter des éléments de preuve.

36. Compte tenu des compétences qu'exige l'activité d'établissement des faits, l'évolution des méthodes de travail dans le domaine des droits de l'homme s'est accompagnée d'une professionnalisation des organisations de défense de ces droits[3]. Ces méthodes de travail ont été élaborées par ce que l'on décrit comme trois générations d'acteurs, qui se sont attachés à surveiller le respect des droits de l'homme dans le monde, chacun à leur manière. Il y a d'abord eu l'examen systématique des informations disponibles par un groupe d'éminents juristes pour le compte d'organisations intergouvernementales. Le domaine de l'établissement des faits a ensuite été le cadre d'une révolution menée par de grandes organisations non gouvernementales (ONG) internationales de défense des droits de l'homme, qui ont considérablement élargi le champ d'action dans ce domaine tout en restant attachées aux entretiens avec les témoins, qui permettent d'obtenir des témoignages de première main et très détaillés, mais peuvent être très chronophages et être la cause d'interférences et de biais de sélection. Au fil du temps, les acteurs de la première génération, notamment les titulaires de mandat au titre des procédures spéciales du Conseil des droits de l'homme, ont intégré les méthodes de travail de la deuxième génération aux leurs. Aujourd'hui, le domaine connaît une nouvelle transformation, conduite cette fois-ci par un ensemble varié et toujours plus vaste d'initiés aux technologies numériques (la troisième génération), dont des témoins, des observateurs et des militants, qui se caractérisent par une plus grande souplesse en ce qui concerne les méthodes à appliquer et les résultats à obtenir dans le cadre de l'établissement des faits[4]. Chaque génération a élargi la palette des participants aux enquêtes sur les violations des droits de l'homme. Aucune n'a invalidé les travaux déjà menés, mais chacune doit pouvoir tirer parti des points forts des autres sans compromettre ses propres capacités.

37. Il ne fait plus de doute que les technologies de l'information et de la communication (TIC), à savoir le matériel et les logiciels qui facilitent la production, la transmission, la réception, l'archivage et le stockage des informations, peuvent jouer un rôle croissant dans la protection de tous les droits de l'homme, dont le droit à la vie. Les TIC peuvent non seulement être utiles pour garantir l'établissement des responsabilités, mais aussi assurer une certaine visibilité des personnes courant un danger immédiat ou mobiliser un appui en leur faveur.

---

[2] Le Rapporteur spécial remercie le Centre de la gouvernance et des droits de l'homme de l'Université de Cambridge, en particulier Ella McPherson et Thomas Probert, de l'aide précieuse qu'ils lui ont apportée dans le cadre de ses travaux de recherche. Des descriptifs d'un grand nombre des applications et des projets examinés dans le présent rapport ont été regroupés et sont consultables à la page suivante: http://ictandhr.tumblr.com/.

[3] Molly K. Land, «Networked activism», *Harvard Human Rights Journal*, vol. 22 (2009), p. 205 à 243.

[4] Philip Alston «Introduction: third generation human rights fact-finding», *Proceedings of the Annual Meeting of the American Society of International Law*, vol. 107 (avril 2013), p. 61 et 62.

38. Dans sa tâche quotidienne consistant à répertorier les allégations d'exécutions illicites et à en évaluer la véracité, le Rapporteur spécial, comme bien d'autres acteurs du domaine, est de plus en plus tributaire de données numériques. À titre d'exemple, on peut citer les images prises avec des téléphones portables durant la guerre civile à Sri Lanka et utilisées pour inciter aussi bien les pouvoirs publics que la communauté internationale à enquêter de manière plus approfondie sur les violations généralisées d'un grand nombre de droits de l'homme, notamment du droit à la vie, qui se seraient produites (A/HRC/17/28/Add.1). De même, lors de l'élaboration du rapport au Conseil des droits de l'homme sur la sécurité des journalistes, il est apparu clairement que les journalistes et médias citoyens étaient devenus incontournables en recourant aux TIC pour appeler l'attention sur les violations commises dans le monde et collecter des informations sur celles-ci (A/HRC/20/22 et Corr.1).

39. La quantité croissante de moyens numériques disponibles permet à tout un chacun de participer bien davantage à la surveillance du respect des droits de l'homme. Les TIC non seulement ouvrent des perspectives de pluralisme qui peuvent permettre de démocratiser le processus d'enquête sur les droits de l'homme, mais fournissent aussi des mécanismes de responsabilisation sociale dont les citoyens peuvent se servir pour obliger les pouvoirs publics et d'autres acteurs à rendre des comptes[5]. Avec les réseaux sociaux, les civils disposent d'une multitude de moyens d'exposer les violations des droits de l'homme dont ils sont témoins, lesquels moyens ne font le plus souvent pas intervenir de structure intergouvernementale ou non gouvernementale officielle. Cette nouvelle donne modifie profondément les rapports de force dans la surveillance du respect des droits de l'homme, la communauté des observateurs étant beaucoup plus large qu'avant, et ouvre aussi des possibilités dans des situations qui, autrement, ne pourraient peut-être faire l'objet d'aucune surveillance. Lorsque la présence physique d'enquêteurs sur les droits de l'homme peut poser des difficultés, l'utilisation réfléchie des TIC peut permettre de pallier le manque d'informations sur des situations qui intéressent vivement la communauté des défenseurs de ces droits.

40. Le développement des TIC ne devrait toutefois pas être considéré comme un bien absolu pour la protection des droits de l'homme. Les moyens permettant aux États de surveiller les activités de la société civile et de s'immiscer dans celles-ci se multiplient dans l'espace numérique, et le Conseil des droits de l'homme devrait être vigilant face aux dangers que posent les TIC et à ce qu'elles permettent de faire[6]. En recourant aux TIC, les militants des droits de l'homme et d'autres acteurs peuvent s'exposer à tout un ensemble de risques, dont beaucoup d'entre eux n'ont peut-être pas conscience.

41. Pour faire en sorte que l'action en faveur des droits de l'homme mette pleinement à profit les possibilités offertes par les TIC, il est impératif de s'attaquer au problème du fossé numérique tant dans l'accès aux TIC que dans la maîtrise de celles-ci. Les TIC favorisent le pluralisme dans les activités relatives aux droits de l'homme en permettant aux profanes de seconder les professionnels. Elles peuvent par contre créer des perspectives d'inclusion ou d'exclusion qui correspondent bien souvent aux obstacles préexistants à l'accès à des ressources et à un pouvoir d'action, tels que la langue, le niveau d'instruction, la situation financière ou le sexe[7]. Lorsque l'on parle de pluralisme, il est question non seulement d'avoir la possibilité de s'exprimer, mais aussi d'être entendu. Être entendu par

[5] Molly K. Land *et al*., *#ICT4HR: Information and Communication Technologies for Human Rights* (Institut de la Banque mondiale, 2012).

[6] Le Rapporteur spécial relève qu'à sa vingt-huitième session, le Conseil des droits de l'homme a décidé de nommer un rapporteur spécial sur le droit à la vie privée à l'ère du numérique.

[7] A. Trevor Thrall, Dominik Stecula et Diana Sweet, «May we have your attention please? Human rights NGOs and the problem of global communication», *International Journal of Press/Politics*, vol. 19, n° 2 (avril 2014), p. 135 à 159.

des enquêteurs sur les droits de l'homme peut dépendre de la capacité d'un individu de fournir des informations vérifiables, qui peut elle-même dépendre de sa connaissance des technologies numériques et de son empreinte numérique[8]. Parce que l'on dispose de nombreuses informations numériques sur des violations des droits de l'homme commises dans un contexte ou une région, on risque d'accorder la priorité à ces violations plutôt qu'à des violations plus graves mais moins visibles perpétrées ailleurs.

42. Il ne fait aucun doute que si elles sont utilisées de façon judicieuse, les TIC peuvent améliorer la protection des droits de l'homme, notamment du droit à la vie. Plusieurs composantes du système des Nations Unies ont investi beaucoup de temps et de moyens dans l'ajustement de leurs méthodes de travail aux possibilités offertes par les TIC. Le Bureau de la coordination des affaires humanitaires et le Département des opérations de maintien de la paix développent actuellement des techniques avancées de suivi et de cartographie des zones de crise, et la Cour pénale internationale a entrepris d'examiner la façon dont elle traitait les éléments de preuve numériques. Cela étant, il semble que la communauté des défenseurs des droits de l'homme n'ait toujours pas effectué d'examen systématique de toutes les possibilités offertes par les TIC, ni ne s'en soit prévalue (voir le document A/65/321, par. 3 à 10).

