Nations Unies A/HRC/13/37

Assemblée générale

Distr. générale
28 décembre 2009
Français
Original: anglais

Conseil des droits de l'homme
Treizième 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 des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Martin Scheinin

Résumé

Au chapitre premier du présent rapport, le Rapporteur spécial énumère les principales activités qu'il a menées du 1er août au 15 décembre 2009. Dans la partie principale du rapport, correspondant au chapitre II, il évoque plusieurs de ses préoccupations quant à la protection du droit au respect de la vie privée dans la lutte antiterroriste. La section A traite en particulier de l'importance du droit au respect de la vie privée et de la protection des données.

L'article l7 du Pacte international relatif aux droits civils et politiques est suffisamment flexible pour que des restrictions nécessaires, légitimes et proportionnées puissent être imposées à l'exercice du droit au respect de la vie privée. Dans la section B, le Rapporteur spécial fait valoir que l'article 17 devrait être interprété comme énonçant les conditions dans lesquelles des restrictions peuvent être permises. À cet égard, il demande aux États d'expliquer pourquoi la réalisation d'un objectif précis justifie légitimement l'imposition de restrictions à l'article 17, et invite le Comité des droits de l'homme à adopter une nouvelle observation générale sur l'article 17.

Dans la section C, le Rapporteur spécial examine la question de l'érosion du droit au respect de la vie privée dans la lutte antiterroriste, érosion due à l'utilisation du pouvoir de surveillance et des nouvelles technologies sans garanties juridiques suffisantes. Les États ont mis en danger la protection du droit au respect de la vie privée en négligeant les garanties en vigueur dans leur coopération avec des pays tiers et des acteurs privés. Les mesures prises ont non seulement abouti à des violations du droit au respect de la vie privée mais ont aussi eu des incidences sur le droit à une procédure régulière et la liberté de circulation, en particulier aux frontières. En outre, elles peuvent avoir des effets néfastes sur la liberté d'association et la liberté d'expression.

En l'absence d'un ensemble de garanties juridiques rigoureuses et de moyens permettant de déterminer si leur ingérence est nécessaire, proportionnée et légitime, les États ne disposent d'aucun cadre pour réduire au minimum les effets de leurs nouvelles politiques sur la vie privée. Dans la section D, le Rapporteur spécial a recensé un certain nombre de garanties juridiques qui se dégagent de l'élaboration et de l'analyse de politiques, de la jurisprudence et des bonnes pratiques de par le monde.

En conclusion, le Rapporteur spécial adresse des recommandations à divers acteurs clefs (les parlements nationaux, les gouvernements et l'ONU) en vue d'améliorer la protection du droit au respect de la vie privée dans la lutte antiterroriste.

Table des matières

I. Introduction

1. Le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste soumet le présent rapport au Conseil des droits de l'homme en application de la résolution 63/185 de l'Assemblée générale et de la résolution 10/15 du Conseil des droits de l'homme. Dans le corps du document, il présente les activités qu'il a menées du 1er août au 15 décembre 2009 et met l'accent sur le droit au respect de la vie privée en tant que droit de l'homme dans le contexte de la lutte antiterroriste. Les additifs se composent d'un rapport sur les communications (A/HRC/13/37/Add.1) et d'un rapport sur la mission d'enquête effectuée en Égypte du 17 au 21 avril 2009 (A/HRC/13/37/Add.2).

2. S'agissant des futures visites de pays, le Rapporteur spécial espère se rendre en Tunisie avant la présentation du présent rapport, fin janvier-début février 2010 et attend une réponse du Gouvernement tunisien à ce sujet. Il compte aussi effectuer des visites officielles au Chili et au Pérou en 2010. Il attend une réponse à ses demandes de visite adressées à l'Algérie, à la Malaisie, au Pakistan, aux Philippines et à la Thaïlande.

II. Activités du Rapporteur spécial

3. Les 18 et 19 septembre 2009, le Rapporteur spécial a organisé une réunion d'experts à l'Institut universitaire européen de Florence afin de débattre de questions thématiques liées à son mandat[1]. La réunion s'est tenue pratiquement en même temps qu'une manifestation publique sur le thème «La lutte contre le terrorisme: défis pour le judiciaire», organisée conjointement par la Commission de Venise et le Comité européen pour les problèmes criminels du Conseil de l'Europe. La réunion était cofinancée par l'Institut des droits de l'homme de l'Université Åbo Akademi dans le cadre de son projet de soutien au mandat du Rapporteur spécial.

4. Les 29 et 30 septembre 2009, le Rapporteur spécial et d'autres titulaires de mandat intéressés ont pris part à Genève à des consultations officieuses relatives à une étude conjointe mondiale sur la détention au secret (A/HRC/13/42). Il s'est aussi entretenu avec des représentants des Missions permanentes de l'Égypte et de la Tunisie au sujet des visites réalisées ou prévues.

5. Les 2 et 3 octobre 2009, le Rapporteur spécial a participé à une conférence de Wilton Park intitulée «Terrorism, security and human rights: opportunities for policy change» et a pris part à un débat sur le rôle des organisations internationales dans la lutte antiterroriste et la protection des droits de l'homme.

6. Le 4 octobre 2009, le Rapporteur spécial a prononcé une allocution à l'occasion de l'ouverture de l'année universitaire à la faculté de droit de l'Université du Pays basque (Universidad del País Vasco) à Bilbao (Espagne).

7. Du 12 au 14 octobre 2009, le Rapporteur spécial a participé à deux manifestations à Vienne: l'Atelier international réunissant les coordonnateurs nationaux de la lutte antiterroriste et le séminaire de l'Équipe spéciale de lutte contre le terrorisme. L'atelier était conjointement organisé par plusieurs États Membres et par l'Office des Nations Unies contre la drogue et le crime, en étroite collaboration avec le Bureau de l'Équipe spéciale de

[1] Le Rapporteur spécial remercie les membres du comité d'experts, M. Gus Hosein et son assistant de recherche, M. Mathias Vermeulen, ainsi que les participants au séminaire de doctorat de l'Institut universitaire européen, pour leur contribution à l'élaboration du présent rapport.

lutte contre le terrorisme et la Direction exécutive du Comité contre le terrorisme. Il a fourni l'occasion d'échanger des vues sur les moyens de mieux coordonner les initiatives antiterroristes aux niveaux national et mondial en renforçant la coopération entre les coordonnateurs nationaux et en les aidant à jouer leur rôle d'interface entre les initiatives antiterroristes nationales, régionales et mondiales. Le séminaire de l'Équipe spéciale de lutte contre le terrorisme a mis l'accent sur les moyens de renforcer et développer les partenariats entre les États Membres, les organismes des Nations Unies, les organisations régionales et d'autres organisations, et la société civile dans le cadre de la mise en œuvre de la Stratégie antiterroriste mondiale de l'ONU[2].

8. Le 20 octobre 2009, le Rapporteur spécial a été représenté lors d'un séminaire tenu à Bruxelles sur le renforcement des sanctions ciblées de l'ONU au moyen de procédures transparentes et justes, organisé par le Service public fédéral belge pour les affaires étrangères, le commerce extérieur et la coopération au développement.

9. Du 26 au 28 octobre 2009, le Rapporteur spécial était à New York pour présenter à la Troisième Commission de l'Assemblée générale son rapport[3], qui traite principalement des effets des mesures antiterroristes sur l'égalité entre les sexes. Il a rencontré officiellement les membres du Comité des sanctions contre Al-Qaida et les Talibans du Conseil de sécurité et s'est entretenu avec le Directeur de la Direction exécutive du Comité contre le terrorisme. Il a participé à un débat dans le cadre d'une manifestation parallèle intitulée «Engendering Counter-terrorism and National Security», organisée par le Centre for Human Rights and Global Justice de la faculté de droit de la New York University. Il a aussi rencontré un certain nombre d'organisations non gouvernementales et donné une conférence de presse.

10. Le 29 octobre 2009, le Rapporteur spécial a rencontré le Secrétaire d'État adjoint chargé des questions liées à la démocratie, aux droits de l'homme et au travail et d'autres représentants du Département d'État des États-Unis à Washington afin de débattre avec la nouvelle administration des faits nouveaux et des projets dans le domaine juridique, au titre du suivi de la visite qu'il avait effectuée aux États-Unis en 2007[4], et d'autres questions plus générales concernant le droit international humanitaire et le droit des droits de l'homme dans le cadre de la lutte antiterroriste.

III. Le droit au respect de la vie privée

A. Le droit au respect de la vie privée tel qu'il est consacré par les constitutions et les instruments internationaux relatifs aux droits de l'homme

11. Le droit au respect de la vie privée est un droit fondamental fondé sur la présomption que tout individu a droit à un espace dans lequel il peut s'épanouir, interagir et jouir d'une liberté en toute autonomie, une «sphère privée» dans laquelle il est libre d'interagir ou non avec d'autres personnes et peut échapper à l'intervention de l'État et à toute intervention excessive non sollicitée d'une tierce partie[5]. Ce droit a évolué dans deux directions. Les instruments universels relatifs aux droits de l'homme ont mis l'accent sur

[2] Voir la résolution 60/288 de l'Assemblée générale.
[3] A/64/211.
[4] Voir A/HRC/6/17Add.3.
[5] Lord Lester et D. Pannick (éd.), *Human Rights Law and Practice* (Londres, Butterworth, 2004), par. 4.82.

l'aspect négatif du droit au respect de la vie privée, en interdisant toute immixtion arbitraire dans la vie privée, la famille, le domicile ou la correspondance d'une personne[6], tandis que certains instruments régionaux et nationaux tiennent aussi compte d'aspects positifs: tout individu a droit au respect de sa vie privée et de sa vie familiale, de son domicile et de sa correspondance[7], ou a le droit de voir sa dignité, son intégrité ou sa bonne réputation reconnues et respectées[8]. Si le respect de la vie privée n'est pas toujours expressément mentionné comme un droit distinct dans les constitutions, la quasi-totalité des États reconnaissent sa valeur en tant que question d'importance constitutionnelle. Dans certains pays, le droit au respect de la vie privée s'est imposé par extension de la règle de *common law* relative à la divulgation d'informations confidentielles, du droit à la liberté, de la liberté d'expression ou du droit à une procédure régulière. Dans d'autres pays, il est apparu comme une valeur religieuse. Il s'agit donc non seulement d'un droit fondamental, mais aussi d'un droit de l'homme qui nourrit d'autres droits de l'homme et constitue la base de toute société démocratique.

