Nations Unies A/HRC/23/40

Assemblée générale

Distr. générale
17 avril 2013
Français
Original: anglais

Conseil des droits de l'homme
Vingt-troisième 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 la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue*

Résumé

Le présent rapport, soumis en application de la résolution 16/4 du Conseil des droits de l'homme, analyse les effets de la surveillance des communications par les États sur l'exercice des droits à la vie privée et à la liberté d'opinion et d'expression. Tout en prenant en compte l'incidence des progrès technologiques importants dans le domaine des communications, le rapport souligne l'urgente nécessité d'examiner plus en détail les nouveaux modes de surveillance et de réviser les lois nationales réglementant ces pratiques conformément aux normes relatives aux droits de l'homme.

* Soumission tardive.

GE.13-51728 (EXT)
1351728

Table des matières

I. Introduction

1. Le présent rapport analyse les effets de la surveillance des communications par les États sur l'exercice des droits à la vie privée et à la liberté d'opinion et d'expression. Tout en prenant en compte l'incidence des progrès technologiques importants dans le domaine des communications, le rapport souligne l'urgente nécessité d'examiner plus en détail les nouveaux modes de surveillance et de réviser les lois nationales réglementant ces pratiques conformément aux normes relatives aux droits de l'homme.

2. L'innovation technologique a accru les possibilités de communication et de protection de la liberté d'expression et d'opinion, en permettant l'anonymat, le partage rapide d'informations et le dialogue interculturel. Simultanément, elle a accru les possibilités de surveillance et d'interventions de l'État dans les communications privées.

3. Les problèmes liés à la sécurité nationale et aux activités criminelles peuvent justifier le recours exceptionnel aux technologies de surveillance des communications. Toutefois, les lois réglementant ce qui constitue l'intervention nécessaire, légitime et proportionnée de l'État en matière de surveillance des communications, sont souvent inadéquates ou inexistantes. Un cadre juridique national inadapté crée un terrain propice aux violations arbitraires et illégales du droit au secret des communications et porte ainsi également atteinte à la protection du droit à la liberté d'opinion et d'expression.

4. Dans des rapports antérieurs (A/HRC/17/27 et A/66/290), le Rapporteur spécial a analysé l'incidence sans précédent d'Internet sur le développement des possibilités offertes aux individus d'exercer leur droit à la liberté d'opinion et d'expression. Il s'est dit inquiet des multiples mesures adoptées par les États pour restreindre le flux de l'information en ligne ou pour lui faire obstacle, et a souligné la protection inadéquate du droit à la vie privée sur Internet.

5. En s'appuyant sur les précédentes analyses du Rapporteur spécial, le présent rapport vise à recenser les risques que posent les nouveaux moyens et modes de surveillance des communications pour les droits de l'homme, notamment pour les droits au respect de la vie privée et à la liberté d'opinion et d'expression.

6. Les termes suivants sont employés dans le présent rapport pour décrire les modes de surveillance des communications les plus courants:

a) Surveillance des communications: contrôle, interception, collecte, sauvegarde et conservation de l'information qui a été communiquée, retransmise ou recueillie sur les réseaux de communication;

b) Données des communications: renseignements sur les communications d'un individu (courriers électroniques, appels téléphoniques et messages textes envoyés et reçus, messages sur les réseaux sociaux et courrier postal), identité, comptes réseau, adresses, sites Web visités, livres et autres documents lus, consultés ou écoutés, recherches effectuées, ressources utilisées, échanges (origines et destinations des communications, personnes fréquentées, amis, famille, connaissances), et localisation temporelle et géographique d'un individu, (notamment sa proximité avec les autres);

c) Filtrage d'Internet: surveillance automatique ou manuelle des contenus Internet (notamment des sites Web, blogs, sources des médias en ligne, et courriers électroniques) exercée pour restreindre ou supprimer des textes, images, sites Web, réseaux, protocoles, activités ou services particuliers.

II. Activités du Rapporteur spécial

7. Durant la période à l'étude, le Rapporteur spécial a participé à de nombreuses manifestations nationales et internationales portant sur les questions auxquelles il s'était attaché dans ses précédents rapports telles que la liberté d'expression sur Internet, la prévention des discours haineux et la protection des journalistes. Il a accordé une attention particulière aux initiatives nationales visant à promouvoir la protection des journalistes; à cet égard, il a participé à des réunions portant sur les initiatives adoptées au Brésil, en Colombie, au Honduras et au Mexique. Il a également participé à la «Réunion interinstitutions des Nations Unies sur la sécurité des journalistes et la question de l'impunité», tenue en novembre 2012 à Vienne.

8. Son dernier rapport à l'Assemblée générale des Nations Unies mettait l'accent sur la prévention des discours haineux et de l'incitation à la haine[1]. Le même sujet a été traité lors d'une réunion parallèle à l'Assemblée générale, organisée conjointement par le Rapporteur spécial et le Conseiller spécial pour la prévention du génocide en février 2013. Au cours du même mois, le Rapporteur spécial s'est encore attaché à ces questions avec le lancement du «Plan d'action de Rabat sur l'interdiction de l'appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence», à Genève, et au cours du Cinquième forum mondial de l'Alliance des civilisations des Nations Unies, à Vienne.

9. Le Rapporteur spécial a entrepris une mission au Honduras du 7 au 14 août 2012. Ses principales conclusions et recommandations à ce sujet figurent dans l'additif du présent rapport (A/HRC/20/40/Add.1). En janvier 2013, le Gouvernement indonésien l'a invité à visiter le pays. Malheureusement, ce gouvernement a souhaité reporter la visite et de nouvelles dates doivent encore être fixées à ce sujet.

10. Pour préparer le présent rapport, le Rapporteur spécial a revu les études pertinentes et consulté des experts sur les questions relatives à la surveillance des communications. En décembre 2012, il a participé à l'Atelier sur la surveillance électronique et les droits de l'homme, organisé par la «Electronic Frontier Foundation». En février 2013, pour préparer le présent rapport, il a organisé une consultation d'experts qui est intervenue parallèlement aux activités de la «Réunion + 10 du Sommet mondial sur la société de l'information» tenue à l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) à Paris, où il a également participé à l'ouverture de la séance plénière.

III. Évolution des technologies de surveillance

11. L'innovation technologique a permis d'accroître les possibilités de communication et de liberté d'expression, en permettant l'anonymat, le partage rapide d'informations et le dialogue interculturel. Parallèlement, les évolutions technologiques ont également offert aux États de nouveaux moyens de surveillance et d'intervention dans la vie privée des individus.

12. Dès l'apparition de la première forme de communications à distance, les États ont cherché à intercepter et à surveiller les communications privées à des fins de maintien de l'ordre et de sûreté nationale. Par le biais des communications, les informations les plus personnelles et intimes, notamment les actes passés ou à venir d'un individu ou d'un groupe peuvent être révélés. Les communications représentent une source de preuve précieuse sur

[1] A/67/357.

laquelle les États peuvent s'appuyer pour prévenir ou poursuivre en justice les délits graves ou anticiper les cas d'urgence potentiels mettant en jeu la sécurité nationale.

13. Tout au long du XX^{e} siècle, les innovations technologiques ont changé la nature et les incidences de la surveillance des communications. Les moyens permettant aux individus de communiquer et la fréquence à laquelle ils peuvent le faire se sont considérablement développés. Le passage de la téléphonie fixe à la téléphonie mobile et la réduction des coûts des services de communication ont entraîné un considérable essor de l'usage du téléphone. L'avènement d'Internet a vu la naissance de nombreux nouveaux outils et applications pour communiquer gratuitement, ou à un coût très abordable. Ces avancées ont permis une plus grande connectivité, facilité la circulation globale de l'information et des idées, et accru les possibilités de croissance économique et d'évolution sociale.

14. Les technologies de l'information et des communications ont évolué, tout comme les moyens par lesquels les États ont cherché à surveiller les communications privées. L'usage accru du téléphone a engendré celui des écoutes qui consiste à placer un dispositif de surveillance sur une ligne téléphonique pour espionner les conversations privées. Avec le remplacement des réseaux téléphoniques analogiques par la fibre optique et les commutateurs numériques dans les années 1990, les États ont réorganisé la technologie de réseau pour inclure des capacités d'interception («portes dérobées») et pouvoir ainsi exercer une surveillance en rendant les réseaux téléphoniques modernes accessibles et commandés à distance.

15. Le dynamisme de la technologie a non seulement changé la pratique de la surveillance, mais également son «objet». En facilitant la création de divers moyens de communication et de partage de l'information, Internet a également favorisé le développement d'un grand nombre de données transactionnelles par et sur les individus. Ces renseignements, connus comme des données de communications ou métadonnées, incluent des informations personnelles sur les individus, leur localisation, leurs activités en ligne, et les connexions et informations liées aux courriers électroniques et aux messages qu'ils envoient ou reçoivent. Les données des communications peuvent être stockées et sont accessibles et consultables; leur divulgation aux pouvoirs publics et leur utilisation par ces derniers ne sont que très peu réglementées. L'analyse de ces données peut être à la fois très révélatrice et invasive, en particulier lorsqu'elles sont conjuguées et agrégées. De ce fait, les États s'appuient de plus en plus sur les données des communications pour favoriser le maintien de l'ordre ou les enquêtes portant sur la sécurité nationale. Ils imposent également la sauvegarde et la conservation de ces données pour pouvoir effectuer un historique de la surveillance.

