Standards internationaux

Compilation de bonnes pratiques pour le contrôle des services de renseignement

Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste

Centre pour le Contrôle Démocratique des Forces Armées - Genève (DCAF)

Standards internationaux

Compilation de bonnes pratiques pour le contrôle des services de renseignement

Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste

Centre pour le Contrôle Démocratique des Forces Armées - Genève (DCAF)

À propos de DCAF

Le Centre pour le Contrôle Démocratique des Forces Armées – Genève (DCAF) promeut la bonne gouvernance et la réforme du secteur de la sécurité. Le Centre mène des recherches sur les bonnes pratiques et encourage la mise en place de normes appropriées aux niveaux national et international. Il émet en outre des recommandations de politique générale, fournit un soutien consultatif aux acteurs sur le terrain ainsi que des programmes d'assistance pratique. Les partenaires de DCAF sont des gouvernements, des parlements, des sociétés civiles, des organisations internationales ainsi que les forces de sécurité tels que les forces de police, les autorités judiciaires, les services de renseignements, les services des douanes et les armées.

De plus amples informations sur DCAF sont disponibles sur :
www.dcaf.ch

Remerciements

DCAF souhaite remercier les membres du comité de rédaction pour leur engagement et le temps qu'ils ont consacré à l'examen de cette brochure.

Ceci est une reproduction du rapport de l'ONU A/HRC/14/46, rédigé le 17 mai 2010. La langue d'origine de ce rapport est l'anglais. La traduction française est la traduction officielle de l'ONU.

Éditeur

Centre pour le Contrôle Démocratique des Forces Armées – Genève.

Image de couverture : Logo Conseil des droits de l'homme des Nations Unies.

ISBN: 978-92-9222-156-0

Comité de rédaction

Le comité de rédaction de la série de brochures sur le contrôle du renseignement comprend :

- Hans Born, Genève
- Arnold Luethold, Genève

Rédacteur de la série

- Aidan Wills, Genève

TABLE DES MATIÈRES

Introduction au guide

Légiférer sur le secteur de la sécurité est une tâche complexe et ardue. Il est donc tentant pour de nombreux législateurs de reproduire la législation d'autres pays. Cela accélère le processus de rédaction, particulièrement lorsque les textes sont disponibles dans la langue du législateur. Malheureusement, le résultat est le plus souvent une mauvaise législation. Même une fois amendées, ces lois copiées sont souvent obsolètes avant même d'entrer en vigueur. Elles ne sont parfois plus conformes aux normes internationales, ou alors elles ne répondent pas totalement aux besoins locaux. En outre, ces lois sont parfois en contradiction avec la législation nationale en vigueur.

Dans certains cas, il n'y a simplement aucun modèle de loi disponible dans la région pour le type de législation nécessaire. Cela est relativement courant dans le monde arabe, où les questions relatives au secteur de la sécurité commencent à peine à être publiquement débattues. Il est donc difficile de trouver des modèles de lois adéquats sur la police ou sur le contrôle parlementaire des services de renseignements.

Par conséquent, il n'est pas surprenant que de nombreux législateurs des pays arabes se soient sentis dépités ou dépassés par l'ampleur de la tâche. Ils ont rencontré de nombreuses difficultés en termes d'accès aux normes internationales étant donné la rareté, voir l'absence, de ressources disponibles en arabe. Nombre d'entre eux ne savaient pas où chercher des modèles de lois et étaient sur le point d'abandonner. Certains ont finalement sollicité l'aide de DCAF.

L'idée d'un guide pratique pour les législateurs du monde arabe est née du constat de ce manque de ressources. Les juristes recherchaient des standards et extraits de lois en arabe qui pourraient les aider à rédiger de nouvelles lois. Des experts du monde arabe et DCAF ont donc décidé de collaborer et développer des outils pour les législateurs.

A qui s'adresse ce guide ?

Ce guide s'adresse principalement aux personnes impliquées dans la rédaction de législation pour le secteur de la sécurité dans le monde arabe. Cela inclut des parlementaires, des fonctionnaires, des experts juridiques et des organisations non gouvernementales. Ce guide peut également être utile aux fonctionnaires de sécurité et peut en outre servir d'ouvrage de référence aux chercheurs et aux étudiants intéressés à la législation du secteur de la sécurité.

Que contient ce guide ?

Ce guide bilingue contient une série de brochures, en français et en arabe, qui fournissent des normes et des standards ainsi que des cas pratiques dans différents domaines de la réforme du secteur de la sécurité.

Les séries suivantes ont été publiées ou sont en cours de publication:

- Légiférer sur la police
- Légiférer sur les services de renseignement
- Légiférer sur la justice militaire
- Accord sur le statut des forces

Des séries supplémentaires seront créées en fonction des besoins. La série existante peut d'ailleurs facilement être élargie en ajoutant de nouvelles brochures à la demande des législateurs du monde arabe.

Une liste des publications est régulièrement mise à jour sur : www.dcaf.ch/publications

Quel est le but du guide ?

Le guide fournit un soutien aux législateurs du monde arabe en les aidant à répondre aux attentes des citoyens. Les populations arabes attendent de leurs forces de police et de sécurité un service professionnel et efficace qui répond à leurs besoins. Ils veulent des forces de police et de sécurité qui respectent la loi et les principes des droits humains et qui soient en outre tenues pour responsables de leur performance et de leur conduite. Le guide promeut par conséquent des standards internationaux en matière de législation du secteur de la sécurité

tels que le contrôle démocratique, la bonne gouvernance et la transparence.

Le guide offre un accès facile, en arabe et en français, aux normes internationales ainsi qu'à des exemples de législation hors du monde arabe. Cela permet de comparer des expériences et des pratiques différentes.

Le manque de littérature en arabe concernant la législation du secteur de la sécurité est un problème majeur pour les législateurs du monde arabe. Ce guide cherche à combler ce manque. L'un des ses objectifs est de diminuer le temps que les législateurs passent à chercher des informations, ce qui leur permettra de se concentrer sur leur tâche principale. S'ils disposent de plus d'informations en arabe, il sera plus facile pour les citoyens et organisations de la société civile de formuler leurs attentes vis-à-vis de la police et des forces de sécurité et de participer au développement d'un cadre légal moderne et solide pour le secteur de la sécurité.

Pourquoi est-il important d'avoir un solide cadre légal pour le secteur de la sécurité ?

La mise en place d'un solide cadre légal est une condition nécessaire à une gouvernance efficace et responsable du secteur de la sécurité car le cadre légal :

- Définit le rôle et la mission des différentes organisations de sécurité
- Définit les prérogatives et limite les pouvoirs des organisations de sécurité
- Définit le rôle et les pouvoirs des institutions qui contrôlent les organisations de sécurité
- Fournit une base pour définir la notion de responsabilité car il trace une ligne nette entre les comportements légaux et illégaux
- Augmente la confiance du public et renforce la légitimité du gouvernement et des forces de sécurité.

Pour toutes ces raisons, la réforme du secteur de la sécurité commence souvent par une révision et une réforme complète de la législation nationale du secteur de la sécurité. Le but est d'identifier et de résoudre les contradictions et le manque de clarté concernant les rôles et les mandats des différentes institutions.

Introduction à la Compilation par le DCAF

Le Recueil de bonnes pratiques relatives aux cadres et mesures institutionnels et juridiques qui garantissent le respect des droits de l'homme de la part des services de renseignement dans la lutte contre le terrorisme, y compris en matière de surveillance est la première tentative de la part d'un organe onusien d'identifier des normes sur la gouvernance du renseignement.

Le DCAF a joué un rôle important dans le soutien au Rapporteur Spécial tout au long de l'élaboration du recueil de bonnes pratiques qui est reproduit dans cette brochure. Le Centre a été chargé de rédiger une étude approfondie pour identifier les bonnes pratiques exercées à travers le monde dans chacun des domaines thématiques examinés dans le recueil. Par la suite, le DCAF a mené un processus de consultation multipartite, qui comprenait un atelier d'experts, ainsi que des observations écrites venant de professionnels du renseignement et de la sécurité, d'universitaires, de juristes et de représentants d'ONG. Enfin, le DCAF a travaillé étroitement avec le Rapporteur Spécial dans la rédaction du recueil final. Le Rapporteur Spécial a présenté ce recueil en tant que rapport devant le Conseil des droits de l'homme en juin 2010. Bien que le rapport n'ait pas été soumis à un vote lors du Conseil des droits de l'homme, il a reçu un soutien important de la part de nombreux États lors du dialogue interactif avec le Rapporteur Spécial.

Résumé

Le présent document est une compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans le contexte de la lutte antiterroriste, préparée à la demande du Conseil des droits de l'homme par le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste. Cette compilation est le fruit d'une procédure de concertation à laquelle les gouvernements, les experts et les praticiens ont contribué de diverses manières. En particulier, les documents adressés par écrit par les gouvernements et reçus avant la date butoir du 1er mai 2010 ont été pris en compte. Ces documents seront reproduits sous la forme d'un addendum (A/HRC/14/46/Add.1).

Cette compilation se fonde également sur les instruments internationaux, les résolutions d'organisations internationales et la jurisprudence de juridictions régionales.

Le contenu desdites bonnes pratiques est explicité dans le commentaire, normalement présenté séparément de chacune des 35 pratiques. Les sources des bonnes pratiques sont indiquées dans les notes de bas de page insérées au fil du commentaire, en mentionnant les États spécifiques concernés.

La notion de « bonne pratique » fait référence à des cadres juridiques et institutionnels qui servent à promouvoir les droits de l'homme et le respect de la légalité dans le travail des services de renseignement. L'idée de « bonne pratique » ne renvoie pas seulement à ce qu'exige le droit international, en particulier humanitaire, mais à des pratiques qui vont au-delà de ces obligations juridiques.

Les 35 bonnes pratiques identifiées dans cette compilation sont rassemblées dans quatre sous-domaines, à savoir les fondements juridiques (pratiques 1 à 5), le contrôle et la responsabilisation (pratiques 6 à 10 et 14 à 18), le respect du droit humanitaire substantiel (pratiques 11 à 13, et 19-20) et les questions liées aux fonctions spécifiques des services derenseignement (pratiques 21 à 35).