12. Avec le développement des technologies de l'information, il est devenu de plus en plus facile à l'État de tenir des registres. La puissance accrue des ordinateurs a permis l'apparition de formes jusqu'alors inimaginables de collecte, de stockage et de partage de données personnelles. Des principes de protection des données de base ont été élaborés au niveau international, notamment l'obligation d'obtenir des données personnelles en toute légalité et transparence; de limiter l'utilisation des données à des fins initialement spécifiées; de veiller à ce que le traitement des données soit adéquat, pertinent et non excessif; de garantir l'exactitude des données et de préserver leur caractère confidentiel; de supprimer les données lorsqu'on n'en a plus l'utilité; et de donner à toute personne le droit d'avoir accès aux informations qui la concernent et de demander qu'elles soient rectifiées[9]. Dans son Observation générale n° 16, le Comité des droits de l'homme a clairement indiqué que ces principes étaient inhérents au droit au respect de la vie privée[10] même si la protection des données apparaît de plus en plus comme un droit fondamental ou un droit de l'homme distinct. Un certain nombre de pays ont même reconnu que la protection des données était un droit constitutionnel, insistant ainsi sur son importance en tant qu'élément de toute société démocratique. L'article 35 détaillé de la Constitution portugaise de 1976 est un excellent exemple à cet égard.

13. Le droit au respect de la vie privée n'est pas un droit absolu. Une fois qu'une personne a fait l'objet d'une enquête officielle ou d'un contrôle de sécurité, ses données

[6] Voir la Déclaration universelle des droits de l'homme (art. 12), le Pacte international relatif aux droits civils et politiques (art. 17), la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille (art. 14) et la Convention relative aux droits de l'enfant (art. 16).

[7] Voir la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) et la Déclaration du Caire sur les droits de l'homme en islam (A/45/421-S/21797, art. 18) du 5 août 1990.

[8] Charte africaine des droits de l'homme et des peuples (art. 11). Voir aussi la Déclaration de principes de l'Union africaine sur la liberté d'expression en Afrique (art. 4.3) et la Déclaration américaine des droits et devoirs de l'homme (art. 5).

[9] Voir la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (n° 108) du Conseil de l'Europe, 1981; les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel (1980); et les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (résolution 45/95 de l'Assemblée générale et E/CN.4/1990/72).

[10] Observation générale n° 16 (1988) du Comité des droits de l'homme sur le droit au respect de la vie privée, de la famille, du domicile et de la correspondance, et sur la protection de l'honneur et de la réputation (art. 17).

personnelles sont échangées entre les organismes de sécurité aux fins de la lutte antiterroriste et son droit au respect de la vie privée en est presque automatiquement altéré. C'est ce qui se produit lorsque les États sont légitimement habilités à restreindre le droit au respect de la vie privée en vertu du droit international des droits de l'homme. Toutefois, on ne saurait invoquer la lutte antiterroriste pour légitimer automatiquement toute atteinte au droit au respect de la vie privée. Dès lors qu'on risque de porter atteinte à ce droit, il faut procéder à une analyse critique de la situation.

B. Restrictions permises au droit au respect de la vie privée

14. L'article 17 du Pacte international relatif aux droits civils et politiques est la disposition juridiquement contraignante la plus importante à l'échelon international en ce qui concerne le droit au respect de la vie privée. Le Pacte a été ratifié par 165 États et signé par 6 autres[11]. L'article 4 du Pacte permet aux États parties de déroger à certaines dispositions du Pacte, y compris à l'article 17. Ces dérogations, qui ne sont possibles qu'en période d'état d'urgence, lorsque l'existence de la nation est menacée, sont assorties de plusieurs conditions[12]. Depuis l'entrée en vigueur du Pacte en 1976, il y a plus de trente ans, moins de 10 États parties ont proclamé l'état d'urgence en se référant à des actes ou des menaces de terrorisme[13]. Quatre d'entre eux ont, dans ce contexte, cherché à déroger aussi à l'article 17 du Pacte[14]. Huit autres États ont notifié des dérogations à l'article 17 sans se référer expressément au terrorisme pour justifier l'état d'urgence[15]. Toutefois, ces notifications étaient plutôt générales et ne précisaient pas, comme l'exige pourtant l'article 4 du Pacte, quelles mesures concrètes dérogeant à l'article 17 étaient nécessaires compte tenu de la situation[16]. D'une manière générale, il n'y a pas un seul cas d'État cherchant à déroger à l'article 17 du Pacte au nom de la lutte antiterroriste qui répondrait pleinement à toutes les exigences de l'article 4. Un seul État a d'ailleurs notifié qu'il dérogeait aux dispositions du Pacte en se référant à l'actuelle menace de terrorisme international (liée aux événements du 11 septembre 2001)[17]. Il en va de même en ce qui concerne les réserves à l'article 17. Bien que le droit international autorise généralement les États à formuler des réserves aux instruments internationaux relatifs aux droits de l'homme,

[11] Au 16 novembre 2009, les six pays dont la signature n'avait pas encore été suivie d'une ratification étaient les suivants: Chine, Cuba, Guinée-Bissau, Nauru, Panama et Saint-Marin.

[12] En ce qui concerne la position de l'organe conventionnel compétent au sujet de la portée et de l'effet des dérogations, voir l'Observation générale n° 29 (2001) du Comité des droits de l'homme.

[13] L'Azerbaïdjan, le Chili, la Colombie, El Salvador, la Fédération de Russie, Israël, le Népal, le Pérou, et le Royaume-Uni.

[14] La Colombie, El Salvador, la Fédération de Russie et le Népal.

[15] L'Algérie, l'Arménie, l'Équateur, le Nicaragua, Panama, la Serbie-Monténégro, Sri Lanka et la République bolivarienne du Venezuela. Dans certains cas, il y a pu y avoir des liens avec le terrorisme mais cela n'a pas été indiqué dans la notification de la déclaration d'état d'urgence.

[16] Par exemple, lorsqu'ils ont dérogé aux dispositions du Pacte, nombre d'États latino-américains ont simplement indiqué que telles ou telles dispositions du Pacte seraient «suspendues», ce qui n'est pas conforme aux exigences de l'article 4 comme il est expliqué dans l'Observation générale n° 29.

[17] Le Royaume-Uni le 18 décembre 2001. Les dérogations ne portaient pas sur l'article 17 et ont été retirées le 15 mars 2005.

à moins qu'elles ne soient incompatibles avec l'objet et le but de l'instrument[18], un seul État partie a émis une réserve à l'article 17[19].

15. Les États semblent donc avoir eu rarement recours aux mécanismes reconnus par le droit international en général et par le Pacte en particulier pour déroger unilatéralement au droit au respect de la vie privée. Même lorsque des notifications de dérogation à l'article 17 ont été soumises, loin de se référer à des mesures concrètes et à des formes spécifiques de dérogation, les États sont restés très vagues. De l'avis du Rapporteur spécial, cette pratique montre qu'en règle générale les États semblent considérer que le cadre offert par l'article 17 est suffisamment flexible pour permettre des restrictions nécessaires, légitimes et proportionnées au droit au respect de la vie privée, dans la mesure où elles sont autorisées, y compris dans le cadre de la lutte antiterroriste. Le Rapporteur spécial partage ce point de vue. L'article 17 est libellé de telle sorte qu'il permet aux États parties d'imposer des restrictions ou des limitations aux droits qu'il consacre, y compris le droit au respect de la vie privée. Ces restrictions et limitations doivent faire l'objet d'un contrôle de la part du Comité des droits de l'homme, en sa qualité d'organe conventionnel chargé d'interpréter les dispositions du Pacte et de vérifier comment les États parties s'acquittent de leurs obligations conventionnelles. Le Comité dispose essentiellement pour ce faire de la procédure d'examen des rapports que les États sont tenus de soumettre en vertu de l'article 40 du Pacte et, pour les 113 États qui ont ratifié le premier Protocole facultatif se rapportant au Pacte, de la procédure d'examen des plaintes émanant de particuliers.

16. L'article 17 du Pacte est rédigé de telle façon qu'il interdit les immixtions «arbitraires ou illégales» dans la vie privée, la famille ou la correspondance, ainsi que les «atteintes illégales» à l'honneur et à la réputation d'une personne, disposition à mettre en parallèle avec les dispositions du paragraphe 3 de l'article 12, du paragraphe 3 de l'article 18, du paragraphe 3 de l'article 19, de l'article 21 et du paragraphe 2 de l'article 22, qui énoncent tous les conditions dans lesquelles des restrictions peuvent être permises. Ces conditions, qui sont exposées de la façon la plus détaillée à l'article 21 et au paragraphe 3 de l'article 22, sont au nombre de trois: a) les restrictions doivent être prévues par la loi; b) elles doivent être nécessaires dans une société démocratique; et c) elles doivent répondre à l'un des buts légitimes énoncés dans chacun des articles contenant une clause restrictive.