43. Dans le présent rapport, le Rapporteur spécial examine les possibilités qu'offrent et les difficultés que posent les TIC en ce qui concerne les aspects essentiels de l'action en faveur des droits de l'homme, qui consistent à promouvoir et à protéger ces droits et à en surveiller le respect ou à enquêter pour garantir l'établissement des responsabilités en cas de violation. Bien que la question de l'incidence des TIC et des réseaux sociaux sur les espaces de sensibilisation ait déjà été traitée par d'autres, le Rapporteur l'aborde brièvement ci-après, tout comme la question de savoir en quoi les TIC permettent d'être protégé physiquement, ainsi que la question des mesures de sécurité qui s'imposent pour que l'environnement numérique soit sûr, deux questions pertinentes au regard du mandat. Le Rapporteur spécial s'intéresse ensuite au recours aux TIC pour collecter des informations sur les violations commises − lequel peut faciliter l'établissement des responsabilités - en s'attachant notamment à examiner les problèmes qui se posent, tels que la vérification. Enfin, le Rapporteur spécial étudie la mesure dans laquelle les mécanismes internationaux des droits de l'homme recourent actuellement à des éléments de preuve numériques.

B. Promotion et sensibilisation

44. Les moyens plus nombreux permettant de partager l'information et de communiquer offrent des possibilités manifestes et aujourd'hui largement mises à profit de diffuser des informations sur les droits de l'homme, que ce soit dans un objectif général, à des fins d'éducation, ou dans un objectif plus précis consistant à militer pour une modification de la législation ou des politiques ou à appeler à des enquêtes ou à l'établissement des responsabilités dans des affaires données. En complément de leurs stratégies de communication dans les médias traditionnels, les organisations de défense des droits de l'homme peuvent recourir à des instruments qui leur permettent de s'adresser directement au public.

45. À titre d'exemple, les organisations intergouvernementales et non gouvernementales, ainsi que les États, ont recours à des sites Web pour mettre à la disposition du plus grand nombre possible de personnes des informations sur les normes ou règles juridiques relatives aux droits de l'homme. Dans des rapports précédents, le

[8] Ella McPherson, «Advocacy organizations evaluation of social media information for NGO journalism: the evidence and engagement models», *American Behavioral Scientist*, vol. 59, n° 1 (juillet 2014), p. 124 à 148.

Rapporteur spécial a souligné l'importance de cadres juridiques clairs et consultables par le public pour prévenir les exécutions arbitraires par le recours à la force ou l'application de la peine de mort (A/HRC/26/36 et A/67/275)[9]. Les TIC permettent incontestablement aux États d'être plus transparents vis-à-vis de la population et de la communauté internationale.

46. Nombre d'organisations de défense des droits de l'homme communiquent donc par voie numérique et ont également acquis des compétences qui leur permettent de se servir rapidement et directement des réseaux sociaux pour mobiliser l'opinion publique. Les TIC peuvent ouvrir de nouvelles perspectives en matière d'éducation qui favorisent la création de conditions propices au respect des droits de l'homme. Au Kenya, une initiative (PeaceTXT) a consisté à envoyer aux abonnés des sms de promotion de la paix en vue de prévenir les conflits potentiels. Ailleurs, des ONG ont recouru à la caméra cachée pour révéler au grand jour des cas extrêmes de sectarisme et de harcèlement à des fins de sensibilisation du public[10].

47. Les TIC numériques peuvent donc aider à assurer une large visibilité des droits de l'homme, du moins auprès de ceux qui sont présents sur les réseaux sociaux. Des applications telles que AiCandle ou Pocket Protest permettent de signer des pétitions, d'adresser des courriers électroniques ou de recevoir des informations en rapport avec les droits de l'homme via son téléphone portable ou son smartphone et sont particulièrement utiles pour mobiliser en urgence[11]. En outre, des plates-formes telles que Thunderclap permettent d'amplifier l'écho de messages. En définitive, il peut être utile de recourir à de telles stratégies pour amener les pouvoirs publics à s'intéresser à une question ou une affaire[12].

48. La question est de savoir si ces possibilités modifient sensiblement et pour le mieux la dynamique des activités de sensibilisation. Les campagnes sont en concurrence les unes avec les autres pour capter l'attention du public dans un contexte où le volume d'informations ne cesse de croître et ne peuvent, du moins dans un premier temps, trouver un écho qu'auprès de ceux qui sont au fait des technologies numériques[13]. Qui plus est, la brièveté des messages et le caractère instantané de Twitter peuvent empêcher de rendre compte de situations complexes ou donner de telles situations une image simpliste, et les contenus attestant de violations des droits de l'homme ne réunissent parfois guère les conditions qui font que quelque chose devient viral[14]. Les réseaux sociaux sont un moyen efficace d'accroître la participation, en partie parce qu'ils n'exigent pas autant de motivation que d'autres outils pour participer, ce qui peut toutefois conduire à un militantisme paresseux ou éphémère (ce que l'on appelle le «clictivisme»)[15]. D'aucuns font toutefois valoir que bien qu'ils le paraissent, les témoignages de ce militantisme ne sont pas

[9] Voir également www.use-of-force.info.

[10] Cynthia Romero, «What next? The quest to protect journalists and human rights defenders in a digital world», conference report, Freedom House, Mexico, (février 2014), https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20 Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf.

[11] Voir Amnesty International UK, «What is pocket protest?» (juin 2013), www.amnesty.org.uk/what-pocket-protest.

[12] Voir Jiva Manske, «Case studies: concrete examples of compelling and strategic use of social media», *New Tactics in Human Rights* (9 mai 2013), https://www.newtactics.org/comment/6124.

[13] Thrall, Stecula et Sweet, «May we have your attention please?» (voir la note de bas de page 7).

[14] Dustin N. Sharp, «Human rights fact-finding and the reproduction of hierarchies» (6 juin 2014), *Social Science Research Network*, http://papers.ssrn.com/abstract=2341186.

[15] Malcolm Gladwell, «Small change: why the revolution will not be tweeted», *The New Yorker* (4 octobre 2010), www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

insignifiants du fait qu'ils s'additionnent, ce qui atteste d'un «milieu solidaire» et permet d'«appeler l'attention»[16].

C. Prévention et protection

49. Les TIC peuvent aider de bien des manières différentes à prévenir les violations du droit à la vie par des acteurs étatiques ou non étatiques. Pour commencer, les applications d'alerte peuvent assurer une protection physique et numérique aux groupes potentiellement vulnérables, tels que les défenseurs des droits de l'homme. Si elle peut être mise à profit par les réseaux, la connectivité numérique représente un danger pour ceux qui sont exposés à la surveillance du trafic des données numériques ou à d'autres formes de surveillance. Il faut éduquer à la sécurité et à la sûreté numérique. La surveillance peut toutefois aussi être un outil de prévention, et des pratiques allant de la retransmission en direct sur Internet de manifestations ou d'opérations policières au recours à l'imagerie satellite seront examinées plus bas.

1. Les applications d'alerte

50. Plusieurs organisations créent des applications d'alerte auxquelles peuvent avoir recours les militants, les journalistes et d'autres acteurs pour faire savoir qu'ils sont en danger. À titre d'exemple, Amnesty International a développé Panic Button, une application déguisée en application utilitaire qui permet aux utilisateurs de déclencher en secret une alarme par l'envoi d'un sms et, à titre facultatif, de données de géolocalisation, à des contacts sélectionnés au préalable en appuyant rapidement sur le bouton d'allumage du téléphone. Lorsque des militants ou des journalistes sont agressés ou arrêtés, on leur prend bien souvent leur téléphone pour obtenir la liste de contacts qu'ils contiennent. Panic Button envoie des notifications en continu, notifications qui constituent non seulement des appels à l'aide mais aussi des mises en garde encourageant les contacts de la personne à prendre eux-mêmes des mesures de précaution[17]. Il existe d'autres applications ou dispositifs avec le même objectif[18].

51. Ce type d'applications permet de remédier aux problèmes que posent le manque d'informations et le délai de réaction, qui peuvent restreindre les efforts de protection des personnes en danger. Les praticiens estiment qu'après qu'une personne a été mise en détention ou menacée, il y a une fenêtre de quelque quarante-huit heures durant lesquelles la probabilité est la plus élevée qu'une réponse de grande ampleur ait son impact maximal. L'on recense dans le monde nombre d'exemples où une telle réponse à une mise en détention, coordonnée via les réseaux sociaux ou autrement, a permis de convaincre les autorités de réévaluer le bien fondé de maintenir une personne en détention.

52. Les nouvelles technologies s'inscrivent donc dans des stratégies plus larges et durables consistant à communiquer avec un réseau digne de confiance en situation de danger et à appeler une vaste communauté à s'élever, notamment verbalement, contre un acte arbitraire perpétré contre quelqu'un. Cela étant, il importe de garder à l'esprit les risques inhérents à ces technologies, qui pourraient servir à repérer et prendre pour cible des personnes.

[16] Stephanie Vie, «In defense of "slacktivism": the Human Rights Campaign Facebook logo as digital activism», *First Monday*, vol. 19, n° 4 (avril 2014), http://firstmonday.org/ojs/index.php/fm/article/view/4961.

[17] Voir https://panicbutton.io/.

[18] BBC News, «Smart bracelet protects aid workers» (5 avril 2013), www.bbc.com/news/technology-22038012.

2. Importance de la sécurité numérique

53. Si elles offrent des moyens supplémentaires à ceux qui travaillent sur les questions relatives aux droits de l'homme, les TIC peuvent également être la source de risques supplémentaires. Pour limiter ces risques, les personnes susceptibles d'être victimes de violations, telles que les défenseurs des droits de l'homme, doivent prendre très au sérieux certaines règles de sécurité. La sécurité numérique passe par exemple par l'utilisation d'applications de détection de logiciels espions, le recours à des ressources telles que Security in-a-Box, ou encore des services d'assistance ou des forums en ligne[19].