Résumé des bonnes pratiques

Pratique 1. Les services de renseignement jouent un rôle important dans la protection de la sécurité nationale et de la légalité. Leur principale fonction consiste à rechercher, analyser et diffuser des renseignements qui aident les décideurs et les autres entités publiques à prendre des mesures pour protéger la sécurité nationale, et notamment pour protéger la population et ses droits fondamentaux.

Pratique 2. Le mandat des services de renseignement est défini en termes restrictifs et précis dans une loi accessible au public. Il est strictement limité à la protection d'intérêts légitimes de sécurité nationale indiqués dans des lois ou des mesures relatives à la sécurité nationale, qui sont accessibles au public. Les menaces affectant la sécurité nationale que les services de renseignement sont chargés de traiter sont identifiées. Si le terrorisme fait partie de ces menaces, il est également défini en termes restrictifs et précis.

Pratique 3. Les pouvoirs et compétences dévolus aux services de renseignement sont définis en termes clairs et de manière exhaustive par la législation nationale. Les services de renseignement sont tenus d'utiliser ces pouvoirs exclusivement à des fins conformes aux motifs pour lesquels ils ont été conférés. En particulier, tout pouvoir conféré aux services de renseignement afin de lutter contre le terrorisme doit être utilisé exclusivement à cette fin.

Pratique 4. Tous les services de renseignement sont constitués et opèrent en vertu de lois disponibles au public qui sont conformes à la constitution et au droit humanitaire international. Les services de renseignement peuvent entreprendre, ou recevoir l'ordre d'entreprendre uniquement des activités prescrites par la législation nationale et conformes à ses dispositions. Le recours à une réglementation subsidiaire non publique est strictement limité; ces règles sont à la fois autorisées par la loi et demeurent conformes aux paramètres fixés par les lois publiques. La réglementation non publique ne saurait servir de fondement à une quelconque action restreignant les droits de l'homme.

Pratique 5. Il est explicitement interdit aux services de renseignement de se livrer à des actes quelconques qui seraient contraires à la constitution ou au droit international humanitaire. Cette interdiction vise non seulement les actes des services de renseignement sur leur territoire national, mais aussi leur action à l'étranger.

Pratique 6. Les services de renseignement sont contrôlés par une combinaison d'instances de contrôle interne, exécutif, parlementaire, judiciaire et spécialisé dont les mandats et les compétences reposent sur des lois publiques. Un système efficace de contrôle des services de renseignement inclut au moins une institution civile indépendante des services de renseignement et de l'exécutif. La sphère de compétence combinée des instances de contrôle couvre tous les aspects du travail des services de renseignement: leur respect des lois, l'effectivité et l'efficacité de leurs activités, leurs finances et leurs pratiques administratives.

Pratique 7. Les institutions de contrôle disposent des compétences, des ressources et de l'expertise nécessaires pour engager et conduire leurs propres enquêtes et pour accéder pleinement et sans obstacle à l'information, aux fonctionnaires et aux installations dont elles ont besoin pour remplir leur mandat. Elles bénéficient de l'entière coopération des services de renseignement et des services répressifs pour auditionner les témoins et obtenir des éléments de preuve documentaires et autres.

Pratique 8. Les institutions de contrôle prennent toutes les mesures qui s'imposent pour protéger les renseignements classés et les données personnelles auxquels elles ont accès dans le cadre de leur travail. Des sanctions sont prévues à l'encontre des membres des institutions de contrôle qui enfreignent ces prescriptions.

Pratique 9. Toute personne estimant que ses droits ont été violés par des services de renseignement est habilitée à déposer une plainte auprès d'un tribunal ou d'une institution de contrôle comme le Bureau de médiation, le ou la commissaire aux droits de l'homme ou une institution nationale de défense des droits de l'homme. Les personnes affectées par les

actes illégaux de services de renseignement introduisent un recours devant une institution à même d'y remédier efficacement, notamment en ordonnant que le tort subi soit pleinement réparé.

Pratique 10. Les institutions chargées de traiter les plaintes et les demandes de recours effectif nées des activités des services de renseignement sont indépendantes des services de renseignement et de l'exécutif politique. Ces institutions ont un accès illimité et sans obstacle à toutes les informations pertinentes, aux ressources et à l'expertise nécessaires pour conduire leurs enquêtes, et sont habilitées à délivrer des ordonnances contraignantes.

Pratique 11. Les services de renseignement conduisent leurs travaux d'une manière qui contribue à la promotion et la protection des droits de l'homme et des libertés fondamentales de toutes les personnes placées sous la juridiction de l'État. Les services de renseignement n'opèrent aucune discrimination à l'encontre de personnes ou de groupes en raison de leurs sexe, race, couleur de peau, langue, religion, opinions politiques ou autres, origine nationale ou sociale ou pour toute autre raison.

Pratique 12. Le droit national interdit aux services de renseignement de se livrer à des activités politiques ou d'agir en vue de promouvoir ou protéger les intérêts d'un groupe politique, religieux, linguistique, ethnique, social ou économique particulier.

Pratique 13. Les services de renseignement ne sont pas autorisés à user de leurs pouvoirs contre des activités politiques légales ou de rassemblements et modes d'expression pacifiques.

Pratique 14. Les États assument une responsabilité internationale à l'égard des activités de leurs services de renseignement et de leurs agents ainsi que de tout entrepreneur privé employé par eux, quels que soient l'endroit où ces activités ont lieu et la victime de la conduite ayant causé un préjudice international. C'est pourquoi l'exécutif prend des mesures pour exercer un contrôle global sur ses services de renseignement et assumer ses responsabilités à l'égard de leurs actes.

Pratique 15. Le droit constitutionnel, la législation et le droit pénal international s'appliquent à tous les agents des services de renseignement, comme ils s'appliquent à tout autre fonctionnaire. Les exceptions autorisant les agents des services de renseignement à agir d'une manière normalement contraire aux lois nationales sont strictement limitées et prescrites par la loi. Ces exceptions n'autorisent jamais une violation des normes impératives du droit international ou des obligations de l'État en matière de respect des droits de l'homme.

Pratique 16. Les lois nationales prévoient des sanctions pénales, civiles ou autres à l'encontre de tout membre des services de renseignement ou de toute personne agissant en leur nom qui enfreint ou ordonne d'enfreindre les lois nationales ou le droit international humanitaire. Ces lois établissent également des procédures pour contraindre les auteurs de ces infractions à rendre compte de leurs actes.

Pratique 17. Les agents des services de renseignement sont légalement tenus de refuser de se soumettre à des ordres d'un supérieur qui enfreindraient les lois nationales ou le droit international humanitaire. Dans ce contexte, une protection appropriée est accordée aux agents des services de renseignement réfractaire.

Pratique 18. Des procédures internes sont en place pour permettre aux agents des services de renseignement de signaler les infractions. Elles sont complétées par un organe indépendant dûment mandaté, ayant accès aux informations nécessaires pour conduire des enquêtes approfondies et prendre des mesures pour mettre un terme aux abus lorsque les procédures internes se sont révélées inadéquates. Les agents des services de renseignement qui, de bonne foi, signalent des infractions sont protégés par la loi contre toutes formes de représailles. Sont ainsi protégés ceux qui divulguent des informations aux médias ou à l'opinion publique, s'il s'agit d'une mesure prise en dernier recours et si les faits présentent un intérêt significatif pour l'opinion publique.

Pratique 19. Les services de renseignement et leurs institutions de contrôle prennent des mesures pour encourager le professionnalisme au sein de l'institution et une culture institutionnelle basée sur le respect de la

légalité et des droits de l'homme. En particulier, les services de renseignement sont responsables de former leurs membres aux dispositions pertinentes des droits interne et international, et notamment du droit international humanitaire.

Pratique 20. Toute mesure prise par les services de renseignement de nature à restreindre les droits de l'homme et les libertés fondamentales est conforme aux critères suivants:

a. Les mesures sont prescrites par des lois publiques conformes aux normes du droit international humanitaire;

b. Elles sont strictement nécessaires pour permettre aux services de renseignement de s'acquitter de leurs fonctions, telles qu'elles sont prescrites par la loi;

c. Elles sont proportionnées à l'objectif ciblé; ceci implique que les services de renseignement sélectionnent la mesure la moins restrictive sous l'angle des droits de l'homme, qu'ils soient particulièrement attentifs à minimiser l'impact de ces mesures sur les droits de l'homme, et surtout sur les droits des personnes qui ne sont pas soupçonnées d'avoir enfreint la loi;

d. Les mesures prises par les services de renseignement ne sont en aucun cas contraires aux normes impératives du droit international ou à l'un quelconque des droits fondamentaux de l'homme;

e. Il existe un système clair et exhaustif applicable à l'autorisation, au suivi et au contrôle de toutes les mesures qui restreignent les droits de l'homme;

f. Les personnes dont les droits ont été restreints par les services de renseignement peuvent déposer une plainte auprès d'une institution indépendante pour obtenir un recours effectif.

Pratique 21. Le droit interne définit: le type de mesures de recherche de renseignements à la disposition des services secrets; les objectifs de la recherche de renseignements autorisés; les catégories de personnes et d'activités pouvant être visées par la recherche du renseignement; le niveau de suspicion requis pour justifier le recours à des mesures de recherche du renseignement; la durée maximum d'application desdites mesures; et la procédure d'autorisation, de contrôle et d'analyse du recours à ces mesures.

Pratique 22. Les mesures de recherche du renseignement qui limitent significativement les droits de l'homme sont autorisées et contrôlées par au moins une institution extérieure aux services de renseignement et indépendante d'eux. Cette institution est habilitée à ordonner la révision, la suspension et l'abandon de ces mesures. Celles de ces mesures qui limitent significativement l'exercice des droits de l'homme sont soumises à une procédure d'approbation à plusieurs niveaux, par les services de renseignement eux-mêmes, par l'exécutif politique et par une institution indépendante des services de renseignement et de l'exécutif.

Pratique 23. Une loi publique définit les types de données personnelles que les services de renseignement sont autorisés à détenir, ainsi que les critères applicables à leur utilisation, conservation, suppression et divulgation. Les services secrets sont autorisés à conserver les données personnelles qui sont strictement nécessaires en vue de remplir leur mandat.