17. Le Rapporteur spécial estime que même s'il est libellé différemment, l'article 17 du Pacte devrait être aussi interprété comme énonçant les conditions dans lesquelles des restrictions peuvent être permises. Les restrictions qui ne sont pas prévues par la loi sont «illégales» au sens de l'article 17 et celles qui ne sont pas nécessaires ou ne servent pas un but légitime constituent des immixtions «arbitraires» dans l'exercice des droits visés à l'article 17. En conséquence, les restrictions qui peuvent être imposées au droit au respect de la vie privée ou à d'autres droits énoncés à l'article 17 sont soumises à des conditions, telles qu'elles sont définies par le Comité des droits de l'homme dans son Observation générale n° 27 (1999). Cette Observation générale traite de la liberté de circulation (art. 12), l'un des articles qui contient une clause restrictive. Parallèlement, elle codifie la position du Comité des droits de l'homme en ce qui concerne les limitations qui peuvent être imposées aux droits consacrés par le Pacte. Les conditions dans lesquelles des restrictions peuvent être permises, telles qu'elles sont énoncées dans l'Observation générale, sont notamment les suivantes:

[18] En ce qui concerne la position de l'organe conventionnel compétent au sujet des réserves au Pacte et au Protocole facultatif s'y rapportant, voir l'Observation générale n° 24 (2004) du Comité des droits de l'homme.

[19] Le Liechtenstein maintient une réserve concernant la portée du droit au respect de la vie familiale en ce qui concerne les étrangers.

a) Les restrictions doivent être prévues par la loi (par. 11 et 12);

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

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

d) Les lois autorisant l'application de restrictions ne peuvent pas conférer des pouvoirs illimités aux personnes chargées de veiller à leur application (par. 13);

e) Il ne suffit pas que les restrictions servent les buts légitimes autorisés; elles doivent être également nécessaires pour protéger ces buts (par. 14);

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

g) L'imposition des restrictions doit être compatible avec le respect des autres droits garantis dans le Pacte (par. 18)[20].

18. Le Rapporteur spécial estime que ces considérations s'appliquent aussi à l'article 17 du Pacte, en ce sens qu'elles précisent les notions d'«illégales» et d'«arbitraires». Là où la différence terminologique est importante entre l'article 17 et les dispositions du Pacte qui énoncent expressément les conditions dans lesquelles des restrictions peuvent être permises, c'est que l'article 17 ne contient aucune liste exhaustive de buts légitimes. C'est pourquoi le Rapporteur spécial demande aux États d'expliquer les raisons pour lesquelles la réalisation d'un objectif précis justifie légitimement l'imposition de restrictions à l'article 17, et au Comité des droits de l'homme de continuer à surveiller les mesures prises par les États parties, notamment par le biais de l'examen des rapports périodiques et des plaintes émanant de particuliers.

19. De l'avis du Rapporteur spécial, le Comité des droits de l'homme devrait élaborer et adopter une nouvelle observation générale sur l'article 17, qui remplacerait l'Observation générale n° 16 (1988). Celle-ci est très brève et ne reflète pas l'ensemble de la pratique du Comité, qui a évolué depuis l'adoption de l'Observation, il y a plus de vingt ans. Cela étant, parmi les éléments d'une clause restrictive bien conçue, tels que ceux présentés plus haut à la lumière de l'Observation générale n° 27, beaucoup étaient déjà présents en 1988[21]. Dans sa jurisprudence ultérieure au titre du Protocole facultatif, le Comité a souligné qu'une immixtion dans l'exercice des droits garantis par l'article 17 devait répondre de façon cumulative à plusieurs conditions, c'est-à-dire qu'elle devait être prévue par la loi, être conforme aux dispositions, aux buts et aux objectifs du Pacte, et être raisonnable eu égard aux circonstances de l'espèce[22]. En outre, pour décider qu'il y avait eu violation de l'article 17, le Comité a appliqué les critères de but légitime, de nécessité et de proportionnalité[23].

[20] Voir l'Observation générale n° 27 (1999) du Comité des droits de l'homme.

[21] Voir l'Observation générale n° 16 (1988) du Comité des droits de l'homme. Voir, en particulier, les paragraphes 3 et 4 qui précisent les notions d'«immixtions arbitraires et illégales» figurant à l'article 17 du Pacte.

[22] Voir la communication n° 903/1999, *Van Hulst* c. *Pays-Bas*, de 2004.

[23] Voir la communication n° 1011/2001, *Madafferi* c. *Australie*, de 2004, et la communication n° 1482/2006, *M. G.* c. *Allemagne*, de 2008.

C. Érosion du droit au respect de la vie privée par les politiques antiterroristes

20. Lorsqu'ils envisagent d'adopter une politique antiterroriste, les États font souvent valoir qu'ils doivent tenir compte de deux nouvelles dynamiques en ce qui concerne la protection de la vie privée. Premièrement, ils soutiennent que leur capacité de prévenir les actes terroristes et d'enquêter sur ceux-ci est étroitement liée au renforcement de leurs pouvoirs de surveillance. La plupart des textes de loi adoptés depuis les événements du 11 septembre 2001 ont donc cherché à accroître les pouvoirs des gouvernements en matière de surveillance. Deuxièmement, les États affirment que, le terrorisme étant une activité mondiale, la recherche de terroristes doit transcender les frontières nationales, avec le concours de tierces parties susceptibles d'être des mines d'informations sur les individus et, partant, une ressource précieuse pour identifier et contrôler des personnes soupçonnées de terrorisme. Les États où, jusqu'alors, il n'existait pas de garanties constitutionnelles ou légales, ont pu faire évoluer considérablement leurs pouvoirs de surveillance en prévoyant très peu de restrictions. Dans les autres pays, les gouvernements ont sapé la protection du droit à la vie privée en n'appliquant pas les garanties existantes à leurs activités de coopération avec des pays tiers et des acteurs privés ou en faisant en sorte que leur système de surveillance échappe aux garanties prévues dans leur Constitution.

1. Durcissement des mesures de surveillance

21. La gamme des opérations de surveillance est très vaste, allant du spécifique au général. Pour ce qui est du spécifique, des systèmes juridiques permettent d'autoriser et de superviser les opérations d'infiltration et de surveillance secrète pour détecter tout comportement illégal, l'accumulation de renseignements sur tel ou tel individu afin de repérer les infractions qu'il commettrait, et la surveillance ciblée d'individus pour constituer un dossier judiciaire. Le Rapporteur spécial avait déjà indiqué que les États pouvaient avoir recours à des mesures de surveillance ciblée, à condition qu'elles soient ponctuelles et exécutées sur mandat décerné par un juge si des motifs raisonnables et suffisants avaient été produits et si certains faits en relation avec le comportement d'un individu justifiaient de le soupçonner d'être en train de préparer un attentat terroriste[24]. Au niveau mondial, la surveillance des communications s'est développée avec l'interception des communications par les services de renseignements et les forces de police. Il existe une remarquable convergence dans les types de politiques mises en œuvre pour renforcer les pouvoirs de surveillance face aux menaces terroristes. La plupart d'entre elles tirent parti de technologies existantes ou nouvelles, telles que les technologies d'écoute et de traçage qui permettent de localiser les téléphones mobiles, de suivre les conversations privées d'usagers de messageries téléphoniques sur Internet[25], ou d'installer des logiciels espions sur les ordinateurs de personnes suspectes afin d'avoir accès à distance à leurs données[26]. Dans plusieurs pays, les services de sécurité ont même proposé d'interdire les technologies de communication qui rendraient les interceptions plus difficiles, telles que les téléphones

[24] A/HRC/10/3, par. 30.

[25] D. O'Brien, «Chinese Skype client hands confidential communications to eavesdroppers», Electronic Frontier Foundation, 2 octobre 2008.

[26] Voir l'article ci-après: http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html.

intelligents[27]. Le Rapporteur spécial est aussi préoccupé par le contrôle des communications transfrontières sans autorisation judiciaire[28].

22. Au nom de la lutte contre le terrorisme, les États ont multiplié les initiatives visant à identifier, scanner et référencer tout un chacun en ayant recours à des techniques multiples qui risquent de porter atteinte au droit au respect de la vie privée. Lorsqu'il y a surveillance de lieux et de groupes de personnes à grande échelle, celle-ci se fait en général sans grand contrôle ni autorisation. Les normes relatives aux droits de l'homme sont mises à rude épreuve et bafouées lorsqu'il y a recours à des interpellations avec fouille, à la compilation de listes et de bases de données, à la surveillance accrue des opérations financières, des communications et des données de voyage, au profilage pour l'identification de suspects potentiels et à la constitution de bases de données toujours plus vastes pour calculer la probabilité d'activités suspectes et identifier les individus devant faire l'objet d'une surveillance renforcée. Des techniques encore plus poussées sont utilisées telles que la collecte de données biométriques ou l'utilisation de «scanners corporels» qui peuvent détecter tout objet à travers les vêtements[29]. Certaines intrusions dans la vie des gens peuvent être permanentes dans la mesure où les informations biographiques et physiques détaillées sur les personnes sont souvent centralisées dans des bases de données.

a) Interpellations avec fouille

23. Les États ont renforcé leurs pouvoirs d'interpeller, d'interroger, de fouiller et d'identifier des personnes tout en réduisant les moyens de contrôle pour prévenir d'éventuels abus. Ces pouvoirs ont fait naître des inquiétudes au sujet du profilage racial et de la discrimination en Europe[30] et dans la Fédération de Russie[31], les opposants à de telles pratiques faisant valoir qu'elles dressaient les citoyens contre l'État. De même, si les restrictions au droit au respect de la vie privée doivent être évaluées à l'aune du critère de la proportionnalité, on peut se demander si les interpellations généralisées avec fouille auxquelles il est procédé dans les zones de sécurité en Fédération de Russie[32] ou au Royaume-Uni[33] sont vraiment nécessaires dans une société démocratique.

b) Utilisation de données biométriques et dangers des systèmes d'identité centralisés

24. Un élément clef des nouvelles politiques en matière d'identité réside dans l'utilisation de techniques biométriques telles que la reconnaissance par analyse morphologique (traits du visage, empreintes digitales, iris). Ces techniques peuvent, dans certaines circonstances, être légitimes pour identifier des personnes soupçonnées de terrorisme, mais le Rapporteur spécial est particulièrement préoccupé par les cas où les données biométriques sont stockées non pas dans un document d'identité mais dans une base de données centrale, ce qui multiplie les risques pour la sécurité de l'information et rend les personnes plus vulnérables. Au fur et à mesure que la collecte de données

[27] S. Das Gupta et L. D'Monte, «*BlackBerry security issue markes e-com insecure*», Business Standard, 12 mars 2008.