16. L'évolution technologique s'est accompagnée d'un changement des comportements à l'égard de la surveillance des communications. Lorsque la pratique officielle des écoutes téléphoniques a débuté aux États-Unis d'Amérique, elle était exercée de manière restreinte et rarement sanctionnée par les tribunaux[2]. Elle a été considérée comme une telle menace pour le droit à la vie privée que son usage a dû être limité à la recherche et à la poursuite

[2] Lors de la première validation par la justice des écoutes téléphoniques, le juge Brandeis de la Cour suprême des États-Unis, a rédigé un avis fortement défavorable spécifiant que les écoutes téléphoniques étaient «un moyen subtil et plus radical d'empiéter sur la vie privée» qui ne pouvait se justifier en vertu de la Constitution. Dans une prévision d'une précision inquiétante, l'éminent juriste déclarait: «Des moyens peuvent un jour être inventés qui permettront au gouvernement, sans vider les tiroirs secrets des documents qu'ils contiennent, de les reproduire devant un tribunal, et d'exposer ainsi à un jury les faits les plus intimes de la vie d'un ménage. Les progrès des sciences psychiques et des sciences connexes peuvent fournir les moyens d'explorer les croyances, les pensées et les émotions inexprimées.». *Olmstead v. United States*, 277 U. S. 438 (1928).

des délits les plus graves. Toutefois, au fil du temps, les États ont étendu leurs pouvoirs de surveillance, en abaissant les seuils autorisés et en multipliant les justifications à cet égard.

17. Dans de nombreux pays, la législation et les pratiques en vigueur n'ont pas été révisées et mises à jour pour s'attacher à résoudre les menaces et les problèmes inhérents à la surveillance des communications à l'ère du numérique. Les notions traditionnelles d'accès à la correspondance écrite, par exemple, ont été introduites dans la législation autorisant l'accès aux ordinateurs personnels et aux autres technologies de l'information et de la communication, sans tenir compte de l'usage étendu de ces dispositifs et des incidences pour les droits des individus. Parallèlement, l'absence de législation pour réglementer la surveillance globale des communications et les modalités de partage a entraîné des pratiques ad hoc qui vont au-delà de la supervision d'une quelconque autorité indépendante. Actuellement, dans de nombreux États, divers services publics ont, à des fins multiples, accès aux données des communications, souvent sans autorisation judiciaire et sans dispositif indépendant de contrôle. En outre, les États ont cherché à adopter des dispositifs de surveillance qui visent à avoir un effet extraterritorial.

18. Les mécanismes relatifs aux droits de l'homme ont été également lents à évaluer les incidences en matière de droits fondamentaux d'Internet et des nouvelles technologies sur la surveillance des communications et sur l'accès aux données des communications. Les conséquences de l'extension des pouvoirs et des pratiques de surveillance des États pour les droits à la vie privée et à la liberté d'opinion et d'expression et l'interdépendance de ces deux droits, doivent encore être étudiées de manière approfondie par le Conseil des droits de l'homme, les titulaires de mandats au titre des procédures spéciales, ou les organes créés en vertu d'instruments internationaux relatifs aux droits de l'homme. Le présent rapport s'y emploie.

IV. Cadre international des droits de l'homme

19. Le droit à la liberté d'opinion et d'expression est garanti en vertu des articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques qui disposent que chacun a le droit d'avoir des opinions sans ingérence, et de rechercher, recevoir et transmettre des informations et des idées de toute espèce, par n'importe quel média et sans considération de frontières. Au niveau régional, ce droit est protégé par la Charte africaine des droits de l'homme et des peuples (art. 9), la Convention américaine relative aux droits de l'homme (art. 13) et la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (art. 10).

20. Tant au niveau national qu'international, le respect de la vie privée est unanimement reconnu comme un droit fondamental, consacré par la Déclaration universelle des droits de l'homme (art. 12), le Pacte international relatif aux droits civils et politiques (art. 17), la Convention relative aux droits de l'enfant (art. 16), et la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille (art. 14). Au niveau régional, le droit au respect de la vie privée est protégé par la Convention européenne des droits de l'homme (art. 8) et la Convention américaine relative aux droits de l'homme (art. 11).

21. Bien que l'obligation de protéger la vie privée soit largement admise, le contenu spécifique de ce droit n'a pas été pleinement exposé par les mécanismes internationaux de protection des droits fondamentaux lors de son intégration aux instruments des droits de l'homme mentionnés ci-dessus. L'absence d'énoncé explicite du contenu de ce droit a

contribué à en rendre l'application et le respect difficiles[3]. Le droit au respect de la vie privée étant un droit assorti de restrictions, son interprétation soulève des difficultés pour déterminer en quoi consiste la sphère privée et définir les notions de ce qui constitue l'intérêt général. L'évolution rapide et spectaculaire des technologies de la communication et de l'information survenue au cours des dernières décennies a également modifié de manière irréversible notre conception des frontières existant entre sphères publique et privée.

22. Le respect de la vie privée peut se définir comme la présomption selon laquelle les individus devraient disposer d'un domaine de développement autonome, d'échanges et de liberté, une «sphère privée» avec ou sans interaction avec autrui, libre de toute intervention de l'État et ingérence excessive non sollicitée d'autres individus[4]. Le droit au respect de la vie privée implique également la capacité des individus de déterminer qui détient l'information les concernant et comment cette information est employée.

23. Pour que les individus exercent leur droit au secret des communications, ils doivent pouvoir garantir que celles-ci restent privées, sûres et, s'ils le choisissent, anonymes. La confidentialité des communications implique que les individus puissent échanger des informations et des idées dans un espace inaccessible aux autres membres de la société, au secteur privé et enfin, à l'État lui-même. La sûreté des communications signifie que les personnes devraient être en mesure de vérifier que leurs communications ne sont reçues que par leurs destinataires, sans ingérence ou modification, et que celles qu'ils reçoivent sont également dépourvues de toute intrusion. L'anonymat des communications est l'un des progrès majeurs obtenus par Internet, et il permet aux individus de s'exprimer librement sans crainte de représailles ou de condamnation.

A. Interdépendance entre droit à la protection de la vie privée et droit à la liberté d'opinion et d'expression

24. Le droit au respect de la vie privée est souvent perçu comme un préalable essentiel à la réalisation du droit à la liberté d'expression. Une atteinte indue à la vie privée des personnes peut directement et indirectement limiter la liberté de développement et d'échange des idées. Les restrictions à l'anonymat des communications, par exemple, ont une incidence redoutable manifeste sur les victimes de toutes les formes de violence et d'abus qui peuvent être réticentes à les signaler par crainte de double victimisation. A cet égard, l'article 17 du Pacte international relatif aux droits civils et politiques traite directement de la protection contre l'ingérence avec la «correspondance», terme qui devrait être interprété de manière à englober toutes les formes de communication, en ligne et hors ligne[5]. Comme l'a relevé le Rapporteur spécial dans un précédent rapport[6], le droit à la confidentialité de la correspondance entraîne pour l'État l'obligation globale de garantir que les courriers électroniques et autres formes de communications en ligne parviennent réellement au destinataire prévu sans ingérence ou inspection des organes publics ou de tierces parties[7].

[3] UNESCO, Enquête à l'échelle mondiale sur la protection de la vie privée sur Internet et la liberté d'expression, 2012, p. 51.

[4] Lord Lester et D. Pannick (éd.). *Huam Rights law and Practice.* London, Butterworth, 2004, par. 4.82.

[5] Pacte international relatif aux droits civils et politiques, commentaire, p. 401.

[6] A/HRC/17/23.

[7] Pacte international relatif aux droits civils et politiques, commentaire, p.401.

25. Le Comité des droits de l'homme a analysé la teneur du droit au respect de la vie privée (art. 17) dans son observation générale n° 16 (1988), selon laquelle l'article 17 vise à protéger les personnes de toute immixtion illégale et arbitraire dans leur vie privée, leur famille, leur domicile ou leur correspondance, et les législations nationales doivent prévoir la protection de ce droit. Cette disposition impose les obligations spécifiques liées à la protection de la confidentialité des communications, en soulignant que «la correspondance devrait être délivrée au destinataire sans interception et sans avoir été ouverte ou lue d'une quelconque manière. La surveillance, électronique ou autre, l'interception de communications téléphoniques, télégraphiques et autres formes de communications, les écoutes téléphoniques et l'enregistrement des conversations, devraient être interdits»[8]. Il est aussi indiqué dans l'observation générale que «la collecte et la conservation d'informations personnelles sur les ordinateurs, les banques de données et autres dispositifs, par les autorités publiques ou des personnes ou organes privés, doivent être réglementées par la loi»[9]. A l'époque de l'adoption de cette observation générale, l'incidence des progrès technologiques en matière d'information et de communications sur le droit au respect de la vie privée était mal comprise.