Pratique 24. Les services de renseignement évaluent régulièrement la pertinence et l'exactitude des données personnelles qu'ils détiennent. Ils sont tenus par la loi de détruire ou mettre à jour toute information considérée comme inexacte ou ayant cessé d'être pertinente à l'égard de leur mandat, du travail des institutions de contrôle ou d'un éventuel procès.

Pratique 25. Une institution indépendante existe pour contrôler l'utilisation faite des données personnelles par les services de renseignement. Cette institution a accès à tous les fichiers détenus par lesdits services et elle est habilitée à ordonner la divulgation d'informations aux personnes concernées, ainsi que la destruction des fichiers ou des renseignements personnels qu'ils contiennent.

Pratique 26. Les personnes physiques ont la possibilité de demander à accéder aux données personnelles les concernant détenues par les services de renseignement. Elles peuvent exercer ce droit en adressant une requête aux autorités concernées ou par le biais d'une institution indépendante chargée de la protection ou du contrôle des données. Elles ont le droit

de corriger toute erreur contenue dans leurs données personnelles. Les éventuelles exceptions à ces règles générales sont prescrites par la loi, strictement limitées, proportionnées et nécessaires pour permettre aux services de renseignement de remplir leur mandat. Il revient aux services de renseignement de justifier devant une institution de contrôle indépendante toute décision de ne pas communiquer des renseignements personnels.

Pratique 27. Les services de renseignement ne sont pas autorisés à user de leurs pouvoirs d'arrestation et de détention s'ils ne sont pas mandatés pour exercer des fonctions de répression. Ils ne sont pas investis de pouvoirs d'arrestation et de détention si les services répressifs compétents pour accomplir les mêmes actes sont déjà mandatés pour ce faire.

Pratique 28. Si les services de renseignement sont investis de pouvoirs d'arrestation et de détention, ceux-ci sont fondés sur des lois disponibles au public. Ces pouvoirs ne sont exercés que dans les cas où il existe des motifs raisonnables de soupçonner qu'une personne a commis ou est sur le point de commettre une infraction pénale particulière. Les services de renseignement ne sont pas autorisés à priver une personne de sa liberté uniquement à des fins de recherche du renseignement. Le recours des services de renseignement à des pouvoirs d'arrestation et de détention est soumis au même degré de contrôle que le recours à ces pouvoirs par les forces de l'ordre, et notamment à un contrôle judiciaire de la légalité de toute privation de liberté.

Pratique 29. Si les services de renseignement sont investis de pouvoirs d'arrestation et de détention, ceux-ci doivent être conformes aux normes de droit international humanitaire concernant les droits à la liberté, à un procès équitable, et l'interdiction de la torture et des traitements inhumains ou dégradants. Dans l'exercice de ces pouvoirs, les services de renseignement se conforment aux normes internationales notamment énoncées dans l'Ensemble de principes pour la protection de toutes les personnes soumises à une forme quelconque de détention ou d'emprisonnement, le Code de conduite pour les responsables de l'application des lois et les Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois.

Pratique 30. Les services de renseignement ne sont pas autorisés à administrer leurs propres centres de détention ni à faire usage d'un quelconque centre de détention non reconnu administré par des tiers.

Pratique 31. Le partage de renseignements entre différents services de renseignement d'un même État ou avec les autorités d'un autre État est fondé sur une loi nationale qui définit les paramètres de l'échange de renseignements, et notamment les conditions devant être réunies pour que des informations puissent être partagées, les instances avec lesquelles le partage de renseignement est permis et les garanties entourant l'échange de renseignements.

Pratique 32. La législation nationale définit la procédure d'autorisation des accords de partage de renseignements, ainsi que la procédure applicable au partage ad hoc de renseignements. Tout accord de partage de renseignements avec une entité étrangère doit être approuvé par l'exécutif, de même que tout partage de renseignements pouvant avoir des conséquences importantes pour les droits de l'homme.

Pratique 33. Avant de conclure un accord de partage de renseignements ou de procéder à un partage ad hoc de renseignements, les services de renseignement évaluent les résultats de leurs homologues dans le domaine des droits de l'homme et de la protection des données, ainsi que les garanties légales et les contrôles institutionnels auxquels ils sont soumis. Avant de transmettre des informations, les services de renseignement s'assurent que toutes les données partagées sont pertinentes eu égard au mandat du récepteur, qu'elles seront utilisées conformément aux conditions stipulées et qu'elles ne seront pas utilisées à des fins contraires aux droits de l'homme.

Pratique 34. Les institutions indépendantes de contrôle sont en mesure d'examiner les accords de partage de renseignements, ainsi que toute information adressée par des services de renseignement à des entités étrangères.

Pratique 35. Il est expressément interdit aux services de renseignement de recourir à l'assistance de services de renseignement étrangers de quelque manière que ce soit, si cela a pour conséquence de circonvenir les normes du droit interne et les contrôles institutionnels applicables à leurs activités. Si les États demandent à des services de renseignement étrangers de mener des activités en leur nom, ils imposent à ces services de se conformer aux mêmes normes légales que celles qui seraient applicables si lesdites activités étaient menées par leurs propres services de renseignement.

Introduction*

La présente compilation de bonnes pratiques en matière de cadres juridiques et institutionnels pour le contrôle des services de renseignement est le fruit d'une procédure de concertation lancée à la demande du Conseil des droits de l'homme qui, dans sa Résolution 10/15, a demandé au Rapporteur spécial de préparer, en concertation avec les États et les autres parties prenantes, une compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans le contexte de la lutte antiterroriste.

Les services de renseignement[1] jouent un rôle crucial dans la protection de l'État et de sa population contre ce qui menace la sécurité nationale, comme le terrorisme. Ils contribuent à permettre aux États de s'acquitter concrètement de leur obligation de protéger les droits de tous les êtres humains vivant sous leur juridiction. Aussi les impératifs d'efficacité et de protection des droits de l'homme peuvent-ils être des objectifs complémentaires des services de renseignement.

Cette compilation tire sa substance de pratiques existantes et émergeantes dans un large éventail d'États de par le monde. Ces pratiques proviennent avant tout de lois nationales, de modèles institutionnels, de règles de jurisprudence et de recommandations formulées par des institutions nationales de contrôle et des organisations issues de la société civile. La présente compilation s'appuie également sur les traités internationaux, les résolutions d'organisations internationales et la jurisprudence de tribunaux régionaux. Dans ce contexte, la notion de « bonne pratique » fait référence à des cadres juridiques et institutionnels qui servent à promouvoir les droits de l'homme et le respect de la légalité dans le travail des services de renseignement. Elle ne renvoie pas simplement à ce qu'exige le droit international, en particulier humanitaire, mais à des pratiques qui vont au-delà des ces obligations juridiques.

Bien peu d'États ont intégré la totalité des pratiques décrites ci-après aux règles juridiques et institutionnelles régissant le contrôle de leurs services de renseignement. Certains États pourront se reconnaître comme faisant partie de ceux qui suivent la majorité des 35 bonnes pratiques. D'autres pourront commencer par se consacrer à l'intégration d'un petit nombre d'éléments qu'ils considèrent essentiels pour promouvoir le respect des droits de l'homme par les services de renseignement et leurs organes de contrôle.

L'objet de cette compilation n'est pas de promulguer un ensemble coordonné de normes qui devraient s'appliquer en tout temps et en tout lieu. C'est pourquoi les bonnes pratiques contenues dans ce rapport sont présentées en termes descriptifs et non normatifs. Néanmoins, il est possible d'identifier des pratiques communes qui contribuent à garantir le respect de la légalité et des droits de l'homme par les services de renseignement.

Le Conseil des droits de l'homme a commandé la présente compilation de bonnes pratiques dans le contexte particulier du rôle joué par les services de renseignement dans la lutte antiterroriste. Nonobstant, il convient de noter que les cadres juridiques et institutionnels applicables aux activités antiterroristes des services de renseignement ne sauraient être examinés séparément de ceux qui régissent leur activité en général. Si, depuis 2001, le terrorisme international a modifié le contexte dans lequel opèrent les services de renseignement, les conséquences de ce changement ne se limitent pas au domaine de la lutte antiterroriste.

Dans cette compilation sont mis en exergue des exemples de bonnes pratiques provenant d'un vaste ensemble de lois nationales et de modèles institutionnels. Cependant, il importe de noter que le fait de citer une disposition juridique ou un modèle institutionnel national spécifique n'implique nullement une validation générale de ces lois ou institutions en tant que modèles de bonne pratique permettant de protéger les droits de l'homme dans la lutte antiterroriste. De surcroît, le Rapporteur spécial souhaite souligner que si l'existence de cadres juridiques et institutionnels conformes aux bonnes pratiques revêt une importance cruciale, elle ne suffit pas à garantir que les services de renseignement respectent les droits de l'homme dans leur action antiterroriste.

Les 35 bonnes pratiques identifiées dans cette compilation sont rassemblées dans quatre sous-domaines, à savoir les fondements juridiques (pratiques 1 à 5), le contrôle et la responsabilisation (pratiques 6 à 10 et 14 à 18), le respect du droit humanitaire substantiel (pratiques 11 à 13, 19 et 20) et les questions liées aux fonctions spécifiques des services de renseignement (pratiques 21 à 35). Pour des raisons purement formelles, les bonnes pratiques sont présentées sous un nombre légèrement plus important de subdivisions.

Compilation de bonnes pratiques en matière de cadres juridiques et institutionnels pour le contrôle des services de renseignement

Mandats et fondements juridiques

Pratique 1

Les services de renseignement jouent un rôle important dans la protection de la sécurité nationale et de la légalité. Leur principale fonction consiste à rechercher, analyser et diffuser des renseignements qui aident les décideurs et les autres entités publiques à prendre des mesures pour protéger la sécurité nationale, et notamment pour protéger la population et ses droits fondamentaux.