54. Les militants peuvent communiquer de façon plus sûre en passant par des réseaux privés virtuels (VPN), ou en utilisant des programmes de cryptage ou le réseau TOR, qui permet d'améliorer la confidentialité de la navigation sur Internet. Les développeurs et les formateurs doivent néanmoins avertir les utilisateurs qu'il est impossible de garantir la confidentialité et l'anonymat sur Internet. Les grands organismes intergouvernementaux ou non gouvernementaux de défense des droits de l'homme doivent également prendre la mesure des risques qu'ils courent en interagissant avec des organisations de taille plus modeste ou des particuliers.

55. L'évaluation des avantages et des inconvénients du cryptage des données numériques ne relève évidemment pas du mandat du Rapporteur spécial. Cependant, à l'heure où les enquêtes sur les droits de l'homme suscitent des exigences contradictoires, il s'agit d'un problème complexe, dont l'actuel titulaire du mandat commence à se préoccuper dans la mesure où il peut avoir des effets néfastes, qui peuvent aller jusqu'à la commission d'exécutions extrajudiciaires. L'utilisation des médias sociaux traditionnels pour le partage d'informations sur les droits de l'homme peut être risquée, aussi bien pour les témoins civils que pour les personnes à propos desquelles ils témoignent.

3. Surveillance aux fins de la protection

56. Non seulement la prolifération des moyens de surveillance et d'enregistrement informatiques renforce considérablement la possibilité de demander des comptes aux citoyens (voir ci-dessous), mais elle peut aussi empêcher la commission d'infractions. Le fait de se savoir surveillé peut avoir un puissant effet dissuasif lorsqu'il s'accompagne d'un régime de sanctions crédible, comme c'est le cas avec la vidéosurveillance anticriminalité. La croyance en cet effet dissuasif est si forte que certains militants font semblant de filmer, même si la batterie de leur téléphone portable est vide, pour éviter enlèvements ou arrestations[20].

57. Le meilleur exemple, dans ce domaine, est peut-être le port de caméras par les policiers pour éviter l'emploi d'une force excessive − comportement des forces de l'ordre qui constitue l'une des principales préoccupations du Rapporteur spécial. Une étude récemment menée en Californie (États-Unis d'Amérique) montre que le recours à ces appareils a fait baisser de 59 % l'emploi de la force par la police et que les plaintes pour emploi excessif de la force ont chuté de près de 90 %[21]. D'autres expériences telles que l'utilisation, au lieu de caméras, de smartphones transmettant des images, du son et des

[19] Les ressources fournies par des initiatives telles que New Tactics in Human Rights (https://www.newtactics.org/) permettent aux utilisateurs d'échanger en ligne leurs connaissances sur les différents aspects de la défense des droits de l'homme et, notamment, sur la sécurité numérique.

[20] Stephanie Hankey et Daniel Ó Clunaigh, «Rethinking risk and security of human rights defenders in the digital age», *Journal of Human Rights Practice*, vol.5, n° 3 (novembre 2013), p. 543.

[21] Barak Ariel, William A. Farrar et Alex Sutherland, «The effect of police body-worn cameras on use of force and citizens complaints against the police: a randomized controlled trial», *Journal of Quantitative Criminology* (novembre 2014).

données de géolocalisation, sont actuellement en cours en Afrique du Sud, au Brésil et au Kenya[22].

58. La vidéosurveillance étant plus efficace lorsqu'on se sait filmé, certains affirment que les caméras portées par les policiers ont un effet dissuasif puisque ces derniers sont tenus par le règlement de signaler qu'un enregistrement est en cours, ceci leur rappelant, ainsi qu'aux civils, qu'ils sont surveillés[23].

59. Le port de caméras laissant craindre une atteinte au droit à l'intimité, il a été suggéré que les policiers déconnectent ces appareils lorsqu'ils entraient dans les maisons ou lorsqu'ils parlaient à des victimes. Il a également été estimé que pour éviter tout filtrage des informations, les agents ne devaient pas disposer du contrôle de leur caméra[24]. L'accès aux enregistrements et leur mise en lieu sûr sont d'autres sujets de préoccupation. Cependant, bien que certaines interrogations demeurent sans réponse, beaucoup estiment que l'effet dissuasif des caméras portées par les policiers justifie leur généralisation[25]. Les enregistrements effectués par la police sont certes prometteurs, mais il est important de protéger le droit des citoyens d'enregistrer les faits et gestes de la police.

60. Les caméras portatives permettent d'exercer un contrôle à l'échelle la plus petite, celle des relations humaines. À l'échelle la plus grande, la télédétection peut se faire par le biais de dispositifs comme les satellites ou les drones. Des initiatives telles que le Satellite Sentinels Project et la campagne Eyes on Darfur d'Amnesty International ont mis en lumière le potentiel de tels dispositifs. La surveillance ostentatoire des zones sensibles peut dissuader les auteurs potentiels de violations de passer à l'acte, tout au moins lorsqu'un repérage à distance est possible[26]. Ce type de surveillance est toutefois coûteux et il peut y avoir une part d'arbitraire dans le choix des populations ou des lieux à surveiller. Comme pour d'autres méthodes de surveillance, les moyens techniques ont un effet dissuasif parce que leur existence est connue (d'où l'importance de campagnes d'information parallèles) et que la menace de sanctions est réelle[27].

61. Ces méthodes de surveillance encouragent les bons comportements en faisant planer la menace de sanctions. Il est également possible d'exploiter la capacité des TIC d'utiliser des informations (récemment) collectées pour avoir prise sur les événements présents.

---

[22] Graham Denyer Willis *et al.*, «Smarter policing: tracking the influence of new information technology in Rio de Janeiro», *Igarapé Institute Strategic Note 10* (novembre 2013); voir également: the Smart Policing initiative (disponible à l'adresse suivante: http://en.igarape.org.br/smart-policing/).

[23] Comme l'a magistralement montré Jeremy Bentham, le fait de se savoir surveillé influe sur le comportement, mais les effets de cette surveillance sur la criminalité, tout comme ses dangers potentiels, n'ont que récemment été mis en évidence, grâce aux progrès techniques.

[24] Bracken Stockley, «Public support for police body cameras – but who controls on/off switch?», *The justice gap* (mars 2014), disponible à l'adresse suivante: http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/.

[25] Robert Muggah, «Why police body cameras are taking off, even after Eric Garner's death», *IPI Global Observatory* (11 décembre 2014), disponible à l'adresse suivante: http://theglobal observatory.org/2014/12/police-body-cameras-eric-garner/; voir aussi Alexandra Mateescu, Alex Rosenblat et Danah Boyd, «Police body-worn cameras», Data & Society Research Institute Working Paper (février 2015), disponible à l'adresse suivante: www.datasociety.net/pubs/dcr/ PoliceBodyWornCameras.pdf.

[26] Nathaniel A. Raymond *et al.*, «While we watched: assessing the impact of the satellite sentinel project», *Georgetown Journal of International Affairs* (26 juillet 2013), disponible à l'adresse suivante: http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/.

[27] Patrick Meier, «Will using 'live satellite imagery to prevent war in the Sudan actually work?», *iRevolutions* (30 décembre 2010), disponible à l'adresse suivante: http://irevolution.net/ 2010/12/30/sat-sentinel-project/.

L'analyse des médias sociaux pourrait ainsi servir, dans le domaine des droits de l'homme, à anticiper les crises. La base de données Hatebase, par exemple, fondée sur l'idée qu'il existe une corrélation entre discours de haine et risques de génocide, recueille des données sur le vocabulaire et la fréquence des propos haineux véhiculés par les médias sociaux afin de prédire les éruptions de violence à l'échelle régionale[28].

62. Il y a cependant des limites aux possibilités des TIC en matière d'alerte rapide. Si le «big data mining», c'est-à-dire la collecte de grandes quantités de données, est considéré comme un bon outil de prévision et de prévention des conflits, cette technique est moins probante pour ce qui est de l'analyse et de l'intervention[29].

63. Le recours à la collecte de grandes quantités de données et à la télédétection pour prévenir les violations des droits de l'homme soulève aussi des questions de méthode et d'éthique. Les populations vulnérables, par exemple, peuvent courir un danger si l'on peut repérer et établir à distance leur position et leur situation[30]. En outre, l'analyse statistique des données relatives aux droits de l'homme peut se révéler inexacte du fait d'éventuels biais de sélection, du chevauchement de certaines données ou de difficultés rencontrées lors de la collecte[31].

4. Vers un devoir de précaution numérique

64. La surveillance est parfois si utile pour empêcher les violations des droits de l'homme que les États qui en ont les moyens se doivent d'en faire usage. Des caméras sont déjà présentes dans les véhicules de la police et dans les salles d'interrogatoire, mais il serait bon d'envisager leur utilisation en d'autres lieux où la surveillance est susceptible d'avoir un effet préventif, tels que les prisons, sous réserve des limitations imposées par d'autres droits, comme celui au respect de la vie privée.