[28] Voir, par exemple, le projet de loi du Gouvernement suédois sur l'ajustement des activités du renseignement militaire, adopté en juin 2008, p. 83.

[29] Voir la résolution du Parlement européen en date du 23 octobre 2008 sur l'impact des mesures de sûreté de l'aviation et des scanners corporels sur les droits de l'homme, la vie privée, la dignité personnelle et la protection des données.

[30] Open Society Justice Initiative, «Ethnic Profiling by Police in Europe», juin 2005.

[31] Open Society Justice Initiative and JURIX, «Ethnic Profiling in the Moscow Metro», juin 2006.

[32] Voir loi fédérale n° 35 de 2006 relative à la lutte contre le terrorisme.

[33] Voir, par exemple, l'arrêt de la cour d'appel du Royaume-Uni, *R.* v. *Commissioner of Police for the Metropolis and another*, 2006.

biométriques se développe, les taux d'erreurs augmentent sensiblement[34]. Cette situation fait parfois que des personnes sont stigmatisées ou sont accusées par erreur. De surcroît, contrairement à d'autres éléments d'identification, les données biométriques ne peuvent pas être supprimées: une fois copiées et/ou utilisées à des fins frauduleuses par des tiers malhonnêtes, il est impossible de délivrer à quelqu'un une nouvelle signature biométrique[35]. Dans ce contexte, il convient de noter qu'en dépit de leur objectivité scientifique les preuves par l'ADN peuvent aussi être falsifiées[36].

25. La collecte centralisée de données biométriques crée des risques d'erreur judiciaire comme en témoigne l'exemple suivant. À la suite des attentats de Madrid le 11 mars 2004, la police espagnole est parvenue à relever des empreintes digitales sur un engin non explosé. Selon des experts en empreintes digitales du Federal Bureau of Investigation (FBI) des États-Unis, les empreintes d'un avocat correspondaient à celles relevées sur le lieu de l'attentat. Les empreintes de cette personne figuraient dans le système national des empreintes digitales parce qu'il s'agissait d'un ancien soldat américain. L'intéressé a été placé en régime cellulaire pendant deux semaines alors même que les empreintes n'étaient pas les siennes. Les experts n'avaient pas suffisamment réexaminé les échantillons relevés et la situation s'était aggravée lorsqu'on avait découvert que l'avocat en question avait défendue une personne reconnue coupable de terrorisme, était marié à une immigrée égyptienne et s'était converti à l'islam[37].

c) Diffusion de listes secrètes de personnes à surveiller

26. Une autre technique de surveillance consiste à diffuser des listes de personnes, les plus courantes étant les listes de passagers indésirables (appelées «no-fly/selectee» list). Ces listes sont transmises aux compagnies aériennes et aux responsables de la sécurité, assorties d'instructions leur demandant d'arrêter et d'interroger tout passager portant un certain nom. Il est difficile de savoir à quel point ces listes sont utilisées, mais là où de tels systèmes sont opérationnels, un certain nombre d'erreurs se sont produites et des problèmes d'atteinte à la vie privée ont été signalés, en particulier aux États-Unis[38] et au Canada[39]. Des problèmes continuent de se poser en ce qui concerne l'intégrité des données, car il faut constamment vérifier les listes pour repérer les erreurs et suivre les procédures d'identification avec le plus grand soin. Ces listes sont souvent tenues secrètes pour ne pas fournir de pistes aux personnes soupçonnées de terrorisme, mais leur caractère confidentiel pose des problèmes dans la mesure où des individus font l'objet d'une surveillance de tous les instants sans savoir qu'elles figurent sur une liste et sans qu'il y ait de supervision indépendante efficace. Ce type de surveillance pourrait constituer une violation du droit au respect de la vie privée consacré par l'article 17 du Pacte.

---

[34] Voir, par exemple, M. Cherry et E. Imwinkelried, «A cautionary note about fingerprint analysis and reliance on digital technology», *Judicature*, vol. 89, n° 6 (2006).

[35] Voir E. Kosta et consorts, «An analysis of securité and privacy issues relating to RFID enables ePassports», Fédération internationale pour le traitement de l'information, n° 232 (2007), p. 467 à 472 de l'anglais.

[36] Voir, par exemple, D. Frumkin et consorts, «Authentification of forensic DNA samples» Forensic Science International: Genetics (17 juillet 2009).

[37] Voir Département de la justice des États-Unis, Bureau de l'Inspecteur général, *A Review of the FBI's Handling of the Brandon Mayfield Case*, janvier 2006.

[38] Voir Département de la justice des États-Unis, *Audit of the FBI Terrorist Watchlist Nomination Practices*, mai 2009.

[39] Voir Commissariat à la protection de la vie privée du Canada, *Vérification du Programme de protection des passagers de Transports Canada*, novembre 2009.

27. Lorsque des listes de terroristes sont rendues publiques, l'article 17 du Pacte peut être invoqué d'une autre manière. Le Comité des droits de l'homme a considéré que l'inclusion non justifiée d'une personne sur la liste récapitulative du Comité du Conseil de sécurité créé par la résolution 1267 constituait une violation de l'article 17. Il a estimé que la divulgation d'informations personnelles constituait une atteinte à l'honneur et à la réputation des personnes figurant sur la liste, en raison de l'association négative qui pouvait être faite par certains entre leur nom et l'intitulé de la liste des sanctions[40].

28. Les listes secrètes et publiques de personnes à surveiller portent aussi souvent atteinte aux principes fondamentaux de la protection des données. Des informations recueillies à des fins précises sont souvent réutilisées à d'autres fins et parfois échangées avec d'autres institutions, à l'insu ou sans le consentement des personnes intéressées. Des renseignements erronés servent à prendre des décisions sur des personnes, notamment pour restreindre leurs déplacements. Ces personnes peuvent se voir refuser un visa, être refoulées à la frontière ou être interdites d'embarquement par des compagnies aériennes, sans qu'aucune preuve d'une infraction quelconque ne leur soit présentée.

d) Points de contrôle et frontières

29. Grâce aux nouvelles technologies et face à la montée des inquiétudes concernant le terrorisme, les États cherchent de plus en plus à superviser, réglementer, encadrer et contrôler la circulation des personnes aux frontières. Aujourd'hui, s'appuyant sur des techniques plus poussées et des accords d'échange de données, les États créent des profils détaillés sur les voyageurs étrangers pour identifier les terroristes et les malfaiteurs avant même qu'ils n'arrivent à leurs frontières, en accédant aux listes de passagers et aux fichiers de réservation des compagnies de transport. Ils analysent cette information pour repérer les profils qui correspondent à ceux de terroristes ou de malfaiteurs. Aux points de passage des frontières, les personnes sont soumises à d'autres pratiques − potentiellement attentatoires à la vie privée − de collecte d'informations.

30. Nombre d'États obligent désormais les transporteurs à communiquer les listes de passagers avant les départs. Les États demandent aussi à accéder aux dossiers passagers, qui contiennent des éléments d'identification (nom, numéro de téléphone), des renseignements sur la transaction (dates de réservations, agence de voyage, itinéraires), les numéros de vol et de siège, des données financières (numéro de carte de crédit, adresse de facturation), les préférences de repas, des renseignements sur le lieu de résidence, des données médicales, des renseignements sur les voyages précédents et les données relatives à la participation à un programme de fidélisation. Les autorités utilisent ces informations pour établir le profil des passagers et évaluer s'ils présentent un risque, généralement en interrogeant des bases de données et des listes de surveillance communes de divers services de police et de lutte antiterroriste. Une compagnie de transports étrangère peut ainsi se voir interdire de délivrer une carte d'embarquement à une personne uniquement d'après les résultats d'une recherche effectuée dans une base de données du pays de destination, en dehors de toute procédure régulière.

31. La surveillance accrue des migrants et des voyageurs pour des motifs divers soulève plusieurs problèmes de respect de la vie privée. Des États obtiennent des informations sur les voyageurs auprès de tiers qui sont forcés d'obtempérer sous peine de se voir refuser les droits d'atterrissage ou imposer des amendes à titre de sanction, quand bien même les garanties offertes en matière de protection de la vie privée ne répondraient pas aux critères de la législation nationale en la matière. De plus, ces pays peuvent ne pas accorder aux étrangers le même accès aux recours judiciaires, et généralement, une limitation

[40] Voir communication n° 1472/2006 du Comité des droits de l'homme, par. 10.12 et 10.13.

significative des droits s'applique à la frontière. La politique du Gouvernement des États-Unis sur l'accès aux ordinateurs portables de voyageurs en est un bon exemple. Malgré la nécessité d'observer les dispositions constitutionnelles sur le respect des formes régulières pour s'introduire dans un ordinateur portable aux États-Unis, le Département de la sécurité du territoire a approuvé l'accès aux ordinateurs de voyageurs en l'absence d'autorisation judiciaire[41].