Les fonctions assignées aux services de renseignement diffèrent d'un pays à un autre; toutefois, la recherche, l'analyse et la diffusion de renseignements afférents à la protection de la sécurité nationale est la principale mission remplie par la plupart des services de renseignement.[2] De fait, de nombreux États limitent le rôle de leurs services de renseignement à l'exécution de cette fonction. Il s'agit d'une bonne pratique, parce que cela évite que les services de renseignement ne se livrent à d'autres activités en rapport avec la sécurité qui relèvent déjà du domaine de compétence d'autres entités publiques, activités qui pourraient constituer une menace particulière pour les droits de l'homme si elles étaient conduites par les services de renseignement. Non contents de définir le type d'actions que leurs services de renseignement peuvent mener, de nombreux États limitent aussi le mobile de leur action à la protection de la sécurité nationale. Si les États ont des vues divergentes quant à la définition de la sécurité nationale, il est bon, en pratique, que la sécurité nationale et ses valeurs constitutives soient clairement définies par des lois adoptées par le parlement.[3] Ceci est important pour s'assurer que les services de renseignement limitent leur action à contribuer à protéger des valeurs consacrées par une définition publique de la sécurité nationale. Dans bien des cas, la protection de la sécurité nationale inclut nécessairement la protection de la population et de ses droits fondamentaux.[4] De fait, plusieurs États mentionnent spécifiquement la protection des droits de l'homme comme étant l'une des fonctions essentielles de leurs services de renseignement.[5]

Pratique 2

Le mandat des services de renseignement est défini en termes restrictifs et précis dans une loi accessible au public. Il est strictement limité à la protection d'intérêts légitimes de sécurité nationale indiqués dans des lois ou des mesures relatives à la sécurité nationale, qui sont accessibles au public. Les menaces affectant la sécurité nationale que les services de renseignement sont chargés de traiter sont identifiées. Si le terrorisme fait partie de ces menaces, il est également défini en termes restrictifs et précis.

Le mandat assigné aux services de renseignement est l'un des principaux moyens de garantir que leur action (notamment antiterroriste) est au service des intérêts de la nation et de sa population, et qu'elle ne menace pas l'ordre constitutionnel et/ou les droits de l'homme. Dans la majorité des États, le mandat des services de renseignement est clairement délimité dans une loi mise à la disposition du public et promulguée par le parlement.[6] Le fait de définir en termes restrictifs et précis le mandat des services de renseignement et d'énumérer toutes les menaces affectant la sécurité nationale qu'ils sont chargés de traiter

constitue une bonne pratique.[7] Un mandat clairement et précisément défini facilite la prise de responsabilité en permettant aux organes de contrôle et de suivi de demander aux services de renseignement de rendre compte de la manière dont ils s'acquittent de missions spécifiques. Enfin, la clarté de la définition des menaces est particulièrement pertinente dans le contexte de la lutte antiterroriste. De nombreux États ont adopté des lois qui donnent une définition précise du terrorisme, ainsi que des groupes et des actes terroristes.[8]

Pratique 3

Les pouvoirs et compétences dévolus aux services de renseignement sont définis en termes clairs et de manière exhaustive par la législation nationale. Les services de renseignement sont tenus d'utiliser ces pouvoirs exclusivement à des fins conformes aux motifs pour lesquels ils ont été conférés. En particulier, tout pouvoir conféré aux services de renseignement afin de lutter contre le terrorisme doit être utilisé exclusivement à cette fin.

Un principe fondamental de l'état de droit veut que tous les pouvoirs et compétences dévolus aux services de renseignement proviennent de la loi.[9] Une énumération exhaustive des pouvoirs et compétences confiés aux services de renseignement va dans le sens de la transparence et permet aux gens de prévoir quels pouvoirs pourront être utilisés à leur encontre. Ceci est particulièrement important dans la mesure où souvent, les pouvoirs dévolus aux services de renseignement donnent la possibilité d'enfreindre les droits de l'homme et les libertés fondamentales.[10] Cette bonne pratique est étroitement liée à la précédente (n° 2), puisque le mandat des services de renseignement sert à définir le cadre dans lequel ils sont autorisés à utiliser les pouvoirs conférés par le législateur.[11] L'interdiction du détournement de pouvoir est implicite dans les lois de nombreux États, puisque les services de renseignement sont uniquement autorisés à faire usage de leurs pouvoirs à des fins très précises. Ceci est particulièrement vrai dans la lutte antiterroriste, car beaucoup de services de renseignement se sont vus conférer des pouvoirs étendus dans ce contexte.

Pratique 4

Tous les services de renseignement sont constitués et opèrent en vertu de lois disponibles au public qui sont conformes à la constitution et au droit humanitaire international. Les services de renseignement peuvent entreprendre, ou recevoir l'ordre d'entreprendre uniquement des activités prescrites par la législation nationale et conformes à ses dispositions. Le recours à une réglementation subsidiaire non publique est strictement limité; ces règles sont à la fois autorisées par la loi et demeurent conformes aux paramètres fixés par les lois publiques. La réglementation non publique ne saurait servir de fondement à une quelconque action restreignant les droits de l'homme.

Pratique 5

Il est explicitement interdit aux services de renseignement de se livrer à des actes quelconques qui seraient contraires à la constitution ou au droit international humanitaire. Cette interdiction vise non seulement les actes des services de renseignement sur leur territoire national, mais aussi leur action à l'étranger.

Les services de renseignement sont des organes de l'État et partant, à l'instar d'autres organes exécutifs, ils sont liés par les dispositions pertinentes du droit national et international, en particulier celles du droit humanitaire.[12] Ceci implique que leur existence et leur fonctionnement sont fondés sur des lois mises à la disposition du public qui sont conformes à la constitution de l'État, mais aussi, entre autres, aux obligations découlant pour l'État du droit international humanitaire. Les États ne peuvent invoquer le droit interne pour justifier une violation du droit international humanitaire, ni même, d'ailleurs, une quelconque autre obligation juridique internationale.[13] Le respect de la légalité impose que les activités des services de renseignement, ainsi que toutes les instructions que leur donne l'exécutif politique, soient conformes à tous les aspects de ces lois.[14] Aussi est-il interdit aux services de renseignement de se livrer, ou de recevoir l'ordre de se livrer à tout acte qui serait contraire au droit interne positif, à la constitution ou à des obligations de l'État en matière de droits

de l'homme. Dans de nombreux États, ces prescriptions sont implicites. Nonobstant, le fait que la législation nationale fasse explicitement référence à ces obligations juridiques générales, et en particulier à l'obligation de respecter les droits de l'homme, est une bonne pratique notoire.[15] La réglementation subsidiaire concernant les procédures internes et les activités des services de renseignement est parfois dissimulée au public afin de protéger les méthodes de travail de ces derniers. Ce type de réglementation ne doit pas servir de base à des activités qui portent atteinte aux droits de l'homme. Le fait que toute réglementation subsidiaire soit fondée sur, et soit conforme à la législation publique applicable constitue une bonne pratique.[16]

Institutions de contrôle

Pratique 6

Les services de renseignement sont contrôlés par une combinaison d'instances de contrôle interne, exécutif, parlementaire, judiciaire et spécialisé dont les mandats et les compétences reposent sur des lois publiques. Un système efficace de contrôle des services de renseignement inclut au moins une institution civile indépendante des services de renseignement et de l'exécutif. La sphère de compétence combinée des instances de contrôle couvre tous les aspects du travail des services de renseignement: leur respect des lois, l'effectivité et l'efficacité de leurs activités, leurs finances et leurs pratiques administratives.

À l'instar des services de renseignement, les institutions qui contrôlent leurs activités sont régies par les lois, ainsi, dans certains, que par la constitution.[17] Il n'existe pas de modèle unique en matière de contrôle des services secrets. Cependant, les éléments suivants sont communément inclus dans les systèmes exhaustifs de contrôle:[18] des mécanismes de gestion et de contrôle internes au sein des services de renseignement;[19] un contrôle exercé par l'exécutif;[20] un contrôle exercé par des organes parlementaires,[21] et un autre par des organes spécialisés et/ou judiciaires.[22] Une bonne pratique consiste à inclure dans ce système de contrôle à plusieurs niveaux au moins une institution pleinement indépendante à la fois des services de renseignement et du corps exécutif. Cette approche permet de garantir la séparation des pouvoirs de contrôle des services de renseignement. Ainsi, les institutions qui commandent, celles qui exécutent et celles qui tirent parti de l'action des services de renseignement ne sont pas les seules à contrôler leurs activités. Tous les aspects du travail des services de renseignement sont contrôlés par une ou plusieurs institutions externes. L'une des fonctions primordiales d'un système de contrôle consiste à vérifier que les services de renseignement respectent les lois applicables, et notamment les droits de l'homme. Les institutions de contrôle sont mandatées pour s'assurer que les services de renseignement et leurs employés rendent compte de toute violation des lois.[23] De plus, elles évaluent les performances des services de renseignement.[24] Ceci inclut le fait d'examiner si les services de renseignement font un usage efficace des fonds publics qui leur sont alloués.[25] L'efficacité du système de contrôle est particulièrement importante dans le domaine du renseignement parce que les services de renseignement conduisent la majeure partie de leur travail à l'abri des regards et de ce fait, ils ne peuvent aisément être contrôlés par le public. Les institutions de contrôle des services de renseignement servent à renforcer la confiance du public dans le travail de ces services, en s'assurant qu'ils accomplissent leur mission légale dans le respect de la légalité et des droits de l'homme.[26]

Pratique 7

Les institutions de contrôle disposent des compétences, des ressources et de l'expertise nécessaires pour engager et conduire leurs propres enquêtes et pour accéder pleinement et sans obstacle à l'information, aux fonctionnaires et aux installations dont elles ont besoin pour remplir leur mandat. Elles bénéficient de l'entière coopération des services de renseignement et des services répressifs pour auditionner les témoins et obtenir des éléments de preuve documentaires et autres.