26. Dans son observation générale n° 34 (2011) sur le droit à la liberté d'expression, le Comité des droits de l'homme a indiqué que les États parties devraient prendre en compte le fait que les évolutions technologiques en matière d'information et de communication ont considérablement modifié les pratiques de communication. Le Comité a également appelé les États parties à adopter toutes les dispositions nécessaires pour encourager l'indépendance de ces nouveaux médias. L'observation générale analyse également la relation entre protection de la vie privée et liberté d'expression et elle recommande aux États parties de respecter cet élément du droit à la liberté d'expression qui inclut la prérogative journalistique restreinte de ne pas divulguer les sources d'information[10].

27. Il existe aussi des tensions entre droit au respect de la vie privée et droit à la liberté d'expression, par exemple, lorsqu'une information jugée privée est diffusée par les médias. Dans ce sens, l'article 19 3) prévoit des restrictions à la liberté d'expression et d'information pour protéger les droits d'autrui. Toutefois, comme pour toutes les restrictions autorisées au droit à la liberté d'expression (voir ci-dessous), le principe de proportionnalité doit être strictement observé, sous peine de porter atteinte à la liberté d'expression. En particulier dans le domaine politique, toute atteinte à la bonne réputation des politiciens ne doit pas être autorisée, car sinon la liberté d'expression et d'information serait vidée de l'importance capitale qu'elle revêt pour se forger des opinions politiques[11], défendre la transparence et lutter contre la corruption. La jurisprudence internationale au niveau régional indique qu'en cas de conflit entre protection de la vie privée et liberté d'expression, il convient de se reporter à l'intérêt général pour les questions en cause[12].

B. Restrictions autorisées à la protection de la vie privée et à la liberté d'expression

28. Dans le cadre de l'article 17 du Pacte international relatif aux droits civils et politiques, des restrictions nécessaires, légitimes et proportionnées au droit à la vie privée

[8] Centre pour les droits civils et politiques, observation générale n° 16. (Observations générales), p. 8.
[9] Ibid., p. 10.
[10] Observation générale n° 34.
[11] Nowak, Manfred, Pacte international relatif aux droits civils et politiques: Commentaire (1993), p. 462.
[12] UNESCO, Enquête à l'échelle mondiale sur la protection de la vie privée sur Internet et la liberté d'expression, 2012, p. 53 et 99.

sont possibles au moyen de limitations licites. Contrairement aux dispositions de l'article 19, paragraphe 3, qui énoncent les conditions dans lesquelles des restrictions peuvent être permises[13], l'article 17 ne contient pas de clause restrictive. Malgré ces différences de formulation, l'article 17 devrait également être interprété comme incluant des critères relatifs aux restrictions autorisées, déjà décrits dans d'autres observations générales du Comité des droits de l'homme[14].

29. Á cet égard, le Rapporteur spécial a estimé que le droit au respect de la vie privée devrait être soumis aux mêmes conditions de restrictions autorisées que le droit à la liberté de circulation, telles qu'elles sont définies dans l'observation générale n° 27[15]. Ces conditions sont notamment les suivantes:

a) Toute restriction doit être prévue par la loi (par. 11 et 12);

b) Les restrictions ne doivent pas porter atteinte à l'essence même d'un droit fondamental (par. 13);

c) Les restrictions doivent être nécessaires dans une société démocratique (par. 11);

d) Le pouvoir exercé pour appliquer les restrictions ne doit pas être illimité (par. 13);

e) Pour qu'une restriction soit autorisée, il ne suffit pas qu'elle serve l'un des objectifs légitimes énoncés. Elle doit être indispensable à l'obtention de cet objectif (par. 14);

f) Les mesures restrictives doivent être conformes au principe de proportionnalité; elles doivent être appropriées pour remplir leur fonction de protection, constituer le moyen le moins perturbateur parmi ceux susceptibles d'obtenir le résultat recherché, et être proportionnées à l'intérêt à protéger (par. 14 et 15).

C. Examens récents menés par les mécanismes internationaux de défense des droits de l'homme

30. Dans de précédents rapports, le Rapporteur spécial a évalué l'incidence d'Internet sur l'exercice du droit à la liberté d'opinion et d'expression (A/HRC/17/27 et A/66/290). Il a relevé que même si les usagers peuvent jouir d'un relatif anonymat sur Internet, les États et les acteurs privés ont également accès à de nouvelles technologies qui leur permettent de surveiller et de recueillir des informations sur les communications et les activités des individus. Ces technologies peuvent potentiellement violer le droit au respect de la vie privée; elles portent ainsi atteinte à la confiance des usagers et à la sécurité sur Internet et entravent la libre circulation de l'information et des idées en ligne. Le Rapporteur spécial a exhorté les États à adopter des lois efficaces de protection de la vie privée et des données conformément aux normes relatives aux droits de l'homme, et toutes les mesures appropriées pour que les individus puissent s'exprimer de façon anonyme sur Internet[16].

[13] La liste des restrictions autorisées figure également à l'article 12 3), relatif au droit à la liberté de circulation et à la liberté de choisir sa résidence; à l'article 18 3) relatif au droit à la liberté de pensée, de conscience et de religion; à l'article 21, relatif au droit de réunion pacifique; et à l'article 22 2) relatif au droit à la liberté d'association.

[14] Ibid.

[15] Voir également observation générale n° 34 – Pacte international relatif aux droits civils et politiques.

[16] A/HRC/17/27, p. 22.

31. Les autres experts mandatés au titre des procédures spéciales ont étudié la question des ingérences avec le droit au respect de la vie privée. Le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a étudié l'évolution des pratiques et des technologies de surveillance qui ont fâcheusement porté atteinte au droit au respect de la vie privée, sous prétexte de lutte antiterroriste[17]. Il a souligné que ces mesures ont non seulement conduit à des violations du droit au respect de la vie privée, mais qu'elles ont aussi eu un impact sur le droit à une procédure régulière et sur les droits à la liberté de circulation, à la liberté d'association et à la liberté d'expression. Il a exhorté les gouvernements à présenter en détail la manière dont leurs politiques de surveillance respectent les principes de proportionnalité et de nécessité, conformément aux normes internationales relatives aux droits de l'homme, et les mesures adoptées pour éviter les abus. Le Rapporteur spécial a également demandé l'adoption de lois globales de protection des données et de la vie privée et la création d'organes de surveillance efficaces et indépendants mandatés pour contrôler l'usage de techniques de surveillance intrusives et le traitement des données à caractère personnel. Il a en outre appelé à consacrer des moyens de recherche et de développement aux techniques permettant de renforcer la protection de la vie privée.

32. D'autres mécanismes de protection des droits de l'homme ont également récemment prêté attention à l'incidence de la surveillance des communications sur la protection des droits à la vie privée et à la liberté d'expression. Le Comité des droits de l'homme a, par exemple, fait part de ses préoccupations concernant les allégations de surveillance par l'État de l'usage de l'Internet, et de blocage de l'accès à certains sites web[18] et il a recommandé de réviser la législation qui donne à l'exécutif des pouvoirs de surveillance étendus en matière de communications électroniques[19]. L'Examen périodique universel a également inclus des recommandations pour garantir, par exemple, que la législation relative à l'Internet et aux autres nouvelles techniques de communication respecte les obligations internationales en matière de droits de l'homme[20].

V. Modalités de la surveillance des communications

33. Les technologies modernes de surveillance et les dispositions qui permettent aux États de s'immiscer dans la vie privée d'un individu menacent de gommer la séparation existant entre sphères publique et privée. Elles facilitent la surveillance arbitraire et attentatoire à la vie privée des individus, lesquels peuvent même ne pas être en mesure de savoir qu'ils ont fait l'objet d'une telle surveillance, et se trouver seuls pour la contester. Les progrès technologiques permettent à l'État de se livrer à des activités de surveillance qui ne sont plus limitées par des critères d'échelle ou de durée. La baisse des coûts de la technologie et le stockage des données ont éliminé les obstacles financiers ou pratiques à l'exercice de ce type d'activités. En conséquence, l'État dispose à présent plus que jamais de moyens accrus pour mener des activités de surveillance simultanées, attentatoires à la vie privée, ciblées et à grande échelle.

[17] A/HRC/13/37.
[18] CCPR/C/IRN/CO/3.
[19] CCPR/C/SWE/CO/6.
[20] A/HRC/14/10.

A. Surveillance ciblée des communications

34. Les États ont accès à diverses techniques et technologies pour surveiller les communications privées d'un individu ciblé. Les capacités d'interception en temps réel permettent aux États d'écouter et d'enregistrer les appels téléphoniques passés sur une ligne fixe ou un téléphone portable par n'importe quel individu, grâce à l'utilisation des capacités d'interception destinées à la surveillance par l'État que tous les réseaux de transmission sont tenus d'intégrer à leurs systèmes[21]. Un individu peut être localisé et ses messages textes peuvent être lus et enregistrés. En plaçant un dispositif de surveillance sur la connexion Internet d'un lieu ou d'une personne donnés, les services publics peuvent également surveiller les activités en ligne de la personne en question, notamment les sites Web qu'elle visite.