32. Enfin, les États instaurent des exigences supplémentaires en matière d'information. Des individus peuvent être empêchés de pénétrer sur le territoire d'un État pour avoir refusé de communiquer des informations, et les autorités de cet État peuvent exiger des informations sans vérifier si elles y sont légalement habilitées. En outre, les informations recueillies sont désormais utilisées à d'autres fins que le but initialement prévu; à titre d'exemple, on propose aujourd'hui d'étendre l'application du système européen dactyloscopique (EURODAC) de l'Union européenne, qui utilise le relevé des empreintes digitales pour gérer les demandes faites par des demandeurs d'asile et des immigrants illégaux, à des fins de prévention, de détection et d'enquête relatives à des infractions terroristes et autres infractions graves. Le Contrôleur européen de la protection des données a exprimé des réserves sur la légitimité de ces propositions du point de vue du droit au respect de la vie privée[42].

2. Effets exercés par la surveillance sur d'autres droits

33. Les régimes de surveillance adoptés pour lutter contre le terrorisme ont eu un effet préjudiciable considérable sur l'exercice d'autres droits fondamentaux. Le respect de la vie privée est non seulement un droit en soi, mais c'est la base d'autres droits, sans laquelle ceux-ci ne peuvent pas véritablement s'exercer. L'intimité de la vie privée est nécessaire afin qu'il y ait des espaces où les individus et les groupes puissent penser et nourrir des idées et des relations. D'autres droits comme la liberté d'expression, la liberté d'association et la liberté de circulation ont besoin du respect de la vie privée pour s'épanouir véritablement. La surveillance est aussi à l'origine d'erreurs judiciaires, de l'inobservation des garanties prévues par la loi et d'arrestations injustifiées.

34. Dans de nombreux pays du monde, les utilisateurs sont surveillés pour vérifier quels sites ils fréquentent et avec qui ils communiquent. On a appris en 2006 en Allemagne que les services de renseignements fédéraux épiaient illégalement les journalistes en surveillant les communications et en plaçant des agents dans les rédactions[43]. En Colombie, on s'est aperçu en 2009 que le Département administratif de la sécurité s'était livré pendant sept ans à une surveillance illégale d'employés des médias, de défenseurs des droits de l'homme, de responsables publics et de juges, ainsi que de leur famille[44]. Dans bon nombre de pays, les utilisateurs d'Internet doivent s'identifier et leurs sessions sont enregistrées afin que les autorités puissent utiliser ultérieurement ces informations. Par exemple, en 2007, au Bangladesh, il a été demandé aux fournisseurs d'accès à Internet de remettre aux autorités des fichiers contenant l'identité, les mots de passe et les données de connexion de leurs clients. Certains utilisateurs ont ensuite reçu la visite des autorités, qui ont procédé à une perquisition électronique et inspecté leurs listes de contacts[45]. Aux États-Unis, l'unité

[41] Voir Département de la sécurité du territoire, «Privacy impact assessment for the border searches of electronic devices», 25 août 2009.

[42] Voir communiqué du Contrôleur européen de la protection des données sur l'accès des services de répression à EURODAC, 8 octobre 2009.

[43] Deutsche Welle-World, "Germany stops journalist spying in wake of scandal", 15 mai 2006.

[44] Voir *Semana*, 21 février 2009.

[45] Voir *E-Bangladeshi*, "Crackdown on internet users in Bangladesh", 3 octobre 2007 (translating BBC reports).

antiterroriste du FBI a surveillé les activités de militants pacifistes lors des conventions électorales de 2004[46]. Ces mesures de surveillance effraient les utilisateurs, qui craignent de se rendre sur des sites Web, d'exprimer leur opinion ou de communiquer avec d'autres personnes de peur d'être sanctionnés[47]. Sont spécialement concernées les personnes qui veulent exprimer un désaccord, dont certaines peuvent être dissuadées d'exercer leur droit démocratique de contester la politique du gouvernement.

35. Non contentes d'instaurer des pouvoirs de surveillance, nombre de lois antiterroristes imposent aux individus de communiquer des informations par anticipation et octroient de larges pouvoirs aux agents de l'État, habilités à exiger des informations dans le cadre de leurs enquêtes. Dans ce contexte, le Rapporteur spécial a déjà exprimé précédemment ses préoccupations concernant l'utilisation de réquisitions dans l'intérêt de la sécurité nationale (*National Security Letters*) aux États-Unis[48]. Certains pays ont élargi ces prérogatives au point d'exiger l'accès à des informations recueillies au départ à des fins médiatiques. En Ouganda, la loi de 2002 contre le terrorisme autorise la mise sur écoute et la perquisition de sociétés de médias s'il existe des «motifs raisonnables particuliers» de penser que l'information présente un «intérêt non négligeable» aux fins d'une enquête antiterroriste[49]. Le Rapporteur spécial souligne que l'intérêt légitime à la divulgation d'informations confidentielles détenues par des journalistes ne l'emporte pas sur l'intérêt du public à ce que ces informations ne soient pas divulguées sauf si la preuve est apportée que c'est absolument nécessaire, si la situation est suffisamment grave et urgente et s'il est démontré que l'impératif de divulgation répond à un besoin social urgent[50].

36. L'exercice d'une surveillance menace aussi les droits relatifs à la liberté d'association et à la liberté de réunion. Pour jouir de ces libertés, les personnes doivent souvent se réunir et communiquer en privé afin de s'organiser face aux pouvoirs publics ou à d'autres acteurs puissants. L'extension des pouvoirs de surveillance a eu parfois des effets insidieux, lorsque des services de police ou de renseignements ont qualifié de terroristes certains groupes afin de pouvoir exercer des pouvoirs de surveillance qui ne leur étaient accordés qu'au titre de la lutte contre le terrorisme. Aux États-Unis, des militants écologistes et d'autres contestataires pacifiques ont été placés sur des listes de personnes à surveiller par la police de l'État du Maryland avant les conventions électorales de New York et de Denver[51]. Au Royaume-Uni, des caméras de surveillance sont fréquemment utilisées lors de manifestations politiques et les images conservées dans une base de données[52]. D'après un récent sondage effectué au Royaume-Uni, un tiers des personnes sont réticentes à participer à des manifestations car elles s'inquiètent pour leur vie privée[53].

---

[46] Voir American Civil Liberties Union, "ACLU uncovers FBI Surveillance of main peace activists", 25 octobre 2006.

[47] Voir D. S. Sidhu, "The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, vol. 7 (2007), p. 375.

[48] A/HRC/6/17/Add.3, par. 51.

[49] Loi contre le terrorisme, troisième partie, par. 8.

[50] Voir également la recommandation n° R (2000) 7 du Comité des ministres du Conseil de l'Europe aux États membres sur le droit des journalistes de ne pas révéler leurs sources d'information; ainsi que Cour supérieure de justice de l'Ontario, *O'Neill* v. *Canada* (*Attorney General*), 2006, par. 163.

[51] Voir L. Rein et J. White, "More groups than thought monitored in police spying", *The Washington Post*, 4 janvier 2009.

[52] Voir P. Lewis et M. Vallée, "Revealed: police databank on thousands of protesters", *The Guardian*, 6 mars 2009.

[53] Voir A. Jha et J. Randerson, "Poll shows public disquiet about policing at environmental protests", *The Guardian*, 25 août 2009.

37. La surveillance peut aussi avoir un effet important sur la liberté de circulation. L'établissement de listes secrètes de personnes à surveiller, la collecte et le partage abusifs de données et l'imposition de systèmes de détection intrusifs ou de la biométrie sont autant d'obstacles supplémentaires à la mobilité. Comme on l'a vu plus haut, le volume d'informations collectées tant sur les personnes qui voyagent dans leur pays que sur les voyageurs internationaux a sensiblement augmenté. Il est courant que des informations soient échangées et utilisées pour établir des listes de surveillance, d'où l'apparition de nouvelles entraves aux déplacements. Lorsque des profils et des listes de surveillance sont dressés à partir d'informations provenant de sources multiples et plus ou moins fiables, les personnes peuvent ne pas savoir du tout d'où proviennent ces informations, ne pas mettre en doute leur véracité et ne disposer d'aucun droit de contester les conclusions auxquelles sont parvenues les autorités d'un pays étranger. Une mosaïque de données assemblée à partir de sources multiples peut amener des algorithmes d'extraction de données à désigner des personnes innocentes comme des menaces[54]. Si des personnes tombent sous le coup d'une interdiction de quitter un pays, l'État doit donner des informations sur les raisons qui imposent une restriction à la liberté de circulation. Dans le cas contraire, l'État est susceptible de violer l'article 12 du Pacte international relatif aux droits civils et politiques[55].

38. Un des effets les plus graves des mesures de surveillance est qu'elles peuvent conduire à des erreurs judiciaires et violer les garanties d'une procédure régulière. L'accès à un recours judiciaire pose un problème dans certains régimes juridiques qui ne permettent pas l'accès aux tribunaux à moins que l'intéressé puisse démontrer qu'une ingérence a été commise, ce que ne permet pas le caractère secret des programmes de surveillance. Les individus peuvent ne pas être en mesure de prouver ou de démontrer qu'ils sont effectivement sous surveillance. De ce fait, ils ne peuvent pas s'adresser à un tribunal pour demander réparation. Dans des affaires de ce type, des tribunaux ont estimé que des personnes n'avaient pas qualité pour agir faute d'avoir pu démontrer qu'elles étaient sous surveillance, et que les préjudices éventuels ne pouvaient être considérés que comme hypothétiques[56]. Dans d'autres affaires où l'ingérence pouvait être prouvée, des États ont parfois invoqué le «secret d'État» pour se soustraire à l'examen de projets de surveillance illégaux[57]. Le Rapporteur spécial souscrit à la position de la Cour européenne des droits de l'homme (CEDH) sur le fait qu'une personne n'est pas tenue de prouver avoir subi une mesure concrète de surveillance[58].

3. Expansion des frontières juridiques

39. Des États concluent des traités d'entraide judiciaire pour pouvoir coopérer à l'occasion d'enquêtes et échanger des renseignements dans telle ou telle affaire[59]. Ils en concluent aussi pour pouvoir échanger des renseignements sur les personnes en fonction de leur activité, par exemple sur toutes celles qui se rendent dans un pays étranger ou réalisent

[54] Voir United States National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*, octobre 2008.