Les institutions de contrôle disposent de compétences spécifiques pour leur permettre d'exercer leurs fonctions. En particulier,

elles sont habilitées à lancer leurs propres investigations dans les sphères d'activités des services de renseignement relevant de leur compétence, et elles se voient accorder l'accès à toutes les informations nécessaires pour ce faire. Ce pouvoir d'accès à l'information inclue l'autorité légale nécessaire pour examiner tous les dossiers et documents pertinents,[27] inspecter les locaux des services de renseignement[28] et obtenir que tout membre desdits services témoigne sous serment.[29] Ces compétences contribuent à garantir que les contrôleurs pourront efficacement examiner les activités des services de renseignement et enquêter en profondeur sur d'éventuelles infractions aux lois. Certains États ont pris des mesures pour renforcer le pouvoir d'investigation des institutions de contrôle en introduisant des sanctions en cas de manquement à l'obligation de coopérer avec elles.[30] Ceci implique que les institutions de contrôle puissent recourir aux services répressifs pour obtenir la coopération des personnes concernées.[31] S'il est essentiel que les institutions de contrôle disposent de pouvoirs juridiques étendus pour garantir l'efficacité de leur contrôle, une bonne pratique consiste à associer ces pouvoirs à des ressources humaines et financières suffisantes pour leur permettre de les mettre en oeuvre et donc, de remplir pleinement leur mandat. C'est pourquoi de nombreuses institutions de contrôle disposent de leur propre budget indépendant, octroyé directement par le parlement,[32] sont habilitées à recruter un personnel spécialisé[33] et à faire appel aux services d'experts externes.[34]

Pratique 8

Les institutions de contrôle prennent toutes les mesures qui s'imposent pour protéger les renseignements classés et les données personnelles auxquels elles ont accès dans le cadre de leur travail. Des sanctions sont prévues à l'encontre des membres des institutions de contrôle qui enfreignent ces prescriptions.

Les institutions de contrôle des services de renseignement ont accès à des renseignements classés et des informations sensibles obtenus dans l'exercice de leurs fonctions. Aussi, une gamme de mécanismes est mise en place pour s'assurer que les institutions de contrôle et leurs membres ne les divulguent pas par inadvertance ou intentionnellement. Premièrement, dans pratiquement tous les cas, il est interdit aux membres et au personnel des institutions de contrôle de divulguer des informations sans y être autorisés; les manquements à cette obligation entraînent généralement des sanctions civiles et/ou pénales.[35] Deuxièmement, de nombreuses institutions de contrôle soumettent aussi leur personnel à des procédures d'habilitation de sécurité avant de leur donner accès à des renseignements classés.[36] Alternativement, une approche souvent adoptée par les institutions de contrôle parlementaire consiste à faire signer aux membres un accord[37] de non-divulgation. En définitive, le traitement approprié des renseignements classés par les institutions de contrôle repose aussi sur le professionnalisme des membres desdites institutions.

Plaintes et recours effectifs

Pratique 9

Toute personne estimant que ses droits ont été violés par des services de renseignement est habilitée à déposer une plainte auprès d'un tribunal ou d'une institution de contrôle comme le Bureau de médiation, le ou la commissaire aux droits de l'homme ou une institution nationale de défense des droits de l'homme. Les personnes affectées par les actes illégaux de services de renseignement introduisent un recours devant une institution à même d'y remédier efficacement, notamment en ordonnant que le tort subi soit pleinement réparé.

Il est généralement admis que toute mesure limitant les droits de l'homme doit être accompagnée de garanties adéquates, notamment sous la forme d'institutions indépendantes permettant aux personnes d'obtenir réparation en cas de violation de leurs droits.[38] Les services de renseignement disposent d'un arsenal de pouvoirs, notamment de surveillance, d'arrestation et de détention, qui, en cas d'abus, sont susceptibles d'enfreindre les droits de l'homme. C'est pourquoi il existe des institutions chargées de traiter les plaintes déposées par les personnes estimant que leurs droits ont été enfreints par des services de renseignement et, au besoin, de fournir aux victimes de violations des droits de l'homme un

recours effectif. Globalement, on peut distinguer deux approches à cet égard.[39] Premièrement, les États ont établi des institutions extrajudiciaires pour traiter les plaintes nées des actes des services secrets. Il s'agit notamment du bureau de médiation,[40] de la commission nationale des doits de l'homme,[41] de l'office national de vérification,[42] de l'organe parlementaire de contrôle,[43] de l'inspection générale,[44] de l'organe spécialisé de contrôle des services de renseignement[45] et de la commission de recours contre les actes des services de renseignement.[46] Ces institutions sont habilitées à recevoir les plaintes et à enquêter à leur sujet. Cependant, comme généralement, elles ne peuvent pas délivrer d'ordonnances contraignantes ni remédier aux préjudices causés, les victimes de violations des droits de l'homme doivent saisir les tribunaux pour tenter d'obtenir réparation. Deuxièmement, les instances judiciaires peuvent connaître des plaintes concernant les services de renseignement. Il peut s'agir d'organes judiciaires créés à ces fins exclusives[47] ou d'entités faisant partie du système judiciaire général. Ces institutions sont généralement habilitées à ordonner des sanctions.

Pratique 10

Les institutions chargées de traiter les plaintes et les demandes de recours effectif nées des activités des services de renseignement sont indépendantes des services de renseignement et de l'exécutif politique. Ces institutions ont un accès illimité et sans obstacle à toutes les informations pertinentes, aux ressources et à l'expertise nécessaires pour conduire leurs enquêtes, et sont habilitées à délivrer des ordonnances contraignantes.

Pour qu'une institution puisse offrir un recours effectif contre les violations des droits de l'homme, elle doit être indépendante des institutions impliquées dans les activités contestées, être à même de garantir l'équité de la procédure, disposer de compétences et de moyens suffisants pour enquêter efficacement et être habilitée à délivrer des ordonnances contraignantes.[48] C'est pourquoi les États ont doté ces institutions des pouvoirs juridiques requis pour enquêter au sujet des plaintes et réparer les torts subis par les victimes de violations des droits de l'homme commises par les services secrets. Parmi ces pouvoirs se trouvent celui d'obtenir un accès illimité et sans obstacle à toutes les informations pertinentes, de convoquer des témoins dans le cadre de leurs enquêtes, de recevoir des dépositions sous serment,[49] de définir leurs propres procédures en relation avec tout procès et de délivrer des ordonnances contraignantes.[50]

Impartialité et non-discrimination

Pratique 11

Les services de renseignement conduisent leurs travaux d'une manière qui contribue à la promotion et la protection des droits de l'homme et des libertés fondamentales de toutes les personnes placées sous la juridiction de l'État. Les services de renseignement n'opèrent aucune discrimination à l'encontre de personnes ou de groupes en raison de leurs sexe, race, couleur de peau, langue, religion, opinions politiques ou autres, origine nationale ou sociale ou pour toute autre raison.

Les services de renseignement font partie intégrante de l'appareil étatique et contribuent à protéger les droits de toutes les personnes placées sous la juridiction de l'État. Ils sont liés par le principe bien établi en droit international humanitaire de la non-discrimination. Ce principe impose aux États de respecter les droits et les libertés des personnes, sans discrimination fondée sur l'un quelconque des motifs proscrits.[51] De nombreux États ont inscrit dans leur droit interne le principe selon lequel leurs services de renseignement sont tenus de s'acquitter de leurs fonctions d'une manière qui serve les intérêts de l'État et de la société dans son ensemble. Il est expressément interdit aux services de renseignement d'agir ou d'être utilisés pour défendre les intérêts d'un quelconque groupe ethnique, religieux, politique ou autre.[52] De plus, les États s'assurent que l'intervention de leurs services de renseignement (en particulier dans le cadre de la lutte antiterroriste) est motivée par les agissements des individus et non par leur appartenance ethnique, leur religion ou d'autres critères.[53] Certains États ont aussi expressément interdit à leurs services de renseignement de ficher des personnes pour ce type de motifs.[54]

Pratique 12

Le droit national interdit aux services de renseignement de se livrer à des activités politiques ou d'agir en vue de promouvoir ou protéger les intérêts d'un groupe politique, religieux, linguistique, ethnique, social ou économique particulier.

Les services de renseignement sont investis de pouvoirs susceptibles de promouvoir les intérêts de groupes politiques particuliers, ou de leur porter atteinte. Pour s'assurer que les services de renseignement conservent leur neutralité politique, les droits nationaux interdisent que les services de renseignement agissent en faveur d'un quelconque groupe politique.[55] Cette obligation incombe non seulement aux services de renseignement mais aussi à l'exécutif politique qu'ils servent. Plusieurs États ont également adopté des mesures pour interdire ou limiter l'implication des services de renseignement dans les partis politiques. L'interdiction faite aux employés des services de renseignement d'adhérer à un quelconque parti politique, d'en recevoir des instructions ou de l'argent[56] ou d'agir en sa faveur[57] relève de ce type de mesures. De plus, divers États ont pris des dispositions pour garantir la neutralité des directeurs des services secrets. Par exemple, la nomination du directeur des services de renseignement est soumise au contrôle d'organes non exécutifs;[58] il existe des dispositions juridiques concernant la durée du mandat des directeurs et les raisons pouvant motiver leur destitution, ainsi que des garanties les protégeant contre toute pression indue.[59]

Pratique 13

Les services de renseignement ne sont pas autorisés à user de leurs pouvoirs contre des activités politiques légales ou de rassemblements et modes d'expression pacifiques.

Les services de renseignement utilisent des mesures de recherche du renseignement susceptibles d'interférer avec des activités politiques légitimes et d'autres manifestations de la liberté d'expression, d'association et de rassemblement.[60] Ces droits sont fondamentaux pour le fonctionnement d'une société libre, et notamment pour les partis politiques, les médias et la société civile. Aussi les États ont-ils pris des mesures pour limiter le risque que les services de renseignement prennent pour cible (ou se voient enjoindre de prendre pour cible) les personnes et les groupes qui se livrent à de telles activités. L'interdiction absolue de cibler des activités légales, la stricte limitation de la recherche de renseignements (voir pratique n° 21), de la conservation et de l'utilisation de données personnelles collectées par les services de renseignement (voir pratique n° 23) font partie de ces mesures.[61] Compte tenu du fait que les médias jouent un rôle essentiel dans toute société, certains États ont instauré des mesures spécifiques pour éviter que les services de renseignement ne prennent pour cible les journalistes.[62]

Responsabilité des États à l'égard des services de renseignement

Pratique 14

Les États assument une responsabilité internationale à l'égard des activités de leurs services de renseignement et de leurs agents ainsi que de tout entrepreneur privé employé par eux, quels que soient l'endroit où ces activités ont lieu et la victime de la conduite ayant causé un préjudice international. C'est pourquoi l'exécutif prend des mesures pour exercer un contrôle global sur ses services de renseignement et assumer ses responsabilités à l'égard de leurs actes.