35. L'accès au contenu stocké des courriers et des messages électroniques d'un individu, outre l'accès aux données de communications connexes, peut être obtenu par le biais des entreprises de l'Internet et de ses fournisseurs d'accès. Un motif d'inquiétude tient à l'initiative de l'autorité européenne qui supervise l'élaboration et l'application des normes – l'Institut européen des normes de télécommunications – et qui vise à contraindre les fournisseurs d'informatique en nuage[22] à concevoir des «capacités d'interception légales» dans la technologie nuagique pour permettre aux pouvoirs publics d'accéder directement aux contenus stockés par ces prestataires, y compris aux courriels, messages et messages vocaux[23].

36. Les États peuvent localiser les déplacements de téléphones cellulaires spécifiques, identifier tous les individus équipés d'un téléphone portable dans une zone donnée et intercepter les appels et les messages textes par différentes méthodes. Certains États utilisent des dispositifs de surveillance des mobiles hors antenne, appelés appareils de saisie de l'identité des abonnés à des services internationaux de téléphonie mobile, qui peuvent être installés de manière temporaire (sur les lieux d'une manifestation ou d'un défilé, par exemple), ou permanente (dans un aéroport ou autres points de passage des frontières). Ces appareils imitent les antennes-relais des téléphones mobiles en envoyant des signaux aux téléphones mobiles et en leur répondant, de manière à extraire le numéro de carte du module d'identification unique de l'abonné (SIM) de tous les téléphones mobiles situés dans un périmètre donné.

37. Les États acquièrent également de plus en plus souvent des logiciels qu'ils peuvent utiliser pour infiltrer l'ordinateur, le téléphone portable ou autres appareils numériques d'un particulier[24]. Les logiciels d'intrusion offensive, notamment ceux appelés «chevaux de Troie» (connus également sous le nom de logiciels espions ou malveillants), peuvent être employés pour mettre sous tension le microphone ou la caméra d'un appareil, surveiller l'activité de l'appareil en question, et avoir accès aux informations qui y sont stockées, les

[21] Voir par exemple la loi de 1994 des États-Unis sur l'aide des communications à l'application de la loi, (États-Unis); la loi de 1997 sur les télécommunications, chap. 15 (Australie); la loi de 2000 sur la réglementation des pouvoirs d'enquête, art. 12 à 14 (Royaume-Uni); la loi de 2004 sur les télécommunications (capacité d'interception).

[22] Un fournisseur d'informatique en nuage offre des services interconnectés de stockage en ligne des données.

[23] ETSI DTR 101 567 VO.0.5 (2012-14), Projet de rapport technique: interception illégale; Nuage/Services virtuels.

[24] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin et Natalia Torres, Enquête à l'échelle mondiale sur la protection de la vie privée sur Internet et la liberté d'expression, *Séries de* l'*UNESCO sur la liberté de l'Internet* (2012), p. 41.

modifier ou les effacer. Ce type de logiciel, pratiquement indétectable, offre à l'État un total contrôle sur l'appareil infiltré.

B. Surveillance de masse des communications

38. Les coûts de la surveillance à grande échelle tout comme les obstacles logistiques à cette surveillance diminuent rapidement car les technologies permettant l'interception, la surveillance et l'analyse à grande échelle des communications abondent. A l'heure actuelle, certains États ont la capacité de suivre et d'enregistrer les communications téléphoniques et en ligne au niveau national. En plaçant des dispositifs de surveillance sur des câbles à fibre optique par lesquels la majorité des données de communications numériques transitent, et en employant des mots, des voix et des paroles de reconnaissance, les gouvernements peuvent obtenir un contrôle quasi complet des communications téléphoniques et en ligne. Ce type de systèmes aurait, selon certaines sources, été adopté notamment par les Gouvernements égyptien et libyen avant l'avènement du Printemps arabe[25].

39. Dans de nombreux États, le stockage obligatoire des données facilite la collecte massive des données de communications qui peuvent être ultérieurement filtrées et analysées. La technologie permet à l'État d'explorer les appels téléphoniques et les messages textes pour identifier l'usage de certains mots, voix ou phrases, ou filtrer l'activité sur Internet pour déterminer quand un individu accède à certains sites Web ou à des ressources en ligne particulières. Des «boîtes noires» peuvent être conçues pour inspecter des données transmises par l'Internet, de manière à filtrer et à analyser toutes les informations relatives à l'activité sur le Web. Cette méthode, appelée «inspection des paquets en profondeur», permet à l'État d'aller au-delà de la simple connaissance des sites visités par un individu; elle analyse leur contenu. Elle aurait par exemple, été employée par les États confrontés aux récents soulèvements populaires au Moyen-Orient et en Afrique du Nord[26].

40. Les États recourent régulièrement aujourd'hui à un autre outil: la surveillance des médias sociaux. Ils ont la capacité matérielle de surveiller les activités sur les sites de réseaux sociaux, les blogs et les médias pour analyser les connexions et les relations, les opinions et les associations, et même les localisations. Les États peuvent également appliquer des technologies très sophistiquées d'exploration de données aux informations de notoriété publique ou aux données de communications fournies par des prestataires de service tiers. À un niveau plus élémentaire, les États ont également acquis les moyens techniques d'obtenir les noms d'utilisateurs et les mots de passe d'accès aux réseaux sociaux tels que Facebook[27].

C. Accès aux données des communications

41. Outre l'interception et le suivi du contenu des communications des individus, les États peuvent également chercher à avoir accès aux données des communications détenues par des prestataires de service tiers et par les entreprises d'Internet. Avec l'accroissement progressif de la collecte, par le secteur privé, de données variées qui dévoilent des informations sensibles sur la vie quotidienne des gens, et les individus ou les entreprises qui

[25] Parlement européen, Direction générale des politiques extérieures; Département des politiques, Après le printemps arabe: Nouvelles voies pour les droits de l'homme et Internet dans la politique étrangère européenne (2012), p. 9 et 10.

[26] Mendel *et al.,* op. cit., p. 43.

[27] Parlement européen, op. cit., p. 6.

choisissent des prestataires de services tiers pour stocker le contenu de leurs communications, tels que messages vocaux, courriels et documents, l'accès aux données des communications est une technique de surveillance de plus en plus prisée des États.

42. Les données des communications recueillies par les prestataires de service tiers, notamment les grandes entreprises de l'Internet, peuvent être utilisées par l'État pour composer un profil détaillé des individus concernés. Lorsqu'ils sont consultés et analysés, même les enregistrements apparemment anodins de transactions relatives aux communications peuvent collectivement créer un profil de la vie privée d'un individu, notamment son état de santé, ses opinions et/ou son appartenance politique et religieuse, ses relations et ses intérêts, en révélant autant de détails ou même davantage que ceux qui seraient perceptibles d'après le contenu des seules communications[28]. En combinant les renseignements sur les relations, le lieu, l'identité et l'activité, les États peuvent suivre les déplacements des individus et leurs activités dans différents domaines, depuis leur destination de voyage, le lieu où ils étudient, ce qu'ils lisent et qui ils fréquentent.

43. Les États ont de plus en plus souvent accès aux données des communications. Au cours des trois années pendant lesquelles Google a signalé le nombre des demandes de données de communications qu'il a reçues, ce nombre a presque doublé, pour passer de 12 539 au cours des six derniers mois de 2009, à 21 389 au cours des six derniers mois de 2012[29]. Au Royaume-Uni, où les forces de l'ordre sont habilitées à s'accorder elles-mêmes les demandes de données de communications qu'elles formulent, environ 500 000 demandes de ce type ont été signalées chaque année[30]. En République de Corée, pays de près de 50 millions d'habitants, environ 37 millions de demandes de données de communications ont été signalées chaque année[31].

D. Filtrage et censure de l'Internet

44. Les progrès technologiques n'ont pas seulement facilité l'accès aux communications et leur interception dans des cas spécifiques; ils ont également permis aux États d'opérer un filtrage des activités en ligne à grande échelle, éventuellement à l'échelle nationale. Dans de nombreux pays, le filtrage de l'Internet est effectué sous couvert de préserver l'harmonie sociale ou d'éliminer les propos haineux, mais il sert en fait à étouffer opposition, critique ou militantisme.

45. Les techniques de filtrage susmentionnées facilitent également la surveillance des activités sur le Web en permettant à l'État de détecter les images, les mots, les adresses de sites ou autres contenus interdits, et de les censurer ou de les modifier. Les États peuvent employer ces technologies pour détecter l'usage de mots et de phrases spécifiques de manière à en censurer ou à en réglementer l'usage, ou à identifier les individus qui les emploient. Dans les pays à fort degré de pénétration d'Internet, le filtrage permet, selon les

[28] Alberto Escudero-Pascual et Gus Hosein, "Questioning lawful access to traffic data", *Communications de l'ACM (Association computing machiner)*, vol. 47 Point 3, mars 2004, p. 77 à 82.

[29] Voir http://www.google.com/transparencyreport/userdatarequests/.

[30] Voir http://www.intelligencecommissioners.com/docs/0496.pdf.

[31] Money Today, 23 octobre, 2012, mentionne la révélation de la Korean Communication Commission pour le rapport d'audit annuel de 2013 à la députée Yoo Seung-Hui, http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1.

informations obtenues, de censurer le contenu des sites Web et les communications et il facilite la surveillance des défenseurs des droits de l'homme et des militants[32].