65. Les pouvoirs publics peuvent tirer parti d'autres outils pour s'acquitter de leurs responsabilités en matière de prévention et prendre les précautions qui s'imposent. Par exemple, certains pays préviennent les populations civiles par SMS ou par téléphone avant de lancer des raids aériens. Un meilleur contrôle serait possible grâce aux dispositifs d'enregistrement présents sur certaines armes sophistiquées, mais il faudrait davantage de transparence.

66. Dans l'espace numérique, toutefois, le devoir de précaution ne concerne pas uniquement les États. Les organisations de surveillance du respect des droits de l'homme − intergouvernementales et non gouvernementales − doivent réfléchir aux conséquences de leurs échanges de correspondance ou de leur traitement de l'information. Il faudrait peut-être revoir les interprétations habituelles que l'on fait de la notion de «consentement préalable éclairé».

[28] Voir http://www.hatebase.org/.

[29] Sheldon Himelfarb, «Can big data stop wars before they happen?» (United States Institute of Peace, 25 avril 2014), disponible à l'adresse suivante: www.usip.org/publications/can-big-data-stop-wars-they-happen.

[30] Voir, par exemple, Harvard Humanitarian Initiative, «The Signal Program on Human Security and Technology» (2013), disponible à l'adresse suivante: http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program.

[31] Voir les travaux du Groupe d'analyse de données relatives aux droits de l'homme (Human Rights Data Analysis Group), à l'adresse suivante: https://hrdag.org/coreconcepts/.

D. Surveillance et établissement des faits

67. Comme on l'a déjà dit, l'établissement des faits revêt une importance particulière en raison de la nature même des violations qui intéressent ce mandat. Les organisations des droits de l'homme ont mis au point des méthodes d'enquête rigoureuses, ne serait-ce que pour assurer la crédibilité de leurs éléments de preuve et, par voie de conséquence, protéger leur réputation. Les TIC, qui facilitent la production de contenus par les utilisateurs, ont généralisé et démocratisé les activités d'établissement des faits en donnant aux civils les moyens de témoigner spontanément ou sur demande. La principale difficulté de cette évolution est de concilier la démocratisation avec le maintien de la crédibilité, voire son renforcement, et donc de vérifier les éléments de preuve numériques.

1. Témoins civils et documents vidéo

68. Les militants attachent de la valeur aux enregistrements vidéo depuis plusieurs décennies, tout au moins depuis l'affaire *Rodney King*, survenue au début des années 1990. Le détournement des images de télésurveillance aux fins d'enquêtes publiques est maintenant monnaie courante[32]. Au niveau international, la condamnation par la Cour pénale internationale (CPI) de Thomas Lubanga grâce aux enregistrements d'interrogatoires d'enfants soldats enrôlés dans sa milice, a démontré que la vidéo pouvait servir en cas de manque de preuves[33]. Bien entendu, les auteurs de violations peuvent aussi, au même titre que des témoins ou des victimes de violations, être la source de ce type d'informations. Qui plus est, il n'est pas nécessaire de rendre des informations publiques pour qu'elles soient utiles dans le cadre d'enquêtes sur des violations des droits de l'homme.

69. Les informations émanant de témoins civils jouent depuis longtemps un rôle crucial dans l'établissement de faits relatifs aux droits de l'homme, mais elles ont toujours, jusqu'ici, été recueillies par des professionnels. Ces derniers, ou leurs contacts dignes de confiance, avaient pour habitude de prendre part à la production ou à la transmission des informations par des témoins, par exemple lors d'un entretien. Les TIC permettent aujourd'hui aux témoins civils de recueillir ou de communiquer des informations sans intermédiaire.

70. La façon la plus spontanée de témoigner consiste, pour les civils, à utiliser les outils ou les plates-formes grand public. Omniprésents, les smartphones permettent de capter des images ou des sons qu'il est aisé de transmettre par des canaux numériques tels que des médias sociaux. Ces stratégies de production et de communication présentent l'intérêt de ne pas nécessiter de compétences particulières, mais elles peuvent malheureusement filtrer des métadonnées (telles que l'origine, le lieu et l'heure de l'enregistrement) indispensables à la vérification de l'information. Il existe également des applications telles qu'InformaCam et EyeWitness, spécialement conçues pour améliorer la qualité des métadonnées accompagnant photographies ou vidéos et pour assurer la régularité de transmission et de conservation des informations[34].

[32] Voir, par exemple, Daoud Kuttab, «Video technology exposing Isreali violations in the West Bank», *Al-Monitor* (8 juillet 2014), disponible à l'adresse suivante: www.al-monitor.com/pulse/originals/2014/07/israel-palestine-cctv-camera-footage-occupation-settlers.html.

[33] Matthew Shaer, «The media doesn't care what happens here: can amateur journalism bring justice to Rio's favelas?», *The New York Times* (18 février 2015), disponible à l'adresse suivante: www.nytimes.com/2015/02/22/magazine/the-media-doesnt-care-what-happens-here.html.

[34] Informations sur d'InformaCam disponibles à l'adresse suivante: https://guardianproject.info/informa/; voir également New Perimeter, "eyeWitness to atrocities", disponible à l'adresse suivante: www.newperimeter.org/our-work/access-to-justice/eyeWitness.html.

71. Un certain nombre d'ONG proposent déjà aux particuliers souhaitant témoigner et aux formateurs des cours sur la façon de produire et de diffuser des données plus crédibles. WITNESS, Amnesty International, Tactical Tech et l'Initiative pour la justice des Fondations Open Society mènent ce genre d'action à l'échelle mondiale ou régionale. Ces formations peuvent porter sur des questions de protection individuelle, concernant par exemple la sécurité informatique dont il a été question précédemment, ou fournir des informations pratiques sur le genre de détails que les témoins doivent faire figurer dans leurs vidéos (plaques d'immatriculation, chiffres arborés sur les uniformes ou repères topographiques) et sur la façon de les faire connaître[35].

2. La production participative de données

72. Le «crowdsourcing» et le «crowdseeding» sont des solutions intermédiaires, pour ce qui est des témoins civils, entre les méthodes traditionnelles d'appel à témoignages et la production et la communication spontanées d'informations. Le crowdsourcing consiste à confier une tâche à un groupe de taille importante dont on ne connaît pas la composition, constitué à la suite d'un appel à propositions. Un tel groupe n'est pas nécessairement représentatif dans la mesure où ce type d'appels a tendance à favoriser la participation de personnes bénéficiant, par exemple, de ressources techniques ou financières ou de temps libre. Le crowdseeding est une forme de crowdsourcing dont les participants peuvent être échantillonnés au hasard en fonction de leur représentativité et dotés des outils et ressources nécessaires à la collecte d'informations. La relation de confiance qui s'établit au fil du temps avec les témoins garantit la crédibilité du projet[36].

73. L'intervention massive de citoyens témoins peut non seulement donner plus d'ampleur à l'action en faveur des droits de l'homme, mais encore la rendre plus efficace, puisqu'elle renforce la participation et la sensibilisation et permet de vérifier les faits[37]. Cela n'est toutefois pas sans risques. En divulguant des informations précises les concernant, ces actions de masse peuvent en effet mettre en danger des populations vulnérables. Ces procédés peuvent aussi être employés contre les militants des droits de l'homme, par exemple pour des «tâches de renseignement humain» telles que l'identification de personnes à partir de photographies de manifestations[38].

3. Les données satellitaires

74. Les images satellitaires peuvent avoir des incidences sur les activités de défense des droits de l'homme. L'effet dissuasif des satellites vient principalement du fait que l'on sait qu'il se trouvera toujours quelqu'un pour utiliser leurs images pour dénoncer une éventuelle violation. Au début de cette année, par exemple, des enquêteurs d'Amnesty International et de Human Rights Watch ont réussi à repérer les dégâts importants causés par des incendies dans deux villes du nord-est du Nigéria en comparant des images satellitaires prises à des moments différents. Parce qu'elles corroboraient les dires de témoins oculaires, ces informations ont confirmé que les incendies correspondaient à des attaques de militants au cours desquelles plusieurs centaines de personnes avaient péri. Ces recoupements étaient

[35] Voir, par exemple, Kelly Matheson, «Video as evidence: basic practices», *Witness blog* (16 février 2015), disponible à l'adresse suivante: http://blog.witness.org/2015/02/video-as-evidence-basic-practices/.

[36] Patrick Meier, «From crowdsourcing crisis information to crowdseeding conflict zones (updated)», *iRevolutions* (10 juillet 2012), disponible à l'adresse suivante: http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/.

[37] Molly Beutz Land, «Peer producing human rights», *Alberta Law Review*, vol. 46, n° 4 (2009), p. 1115.

[38] Jonathan Zittrain, «The Internet creates a new kind of sweatshop», *Newsweek* (7 décembre 2009), disponible à l'adresse suivante: www.newsweek.com/internet-creates-new-kind-sweatshop-75751.

importants dans la mesure où les images satellitaires ne sont pas suffisantes pour confondre les coupables ou établir un lien de causalité, mais l'affaire montre l'intérêt de la télédétection pour les zones difficiles d'accès[39].