[55] Voir, dans le même ordre d'idées, Comité des droits de l'homme, *B. Zoolfia* c. *Ouzbékistan*, communication n° 1585/2007, 2009, par. 8.3.

[56] Avis exprimé récemment dans *Amnesty International et al. v. John McConnell et al*, Tribunal de district des États-Unis pour le district sud de New York, 20 août 2009.

[57] Voir Tribunal de district des États-Unis pour le district nord de la Californie, *Al-Haramain Islamic Foundation et al. v. Bush et al.*, 1er mai 2009.

[58] Voir CEDH, *Klass et autres c. Allemagne*, 6 septembre 1978, par. 38.

[59] Voir G. Hosein, International Co-operation as a Promise and a Threat, in Cybercrime and Jurisdiction: A Global Survey (T.M.C. Asser Press), 2006.

des opérations interbancaires. Il existe des accords plus opaques, conclus entre services de renseignements en vue de partager des bases de données et du renseignement. Ces bases de données font souvent l'objet d'amples dérogations au droit national. Même si toutefois la législation interne s'applique, les données peuvent concerner des ressortissants étrangers qui ne peuvent exercer aucun droit devant les juridictions nationales. Les personnes peuvent ne pas être au courant qu'elles sont sous surveillance − ne pas savoir, par exemple, que leur nom figure sur une liste de terroristes présumés − parce que les listes établies par les services de renseignements ne sont pas rendues publiques, ce qui leur interdit tout recours. Dans le cas des listes internationales, il peut être impossible à une personne de déterminer ce qui a d'abord motivé son inscription sur une liste, ou encore, si des listes multiples sont apparues ensuite, d'en faire retirer son nom.

40. Les États n'ont pas seulement intensifié leur coopération mutuelle en matière de lutte contre le terrorisme, mais aussi leur coopération avec des tiers privés qui détiennent des données à caractère personnel sur des individus, dans le but de repérer et de surveiller des personnes soupçonnées de terrorisme. En n'étendant pas les garanties nationales en matière de respect de la vie privée à leur coopération avec des pays tiers et des acteurs privés, certains gouvernements ont fini par compromettre la protection du droit à la vie privée.

41. Des tiers privés comme les banques ou les entreprises de téléphonie, ou même les cybercafés, détiennent désormais d'importants volumes de données personnelles sur les individus. L'accès à cette information procure donc des renseignements non négligeables sur la vie privée des personnes. En même temps, des services de l'État peuvent accéder à cette information avec moins de contraintes que si elle se trouvait au domicile des personnes, voire auprès d'autres services de l'État. Aux États-Unis, par exemple, la Cour suprême a estimé que, dans la mesure où des informations communiquées à des tiers comme les banques ou les compagnies de téléphone l'étaient «librement», les individus ne pouvaient pas raisonnablement s'attendre au respect de leur vie privée[60]. En l'absence de garanties constitutionnelles prescrivant un cadre juridique en matière d'ingérence dans la vie privée des personnes, c'est à l'entreprise privée qu'il revient de décider comment elle donne suite à une demande émanant des services d'un État. En règle générale, le secteur privé préfère que le cadre juridique par lequel des entreprises peuvent être contraintes à produire des données à caractère personnel soit fixé par l'État, car les entreprises sont ainsi dégagées de leur obligation d'apprécier chaque cas.

42. Il est aussi de plus en plus demandé à des tiers privés de recueillir plus d'éléments d'information qu'il n'est nécessaire et de les conserver pendant de longues périodes. Le Royaume-Uni, par exemple, a proposé que les sociétés de télécommunications surveillent activement les activités en ligne des individus, y compris dans le cadre de réseaux sociaux, et conservent les données correspondantes − données que ces entreprises n'ont aucun intérêt justifié à collecter[61]. La directive de l'Union européenne sur la conservation des données[62] a été de même très critiquée. Lorsqu'en 2008 en Allemagne, la Cour constitutionnelle fédérale a suspendu temporairement l'application du texte de loi allemand appliquant cette directive, elle a noté que «la conservation de données sensibles,

[60] Voir Cour suprême des États-Unis, *Smith v. Maryland*, 1979, dans le cas de données sur les communications, et *United States v. Miller*, 1976, dans le cas de renseignements financiers.

[61] Voir British All Party Parliamentary Group on Privacy, Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme, juin 2009.

[62] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *Journal officiel de l'Union européenne*, L 105(2006), p. 54 à 63.

globalement et sans motif, sur presque tous les individus, pour un usage de l'État qu'il est impossible de prévoir en détail au moment du stockage des données, peut produire un effet d'intimidation considérable»[63]. Toujours en Allemagne, des études ont signalé une conséquence inquiétante des politiques de conservation des données: 52 % des personnes interrogées ont indiqué qu'il était peu probable qu'elles utiliseraient les télécommunications pour se mettre en relation avec un toxicologue, un psychothérapeute ou un conseiller conjugal en raison des lois sur la conservation des données[64].

43. Dans ce contexte, le Rapporteur spécial constate avec inquiétude que de nombreux pays ont adopté des lois sur la conservation des données sans assortir l'accès à cette information d'aucune garantie juridique ni tenir compte du fait que l'évolution technologique rendait la distinction entre données de contenu et données de communication de plus en plus floue. Si les dispositions constitutionnelles exigent souvent d'entourer de garanties l'accès au contenu des communications, la protection des relevés de communications est plus limitée. Bien que parfois essentiel à une enquête, ce type d'information peut être tout aussi sensible du point de vue du respect de la vie privée que le contenu des communications.

44. Afin de lutter contre le financement du terrorisme et le blanchiment de capitaux, les États ont contraint le secteur financier à analyser les opérations financières de façon à distinguer automatiquement les opérations «normales» des opérations «suspectes». Par exemple, l'Union européenne a établi en 2005 une directive visant à «prévenir l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme»[65], qui oblige les établissements financiers à être vigilants en signalant les activités suspectes ou les opérations dépassant certains seuils à des cellules de renseignement financier (CRF). Le traitement supplémentaire de ces données par les CRF reste opaque, mais des États comme l'Australie[66] et le Canada[67] traitent des millions de transactions chaque année à l'aide d'outils perfectionnés d'extraction de données.

45. Des tiers peuvent aussi être assujettis à des lois étrangères imposant des obligations en matière de divulgation d'informations. Le Gouvernement des États-Unis, par exemple, a adressé des demandes d'obtention de pièces à la Society for Worldwide Interbank Financial Telecommunication (SWIFT), la société coopérative de droit belge qui gère l'échange de messages financiers entre plus de 7 800 institutions financières dans plus de 200 pays. En obtenant l'accès au centre de données de la SWIFT aux États-Unis, l'administration du Trésor a ensuite été en mesure de surveiller les opérations financières à l'étranger transitant par le réseau SWIFT, afin de rechercher et d'identifier des personnes soupçonnées de terrorisme[68]. Des groupes de défense des droits de l'homme ont déposé plainte devant plus

[63] Décision de la Cour constitutionnelle n° 256/08, 11 mars 2008.

[64] Institut Forsa (Allemagne), *Meinungen der Bunderburger zur Vorratsdatanspeicherung*, 28 mai 2008.

[65] Voir la Directive 2005/60/EC du Parlement européen et du Conseil du 26 octobre 2005 visant à prévenir l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme, Journal officiel, *L 309 (2005), p. 15 à 36.*

[66] Voir Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2008-09*, octobre 2009.

[67] Voir Financial Transaction and Reports Analysis Centre of Canada, *FINTRAC Annual Report 2008*, 11 septembre 2008.

[68] Voir également les déclarations de Stuart Levey, Sous-Secrétaire d'État des États-Unis chargé du renseignement sur le financement du terrorisme, au sujet du Programme de surveillance des activités de financement du terrorisme, 23 juin 2006.

d'une vingtaine de tribunaux en faisant valoir que, en remettant ces informations aux autorités des États-Unis, la SWIFT violait la législation locale sur le droit à la vie privée[69].

46. Le Rapporteur spécial s'inquiète aussi de ce l'on intègre la surveillance dans des infrastructures technologiques, qui créeront des risques pour les individus et les organisations. Par exemple, l'élaboration de normes concernant l'interception légitime de certaines communications oblige les sociétés de télécommunications à prévoir des failles dans la conception de leurs technologies afin que les États soient en mesure d'intercepter des communications. Ces moyens ont été utilisés abusivement en Grèce lorsque des tiers non identifiés sont parvenus à écouter les communications du Premier Ministre grec et de dizaines d'autres hauts responsables[70]. Plus récemment, les mêmes moyens auraient été utilisés par le Gouvernement de la République islamique d'Iran pour surveiller les contestataires[71]. Pour éviter les abus, les systèmes de surveillance devraient tenir un registre des personnes ayant accédé aux données, la trace ainsi conservée permettant de détecter les abus[72].

47. Dans certains pays, des garanties constitutionnelles continuent toutefois de s'appliquer. Au Canada, par exemple, la Charte des droits et libertés protège la confidentialité des renseignements détenus par des tiers s'ils révèlent des «détails intimes sur le mode de vie et les choix personnels de l'individu»[73]. Il convient donc de pondérer les droits sociétaux à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi[74]. La jurisprudence de la Cour européenne des droits de l'homme a, de façon analogue, étendu le droit à la confidentialité aux renseignements détenus par des tiers. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel oblige aussi bien le secteur public que le secteur privé à protéger les renseignements qu'ils détiennent et réglemente la communication d'informations à des services de l'État. Des exceptions s'appliquent lorsqu'une mesure est nécessaire à la protection de la sécurité de l'État, à la sûreté publique ou aux intérêts monétaires de l'État; à la répression des infractions pénales; ou à la protection de la personne concernée et des droits et libertés d'autrui[75].