46. Outre les technologies qui facilitent le filtrage et la censure, nombre d'États organisent un filtrage manuel sur Internet, en mettant en place des forces de police et des inspecteurs en ligne qui surveillent matériellement le contenu des sites Web, les réseaux sociaux, les blogs et autres formes de médias. Dans certains États, des «forces de cyberpolice» sont chargées d'inspecter et de contrôler l'Internet, de rechercher des sites Web et les nœuds critiques qu'ils peuvent contenir (en particulier dans les forums de discussion en ligne), en vue de bloquer ou de fermer les sites Web dont le gouvernement désapprouve le contenu, notamment les critiques à l'égard du pouvoir en place. Cette surveillance est confiée à des intermédiaires privés tels que des moteurs de recherche et des plates-formes de réseaux sociaux, grâce à des lois qui élargissent la responsabilité des contenus prohibés, de l'intervenant original à l'ensemble des intermédiaires.

E. Restrictions à l'anonymat

47. L'une des avancées majeures liée à l'avènement d'Internet a été de pouvoir accéder à des informations, les transmettre de manière anonyme, et communiquer sans risque, sans avoir à s'identifier, et ce, grâce à l'absence de «couche d'identité» d'accès à Internet: initialement, il était impossible de savoir qui était derrière une communication spécifique, une adresse de courrier électronique ou même un ordinateur donné. Toutefois, au nom de la sécurité et du maintien de l'ordre, les États ont progressivement éliminé les possibilités de communication anonymes. Dans nombre d'entre eux, les individus doivent s'identifier dans les cybercafés et leurs activités sur les ordinateurs publics sont enregistrées. L'identification et l'enregistrement sont également de plus en plus souvent requis pour acheter une carte SIM ou un téléphone mobile, visiter certains sites Web importants, ou faire des commentaires sur les sites des médias ou les blogs.

48. Les restrictions à l'anonymat facilitent la surveillance des communications par l'État en simplifiant l'identification des individus qui accèdent à des contenus interdits ou qui les diffusent, et elles les rendent plus vulnérables aux autres formes de surveillance exercées par l'État.

49. Dans ce sens, les restrictions à l'anonymat ont un effet fâcheux en décourageant la libre expression de l'information et des idées. Elles peuvent également se traduire par une exclusion de facto des individus des sphères sociales essentielles, en sapant leurs droits de s'exprimer et de s'informer, et en renforçant les inégalités sociales. En outre, les restrictions à l'anonymat permettent au secteur privé de collecter et de réunir de grandes quantités de données, en confiant largement aux entreprises la charge et la responsabilité de protéger le caractère privé et la sécurité de ces données.

VI. Préoccupations liées aux normes juridiques nationales

50. De manière générale, la législation n'a pas suivi le rythme des changements technologiques. Dans la plupart des États, les normes juridiques sont soit inexistantes, soit inadéquates pour faire face aux conditions modernes de surveillance des communications. De ce fait, les États cherchent de plus en plus à justifier l'usage de nouvelles technologies

[32] Parlement européen, Direction générale des politiques extérieures, Département des politiques, Après le printemps arabe: Nouvelles voies pour les droits de l'homme et Internet dans la politique étrangère européenne (2012), p. 12.

dans le cadre des anciennes structures juridiques, sans admettre que les capacités étendues dont ils jouissent à présent vont nettement au-delà. Dans de nombreux pays, cela signifie que des dispositions juridiques vagues et approximatives sont invoquées pour légitimer et approuver l'usage de techniques gravement intrusives. En l'absence de lois explicites autorisant ce type de technologies et techniques et définissant le champ de leur utilisation, les individus ne peuvent en prévoir – ou même en connaître – l'application. Parallèlement, des textes sont adoptés pour élargir le champ des exceptions liées à la sécurité nationale, en prévoyant la légitimisation des techniques de surveillance intrusives sans contrôle ou examen indépendant.

51. Des normes juridiques inadéquates aggravent le risque de violation des droits fondamentaux des individus, y compris le droit à la protection de la vie privée et le droit à la liberté d'expression. Elles ont également une incidence négative sur divers groupes – membres de certains partis politiques, syndicalistes ou minorités nationales, ethniques et linguistiques, par exemple – qui peuvent être plus vulnérables à la surveillance des communications exercée par l'État. Sans protection juridique forte, journalistes, défenseurs des droits de l'homme et militants politiques risquent de faire l'objet d'activités de surveillance arbitraires.

52. La surveillance des défenseurs des droits de l'homme dans de nombreux pays a été bien documentée. Les défenseurs des droits de l'homme et les militants politiques ont alors signalé l'espionnage de leurs appels téléphoniques, de leurs courriers électroniques et de leurs déplacements. La dépendance des journalistes à l'égard des échanges en ligne les rend également particulièrement vulnérables à la surveillance des communications. Pour recevoir et s'efforcer d'obtenir des informations de sources confidentielles, notamment de personnes dénonçant des abus, ils doivent pouvoir compter sur la confidentialité, la sécurité et l'anonymat de leurs échanges. Un milieu dans lequel la surveillance est courante et non restreinte par le respect de la légalité ou par un contrôle juridictionnel ne peut assurer la pérennité de la présomption de protection des sources. Même un recours restreint, non transparent, non documenté à la surveillance par l'exécutif, peut avoir une incidence fâcheuse sans justification précise et publique de son utilisation, et sans contrôle reconnu et pondération pour prévenir les abus.

53. Les sous-sections suivantes recensent les préoccupations courantes concernant les lois qui autorisent la surveillance des communications par l'État dans des situations portant atteinte aux droits à la liberté d'expression et au respect de la vie privée.

A. Absence de contrôle juridictionnel

54. Bien que la surveillance des communications doive traditionnellement être autorisée par le pouvoir judiciaire, cette règle est de plus en plus souvent allégée ou supprimée. Dans certains pays, l'interception des communications peut être autorisée par un ministre du gouvernement, son délégué ou une commission. Au Royaume-Uni par exemple, elle est autorisée par le Secrétaire d'État[33]; au Zimbabwe, par le Ministre des transports et des communications[34]. Progressivement, la surveillance des communications peut également être autorisée à grande échelle et de manière non ciblée, sans que les forces de l'ordre aient à établir au cas par cas les éléments de fait à l'origine de la surveillance.

55. De nombreux États ont supprimé la nécessité pour les organes chargés de l'application des lois de faire rapport au tribunal à des fins de supervision permanente,

[33] Art. 5, loi de 2000 sur la réglementation des pouvoirs d'enquête.
[34] Art. 5, loi de 2006 sur l'interception des communications.

après l'adoption d'une ordonnance d'interception. En vertu de la loi kényane de prévention du terrorisme de 2012 par exemple, l'interception des communications peut s'effectuer pour une durée illimitée, sans que les organes chargés de l'application des lois aient à en rendre compte à un tribunal ou à demander une prolongation. Certains États imposent un délai à l'exécution des ordonnances d'interception, mais permettent aux forces de l'ordre de renouveler ces ordonnances de manière répétée et pour une durée indéterminée.

56. Même lorsqu'une autorisation judiciaire est légalement requise, il s'agit souvent de fait d'une approbation arbitraire des demandes des forces de l'ordre, ce qui est particulièrement le cas lorsque le seuil à ne pas dépasser par celles-ci est bas. Par exemple, la loi ougandaise de 2010 sur la réglementation de l'interception des communications exige seulement des autorités répressives qu'elles démontrent l'existence de fondements «raisonnables» pour autoriser l'interception. Dans de tels cas, la charge de la preuve pour établir la nécessité de la surveillance est extrêmement faible, compte tenu du risque de voir cette surveillance se traduire par des enquêtes, une discrimination ou des violations des droits de l'homme. Dans d'autres pays, tout un arsenal de lois complexes autorise l'accès aux communications et leur surveillance dans diverses situations. En Indonésie par exemple, la loi sur les psychotropes, la loi sur les stupéfiants, la loi concernant l'information et les transactions électroniques, la loi sur les télécommunications et la loi sur la corruption contiennent toutes un volet relatif à la surveillance des communications. Au Royaume-Uni, plus de 200 organismes, forces de police et autorités pénitentiaires sont autorisés à recueillir les données des communications dans le cadre de la loi de 2000 sur la réglementation des pouvoirs d'enquête. De ce fait, il est difficile aux individus de prévoir quand et par quel organisme public ils peuvent être soumis à une surveillance.

57. Dans de nombreux États, les prestataires des services de communications sont contraints de modifier leur infrastructure pour permettre une surveillance directe, éliminant ainsi toute possibilité de contrôle juridictionnel. Par exemple, en 2012, les Ministères colombiens de la justice et des technologies de l'information et de la communication, ont publié un décret exigeant des prestataires de services téléphoniques la mise en place d'une infrastructure autorisant l'accès direct de la police judiciaire aux communications, sans ordonnance du Ministre de la justice[35]. La loi de l'Ouganda 2010 susmentionnée, relative à la réglementation de l'interception des communications (art. 3), prévoit la création d'un centre de contrôle et impose aux prestataires des services téléphoniques de lui transmettre les communications interceptées (art. 8 1) f). Le Gouvernement indien propose d'installer un système de surveillance centralisé qui dirigera toutes les communications vers le Gouvernement central, en autorisant les services de sécurité à court-circuiter l'interaction avec le prestataire de service[36]. Ce type de dispositifs place la surveillance des communications hors du champ de l'autorisation judiciaire et permet une surveillance non réglementée, secrète, en éliminant toute transparence ou obligation de rendre des comptes de la part de l'État.