En vertu du droit international, les États sont responsables des actes de leurs services de renseignement et de leurs agents, quel que soit l'endroit du monde où ils conduisent leurs opérations. Cette responsabilité s'étend aux actes de tout entrepreneur privé engagé par l'État pour remplir des fonctions de renseignement.[63] Les États sont légalement tenus de garantir que leurs services de renseignement respectent les droits de l'homme et de remédier à ce type de violations subies par des particuliers.[64] Ils prennent donc des mesures pour réguler et administrer leurs services de renseignement d'une manière qui favorise le respect de la légalité et plus particulièrement du droit international humanitaire.[65] Le contrôle des services de renseignement par l'exécutif est essentiel à ces fins, c'est pourquoi il est consacré par de nombreuses lois nationales.[66]

Responsabilité individuelle

Pratique 15

Le droit constitutionnel, la législation et le droit pénal international s'appliquent à tous les agents des services de renseignement, comme ils s'appliquent à tout autre fonctionnaire. Les exceptions autorisant les agents des services de renseignement à agir d'une manière normalement contraire aux lois nationales sont strictement limitées et prescrites par la loi. Ces exceptions n'autorisent jamais une violation des normes impératives du droit international ou des obligations de l'État en matière de respect des droits de l'homme.

Si l'accent est souvent mis sur les responsabilités institutionnelles des services secrets, à titre individuel, les agents des services de renseignement sont aussi responsables et doivent rendre compte de leurs actes.[67] En règle générale, le droit constitutionnel, législatif et le droit pénal international s'appliquent aux agents secrets comme à toute autre personne physique.[68] De nombreux États ont disposé que tout membre des services de renseignement qui enfreint délibérément et/ou ordonne ou demande qu'autrui accomplisse un acte qui enfreint le droit constitutionnel ou la législation commet un délit civil ou une infraction pénale.[69] Cette pratique favorise le respect de la légalité au sein des services de renseignement et contribue à prévenir l'impunité. De nombreux États accordent aux membres de leurs services de renseignement le droit de se livrer à des actes qui, s'ils étaient accomplis par des citoyens ordinaires, constitueraient des infractions pénales.[70] Que toute autorisation de cette nature soit strictement limitée, énoncée par la loi et assortie de garanties adéquates est une bonne pratique.[71] Les dispositions législatives qui autorisent les agents des services de renseignement à accomplir des actes normalement interdits par les lois nationales ne sauraient autoriser des actes contraires à la constitution ou à des normes impératives du droit international. [72]

Pratique 16

Les lois nationales prévoient des sanctions pénales, civiles ou autres à l'encontre de tout membre des services de renseignement ou de toute personne agissant en leur nom qui enfreint ou ordonne d'enfreindre les lois nationales ou le droit international humanitaire. Ces lois établissent également des procédures pour contraindre les auteurs de ces infractions à rendre compte de leurs actes.

Les États s'assurent que les employés des services de renseignement rendent compte de toute violation de la loi en prévoyant et appliquant des sanctions pour toute infraction particulière. Ceci afin de promouvoir le respect de la légalité et des droits de l'homme au sein des services de renseignement. De nombreuses lois nationales régissant les services de renseignement prévoient des sanctions spécifiques réprimant les infractions à ces lois et aux autres dispositions de droit interne ou international commises par les employés de ces services.[73] Comme beaucoup d'activités de ces services sont secrètes, les infractions (commises par les employés) risquent de ne pas être détectées par les magistrats compétents. C'est pourquoi une bonne pratique consiste à intégrer dans les lois nationales une prescription imposant à l'encadrement des services de renseignement de saisir le parquet de tout cas soupçonné d'infraction pénale.[74] En cas de violation grave du droit humanitaire, par exemple en cas de torture, les États sont tenus par le droit international d'engager des poursuites à l'encontre des agents concernés.[75] Les employés des services de renseignement sont pénalement responsables non seulement des actes illicites auxquels ils participent directement, mais également de ceux qu'ils ordonnent de commettre ou dont ils sont complices.[76]

Pratique 17

Les agents des services de renseignement sont légalement tenus de refuser de se soumettre à des ordres d'un supérieur qui enfreindraient les lois nationales ou le droit international humanitaire. Dans ce contexte, une protection appropriée est accordée aux agents des services de renseignement réfractaire.

Le fait d'inclure dans la législation nationale une disposition prescrivant aux agents des services de renseignement de refuser d'exécuter des ordres qui, selon eux, seraient contraires au droit national ou au droit international humanitaire est une bonne pratique.[77] Quoique cette disposition se trouve plus souvent dans les lois régissant les forces armées, plusieurs États l'ont insérée dans les lois régissant leurs services de renseignement.[78] L'obligation faite aux agents des services de renseignement de refuser d'exécuter des ordres illicites constitue une protection importante contre les violations des droits de l'homme, mais aussi contre les gouvernements en exercice qui pourraient ordonner aux services de renseignement d'agir pour protéger ou renforcer leurs propres intérêts. Un principe bien établi en droit international veut que les personnes physiques ne puissent invoquer les ordres d'un supérieur pour se soustraire à leur responsabilité pénale à l'égard d'actes constituant des violations graves du droit international humanitaire.[79] Ainsi, pour éviter d'engager leur responsabilité pénale personnelle, les agents des services de renseignement sont tenus de refuser d'exécuter un ordre s'ils sont censés pouvoir s'apercevoir qu'il est manifestement illégal. Ceci souligne l'importance de la formation des fonctionnaires du renseignement au droit humanitaire, parce qu'il faut qu'ils aient connaissance de leurs obligations et de leurs droits internationaux (voir pratique n° 19). Afin de créer un climat dans lequel les violations des droits de l'homme ne sauraient être tolérées, les États assurent une protection juridique contre les représailles aux agents des services de renseignement qui refusent de se soumettre à des ordres illégaux.[80] L'obligation de refuser d'exécuter des ordres illégaux est étroitement liée à la mise en place de mécanismes internes et externes permettant aux employés des services de renseignement de faire part de leurs préoccupations concernant la légalité des ordres reçus (voir pratique n° 18).

Pratique 18

Des procédures internes sont en place pour permettre aux agents des services de renseignement de signaler les infractions. Elles sont complétées par un organe indépendant dûment mandaté, ayant accès aux informations nécessaires pour conduire des enquêtes approfondies et prendre des mesures pour mettre un terme aux abus lorsque les procédures internes se sont révélées inadéquates. Les agents des services de renseignement qui, de bonne foi, signalent des infractions sont protégés par la loi contre toutes formes de représailles. Sont ainsi protégés ceux qui divulguent des informations aux médias ou à l'opinion publique, s'il s'agit d'une mesure prise en dernier recours et si les faits présentent un intérêt significatif pour l'opinion publique.

Les employés du renseignement sont souvent les premiers à (et les mieux placés pour) identifier les abus commis au sein des services de renseignement tels que des violations des droits de l'homme, les malversations et autres infractions à la législation. De ce fait, une bonne pratique consiste à inclure dans les lois nationales des procédures spécifiques permettant aux agents des services de renseignement de révéler leurs préoccupations concernant ces abus.[81] Ces dispositions ont pour but d'encourager les agents des services de renseignement à signaler les abus, tout en garantissant que les informations potentiellement sensibles seront divulguées et soumises à investigation d'une manière contrôlée. En pratique, les États ont le choix entre plusieurs possibilités pour canaliser ce type de communication: créer des mécanismes internes chargés de recevoir les informations révélées par les agents des services de renseignement et enquêter à leur sujet[82] ou des institutions externes remplissant les mêmes fonctions, et prévoir la communication des informations à ces institutions directement par les agents des services de renseignement.[83] Dans certaines juridictions, les agents des services de renseignement ne sont autorisés à s'adresser à l'institution externe que si l'organe interne n'a pas répondu adéquatement à leur préoccupation.[84] Dans certains États, les agents des services de renseignement sont autorisés à s'adresser à l'opinion publique en dernier recours, ou quand les faits révélés sont particulièrement graves, par exemple lorsque la

vie de personnes est en jeu.[85] Quelle que soit la nature exacte du mode de communication choisi, le fait que le droit interne offre une protection contre les représailles aux personnes qui divulguent des renseignements conformément à la loi est une bonne pratique.[86]

Professionnalisme

Pratique 19

Les services de renseignement et leurs institutions de contrôle prennent des mesures pour encourager le professionnalisme au sein de l'institution et une culture institutionnelle basée sur le respect de la légalité et des droits de l'homme. En particulier, les services de renseignement sont responsables de former leurs membres aux dispositions pertinentes des droits interne et international, et notamment du droit international humanitaire.

La culture institutionnelle fait référence à des valeurs, des attitudes et des pratiques largement partagées ou dominantes parmi les employés. C'est l'un des principaux facteurs pour définir l'attitude des fonctionnaires du renseignement à l'égard du respect de la légalité et des droits de l'homme.[87] En effet, les cadres institutionnels et juridiques seuls ne sauraient garantir que les agents des services de renseignement se conforment à la légalité et au droit humanitaire. Plusieurs États et services de renseignement ont formulé des codes déontologiques ou des principes de professionnalisme pour promouvoir une culture institutionnelle qui accorde de la valeur aux droits de l'homme et encourage le respect de la légalité.[88] Les codes de conduite incluent généralement des dispositions concernant les comportements appropriés, la discipline et les normes éthiques applicables à tous les agents des services de renseignement.[89] Dans certains États, c'est le ministre responsable des services de renseignement qui promulgue ces documents; ceci pour garantir la responsabilisation du niveau politique à l'égard de leur contenu.[90] Que les codes de conduite (et les documents assimilés) soient soumis à la surveillance d'institutions internes et externes de contrôle constitue une bonne pratique.[91] La formation est un deuxième élément clé de la formation d'une culture institutionnelle du professionnalisme au sein des services de renseignement. Nombre d'entre eux ont mis en place des programmes de formation qui mettent l'accent sur le professionnalisme, enseignent aux employés les normes constitutionnelles, législatives et issues du droit international humanitaire pertinentes.[92] Une bonne pratique consiste à faire en sorte que ces programmes de formation soient à la fois prescrits et régis par la loi, et qu'ils s'adressent à tous les agents des services de renseignement.[93] Enfin, la culture du professionnalisme peut être renforcée par des mesures internes de gestion du personnel qui récompensent les conduites éthiques et professionnelles.