D. Pratiques de référence

48. Le Rapporteur spécial constate avec préoccupation l'existence d'une tendance des États à étendre les pouvoirs de surveillance hors du champ de la lutte contre le terrorisme. Au lendemain des événements du 11 septembre 2001, un certain nombre d'assemblées législatives ont adopté des clauses d'extinction et de réexamen dans le cadre des législations antiterroristes, en partant du principe que des pouvoirs extraordinaires seraient peut-être indispensables pendant un court laps de temps pour faire face à la situation dangereuse qui existait alors. Ces clauses d'extinction et de réexamen n'ont pas été adoptées dans certains domaines de l'action gouvernementale, et n'ont même pas été

[69] Voir, par exemple, Privacy International, «Pulling a Swift one? Bank transfer information sent to U.S. authorities», 27 juillet 2006.

[70] Voir, pour information, V. Prevelakis et D. Spinellis, «The Athens Affair», *IEEE Spectrum*, juillet 2007.

[71] Voir, pour information, Nokia Siemens Networks, «Provision of lawful intercept capability in Iran», 22 juin 2009.

[72] Voir note 54.

[73] Voir Cour suprême du Canada, *R. c. Plant*, 1993, et *R. c. Tessling*, 2004.

[74] *R. c. Plant*.

[75] Art. 9 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

envisagées dans le cadre de politiques ultérieures. Bien souvent, les pouvoirs d'enquête accordés aux services de répression dans le cadre des lois antiterroristes peuvent être utilisés pour mener des investigations sans rapport avec le terrorisme. De leur côté, les États calquent leurs politiques les uns sur les autres sans tenir compte des conséquences pour les droits de l'homme. Bon nombre des politiques décrites plus haut ont d'abord constitué des mesures d'exception, mais sont ensuite rapidement devenues la norme aux niveaux régional et international. Collectivement, ces ingérences sont très préjudiciables à la protection du droit à la vie privée, car l'accès aux garanties légales est limité. Sans un ensemble rigoureux de garanties légales et sans moyen de mesurer la nécessité, la proportionnalité ou le caractère raisonnable des ingérences, les États ne disposent pas d'indications sur la manière d'atténuer les risques pour la vie privée créés par leurs politiques nouvelles. Le Rapporteur spécial a recensé les mesures de protection juridique apparues dans le monde dans le cadre de l'élaboration et de l'analyse des politiques, de la jurisprudence et des bonnes pratiques.

1. Principe selon lequel l'intrusion dans la vie privée doit être minimale

49. Certaines immixtions dans la vie privée des personnes sont plus intrusives que d'autres. Le champ de la protection constitutionnelle des biens et des personnes s'est élargi ces cinquante dernières années aux communications[76], aux renseignements biographiques d'ordre personnel[77] et à l'application d'un droit à la confidentialité et à l'intégrité des données pour les systèmes informatisés[78]. Ces protections obligent les États à avoir épuisé les procédés les moins intrusifs avant de recourir à d'autres. La commission des affaires intérieures du Parlement du Royaume-Uni a dégagé de l'examen ces idées, adaptées aux systèmes modernes de surveillance centrée sur les données, le principe de limitation du champ de collecte des données, lui-même étroitement lié au principe de finalité[79]. Dans son analyse, la commission parlementaire a estimé que les gouvernements devraient «résister à la tendance consistant à collecter toujours plus de données à caractère personnel et à créer des bases de données toujours plus volumineuses. Toute décision de créer une base de données importante, d'autoriser un partage de données ou de donner suite à des propositions qui augmenteraient la surveillance, devrait être fondée sur un besoin avéré». Le Rapporteur spécial est d'avis que les États doivent incorporer ce principe dans leurs politiques actuelles et futures et expliquer en quoi leurs politiques sont nécessaires et proportionnées.

2. Restriction des usages secondaires des données eu égard au principe de finalité

50. Alors que le droit relatif à la protection des données est censé protéger les renseignements recueillis à certaines fins, contre toute utilisation qui en serait faite à d'autres fins, les politiques liées à la sécurité nationale et les politiques répressives échappent généralement à de telles restrictions. Cela se traduit par la présence de clauses de secret dans les notifications d'accès légal; des demandes de production de pièces, rédigées en termes vagues, et des procédures dérogatoires comme les décrets au nom de la sécurité nationale, en vertu desquels une base de données peut déroger aux lois sur la protection de la vie privée. Le Rapporteur spécial s'inquiète de ce que cela limite l'efficacité des sauvegardes nécessaires contre les abus. Les États doivent avoir l'obligation d'indiquer le fondement juridique autorisant la réutilisation d'informations, conformément aux principes du droit constitutionnel et des droits de l'homme. Ils doivent agir dans le cadre des droits de

[76] Voir Cour suprême des États-Unis, *Katz v. United States*, 1967.

[77] Voir note 74.

[78] Voir décision n° 370/07 de la Cour constitutionnelle allemande, 27 février 2008.

[79] Voir commission des affaires intérieures du Parlement du Royaume-Uni, *A Surveillance Society? Fifth report of the session 2007-2008*, 8 juin 2008.

l'homme et non pas recourir à des dérogations et des exemptions. C'est particulièrement important lorsque des renseignements sont échangés d'un État à un autre; dans ce cas, les protections et garanties doivent continuer de s'appliquer[80].

3. Principe de contrôle et de réglementation de l'accès légal

51. Les systèmes de surveillance doivent être soumis à un contrôle efficace si l'on veut limiter les risques de préjudice et d'abus. S'il existe des garanties, cela prend le plus souvent la forme d'une autorisation indépendante résultant d'un mandat de l'autorité judiciaire et/ou d'une ordonnance demandant la production de pièces avec possibilité de recours indépendant. Les politiques qui tentent de limiter les contrôles et d'abaisser les seuils d'autorisation sont pourtant nombreuses: des lois sur l'interception des communications ont réduit les critères d'autorisation applicables à certaines communications au minimum; des ordonnances ont été prises au secret pour accéder à des renseignements détenus par des tiers, ce qui réduit la possibilité de se prévaloir des protections judiciaires; et des États laissent de plus en plus les services de renseignement et de police s'autoriser eux-mêmes l'accès à des données personnelles, alors qu'auparavant ils avaient besoin d'une forme ou une autre d'autorisation indépendante et de suivi effectif.

52. Certains États ont pris des mesures pour remédier à la dégradation des garanties. Aux États-Unis, après un certain nombre d'affaires judiciaires et par suite de l'obligation de renouvellement des autorisations prévue dans la loi connue sous le nom de «USA Patriot Act», des possibilités supplémentaires de contrôle judiciaire ont été rétablies. Des modifications apportées aux pratiques de surveillance des communications en Suède et aux États-Unis ont restauré des garanties limitées sous forme de mandats de l'autorité judiciaire. La Cour européenne de justice a estimé quant à elle que les tribunaux devaient contrôler la légalité, par rapport au droit interne, des listes de surveillance internationales[81].

53. Le Rapporteur spécial constate avec préoccupation que le manque de contrôle effectif et indépendant des pratiques et techniques de surveillance conduit à se demander si ces ingérences sont légales − et donc soumises à l'obligation de rendre des comptes − et nécessaires − ce qui soulève la question de la proportionnalité des mesures appliquées. Il rend hommage au travail considérable des autorités de contrôle nationales, y compris les services internes chargés de contrôler le respect de la vie privée, les services d'audit et les inspections générales, qui jouent eux aussi un rôle essentiel pour repérer les abus. Le Rapporteur spécial préconise donc de renforcer les mécanismes de contrôle interne en complément des processus d'autorisation et de contrôle externes indépendants. Grâce à ce système de suivi interne et externe, les individus disposeront de recours efficaces et d'un véritable accès à des mécanismes de réparation.

4. Principe de transparence et d'intégrité

54. Le fait de reconnaître un droit au secret aux systèmes de surveillance rend les assemblées législatives, les organes judiciaires et le public plus difficilement à même d'exercer un contrôle sur les pouvoirs de l'État. Des individus peuvent être soumis à une surveillance indue, facilitant la création de profils à partir de l'extraction de données, et à des jugements erronés, sans avoir été jamais informés auparavant de cette pratique. En

[80] Voir, par exemple, en ce qui concerne les dossiers de passagers, l'avis 8/2004 du Groupe de travail «Article 29» sur l'information des passagers concernant les transferts des données des dossiers passagers (Passenger Name Record – PNR) relatives aux vols entre l'Union européenne et les États-Unis d'Amérique, 30 septembre 2004.

[81] *Yassin Abdullah Kadi et Al Barakaat International Foundation/Conseil et Commission*, septembre 2008.

outre, faute de limites précises et raisonnables aux politiques de surveillance, il est difficile de prouver que ces pouvoirs ne sont pas utilisés de manière arbitraire et aveugle.

55. Le principe de transparence et d'intégrité suppose l'ouverture et la communication au sujet des pratiques de surveillance. Dans certains pays, les individus doivent être informés immédiatement, ou dans les meilleurs délais, qu'ils sont placés sous surveillance et des modalités de cette surveillance. Dans les régimes constitutionnels d'Amérique latine où il existe un droit d'*habeas data*[82], et d'après les lois européennes de protection des données, les individus doivent pouvoir accéder aux données à caractère personnel les concernant qui se trouvent dans des banques de données et des systèmes de surveillance. Les États doivent garantir ces droits indépendamment des frontières, en veillant à ce que les régimes juridiques protègent aussi bien les citoyens que les non-citoyens.

56. Les techniques de surveillance doivent absolument faire l'objet d'un débat ouvert et d'un examen approfondi afin que le public en saisisse les avantages et les limites et en vienne à comprendre la nécessité et la légalité de la surveillance. Dans nombre de pays, le parlement et des organismes indépendants ont été chargés de passer en revue les politiques et procédures de surveillance, parfois avant l'élaboration d'une loi, grâce notamment aux clauses d'extinction et de réexamen prévues dans les lois.