B. Exceptions au titre de la sécurité nationale

58. Les notions vagues et imprécises de «sécurité nationale» sont devenues dans de nombreux pays une justification acceptable à l'accès aux communications et à leur interception. En Inde par exemple, la loi 2008 sur les technologies de l'information autorise l'interception des communications dans l'intérêt *notamment* de «la souveraineté, l'intégrité

[35] Décret 1704 des Ministères de la justice et des technologies de l'information et de la communication. Extrait du Code de procédure pénale de 2004.

[36] Ministère des communications. Gouvernement indien. Rapport annuel 2011-2012, p. 58 – http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf.

ou la défense de l'Inde, des relations amicales avec les États étrangers, de l'ordre public et des enquêtes sur les infractions» (art. 69).

59. Dans de nombreux cas, les services de renseignement nationaux jouissent également d'une exemption sans réserve de l'exigence d'autorisation judiciaire. Par exemple, aux États-Unis, la loi sur la surveillance du renseignement étranger habilite l'Office national de sécurité à intercepter les communications sans autorisation judiciaire lorsqu'une partie à la communication est située en dehors des États-Unis et qu'un participant est raisonnablement soupçonné d'appartenir à une organisation terroriste désignée par l'État. La loi allemande autorise l'écoute automatique, sans autorisation, des communications nationales et internationales par les services nationaux de renseignement, à des fins de protection de l'ordre démocratique libre, de l'existence ou de la sécurité de l'État[37]. En Suède, la loi sur la surveillance des transmissions autorise l'interception des communications après autorisation de la Cour du renseignement étranger. En République-Unie de Tanzanie, la loi de 1996 concernant les services de renseignement et de sécurité habilite les services secrets du pays à mener des enquêtes, notamment sur tout individu ou organe dont il y a de bonnes raisons de penser qu'il constitue un risque, une source de risque, ou une menace pour la sécurité de l'État.

60. L'utilisation d'une notion imprécise de sécurité nationale pour justifier des restrictions invasives à l'exercice des droits de l'homme soulève de vives inquiétudes[38]. Cette notion, définie de manière schématique, est donc propice aux manipulations de l'État pour justifier des actions qui ciblent les groupes vulnérables tels que défenseurs des droits de l'homme, journalistes ou militants. Elle sert aussi à autoriser souvent inutilement le secret autour des enquêtes ou des activités de maintien de l'ordre, portant ainsi atteinte aux principes de transparence et de responsabilité.

C. Accès non réglementé aux données des communications

61. L'accès aux données des communications détenu par les prestataires nationaux de services de communications est souvent autorisé par la législation ou par une clause associée à la délivrance des licences. De ce fait, les États ont généralement carte blanche pour accéder aux données des communications et ne sont soumis qu'à peu de surveillance ou de réglementation. Par exemple, une loi brésilienne de 2012 sur le blanchiment d'argent confère à la police le pouvoir d'accéder à l'enregistrement des informations à partir des fournisseurs d'accès à Internet et des prestataires de communications, sans ordonnance du tribunal[39]. Au niveau international, les traités d'assistance mutuelle réglementent l'offre d'accès aux données des communications. Toutefois, cette coopération intervient souvent en marge de toute légalité en fonction du bon vouloir du prestataire de service ou de l'entreprise de l'Internet. L'accès aux données des communications peut ainsi être obtenu dans de nombreux États, sans autorisation indépendante et avec un contrôle limité.

D. Surveillance extrajuridique

62. Divers moyens de surveillance cités plus haut sortent des cadres juridiques en vigueur mais ont néanmoins été largement adoptés par les États. Les logiciels d'intrusion offensive tels que les chevaux de Troie, ou les capacités d'interception de masse,

[37] Loi G-10.

[38] Résolutions contre le terrorisme du Conseil des droits de l'homme.

[39] Loi fédérale brésilienne 12683/2012. Art. 17-B. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

constituent une telle remise en cause des notions traditionnelles de surveillance qu'ils ne peuvent être conciliés avec les lois en vigueur sur la surveillance et l'accès aux données privées. Il ne s'agit pas simplement de nouvelles méthodes de surveillance, mais de nouvelles formes de surveillance. Du point de vue des droits de l'homme, l'usage de ces technologies est extrêmement préoccupant. Les chevaux de Troie par exemple, permettent à un État d'avoir accès aux appareils, mais également de modifier – par erreur ou à dessein – les données qu'ils contiennent. Cela porte atteinte non seulement au droit à la protection de la vie privée, mais aussi aux droits d'équité procédurale en cas d'utilisation de ce type de preuve dans les procès. La technique d'interception de masse élimine toute considération de proportionnalité, en permettant une surveillance indiscriminée. L'État peut ainsi copier et contrôler chaque acte de communication pris isolément, dans un pays ou une zone donnée, sans avoir à obtenir d'autorisation pour chaque cas individuel d'interception.

63. Souvent, les gouvernements ne reconnaissent pas l'utilisation de ces technologies à des fins de surveillance, ou font valoir qu'elles sont légitimement employées dans le cadre de la législation en vigueur concernant la surveillance. Bien que de toute évidence de nombreux États possèdent des logiciels d'intrusion offensive, telle la technique du cheval de Troie, le fondement juridique à leur utilisation n'a été publiquement débattu dans aucun pays, à l'exception de l'Allemagne. Dans ce contexte, le Land de Rhénanie du Nord-Westphalie a promulgué en 2006 une législation qui autorise «l'accès secret à un système informatique» (par. 5.2 n° 11, loi de protection de la Constitution de la Rhénanie du Nord-Wesphalie) conçu sous forme d'infiltration technique effectuée en installant un programme espion, ou en tirant partie des failles de sécurité du système. La Cour constitutionnelle fédérale allemande a invalidé la loi en février 2008, jugeant que de telles mesures ne seraient conformes aux droits de l'homme que si elles étaient soumises à examen et à une autorisation judiciaire, et intervenaient seulement si un intérêt majeur au regard de la loi se trouvait concrètement menacé[40].

E. Application extraterritoriale des lois concernant la surveillance

64. Suite au flux international accru des données et au fait que la majorité des communications sont stockées par des prestataires de service tiers étrangers, divers États ont commencé à adopter des lois les habilitant à mener une surveillance extraterritoriale ou à intercepter les communications à l'étranger, ce qui pose de sérieux problèmes eu égard à la perpétration extraterritoriale de violations des droits fondamentaux et à l'incapacité des individus de savoir s'ils font l'objet d'une surveillance étrangère, de contester les décisions concernant cette surveillance, ou de chercher des recours. En Afrique du Sud par exemple, le projet de loi portant modification des lois sur les renseignements généraux prévoit la surveillance des communications étrangères en dehors du pays, ou passant par le pays[41]. En octobre 2012, le Ministère néerlandais de la justice et de la sécurité a proposé au Parlement des Pays-Bas des amendements législatifs qui autoriseraient la police à pénétrer par effraction dans les ordinateurs et les téléphones mobiles, à la fois aux Pays-Bas et à l'étranger, en vue d'installer des logiciels espions pour rechercher et détruire des données[42]. En décembre 2012, l'Assemblée nationale du Pakistan a adopté la loi 2012 concernant l'impartialité des procès, dont le paragraphe 31 prévoit l'exécution de mandats de surveillance dans les juridictions étrangères. Plus tard, ce même mois, les États-Unis ont

[40] Disponible en allemand. BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1-67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

[41] Art.1.c. Projet de loi portant modification des lois sur les renseignements généraux. Disponible à l'adresse: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

[42] Voir http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware.

renouvelé la loi de 2008 portant modification des procédures de surveillance de l'activité de renseignement à l'étranger, qui étend les pouvoirs de surveillance du Gouvernement sur les ressortissants étrangers en dehors des États-Unis (par. 1881a), y compris sur tout individu étranger dont les communications sont hébergées par les services informatiques en nuage situés aux États-Unis (tels Google et autres grandes entreprises d'Internet)[43]. Toujours en 2012, l'Institut européen des normes de télécommunications a créé des projets de normes concernant l'interception par les gouvernements européens des services infonuagiques étrangers[44]. Ces innovations laissent entrevoir une tendance alarmante à l'extension des pouvoirs de surveillance au-delà des frontières territoriales, augmentant ainsi le risque d'accords de coopération entre services chargés du maintien de l'ordre et services de sécurité pour permettre la levée des restrictions légales nationales.

F. Conservation obligatoire des données

65. Pour accroître le stockage des données de communications auxquelles ils ont accès, certains États adoptent des lois de conservation obligatoire des données exigeant des fournisseurs d'accès à Internet et des prestataires de service des télécommunications (appelés collectivement «prestataires des services de communications») qu'ils collectent et préservent en permanence le contenu des communications et les renseignements relatifs aux activités en ligne des usagers. Ces lois permettent la compilation de l'historique des courriels et des messages, des lieux, des échanges amicaux et familiaux, etc., d'un individu donné.