75. Il est possible d'améliorer la qualité des informations en couplant l'analyse des données satellitaires avec des procédés de traitement informatiques tels que la visualisation de l'activité des réseaux sociaux. La photographie par satellite permet d'établir l'origine des tirs de missiles ou d'artillerie ou de faire état des dégâts occasionnés par les attaques de drones[40].

76. Actuellement, la plupart des images satellitaires utilisées pour la défense des droits de l'homme émanant d'opérateurs commerciaux, cette source d'information n'est disponible que si la région concernée présente un intérêt commercial. Il importe en outre qu'il n'y ait pas de nuages. Qui plus est, la résolution des photos est généralement assez basse. L'imagerie satellitaire militaire est de meilleure qualité et couvre des zones plus étendues, mais les autorités compétentes rechignent à partager les informations dont elles disposent (et l'on ne parle pas d'images classées défense) avec les enquêteurs des droits de l'homme, même lorsque la sécurité nationale n'est pas en jeu.

E. Évaluation des preuves réunies à l'aide des technologies de l'information et de la communication

77. Le flot d'informations fournies par des témoins civils ne peut servir à établir des faits que si l'on peut rassembler les données et les évaluer. C'est pourquoi il est important pour les organisations de défense des droits de l'homme, notamment parce qu'il est essentiel pour elles d'être crédibles, de pouvoir intégrer ce matériau à leurs méthodes traditionnelles de recherche et d'analyse. Il peut cependant être difficile d'évaluer des contenus numériques fournis par des témoins civils, et notamment de sélectionner les informations pertinentes, de les vérifier et de les stocker. Certaines innovations techniques et certaines mesures d'évaluation de l'information peuvent contribuer à résoudre ces difficultés.

1. Le problème du volume des données

78. Étant donné la prolifération des données produites et communiquées par des civils sous forme numérique, la sélection des témoignages pertinents peut être extrêmement fastidieuse. Une solution intermédiaire serait de confier ce filtrage à des réseaux collaboratifs, mais il sera probablement nécessaire d'exploiter les capacités analytiques des TIC pour tenir compte du problème de «rapport signal-bruit» qui les caractérise. L'une des solutions consiste à filtrer automatiquement les grands ensembles de données susceptibles de receler des données intéressantes. Le projet de CrisisNET, par exemple, est de recueillir et d'harmoniser en temps réel des données de crise numériques émanant de milliers de sources de façon à accélérer et à améliorer le travail des chercheurs. Aucune machine ne peut décider à la place d'un être humain si une information est pertinente et constitue une preuve de violation − une activité en fin de compte subjective −, mais la technologie peut

[39] Christoph Koettl, «The story behind the Boko Haram satellite images», *Amnesty International UK/Blogs* (17 janvier 2015), disponible à l'adresse suivante: www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images.

[40] Bellingcat, «Origin of artillery attacks on Ukrainian military positions in Eastern Ukraine between 14 July 2014 and 8 August 2014» (17 février 2015), disponible à l'adresse suivante: www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/; et Forensic Architecture, «Drone strikes: investigating covert operations through spatial media», disponible à l'adresse suivante: www.forensic-architecture.org/case/drone-strikes/.

aider les observateur des droits de l'homme à se concentrer sur l'essentiel[41]. Cette question devra être examinée de plus près.

79. Il sera probablement toujours nécessaire de se livrer à la conservation de contenus numériques à des fins de surveillance et d'utilisation par les nombreuses parties concernées. Ce travail de conservation fera à la fois appel à l'automatisation et aux compétences traditionnelles en matière d'enquête et de vérification. C'est ce que fait très bien la chaîne des droits de l'homme en ligne de WITNESS, qui diffuse des données vérifiées avec le concours de l'agence de presse Storyful, dont les réseaux sociaux sont la source d'informations.

2. Le problème de la volatilité des données

80. Une grande partie des documents utiles aux enquêtes menées sur les violations des droits de l'homme peuvent n'être disponibles en ligne que pendant une durée limitée (en raison des pressions qui s'exercent sur ceux qui mettent en ligne certains contenus, ou sur les sites hébergeurs)[42]. Il est donc important, pour les enquêteurs, d'avoir les moyens de capter toutes les informations susceptibles de leur servir et de les conserver en lieu sûr. Il convient avant toute chose d'élaborer des directives à l'intention des enquêteurs nationaux ainsi que des observateurs des droits de l'homme[43].

81. La détention de documents relatifs à des enquêtes sur des violations des droits de l'homme peut mettre en danger les militants. Certaines applications telles qu'Eyewitness et International Evidence Locker ont été conçues pour permettre aux témoins de télécharger des éléments de preuve vers une base de données «en nuage» et de les utiliser ou de les supprimer en fonction de la situation. Ces applications permettent également d'informer le public choisi tout en conservant les données et les métadonnées qui les accompagnent. La collaboration entre les enquêteurs et les entreprises technologiques continuera cependant d'être cruciale.

3. Le problème de la vérification

82. La difficulté de la vérification des données est parfois présentée comme un obstacle majeur à la validation des preuves numériques, mais ce problème n'est pas nouveau: il est normal que les institutions vérifient la crédibilité d'une source et l'exactitude des informations avant de donner suite à une plainte ou de mettre en jeu sa réputation en y donnant suite. Même si la nature des informations vérifiées et les techniques utilisées dans ce domaine évoluent au même rythme rapide que les TIC, le travail de vérification consiste invariablement à authentifier et à valider les informations reçues et à contrôler leur provenance.

83. Vérifier consiste généralement à contrôler l'origine et la source de l'information, l'heure et le lieu des faits, ainsi que la régularité de transmission et de conservation des informations. Les enquêteurs doivent prendre le temps d'identifier la source, de rechercher des métadonnées, puis de croiser les informations avec d'autres sources. Une nouvelle spécialité, à laquelle il est souvent fait référence sous le nom de criminalistique numérique, est en train de se mettre en place, mais elle continue de faire abondamment appel aux compétences d'experts et à nécessiter de laborieuses vérifications, comme dans les enquêtes traditionnelles.

---

[41] Voir: http://crisis.net/about/.

[42] Madeleine Bair, «Navigating the ethics of citizen video: the case of a sexual assault in Egypt», *Arab Media & Society*, vol. 19 (2014), disponible à l'adresse suivante: http://arabmediasociety.com/?article=844.

[43] Il existe des guides pour aider les militants à archiver leur documentation (voir, par exemple, http://archiveguide.witness.org/). Le Bureau du Procureur de la Cour pénale internationale est en train de mettre au point des directives à l'usage des enquêteurs.

84. Un témoin peut fournir séparément des informations sur la date, le lieu et la teneur d'un interrogatoire, ou au contraire intégrer ces données au fichier. La première méthode souligne l'importance d'un enrichissement mutuel entre les méthodes des enquêteurs de deuxième et de troisième générations et montre dans quelle mesure une source peut en corroborer une autre. La deuxième consiste à intervenir au moment de la production de l'information, par exemple en annonçant le lieu et la date, ou pendant sa transmission. Certaines informations, telles que les repères terrestres (à l'exemple des panneaux routiers ou des caractéristiques géologiques), la météo, l'habillement, les armes ou les langues employées, peuvent constituer des preuves. Les métadonnées automatiquement intégrées au fichier, telles que l'horodatage, peuvent également servir à authentifier un document. Ces informations peuvent également être corroborées et croisées avec d'autres fichiers et éléments de preuve numériques, par exemple des images satellitaires. Il est possible de synchroniser plusieurs vidéos du même événement de façon à le visionner sous différentes perspectives[44].

85. On reconnaît de plus en plus la nécessité de posséder des compétences spécialisées pour vérifier les données numériques. Plus les enquêteurs s'y connaissent en criminalistique numérique, plus ils sont capables d'exploiter facilement et rapidement les informations numériques émanant de témoins civils. Le *Guide de vérification*, qui a été publié en 2014, est rapidement devenu un manuel de référence pour les travailleurs humanitaires et les enquêteurs des droits de l'homme[45].

86. En améliorant les compétences des témoins civils en matière de vérification, il sera vraisemblablement possible de faciliter le contrôle. WITNESS propose à cet égard un guide précisant les informations devant apparaître dans les vidéos apportant la preuve de violations des droits de l'homme[46].

87. Une autre façon de faciliter la vérification est d'encourager la soumission d'informations en vue de leur vérification ou l'évaluation de ces informations. De telles initiatives, qualifiées d'«aides à la vérification », peuvent reposer sur une intervention humaine ou sur des outils spéciaux. Des applications telles qu'InformaCam automatisent l'ajout de requêtes de vérification au stade de la production et provoquent leur insertion pendant la transmission[47]. Certains outils utilisent a posteriori les ressources de la production participative, comme Verily[48]. D'autres, comme Checkdesk, application en ligne conçue pour les salles de rédaction, permettent à un groupe restreint d'effectuer des vérifications de façon collaborative et transparente.