5. Principe de modernisation efficace

57. Alors même que l'on accède de plus en plus facilement à des données personnelles sensibles, les États n'ont pas mis en place de protections adaptées. En fait, au nom de la modernisation de leurs pouvoirs de surveillance, les États ont parfois cherché délibérément à appliquer des régimes de protection plus anciens et plus fragiles à des catégories de données toujours plus sensibles[83]. Conscients de la nécessité d'examiner en quoi l'évolution des techniques et des politiques pouvait avoir des conséquences néfastes pour les individus, certains États ont adopté des mesures d'évaluation de l'impact sur le droit à la vie privée qui font entrer en considération le respect de la vie privée dans la conception des nouveaux procédés de surveillance, y compris en évaluant comment les décideurs ont tenu compte des nombreux principes énoncés précédemment − intrusion minimale dans la vie privée et droits de recours, notamment. Le Rapporteur spécial estime que le recours à des outils comme l'évaluation de l'impact sur le droit à la vie privée peut aider à informer le public des pratiques de surveillance, tout en suscitant une culture du respect de la vie privée de la part des organes de l'État lorsque ceux-ci définissent de nouveaux systèmes de surveillance pour lutter contre le terrorisme. Des normes internationales doivent aussi être adoptées pour obliger les États à améliorer leurs protections à mesure que les techniques évoluent.

IV. Conclusions et recommandations

A. Conclusions

58. **Le Rapporteur spécial constate avec préoccupation que ce qui était auparavant l'exception est désormais courant. En premier lieu, les États ne limitent plus les dispositifs de surveillance exceptionnels à la lutte contre le terrorisme; au lieu de cela, ils permettent le recours à ces pouvoirs à tout propos. En deuxième lieu, la**

[82] Voir, par exemple, Constitution du Brésil, art. 5 (LXXI); Constitution du Paraguay, art. 135; Constitution de l'Argentine, art. 43.

[83] Voir Policy Engagement Network, *Briefing on the UK Government's Interception Modernisation Programme*, juin 2009.

surveillance est désormais ancrée dans l'élaboration des politiques. Il appartient maintenant à ceux qui contestent des projets de surveillance injustifiés de démontrer pourquoi ces informations supplémentaires ne doivent pas être recueillies, au lieu que ce soient les États, assumant la charge de la preuve, qui justifient pourquoi l'ingérence est nécessaire. En troisième lieu, la qualité et l'efficacité de presque toutes les protections et garanties légales ont été réduites et ce, alors même que l'évolution technologique autorise des pouvoirs de surveillance accrus et plus étendus. Le plus inquiétant, cependant, est que ces technologies et politiques s'exportent actuellement vers d'autres pays, en perdant souvent au passage leurs éléments de protection les plus élémentaires.

59. **Il est indispensable d'élaborer des normes juridiques internationales afin de se prémunir contre ces formes d'abus. Les principes esquissés dans le présent rapport peuvent y contribuer: il s'agit notamment de veiller à ce que la surveillance constitue une intrusion aussi minime que possible, et à ce que de nouveaux pouvoirs ne soient pas mis en œuvre sans garanties et limites appropriées, sans procédures de contrôle et d'autorisation efficaces, et sans qu'il soit rendu des comptes régulièrement, le tout accompagné d'informations détaillées concernant l'impact sur la vie privée. Le grand public et les assemblées élues ont rarement eu l'occasion de débattre sur le point de savoir si de tels pouvoirs antiterroristes étaient nécessaires, proportionnés et raisonnables. De l'avis du Rapporteur spécial, chacun gagnerait sans doute à ce que les bonnes pratiques qui commencent à se faire jour soient suivies.**

B. Recommandations

Recommandations adressées aux assemblées législatives

60. **Le Rapporteur spécial recommande à nouveau que toute ingérence dans le droit à la vie privée et à la famille et à l'inviolabilité du domicile et de la correspondance soit autorisée par des dispositions légales qui soient accessibles au public, soient particulièrement précises, soient proportionnées à la menace pour la sécurité, et offrent des garanties efficaces contre les abus. Les États devraient veiller à ce que les autorités compétentes appliquent des méthodes d'enquête moins intrusives si, ce faisant, il est possible de détecter, prévenir ou poursuivre les infractions terroristes avec une efficacité suffisante. Le pouvoir de décision devrait être structuré de telle sorte que plus l'ingérence dans la vie privée est importante, plus le niveau d'autorisation est élevé.**

61. **Le respect des normes internationales en matière de protection de la vie privée et des droits de l'homme doit être un principe fondamental du droit national. Une législation complète sur la protection des données et le droit à la vie privée s'impose donc si l'on veut qu'il existe des protections juridiques claires pour les individus et que des données personnelles ne puissent pas être collectées abusivement; que le nécessaire soit fait pour assurer l'exactitude des données; que des limites soient créées à l'utilisation, au stockage et à la communication de ces données; et qu'il soit obligatoire d'informer les individus de la manière dont leurs données sont utilisées et du droit qu'ils ont d'y avoir accès et de les rectifier, indépendamment de leur nationalité et de la juridiction dont ils relèvent.**

62. **Des instances de contrôle indépendantes, dotées de mandats robustes, doivent être créées pour examiner les politiques et les pratiques, afin de permettre un contrôle strict de l'utilisation de procédés de surveillance intrusifs et du traitement des informations à caractère personnel. Ainsi, il ne doit y avoir aucun système secret de surveillance qui ne soit placé sous la supervision d'une instance de contrôle efficace, ni**

aucune ingérence qui ne soit autorisée par l'intermédiaire d'un organisme indépendant.

63. **Dans tous les cas, il est indispensable d'évaluer l'impact des politiques de lutte contre le terrorisme, actuelles ou en projet, sur l'exercice du droit à la vie privée, afin d'examiner et de faire connaître comment les politiques et technologies considérées préviennent les risques pour la vie privée et en tiennent compte dès le début du processus d'élaboration des politiques.**

64. **Le Rapporteur spécial recommande de formuler des garanties plus fermes pour que le partage de renseignements entre gouvernements continue de protéger le droit à la vie privée des individus.**

65. **Le Rapporteur spécial recommande aussi que l'on élabore des règles plus fermes en vue de limiter l'accès de l'État à des informations détenues par des tiers, notamment des procédures de notification, et de faire porter le moins possible à des tiers la responsabilité de la collecte d'informations supplémentaires, et que les garanties constitutionnelles et légales s'appliquent lorsque des tiers agissent au nom de l'État.**

66. **Le Rapporteur spécial appelle l'attention sur la nécessité de repenser la formulation des lois pour empêcher que des pouvoirs liés à la lutte contre le terrorisme ne soient utilisés à d'autres fins. Tout nouveau système doit se voir attribuer, dès sa conception, une finalité bien précise.**

Recommandations adressées aux gouvernements

67. **Le Rapporteur spécial encourage vivement les gouvernements à expliquer en détail comment les principes de proportionnalité et de nécessité sont respectés dans leurs politiques de surveillance, conformément aux normes internationales relatives aux droits de l'homme, et quelles mesures ont été prises pour établir des garanties contre les abus.**

68. **Le Rapporteur spécial recommande que les programmes de surveillance centrée sur des données fassent l'objet d'un débat ouvert et qu'il soit régulièrement rendu compte de ces programmes. Le fait de rendre compte aux organes législatifs et aux instances de contrôle, et de soumettre les pratiques à des examens indépendants peut contribuer à éclairer la formulation des politiques futures et les délibérations sur les politiques de lutte contre le terrorisme.**

69. **Tout programme de surveillance utilisant des listes ou des profils de personnes à surveiller doit prévoir des garanties de procédure régulière pour toutes les personnes, notamment un droit de recours. Le principe de transparence doit être appliqué afin que les personnes puissent savoir, sans difficultés indues, pourquoi et comment elles ont été inscrites sur des listes de surveillance, ou comment leur profil a été établi, et de quels recours elles disposent.**

70. **Étant donné les risques inhérents aux systèmes d'extraction de données, le Rapporteur spécial recommande que tout programme antiterroriste centré sur des données soit soumis à un contrôle strict et indépendant. En outre, il se prononce contre le développement et l'utilisation de procédés d'extraction des données à des fins de lutte contre le terrorisme.**

71. **Compte tenu des risques d'utilisation abusive des techniques de surveillance, le Rapporteur spécial recommande que le même volume de moyens de recherche et de développement soit consacré à des techniques qui renforcent la protection de la vie privée.**

Recommandations adressées au Conseil des droits de l'homme

72. **Le Rapporteur spécial recommande l'élaboration d'un programme pour le renforcement des capacités à l'échelle mondiale en matière de protection de la vie privée. Pour faire contrepoids au phénomène de transposition des lois antiterroristes de pays à pays, ainsi qu'aux normes actuellement observées dans le monde en matière de surveillance, il faut une meilleure prise de conscience des garanties nécessaires à la protection de la dignité des individus.**

73. **Le Rapporteur spécial encourage vivement le Conseil des droits de l'homme à mettre en place un processus s'inspirant des principes existants sur la protection des données pour recommander des mesures visant l'élaboration d'une déclaration mondiale sur la protection et la confidentialité des données.**

Recommandations adressées au Comité des droits de l'homme

74. **Le Rapporteur spécial recommande au Comité des droits de l'homme d'entreprendre la rédaction d'une nouvelle observation générale sur l'article 17 du Pacte international relatif aux droits civils et politiques, dans le but de formuler les conditions dans lesquelles des restrictions peuvent être permises, et de fournir ainsi aux États des orientations sur les garanties appropriées. L'observation générale devrait aussi accorder l'attention voulue à la protection des données en tant qu'attribut du droit à la vie privée au sens de l'article 17 du Pacte.**