66. Pour fournir des services à leurs utilisateurs, les prestataires des services de communications donnent aux appareils ou au réseau des abonnés une adresse de protocole Internet (IP)[45] qui change périodiquement. Les données concernant une adresse IP peuvent servir à établir l'identité d'un individu, à le localiser et à suivre ses activités en ligne. Les lois concernant la conservation obligatoire des données obligent les prestataires des services de communications à conserver un certain temps des archives de leurs attributions d'adresses IP, donnant ainsi à l'État plus de latitude pour exiger d'eux qu'ils identifient un individu en fonction d'une adresse IP particulière à une date et à une heure données. Des États cherchent également à présent à contraindre les prestataires de services tiers à collecter et à conserver l'information qu'ils ne collecteraient pas d'ordinaire.

67. Les lois nationales relatives à la conservation des données sont invasives et coûteuses, et elles menacent les droits relatifs à la protection de la vie privée et à la liberté d'expression. En contraignant les prestataires des services de communications à créer de grandes bases de données pour savoir qui communique avec qui, via un téléphone ou l'Internet, la durée de l'échange, et la localisation des usagers, et à conserver ces informations (quelquefois pendant des années), les lois concernant la conservation obligatoire des données élargissent considérablement le champ de la surveillance de l'État, et multiplient ainsi les possibilités de violations des droits de l'homme. Les bases des données de communications deviennent vulnérables au vol, à la fraude et à la divulgation accidentelle.

[43] Voir Parlement européen – Direction générale des politiques internes – Service politique C: Droits des citoyens et affaires constitutionnelles, Lutte contre le crime et protection de la vie privée dans le nuage: étude, 2012.

[44] Projet ESTI DTR 101 567 Interception illégale (IL) Vo.1.0 (2012 - 05); Services virtuels/dans le nuage (CLI). Disponible à l'adresse: www.3gpp.org.

[45] Une adresse de protocole Internet est un numéro de code unique qui identifie tous les ordinateurs ou autres matériels connectés à Internet.

G. Lois relatives à la divulgation de l'identité

68. Dans de nombreux États, des lois exigent de produire une pièce d'identité dans les cybercafés. Ces lois sont particulièrement problématiques dans les pays où les ordinateurs personnels sont rares et où les individus recourent largement aux ordinateurs publics. En Inde par exemple, les Règles 2011 sur les technologies de l'information (Directives destinées aux cybercafés) exigent des propriétaires de cybercafés qu'ils réclament à leurs clients une pièce d'identité et en conservent la trace pendant au moins un an (Règle 4(2)). Le cybercafé doit, pendant cette même période, tenir un registre des connexions contenant entre autres informations, les heures d'ouverture et de fin de session et l'identification du terminal informatique (Règles 5(1) et 5(2)), et stocker et faire des sauvegardes des enregistrements de chaque accès ou connexion des utilisateurs (Règle 5(4)).

69. Dans de nombreux États, les individus doivent en outre aujourd'hui utiliser en ligne leur véritable nom et fournir une pièce d'identité officielle pour prouver leur identité. En République de Corée, la loi sur la communication des données adoptée en 2007, exigeait des utilisateurs qu'ils enregistrent leur véritable nom avant d'accéder aux sites Web ayant plus de 100 000 visiteurs par jour – officiellement pour réduire le harcèlement et les propos haineux en ligne. La loi a été récemment annulée par la Cour constitutionnelle au motif qu'elle restreignait la liberté de parole et portait atteinte à la démocratie[46]. La Chine a récemment adopté la Décision de renforcer la protection des informations en ligne, en exigeant des fournisseurs d'accès à Internet et des prestataires des télécommunications qu'il recueillent les données personnelles des usagers lorsqu'ils s'abonnent à un service d'accès à Internet, et à un service de téléphonie fixe ou mobile. Les prestataires de services qui permettent aux usagers de publier en ligne doivent être en mesure d'établir un lien entre pseudonymes et identités réelles. Cette exigence d'enregistrement des noms réels permet aux autorités d'identifier plus facilement les commentateurs en ligne ou de relier les usagers de téléphones mobiles à des individus spécifiques, éliminant ainsi toute expression anonyme[47].

70. Une autre initiative destinée à lever l'anonymat des communications est l'adoption progressive de directives exigeant que les cartes SIM soient enregistrées avec le nom réel de l'abonné ou un document d'identité officiel. Dans 48 pays d'Afrique des lois exigeant des individus qu'ils enregistrent leurs données personnelles avec leur fournisseur d'accès avant l'activation de cartes SIM prépayées, faciliteraient la création de bases de données importantes contenant des informations sur les usagers, éliminant par là l'anonymat des communications et permettant de les localiser et de simplifier leur surveillance[48]. En l'absence d'une législation dédiée à la protection des données, les renseignements relatifs aux usagers de cartes SIM peuvent être partagés avec les services publics et se combiner avec d'autres bases de données publiques et privées, permettant ainsi à un État de créer des profils détaillés de ses ressortissants. Les individus risquent également de se voir interdire l'utilisation des services de téléphonie mobile (qui peuvent permettre non seulement de communiquer mais aussi d'accéder aux services financiers) s'ils sont incapables ou peu désireux de s'identifier pour s'enregistrer.

[46] Décision 2010 de la Cour constitutionnelle Hun-Ma47 (décision relative aux «Noms réels»), 23 août 2012. Un compte rendu officiel de la décision de la Cour est disponible sur son site Web à l'adresse: http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp, uniquement en Corée.

[47] «La Chine renforce la protection des données sur Internet» – http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm.

[48] Kevin P. Donovan et Aaron K. Martin, "The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance" Groupe de travail sur l'innovation et les systèmes d'information, documents n° 186, London School of Economics and Political Science (2012).

H. Restrictions au chiffrement et principales lois sur la divulgation des données

71. La sécurité et l'anonymat des communications sont aussi mis à mal par des lois qui limitent l'usage d'outils destinés à améliorer la confidentialité des renseignements et susceptibles de protéger les communications, par exemple le chiffrement. De nombreux États ont à présent adopté des lois qui ordonnent un déchiffrement individuel à la demande. La loi sud-africaine de 2002 sur la réglementation de l'interception des communications et les dispositions relatives aux données liées aux communications exige l'aide au déchiffrement de toute personne qui possède la clé de déchiffrement[49]. Des lois similaires existent en Finlande (loi sur les mesures coercitives 1987/450, art. 4 4) a)), en Belgique (loi sur les délits informatiques du 28 novembre 2000, art. 9), et en Australie (loi de 2001 sur la cybercriminalité, art. 12 et 28).

VII. Rôle et responsabilités du secteur privé

72. Les progrès majeurs de la technologie qui ont permis des formes nouvelles et évolutives de communications ont été réalisés essentiellement par le secteur privé. En ce sens, nombre des changements dans la manière dont nous communiquons, recevons et transmettons les informations reposent sur la recherche et les innovations des entreprises.

73. Le secteur privé a également joué un rôle majeur en facilitant de diverses manières la surveillance des individus par l'État. Les entreprises ont dû faire en sorte que les réseaux numériques et l'infrastructure des communications soient conçus pour permettre l'ingérence de l'État. Ces dispositions, adoptées à l'origine par les États dans les années 1990, deviennent obligatoires pour tous les prestataires des services de communications. Les États adoptent de plus en plus souvent une législation exigeant d'eux qu'ils leur permettent d'avoir directement accès aux données des communications, ou qu'ils modifient l'infrastructure pour faciliter de nouvelles formes d'intrusion de l'État.

74. En développant et en déployant de nouvelles technologies et de nouveaux outils de communication dans des voies spécifiques, les entreprises ont également volontairement adopté des mesures qui facilitent la surveillance des communications par l'État. Cette collaboration, dans sa manifestation la plus rudimentaire, a pris la forme de décisions portant sur la manière dont les entreprises collectent et traitent les informations; elles deviennent ainsi les grands dépositaires de données personnelles qui sont alors accessibles à la demande aux États. Les entreprises ont adopté des normes qui permettent l'accès ou l'intrusion de l'État et la collecte d'informations révélatrices et en quantité excessive, ou qui restreignent l'application du chiffrement et autres techniques susceptibles de limiter l'accès aux données tant des entreprises que des gouvernements. Le secteur privé a aussi souvent omis d'utiliser des technologies permettant d'améliorer la protection de la vie privée, ou il les a mises en œuvre de manière moins sûre, non conforme aux règles de l'art.

75. Dans les cas les plus graves, le secteur privé a été complice en élaborant des technologies permettant une surveillance invasive de masse, en contravention avec les normes juridiques en vigueur[50]. Le secteur des entreprises a créé une industrie mondiale

[49] Art. 29. Loi de 2002 sur la réglementation sud-africaine de l'interception des communications et les dispositions concernant les communications – informations connexes. Disponible à l'adresse: http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.