Protection des droits de l'homme

Pratique 20

Toute mesure prise par les services de renseignement de nature à restreindre les droits de l'homme et les libertés fondamentales est conforme aux critères suivants:

- Les mesures sont prescrites par des lois publiques conformes aux normes du droit international humanitaire;
- Elles sont strictement nécessaires pour permettre aux services de renseignement de s'acquitter de leurs fonctions, telles qu'elles sont prescrites par la loi;
- Elles sont proportionnées à l'objectif ciblé; ceci implique que les services de renseignement sélectionnent la mesure la moins restrictive sous l'angle des droits de l'homme, qu'ils soient particulièrement attentifs à minimiser l'impact de ces mesures sur les droits de l'homme, et surtout sur les droits des personnes qui ne sont pas soupçonnées d'avoir enfreint la loi;
- Les mesures prises par les services de renseignement ne sont en aucun cas contraires aux normes impératives du droit international ou à l'un quelconque des droits fondamentaux de l'homme;
- Il existe un système clair et exhaustif applicable à l'autorisation, au suivi et au contrôle de toutes les mesures qui restreignent les droits de l'homme;

- Les personnes dont les droits ont été restreints par les services de renseignement peuvent déposer une plainte auprès d'une institution indépendante pour obtenir un recours effectif.

La plupart des juridictions nationales autorisent les services de renseignement à entreprendre des actions qui restreignent les droits de l'homme. Ces pouvoirs s'exercent avant tout dans le domaine de la recherche du renseignement, mais aussi dans celui de la répression, de l'utilisation et du partage de données personnelles. Les lois nationales contiennent des garanties en matière de droits de l'homme pour deux raisons principales: pour limiter les ingérences dans les droits des personnes à ce que permet le droit international humanitaire, et pour prévenir le recours arbitraire ou discrétionnaire à ce type de mesures.[94]

Toute mesure de restriction des droits de l'homme doit être prescrite par une loi compatible avec les normes de droit international humanitaire et en vigueur au moment où la mesure est adoptée.[95] Ladite loi énonce ces mesures en termes restrictifs et précis, fixe des conditions d'emploi strictes et précise que le recours à de telles mesures est directement lié au mandat assigné aux services de renseignement.[96]

De nombreuses lois nationales imposent également que toute mesure prise par les services de renseignement pour restreindre les droits de l'homme soit nécessaire dans une société démocratique.[97] La notion de nécessité implique que le recours à toute mesure de ce type soit clairement et rationnellement lié à la protection d'intérêts de sécurité nationale légitimes, tels qu'ils sont définis par la législation nationale.[98]

Le principe de la proportionnalité, consacré par les lois de nombreux États, veut que toute mesure restreignant les droits de l'homme soit proportionnée aux fins spécifiques (et légitimes) visées.[99] Pour garantir que les mesures prises par les services de renseignement sont proportionnées, nombre d'États imposent à leurs services de renseignement d'user des moyens les moins intrusifs possibles pour atteindre l'objectif ciblé.[100]

Le droit interne interdit aux services de renseignement de recourir à des mesures contraires aux normes du droit international humanitaire, et/ou aux normes impératives du droit international. Certains États ont inclus dans leur législation relative aux services de renseignement une interdiction explicite de commettre des violations graves du droit humanitaire.[101] S'il est possible de distinguer des droits de l'homme intangibles inviolables, il convient d'indiquer que tous les droits de l'homme contiennent un élément central essentiel qui échappe au domaine des restrictions permises.

Les États s'assurent que les mesures limitant les droits de l'homme prises par les services de renseignement sont soumises à une procédure d'autorisation prescrite par la loi, ainsi qu'à un contrôle et un examen externes (voir pratiques n^{os} 6, 7, 21, 22, 28 et 32).

Que les victimes de violations des droits de l'homme aient la possibilité d'introduire un recours en réparation est une prescription essentielle du droit international humanitaire. De nombreux États ont mis en place des procédures pour garantir que les personnes aient accès à une institution indépendante à même de connaître de ce type de grief[102] (voir pratiques n^{os} 9 et 10 ci-dessus).

Recherche du renseignement

Pratique 21

Le droit interne définit: le type de mesures de recherche de renseignements à la disposition des services secrets; les objectifs de la recherche de renseignements autorisés; les catégories de personnes et d'activités pouvant être visées par la recherche du renseignement; le niveau de suspicion requis pour justifier le recours à des mesures de recherche du renseignement; la durée maximum d'application desdites mesures; et la procédure d'autorisation, de contrôle et d'analyse du recours à ces mesures.

Dans la plupart des États, les services de renseignement ont recours à des mesures intrusives comme la filature et l'interception des communications pour recueillir les renseignements nécessaires à l'accomplissement de leur mandat. Fondamentalement, le respect de la légalité impose que les personnes aient connaissance des mesures que les pouvoirs

publics sont habilités à employer pour restreindre leurs droits, et qu'elles puissent prévoir quels actes peuvent motiver leur emploi.[103] La législation nationale indique les catégories de personnes et d'activités susceptibles d'être soumises à des mesures de recherche du renseignement,[104] et le niveau de suspicion requis pour déclencher le recours à une mesure particulière.[105] Certaines lois nationales imposent également des limites spécifiques à l'emploi de telles mesures contre des catégories professionnelles données, en particulier celles des journalistes et des avocats.[106] Ces dispositions sont conçues pour protéger des privilèges professionnels jugés essentiels au fonctionnement d'une société libre, comme le droit reconnu aux journalistes de ne pas révéler leurs sources ou le secret des communications avocat-client. Limiter strictement le recours aux méthodes de recherche du renseignement intrusives contribue à garantir que cette mesure est nécessaire et qu'elle s'applique uniquement à des personnes et des groupes susceptibles d'être impliqués dans des activités qui menacent la sécurité nationale. Les lois nationales incluent également des indications concernant la durée permise de l'application de la mesure intrusive, et le délai à l'expiration duquel une nouvelle autorisation doit être obtenue pour la proroger.[107] De même, une bonne pratique consiste à intégrer à la législation nationale l'obligation de mettre un terme à la mesure de recherche du renseignement aussitôt que le but recherché à travers son utilisation a été atteint, ou dès qu'il devient clair que l'objectif ciblé ne pourra être atteint.[108] Ces dispositions servent à minimiser les ingérences dans les droits des personnes ciblées et contribuent à garantir que les mesures de recherche du renseignement sont conformes au principe de proportionnalité.

Pratique 22

Les mesures de recherche du renseignement qui limitent significativement les droits de l'homme sont autorisées et contrôlées par au moins une institution extérieure aux services de renseignement et indépendante d'eux. Cette institution est habilitée à ordonner la révision, la suspension et l'abandon de ces mesures. Celles de ces mesures qui limitent significativement l'exercice des droits de l'homme sont soumises à une procédure d'approbation à plusieurs niveaux, par les services de renseignement eux-mêmes, par l'exécutif politique et par une institution indépendante des services de renseignement et de l'exécutif.

Les lois nationales incluent souvent des dispositions détaillées concernant la procédure d'autorisation de toutes les mesures de recherche du renseignement qui restreignent les droits de l'homme.[109] Les procédures d'autorisation obligent les services de renseignement à justifier le recours proposé à ces mesures en se référant à un cadre juridique clairement défini (voir ci-dessus pratiques n^{os} 20 et 21). Il s'agit-là d'un dispositif clé pour s'assurer que les mesures de recherche du renseignement sont utilisées d'une manière conforme à la loi. Le fait que les mesures intrusives soient autorisées par une institution indépendante des services secrets, c'est-à-dire par un membre politiquement responsable de l'exécutif[110] ou par une instance quasi-judiciaire constitue une bonne pratique.[111] Les organes judiciaires sont indépendants du renseignement et sont donc les mieux placés pour conduire une évaluation indépendante et impartiale d'une demande de recours à des mesures de recherche de renseignements intrusives.[112] De plus, le fait de devoir obtenir l'autorisation des cadres supérieurs des services de renseignement, des membres politiquement responsables de l'exécutif et d'une instance quasi-judiciaire, en particulier pour autoriser les méthodes de recherche du renseignement les plus intrusives (par exemple l'interception des communications, du courrier, les perquisitions secrètes) est aussi une bonne pratique.[113]

Les États s'assurent en outre que la recherche du renseignement est soumise au contrôle continu d'une institution extérieure aux services de renseignement. Une bonne pratique consiste à obliger les services de renseignement à signaler le recours à des mesures de recherche du renseignement en continu et d'habiliter l'institution de contrôle externe à ordonner l'abandon desdites mesures.[114] Dans de nombreux États, les organes de contrôle externe conduisent aussi le contrôle externe des mesures de recherche du renseignement pour s'assurer qu'elles sont autorisées et que leur emploi est conforme à la loi.[115] Ce point prend toute son importance à la lumière du fait que les personnes dont les droits sont affectés par la recherche du renseignement ont peu de chance

de s'en rendre compte et d'avoir la possibilité de contester la légalité des mesures.

Gestion et utilisation des données personnelles

Pratique 23

Une loi publique définit les types de données personnelles que les services de renseignement sont autorisés à détenir, ainsi que les critères applicables à leur utilisation, conservation, suppression et divulgation. Les services secrets sont autorisés à conserver les données personnelles qui sont strictement nécessaires en vue de remplir leur mandat.