88. Il convient de ne pas exagérer les difficultés techniques de la vérification, sans pour autant minimiser leur importance. Une organisation de défense des droits de l'homme peut se décrédibiliser en diffusant des informations non vérifiées, mais les canulars peuvent aussi déboucher sur des situations explosives − les fameux «cyber-incendies sauvages» −

[44] Voir, par exemple, le projet Rashomon: http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/.

[45] Craig Silverman (éd.), *Guide de vérification: la référence de la vérification de contenu numérique pour la couverture d'événements dans l'urgence* (Centre Européen de journalisme, 2014), disponible à l'adresse suivante: http://verificationhandbook.com/book_fr/.

[46] Voir «Un guide de terrain pour l'amélioration de la valeur de la vidéo comme preuve pour les droits de l'homme», disponible à l'adresse suivante: http://verificationhandbook.com/book_fr/appendix.php.

[47] Ella McPherson, «Digital civilian witnesses of human rights violations: easing the tension between pluralism and verification at human rights organizations» dans Lind (éd.), *Producing Theory 2.0: The Intersection of Audiences and Production in a Digital World*, vol. 2 (à paraître en 2015).

[48] Voir Victor Naroditskiy, «Veri. ly – getting the facts straight during humanitarian disasters» (août 2014), www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters.

pouvant conduire à des violences[49]. De nombreux États disposent déjà de lois restreignant la liberté d'expression pour éviter les incitations à la violence ou aux mouvements de panique, mais il y a débat sur la manière de les appliquer efficacement aux activités en ligne. Toute réglementation dans ce domaine est forcément complexe et controversée; il a été suggéré à la communauté en ligne de combler elle-même cette lacune, un rôle important étant confié aux responsables et aux modérateurs[50]. Le Rapporteur spécial sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée a soumis en 2014 au Conseil des droits de l'homme un rapport sur la complexité des problèmes qu'il rencontrait dans l'exercice de son mandat du fait d'Internet et des médias sociaux (A/HRC/26/49). Dans ce rapport, il appelle l'attention sur les politiques mises en œuvre par certains grands médias sociaux, tout en soulignant l'importance des initiatives de la société civile.

4. Utilisation des preuves numériques

89. La plupart des informations qu'il est possible de recueillir par le biais des canaux décrits ci-dessus sont des «données de convenance», mais il n'est pas toujours possible d'évaluer immédiatement leur utilité pour une enquête relative aux droits de l'homme. En outre, il importe de ne pas privilégier les images car les blogs ou microblogs fournissent beaucoup d'informations qui peuvent être utilisées pour corroborer d'autres sources.

90. Les aides à la vérification peuvent certes accélérer le processus de vérification, mais les enquêteurs et les témoins civils doivent avoir des connaissances numériques en matière de vérification pour les utiliser**.** Il est difficile de savoir vraiment comment les connaissances relatives à la production et à la transmission d'informations efficaces, sûres et éthiques à des fins de preuve, circulent entre les témoins civils, notamment ceux qui agissent de façon vraiment spontanée. Les mesures préventives visant à former des enquêteurs dans le domaine des droits de l'homme favoriseront les témoins préparés mais, le plus souvent, ce sont les témoins accidentels qui fournissent les informations les plus édifiantes.

91. C'est pourquoi des organisations telles que WITNESS préconisent l'inclusion type d'un mode «témoin oculaire» ou «preuve», à l'instar d'InformaCAm, dans des applications photo et vidéo installées par défaut sur les smartphones et les plates-formes de réseaux sociaux[51]. L'inclusion de ces fonctionnalités dans des applications et plates-formes traditionnelles signifie que les témoins civils vont probablement les connaître et, partant, les utiliser.

F. Utilisation des technologies de l'information et de la communication par les mécanismes relatifs aux droits de l'homme

92. Jusqu'à présent, on s'est intéressé à l'utilisation des TIC dans le cadre de l'action en faveur des droits de l'homme en général plutôt qu'à leur utilisation par les mécanismes internationaux relatifs aux droits de l'homme. Il importe que la communauté internationale soit ouverte à ces nouvelles méthodologies, sinon il sera difficile pour les organisations de défense des droits de l'homme et les témoins civils de tirer pleinement avantage des mécanismes existants en matière d'établissement des responsabilités. Comme on l'a déjà

[49] Cette question a été soulevée dans le rapport «Global Risks 2013» du Forum économique mondial (8e éd., p. 23 à 27).

[50] Voir Lee Howell, «Only you can prevent digital wildfires» (8 janvier 2013), www.nytimes.com/2013/01/09/opinion/only-you-can-prevent-digital-wildfires.html.

[51] Sam Gregory, «How an Eyewitness mode helps activists (and others) be trusted», *WITNESS Blog* (3 mars 2014), http://blog.witness.org/2014/03/eyewitness-mode-helps-activists/.

dit, les preuves numériques ne doivent pas être considérées comme une fin en soi − en l'absence d'obligation réelle de rendre des comptes, elles ne servent à rien − et il est donc essentiel que les canaux officiels chargés d'établir les responsabilités en cas de violations des droits de l'homme soient ouverts à ce type de preuves.

93. La communauté des Nations Unies au sens large a beaucoup investi pour tirer parti du potentiel des TIC, notamment dans le domaine de la gestion de l'information en temps de crise (A/69/517). Le Bureau des technologies de l'information et des communications de l'ONU a, conjointement avec ICT4Peace Foundation, coordonné les travaux du Groupe consultatif pour la gestion de l'information en temps de crise, qui est devenu un forum de discussion sur les avancées technologiques dans le domaine de la gestion l'aide humanitaire et de l'information en temps de crise[52].Le Bureau pour la coordination des affaires humanitaires a examiné les répercussions des TIC sur les réseaux d'aide humanitaire et a, depuis lors, mis en œuvre un certain nombre de projets collaboratifs pour tirer parti du pouvoir de la foule[53]. De son côté, le projet Global Pulse est une initiative de grande envergure concernant l'incidence des métadonnées sur l'aide humanitaire[54].

94. En 2014, le Département des opérations de maintien de la paix a demandé au Groupe d'experts sur les technologies et l'innovation au service des opérations de maintien de la paix des Nations Unies de recommander des moyens d'accroître l'efficacité opérationnelle de la technologie et de l'innovation. En février 2015[55], le Groupe d'experts a publié son rapport final dans lequel il recommandait au Conseil de sécurité, notamment, d'établir une mission technique spéciale pour utiliser les technologies audiovisuelles de supervision et de surveillance dans le cadre de la prise de décisions.

95. Les mécanismes de l'ONU relatifs aux droits de l'homme n'ont pas complétement ignoré les progrès des TIC. Plusieurs d'entre eux ont réussi à être présents dans les médias sociaux dans le cadre de leurs stratégies et campagnes promotionnelles de mobilisation afin d'atteindre des millions d'utilisateurs dans le monde entier. Bien que l'utilisation des TIC numériques à des fins promotionnelles soit importante, le Rapporteur spécial étudiera ci-dessous comment divers mécanismes internationaux et régionaux relatifs aux droits de l'homme utilisent les TIC à des fins d'établissement des faits et des responsabilités.

1. Procédures spéciales et autres mécanismes du Conseil des droits de l'homme

96. Le présent rapport a été motivé en partie par l'enquête du Rapporteur spécial concernant des preuves vidéo attestant d'exécutions commises à la fin de la guerre civile à Sri Lanka (voir A/HRC/17/28/Add.1, appendice). En l'occurrence, le Rapporteur spécial a été en mesure de donner un élan à une vaste coalition en faveur de l'établissement des responsabilités en demandant à des experts techniques de faire des observations en toute indépendance sur les métadonnées des vidéos, la balistique des armes apparaissant dans les vidéos et le mouvement des corps. Compte tenu des progrès rapides dans ce domaine, il est fort possible qu'il soit plus facile aujourd'hui de faire appel à de telles compétences spécialisées mais force est de constater que les capacités du HCDH n'ont guère changé. Les titulaires de mandat au titre des procédures spéciales tireraient grand profit de connaissances techniques internes pour pouvoir choisir les meilleurs experts pour telles ou telles tâches.

[52] Voir http://ict4peace.org/crisis-information-management-advisory-group-cimag-retreat/.

[53] BCHA, Policy and Studies Series, *Humanitarianism in the Network Age: including world humanitarian data and trends 2012* (2013), https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

[54] Voir http://www.unglobalpulse.org/.

[55] Voir http://www.performancepeacekeeping.org/offline/download.pdf.

97. Comme on l'a indiqué précédemment, il est essentiel de vérifier les contenus générés par les utilisateurs pour pouvoir tirer parti des avantages offerts par les TIC afin d'élargir l'accès aux travaux relatifs aux droits de l'homme et d'étendre la portée de ces travaux. Cela étant, la vérification ne doit pas être considérée comme un obstacle à l'utilisation des preuves numériques. Les difficultés techniques liées à la vérification sont parfois exagérées et utilisées comme excuse pour ne pas utiliser ce type de preuves. Il conviendrait de démystifier la vérification au sein des mécanismes internationaux relatifs aux droits de l'homme, afin de mettre davantage à profit les avantages offerts par les preuves numériques.