[50] Pour quelques exemples de technologies de surveillance conçues par le secteur privé et utilisées en Libye, au Bahreïn, en République arabe syrienne, en Égypte et en Tunisie, voir: Parlement européen, Direction générale des politiques externes, Département des politiques, Après le Printemps arabe:

centrée sur l'échange des technologies de surveillance, souvent vendues aux pays où elles risquent fort d'être employées pour violer les droits de l'homme, en particulier ceux de leurs défenseurs, des journalistes ou autres groupes vulnérables. Cette industrie est pratiquement non réglementée car les États n'ont pas suivi le rythme des innovations technologiques et des changements politiques.

76. Les obligations des États en matière de droits de l'homme exigent non seulement qu'ils respectent et encouragent les droits à la liberté d'expression et au respect de la vie privée, mais qu'ils protègent les individus des violations des droits fondamentaux perpétrées par les entreprises. En outre, les États devraient exercer un contrôle adéquat, de manière à remplir leurs obligations internationales en matière de droits de l'homme lorsqu'ils recourent aux services des entreprises ou prévoient de le faire, si cela peut avoir une incidence sur l'exercice des droits de l'homme[51]. Les obligations en matière de droits fondamentaux à cet égard s'appliquent lorsque les entreprises exercent leurs activités à l'étranger[52].

77. Les États doivent garantir que le secteur privé est en mesure de remplir ses fonctions de manière indépendante et propre à promouvoir les droits fondamentaux des individus. Parallèlement, les entreprises ne peuvent être autorisées à participer à des activités qui portent atteinte aux droits de l'homme et les États ont la responsabilité de faire en sorte qu'elles soient tenues de rendre des comptes à cet égard.

VIII. Conclusions et recommandations

78. **Les techniques et les technologies de la communication ont beaucoup évolué, changeant ainsi les modes de surveillance des communications exercés par les États. Les États doivent donc actualiser leurs conceptions et leur réglementation à cet égard et modifier leurs pratiques pour faire en sorte que les droits fondamentaux des personnes soient respectés et protégés.**

79. **Les États ne peuvent garantir aux individus la capacité de rechercher et d'obtenir librement des informations ou de s'exprimer, sans respecter, protéger et promouvoir leur droit à la vie privée. Vie privée et liberté d'expression sont liées et mutuellement dépendantes; le non-respect de l'une peut être à la fois la cause et la conséquence de la violation de l'autre. Sans législation et normes juridiques adéquates pour garantir le respect de la vie privée, la sécurité et l'anonymat des communications, les journalistes, les défenseurs des droits de l'homme et les personnes dénonçant des abus, par exemple, ne peuvent être assurés que leurs communications ne feront pas l'objet d'une surveillance de l'État.**

80. **Pour satisfaire à leurs obligations en matière de droits de l'homme, les États doivent faire en sorte que les droits à la liberté d'expression et à la vie privée soient au cœur de leurs systèmes de surveillance des communications.** A **cet effet, le Rapporteur spécial émet les recommandations suivantes:**

Nouvelles voies pour les droits de l'homme et Internet dans la politique étrangère européenne (2012), p. 9 et 10.

[51] Principes directeurs sur l'entreprise et les droits de l'homme: Application du cadre des Nations Unies «Protection, respect et recours», Principe 5.

[52] Comité des droits de l'homme, observations finales, Allemagne, décembre 2012.

A. Mettre à jour et renforcer les lois et les normes juridiques

81. **La surveillance des communications devrait être considérée comme un acte très intrusif qui empiète potentiellement sur les droits à la liberté d'expression et à la protection de la vie privée et menace les fondements d'une société démocratique. La législation doit stipuler que la surveillance des communications par l'État ne doit intervenir que dans les circonstances les plus exceptionnelles et exclusivement sous le contrôle d'une autorité judiciaire indépendante. Des garanties doivent être clairement énoncées dans la loi en ce qui concerne la nature, l'étendue et la durée des mesures possibles, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les mettre en œuvre et les superviser, et le type de recours prévu par le droit interne.**

82. **Les individus devraient avoir la possibilité légale d'être avisés que leurs échanges ont fait l'objet d'une surveillance, ou que l'État a consulté leurs données de communications. Reconnaissant qu'une notification préalable ou concomitante pourrait compromettre l'efficacité de la surveillance, les individus devraient néanmoins être avisés une fois la surveillance achevée et avoir la possibilité de chercher réparation eu égard aux retombées de l'utilisation de mesures de surveillance des communications.**

83. **Les cadres juridiques doivent garantir que les mesures de surveillance des communications:**

a) Sont ordonnées par la loi et répondent à des normes de clarté et de précision suffisantes pour garantir que les individus en sont avisés au préalable et peuvent en prévoir l'application;

b) Sont strictement et manifestement nécessaires pour parvenir à un objectif légitime; et

c) Se conforment au principe de proportionnalité et ne sont pas employées lorsque des techniques moins invasives existent ou n'ont pas encore été toutes épuisées.

84. **Les États devraient ériger en infraction la surveillance illégale menée par des acteurs publics ou privés. Ces lois ne doivent pas être employées pour cibler les personnes dénonçant des abus ou d'autres individus qui cherchent à faire connaître des violations des droits fondamentaux, ni entraver le contrôle légitime de l'action du gouvernement, exercé par les citoyens.**

85. **La transmission aux États par le secteur privé de données des communications devrait être suffisamment réglementée pour faire en sorte que les droits fondamentaux se voient en tout temps accorder la priorité. L'accès aux données des communications détenu par les entreprises nationales ne devrait être possible qu'après avoir eu recours aux autres techniques moins invasives disponibles.**

86. **La transmission aux États des données de communications devrait être contrôlée par une autorité indépendante telle qu'un tribunal ou un mécanisme de supervision. Au niveau international, les États devraient adopter des traités d'assistance mutuelle pour réglementer l'accès aux données des communications détenu par les entreprises étrangères.**

87. **Les techniques et les pratiques de surveillance employées en dehors de l'état de droit doivent se voir imposer un contrôle législatif. Leur usage extrajuridique compromet les principes fondamentaux de la démocratie et risque d'avoir des incidences politiques et sociales négatives.**

B. Faciliter des communications privées, sûres et anonymes

88. **Les États devraient s'abstenir d'imposer l'identification des usagers comme condition préalable à l'accès aux communications, notamment aux services en ligne, aux cybercafés ou à la téléphonie mobile.**

89. **Les individus devraient pouvoir utiliser librement la technologie de leur choix pour assurer la sécurité de leurs communications. Les États ne devraient pas empêcher l'utilisation des technologies de chiffrement, ni obliger à communiquer les clés de chiffrement.**

90. **Les États ne devraient pas conserver ou exiger la conservation d'informations particulières uniquement à des fins de surveillance.**

C. Améliorer l'accès public à l'information, la prise de conscience et la sensibilisation relatives aux atteintes à la vie privée

91. **Les États devraient agir de manière totalement transparente eu égard à l'utilisation et au champ d'application des pouvoirs et des techniques de surveillance des communications. Ils devraient au minimum publier des informations globales sur le nombre de demandes approuvées et rejetées, et une ventilation des demandes par prestataire de service et par enquête et objet.**

92. **Les États devraient fournir aux personnes suffisamment d'informations pour leur permettre d'appréhender pleinement l'étendue, la nature et l'application des lois autorisant la surveillance des communications. Ils devraient permettre aux prestataires de service de publier les procédures auxquelles ils ont recours pour prendre en charge la surveillance des communications par l'État, se conformer à ces procédures et publier des relevés des activités publiques de surveillance des communications.**

93. **Les États devraient mettre en place des mécanismes de contrôle indépendants capables d'assurer la transparence et la responsabilisation de l'État en matière de surveillance des communications.**

94. **Les États devraient sensibiliser le public à l'usage des nouvelles technologies de la communication de manière à aider les individus à évaluer, gérer, limiter correctement les risques liés aux communications et prendre des décisions éclairées à cet égard.**

D. Réglementer la commercialisation des technologies de surveillance

95. **Les États devraient faire en sorte que les données des communications recueillies par les entreprises prestataires des services de communication répondent aux normes les plus strictes de protection des données.**

96. **Les États doivent s'abstenir de contraindre le secteur privé à appliquer des mesures qui compromettent la confidentialité, la sécurité et l'anonymat des services de communication, notamment en exigeant la conception de moyens d'interception à des fins de surveillance par l'État ou en interdisant le chiffrement.**

97. **Les États doivent prendre des mesures pour éviter la commercialisation des technologies de surveillance, en accordant une attention particulière à la recherche, au développement, à l'échange, à l'exportation et à l'utilisation des technologies, compte tenu de leur capacité de faciliter les violations systématiques des droits de l'homme.**

E. Mieux évaluer les obligations internationales pertinentes dans le domaine des droits de l'homme

98. **Face aux avancées technologiques, il est impératif de faire progresser au niveau international la notion de protection du droit au respect de la vie privée. Le Comité des droits de l'homme devrait envisager de publier une nouvelle observation générale sur le droit à la protection de la vie privée, pour remplacer l'observation générale n° 16 (1988).**

99. **Les mécanismes des droits de l'homme devraient mieux évaluer les obligations des acteurs privés eu égard au développement et à l'offre des technologies de surveillance.**