98. En ce qui concerne les dangers de l'ignorance en matière de sécurité numérique, il y a lieu de noter que de nombreux mécanismes du Conseil des droits de l'homme encouragent les contacts entre les individus par courriel non sécurisé, sans donner d'avertissement concernant la sécurité ni suggérer de solutions alternatives. Bien que ce mode de contact soit louable pour élargir l'accès aux mécanismes du Conseil, ce dernier ne s'acquitte sans doute pas de son devoir de diligence dans la mesure où il ne prévient pas correctement les individus ou les groupes des risques qu'ils sont susceptibles de prendre.

99. Il ne s'agit évidemment pas de laisser entendre que les procédures spéciales du Conseil sont fermées aux informations émanant des nouveaux flux de donnés examinés dans le présent rapport. En fait, la plupart des informations figurant dans les rapports des ONG sur lesquels sont fondées les communications des procédures spéciales proviennent de ces sources. Toutefois, le fait que le Conseil ne soit pas encore disposé à examiner ces preuves ou rapports lui fait courir le risque, d'ici à quelques années, d'être isolé du reste de la communauté des droits de l'homme avec laquelle il n'a pas ménagé ses efforts pour collaborer dans le passé.

2. Commission d'enquête nationales et internationales

100. Des preuves numériques ont été utilisées dans le cadre de diverses enquêtes nationales. La conclusion selon laquelle le décès de Ian Tomlinson durant une manifestation tenue à Londres en 2009 constituait un homicide illégal reposait sur un enregistrement vidéo qui avait été recherché et remis par un journaliste d'investigation à la Commission indépendante chargée d'examiner les plaintes déposées contre la police. De même, dans le cadre de l'enquête en cours sur la fusillade de Marikana (Afrique du Sud), des enregistrements vidéo probants ont été recueillis et la Commission sud-africaine des droits de l'homme les a faits synchroniser par un expert technique[56].

101. Au niveau international, le HCDH a collaboré avec le Programme pour les applications satellites opérationnelles (UNOSAT) de l'ONU et ponctuellement avec divers partenaires extérieurs, afin d'utiliser aussi bien les preuves satellitaires que vidéo dans le cadre des travaux des commissions d'enquête internationales»[57]. Comme on l'a vu plus haut, lorsqu'elle est associée à d'autres techniques de surveillance des droits de l'homme, l'imagerie satellitaire peut fournir des informations extrêmement utiles à inclure dans les rapports au Conseil des droits de l'homme.

102. La Commission d'enquête sur la situation des droits de l'homme en République populaire démocratique de Corée a utilisé l'imagerie satellitaire et a clandestinement enregistré des vidéos et pris des photographies pour démontrer l'existence de plusieurs camps de prisonniers (voir A/HRC/25/63). La Commission s'est appuyée sur les vidéos et les photographies dans la mesure où elle pouvait en confirmer l'authenticité et, s'agissant

[56] Voir «Written submissions of the South African Human Rights Commission regarding "Phase One"», Commission d'enquête de Marikana (29 octobre 2014), www.sahrc.org.za/home/21/files/SAHRC%20PHASE%20ONE%20FINAL%20WRITTEN%20SUBMISSIONS.pdf.

[57] Voir http://www.unitar.org/unosat/.

de l'imagerie satellitaire, sur les séquences commerciales disponibles. La Commission a constaté qu'une imagerie satellitaire à meilleure résolution produite par des États à la pointe de la technologie aurait très certainement fourni de plus amples informations. Malheureusement, en dépit des demandes faites, ces images n'ont pas été mises à la disposition de la Commission (voir A/HRC/25/CRP.1, par. 60 et 61).

103. La Commission d'enquête internationale indépendante sur la République arabe syrienne a également utilisé un certain nombre de documents satellitaires et numériques, comme on pouvait s'y attendre d'un organisme surveillant l'un des conflits les plus documentés de l'histoire[58]. Dans le cadre de son enquête spéciale sur les meurtres d'Houla, par exemple, la Commission a examiné l'imagerie satellitaire pour passer en revue les points d'accès à une zone où des meurtres avaient été commis et les déclarations faites par des personnes interrogées et évaluer les affirmations selon lesquelles le Gouvernement avait rasé des zones civiles à Damas et Hama[59]. La Commission a évoqué des cas où elle avait reçu ou trouvé des vidéos corroborant les allégations de torture ou d'autres formes de mauvais traitements ou des séquences filmées de meurtres, tout en précisant les fois où elle n'avait pas pu vérifier ces enregistrements[60]. Du matériel vidéo a aussi été directement réuni par la Mission de supervision de l'ONU en République arabe syrienne et utilisé dans les rapports de la Commission[61]. Cette dernière a également effectué des examens préliminaires et analysé scientifiquement 26 948 photographies qui auraient été prises entre 2011 et 2013 dans des centres de détention gouvernementaux[62]. Dans ses rapports les plus récents, la Commission a cité plusieurs vidéos qui avaient été réalisées et distribuées par l'État islamique d'Iraq et du Levant; ces vidéos ont posé des problèmes par rapport à la méthodologie actuelle, qui consiste à utiliser des vidéos uniquement pour corroborer des événements appuyés par d'autres témoignages de victimes, mais la Commission les a traitées comme s'il s'agissait d'aveux[63].

3. Établissement des responsabilités pénales au niveau international

104. Les informations émanant de sources numériques sont devenues de plus en plus importantes pour les tribunaux internationaux, notamment ceux qui ont été créés au cours des années 1990, et désormais aussi la Cour pénal internationale. Afin d'évaluer l'importance de ces preuves pour faire progresser ses travaux, la Cour a pris l'initiative d'élaborer des méthodes de travail dans lesquelles il est possible de tenir compte de ces preuves. En 2012 et 2013, la Cour a encouragé les partenaires à échanger des idées et des connaissances sur les moyens d'améliorer la capacité des enquêteurs et des procureurs de réunir et d'analyser des preuves numériques concernant de graves crimes internationaux[64].

105. Ainsi, il a notamment été recommandé au Bureau du Procureur d'«engager des spécialistes formés aux techniques sophistiquées de cyberinvestigation et maîtrisant les technologies de pointe» et ayant «de l'expérience des enquêtes numériques et des compétences dans des domaines particuliers connexes, tels que la médecine légale par ordinateur et smartphone, les enquêtes en ligne, le stockage et la gestion de données, les

[58] Voir Marc Lynch, Deen Freelon et Sean Aday, *Syria's Socially Mediated Civil War* (United States Institute of Peace, 2014).
[59] Voir A/HRC/21/50, annexe IV; et A/HRC/22/59, annexe XIII, par. 18.
[60] A/HRC/21/50, annexe VIII, par. 31; A/HRC/22/59, annex V, par. 22.
[61] A/HRC/21/50, annexe V, par. 14.
[62] A/HRC/27/60, par. 26
[63] A/HRC/28/69 et Corr.1, annexe II, par. 21 à 25.
[64] Voir Centre des droits de l'homme, University of California, *Beyond Reasonable Doubt: Using scientific evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2012); et *Digital fingerprints: Using electronic evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2014).

techniques sophistiquées de cyberinvestigation et la maîtrise de la sécurité numérique». Il a été suggéré que ces mesures contribueraient considérablement à développer les capacités internes de vérifier les données numériques et de produire des preuves de qualité[65]. Sur la base de ces consultations, le Bureau du Procureur a nommé un spécialiste de la vérification du matériel numérique pour qu'il serve de «cyberenquêteur» dans le cadre de son équipe d'autres enquêteurs ayant une expérience du droit et des forces de l'ordre.

106. Conscient de la nature éphémère de la plupart du matériel pertinent, le Bureau du Procureur a adopté la pratique consistant à examiner les preuves numériques disponibles à l'ouverture de l'instruction préliminaire. Comme indiqué plus haut, la Cour a élaboré des directives à l'usage des enquêteurs sur les meilleures pratiques concernant la récupération et le stockage des preuves numériques et les enquêtes à ce sujet, notamment la fermeture de sites Web et la saisie de disques durs.

III. Conclusion

107. **Les TIC ont eu un effet considérable sur l'incidence et la nature des travaux relatifs aux droits de l'homme. Il importe toutefois de ne pas en faire un usage exagéré, en particulier lorsque l'information est rare, auquel cas il sera encore plus important de résister à la tentation de privilégier le matériel numérique. Bien que les technologies nouvelles puissent susciter des attentes en matière d'information, il convient de noter que les activités traditionnelles de surveillance et d'établissement de rapports dans le domaine des droits de l'homme ne se veulent pas exhaustives, et l'analyse des nouveaux flux de données informatisées ne devrait pas non plus avoir cet objectif. Ces flux ne doivent pas être perçus comme un raccourci mais plutôt comme un complément aux stratégies préexistantes utilisées par les acteurs des droits de l'homme.**

108. **Il importe aussi d'adopter les TIC en étant dûment conscient des risques qu'elles présentent. Alors que, dans de nombreux cas, la technologie peut être le moteur du pluralisme, des problèmes liés à la fracture numérique perdurent. Les défenseurs des droits de l'homme doivent être informés des mesures de protection numérique pour pouvoir en profiter. La promotion des droits de l'homme fondée sur les moyens numériques contribuera peut-être à forger une culture de sensibilisation, mais si les ressources utilisées pour ces initiatives s'écartent des canaux plus traditionnels, cela se fera au détriment des groupes vulnérables qui ne sont pas connectés.**

109. **Il importe également de reconnaître la nécessité de s'approprier et de contrôler les mécanismes liés aux TIC. L'utilisation de preuves numériques dépend également souvent de la volonté des entreprises de technologie d'héberger et de stocker les informations et d'en faciliter la recherche. En outre, certains États bloquent l'accès aux plates-formes commerciales de médias sociaux étrangères, telles que Twitter, Facebook et YouTube. Dans d'autres, des réseaux de communication ont été totalement fermés pour supprimer la circulation de l'information.**

110. **Il peut être difficile pour les organisations qui s'occupent des droits de l'homme de rester au fait de la culture numérique et de financer l'accès aux nouvelles technologies. Une solution serait de faire en sorte que les spécialistes des TIC et les experts des droits de l'homme collaborent afin d'élaborer, de mettre en œuvre, voire de commercialiser, des nouvelles applications concernant les droits de l'homme ou de négocier des accords de licence gratuits ou à faible coût pour l'utilisation des applications existantes. Les donateurs s'intéressent au financement des innovations**

[65] Voir Human Rights Center, *Digital fingerprints*, p. 11 (voir note de bas de page 64).

technologiques mais semblent davantage mettre l'accent sur la technologie que sur la formation préalable à sa mise en place. Or, sans formation, la technologie peut être inutile voire dangereuse. Comme l'a relevé un observateur, «tôt ou tard, tous les problèmes technologiques deviennent des problèmes d'éducation»[66].

111. **Le cadre collaboratif peut être encore étoffé davantage. En effet, un large éventail d'organisations sont disposées à aider les mécanismes internationaux relatifs aux droits de l'homme à profiter plus pleinement des TIC. Des efforts de coordination ont été faits mais il semble que la communauté des droits de l'homme ait pris beaucoup de retard pour tirer parti du potentiel offert par rapport aux autres organismes internationaux − en particulier pour ce qui est des interventions en cas de crise[67].**

112. **Les mécanismes de l'ONU relatifs aux droits de l'homme qui agissent directement sur la base de preuves souvent réunies par des tierces parties ont besoin de moyens internes pour réaliser un tri du matériel numérique, dans le cadre d'une première évaluation de la valeur probable de la source, avant que des experts externes ne procèdent à une vérification complète ou à une autre évaluation technique. L'existence d'une capacité de «première opinion» et de liaison au sein du secrétariat des mécanismes internationaux, notamment des procédures spéciales, favoriserait une plus grande utilisation d'informations potentiellement utiles.**

113. **Bien entendu, en termes réels, les progrès technologiques accomplis dans la collecte de preuves ne seront utiles que si les mécanismes d'établissement des responsabilités auxquels ils contribuent sont aussi efficaces, sachant que ces mécanismes ne dépendent pas, en règle générale, de la technologie. En ce sens, l'amélioration des flux d'informations offerts par les TIC est nécessaire, mais pas suffisante, pour mieux protéger les droits de l'homme, y compris le droit à la vie. Il est donc important que les mécanismes internationaux relatifs aux droits de l'homme, y compris le Conseil des droits de l'homme et ses procédures spéciales, soient en mesure d'interagir pleinement avec ces matériels. Certaines ONG actives dans le domaine des droits de l'homme, dites de «deuxième génération», suivent le rythme des innovations de la «troisième génération». Il est essentiel que la première génération rattrape son retard**.

IV. Recommandations

A. À l'attention de l'Organisation des Nations Unies

114. **Le HCDH devrait nommer, à titre consultatif et dans les plus brefs délais, un spécialiste des contenus numériques chargé de donner des conseils au sujet des informations émanant de témoins civils et de servir d'interface avec les réseaux extérieurs d'experts dans ce domaine. Il s'agirait d'une solution provisoire pour garantir la réalisation de progrès rapides dans ce domaine. Dans le même temps, le HCDH devrait, avec l'aide du spécialiste nommé, agir pour créer des capacités à plus long terme.**

[66] Christopher Neu, «Mobile applications for atrocity prevention require mobile students», *TechChange* (19 février 2013), http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/.

[67] Au sujet de l'intervention humanitaire, le Digital Humanitarian Network a établi deux rapports à l'intention des deux parties prenantes de ces partenariats: Voir http://digitalhumanitarians.com/content/guidance-collaborating-formal-humanitarian-organizations et http://digitalhumanitarians.com/content/guidance-collaborating-volunteer-technical-communities.

115. **Étant donné que les commissions internationales d'enquête et les missions d'établissement des faits sont des organes ad hoc à même de recevoir une quantité importante et croissante de preuves numériques, il faudrait prévoir des spécialistes capables d'analyser ces preuves parmi les effectifs de ces mécanismes.**

116. **D'une manière plus générale, le HCDH devrait prendre des mesures pour faire mieux connaître les exigences en matière de sécurité numérique et y familiariser son personnel et ses mécanismes à tous les niveaux. Cela suppose de définir des normes minimales de diligence raisonnable en ce qui concerne la sécurité numérique des sources. Il conviendrait d'élaborer des directives à l'usage du personnel de l'ONU concernant l'éthique liée à l'utilisation de sources ouvertes, notamment dans les médias sociaux, en consultation avec les partenaires compétents.**

B. À l'attention des mécanismes régionaux relatifs aux droits de l'homme

117. **Les mécanismes régionaux relatifs aux droits de l'homme devraient évaluer leur capacité de recevoir et d'utiliser du matériel numérique, ainsi que de promouvoir les meilleures pratiques en matière de sécurité numérique. En cas de besoin, ils devraient collaborer avec le HCDH afin de renforcer leur capacité.**

C. À l'attention des États

118. **Les États devraient respecter et, lorsque cela est nécessaire, protéger le droit d'un individu d'enregistrer une manifestation publique, y compris les agissements des membres des forces de l'ordre, et d'enregistrer également pour lui une activité dans laquelle il est enregistré par un agent de l'État.**

119. **Les États devraient envisager des mesures innovantes pour utiliser les TIC, afin de prévenir les violations du droit à la vie par ses agents, telles que l'usage excessif de la force par des membres des forces de l'ordre, ou dans des établissements de détention. Il pourrait s'agir, notamment mais pas exclusivement, d'innovations telles que des caméras portatives, compte tenu de la nécessité de garantir aussi le droit au respect de la vie privée.**

120. **Les États dotés de capacités de pointe pour prendre des images satellitaires devraient à tout le moins envisager de fournir les informations ainsi obtenues aux mécanismes internationaux relatifs aux droits de l'homme qui en ont besoin, le cas échéant d'une manière confidentielle ou anonyme.**

D. À l'attention des organisations de la société civile et des établissements universitaires

121. **Tout en restant ouvertes aux innovations technologiques en rapide évolution, les organisations de la société civile devraient évaluer, en se fondant sur des preuves, les bénéfices des nouveaux mécanismes en ligne. En collaboration avec des établissements universitaires, elles devraient axer les ressources sur les domaines où les TIC peuvent véritablement améliorer les capacités, tout en poursuivant les travaux essentiels qu'elles effectuent en utilisant d'autres méthodes plus traditionnelles. Les établissements universitaires et les organisations des droits de l'homme devraient également collaborer afin d'accorder la priorité à la recherche dans les domaines où cela est le plus nécessaire, notamment pour relever le «défi du volume».**

122. **Les responsables des programmes relatifs aux droits de l'homme et des programmes de formation devraient envisager d'inclure des modules portant sur l'utilisation effective des TIC afin d'assurer la protection des droits de l'homme. Les plus grandes organisations devraient continuer d'aider celles qui disposent de ressources plus limitées.**

E. À l'attention des donateurs

123. **Les donateurs devraient reconnaître que les solutions technologiques aux problèmes relatifs aux droits de l'homme ne peuvent être efficaces que si les formations qui les accompagnent le sont également. Outre qu'ils doivent s'attendre à de nouvelles évaluations rigoureuses et objectives de l'utilité et de l'incidence de nouvelles applications ou mécanismes, les donateurs devraient également soutenir les efforts visant à améliorer la culture numérique et la connaissance de la sécurité numérique chez les communautés qui en ont le plus besoin.**

F. À l'attention des entreprises de technologie et d'informatique

124. **Les développeurs devraient envisager favorablement d'inclure une fonction «témoin oculaire» ou «preuve» dans les applications d'appareils-photo traditionnelles afin de donner aux utilisateurs la possibilité d'inclure des métadonnées et d'établir l'intégrité du fichier, pour pouvoir utiliser les preuves vidéo sans qu'il soit nécessaire d'avoir téléchargé précédemment une application spécialisée.**

125. **Les plates-formes de réseaux sociaux devraient concevoir un procédé par lequel les contenus produits par les utilisateurs qui peuvent présenter un intérêt pour les enquêtes relatives aux droits de l'homme peuvent rester à la disposition des enquêteurs, quand bien même ils ont été retirés des plates-formes en raison des normes appliquées par les communautés virtuelles.**