Un certain nombre de principes généraux concernant la protection des données personnelles est communément intégré aux lois nationales[116] et aux instruments internationaux.[117] Il s'agit notamment des prescriptions suivantes: les données personnelles doivent être collectées et traitées d'une manière licite et juste; l'utilisation de ces données doit se limiter à l'objectif spécifié à l'origine; des mesures doivent être prises pour s'assurer que les données personnelles enregistrées sont exactes; les fichiers contenant ces données sont supprimés dès qu'ils cessent d'être nécessaires; et les personnes ont le droit d'accéder aux fichiers contenant leurs données personnelles et de les corriger.[118] Dans le contexte de l'utilisation de données personnelles par les services de renseignement, l'ouverture, la conservation et la destruction des fichiers personnels peuvent avoir des répercussions importantes sur les droits de l'homme. C'est pourquoi des directives concernant la gestion et l'utilisation des données personnelles par les services de renseignement sont formulées dans une loi écrite publique. Il s'agit d'une protection juridique pour éviter de donner à l'exécutif ou aux services de renseignement des pouvoirs incontrôlés dans ce domaine.[119] Une deuxième garantie consiste à donner des instructions juridiques pour spécifier et limiter les raisons justifiant l'ouverture et la conservation de fichiers personnels par les services de renseignement.[120] Troisièmement, une pratique établie dans plusieurs États veut que les services de renseignement informent l'opinion publique du type de données personnelles qu'ils conservent. Ces informations concernent notamment le type et la portée des données personnelles susceptibles d'être conservées, mais aussi les motifs justifiant légalement que de telles données soient conservées par les services de renseignement.[121] Quatrièmement, plusieurs États ont criminalisé le fait pour un agent des services de renseignement de divulguer ou utiliser des données personnelles en dehors du cadre défini par la loi.[122] Dernière garantie, les États ont explicitement disposé que les services de renseignement n'étaient pas autorisés à conserver des données personnelles en se fondant sur des motifs discriminatoires.[123]

Pratique 24

Les services de renseignement évaluent régulièrement la pertinence et l'exactitude des données personnelles qu'ils détiennent. Ils sont tenus par la loi de détruire ou mettre à jour toute information considérée comme inexacte ou ayant cessé d'être pertinente à l'égard de leur mandat, du travail des institutions de contrôle ou d'un éventuel procès.

Les États ont pris des mesures pour s'assurer que les services de renseignement vérifient régulièrement si le contenu de leurs fichiers personnels est exact et pertinent à l'égard de leur mandat.[124] Des garanties concernant la pertinence et l'exactitude des données personnelles aident à assurer que toute ingérence dans le droit au respect de la vie privée est limitée dans le temps. Dans certains États, les services de renseignement sont tenus par la loi de détruire non seulement les fichiers qui ne sont plus pertinents,[125] mais également ceux qui sont inexacts ou dont le traitement est inadéquat.[126] Bien que les services de renseignement soient obligés d'effacer les données qui ont cessé d'être pertinentes à l'égard de leur mandat, il importe que ceci ne se fasse pas au détriment du travail des institutions de contrôle ou d'un éventuel procès. Les informations détenues par les services de renseignement peuvent servir de preuve dans des procès et revêtir une grande importance pour les personnes concernées. La disponibilité de ce type de pièces peut être importante pour garantir le droit à un procès équitable. Aussi, c'est

une bonne pratique que d'obliger les services de renseignement à conserver tous les registres (y compris les procès verbaux originels et les notes internes) pouvant déboucher sur l'ouverture d'un procès, et de faire surveiller la destruction de ce type d'informations par une institution extérieure (voir ci-après pratique n° 25).[127]

Pratique 25

Une institution indépendante existe pour contrôler l'utilisation faite des données personnelles par les services de renseignement. Cette institution a accès à tous les fichiers détenus par lesdits services et elle est habilitée à ordonner la divulgation d'informations aux personnes concernées, ainsi que la destruction des fichiers ou des renseignements personnels qu'ils contiennent.

Dans de nombreux États, la gestion des fichiers personnels est soumise à la supervision régulière et continue d'institutions indépendantes.[128] Ces institutions sont mandatées pour conduire des visites d'inspection régulières et des contrôles aléatoires des fichiers personnels concernant les opérations en cours et passées.[129] Les États ont en outre mandaté des instituions de contrôle indépendantes pour vérifier si les directives internes concernant la gestion des fichiers sont conformes à la loi.[130] Ils ont reconnu que les institutions de contrôle devaient adopter leurs méthodes de travail et d'inspection en toute autonomie, et qu'elles devaient disposer de ressources et de capacités suffisantes pour inspecter régulièrement la gestion et l'utilisation des données personnelles par les services de renseignement.[131] Les services de renseignement sont dans l'obligation légale de coopérer pleinement avec les institutions chargées de contrôler leur gestion et leur usage des données personnelles.[132]

Pratique 26

Les personnes physiques ont la possibilité de demander à accéder aux données personnelles les concernant détenues par les services de renseignement. Elles peuvent exercer ce droit en adressant une requête aux autorités concernées ou par le biais d'une institution indépendante chargée de la protection ou du contrôle des données. Elles ont le droit de corriger toute erreur contenue dans leurs données personnelles. Les éventuelles exceptions à ces règles générales sont prescrites par la loi, strictement limitées, proportionnées et nécessaires pour permettre aux services de renseignement de remplir leur mandat. Il revient aux services de renseignement de justifier devant une institution de contrôle indépendante toute décision de ne pas communiquer des renseignements personnels.

De nombreux États accordent aux individus le droit d'accéder aux données personnelles détenues par les services de renseignement les concernant. Ce droit peut être exercé en adressant une requête aux services de renseignement,[133] au ministre compétent[134] ou à une institution de contrôle indépendante.[135] Ce droit individuel d'accéder aux données personnelles doit être envisagé dans le contexte des garanties du droit au respect de la vie privée et de la liberté d'accès à l'information. Ces garanties sont importantes, non seulement parce qu'elles permettent aux personnes de vérifier l'exactitude et la légalité du fichier contenant leurs données personnelles, mais aussi parce qu'elles protègent contre les abus, l'incurie et la corruption. En effet, le droit individuel d'accès aux données personnelles détenues par les services de renseignement sert à renforcer la transparence et la responsabilité de la prise de décision dans les services de renseignement, et il tend donc à favoriser la confiance du citoyen dans l'action du gouvernement.[136] Les États peuvent restreindre l'accès aux fichiers personnels pour des raisons telles que la protection des enquêtes en cours, des sources d'informations et des méthodes de travail des services de renseignement. Cependant, une bonne pratique consiste à énoncer ces restrictions dans une loi et à s'assurer qu'elles sont conformes aux principes de proportionnalité et de nécessité.[137]

Recours au pouvoir d'arrestation et de détention

Pratique 27

Les services de renseignement ne sont pas autorisés à user de leurs pouvoirs d'arrestation et de détention s'ils ne sont pas mandatés pour exercer des fonctions de répression. Ils ne sont pas investis de pouvoirs d'arrestation et de détention si les services répressifs compétents pour accomplir les mêmes actes sont déjà mandatés pour ce faire.

Une bonne pratique largement admise consiste à interdire explicitement aux services de renseignement d'exercer des pouvoirs d'arrestation et de détention si leur mandat légal ne leur impose pas d'exercer des fonctions de répression en rapport avec les infractions menaçant la sécurité nationale, comme le terrorisme.[138] Des arguments convaincants ont été avancés contre l'association des fonctions de renseignement et de répression.[139] Cependant, si la législation nationale confère des pouvoirs d'arrestation et de détention aux services de renseignement, une bonne pratique consiste à limiter explicitement ces pouvoirs par un mandat qui leur confie la responsabilité de remplir des fonctions répressives en cas de menaces spécifiées pesant sur la sécurité nationale, par exemple pour lutter contre le terrorisme.[140] Si des services répressifs nationaux ou régionaux sont mandatés pour faire appliquer le droit pénal dans le contexte des infractions à la sécurité nationale, il n'existe aucune raison légitime de conférer à un service de renseignement distinct des pouvoirs d'arrestation et de détention dans le même contexte. Le danger est que se développe un système répressif parallèle, dans lequel des services de renseignement exerceraient des pouvoirs d'arrestation et de détention pour circonvenir les garanties légales et le contrôle applicables aux forces de l'ordre.[141]

Pratique 28

Si les services de renseignement sont investis de pouvoirs d'arrestation et de détention, ceux-ci sont fondés sur des lois disponibles au public.

Ces pouvoirs ne sont exercés que dans les cas où il existe des motifs raisonnables de soupçonner qu'une personne a commis ou est sur le point de commettre une infraction pénale particulière. Les services de renseignement ne sont pas autorisés à priver une personne de sa liberté uniquement à des fins de recherche du renseignement. Le recours des services de renseignement à des pouvoirs d'arrestation et de détention est soumis au même degré de contrôle que le recours à ces pouvoirs par les forces de l'ordre, et notamment à un contrôle judiciaire de la légalité de toute privation de liberté.

Si des services de renseignement sont investis de pouvoirs d'arrestation et de détention, la législation nationale définit les buts et les circonstances dans lesquels ces pouvoirs peuvent être utilisés.[142] C'est une bonne pratique que de limiter strictement le recours à ces pouvoirs aux cas où il existe des motifs raisonnables de soupçonner qu'un crime (relevant de la compétence des services de renseignement) a été, ou est sur le point d'être commis. Il s'ensuit que les services de renseignement ne sont pas autorisés à user de ces pouvoirs simplement pour recueillir des renseignements.[143] L'arrestation et la détention de personnes en l'absence de soupçons raisonnablement justifiés qu'elles ont commis ou sont sur le point de commettre une infraction pénale, ou en l'absence d'autres motifs internationalement reconnus de détention, ne sont pas autorisées en droit international humanitaire.[144] Si les lois nationales autorisent les services de renseignement à arrêter et détenir des personnes, une bonne pratique consiste à soumettre l'exercice de ces pouvoirs au même degré de contrôle que l'exercice de ces mêmes pouvoirs par les forces de l'ordre.[145] Il importe surtout de noter que le droit humanitaire exige que les personnes aient la possibilité de contester la légalité de leur détention devant un tribunal de justice.[146]

Pratique 29

Si les services de renseignement sont investis de pouvoirs d'arrestation et de détention, ceux-ci doivent être conformes aux normes de droit international humanitaire concernant les droits à la liberté, à un procès équitable, et l'interdiction de la torture et des traitements inhumains ou dégradants. Dans l'exercice de ces pouvoirs, les

services de renseignement se conforment aux normes internationales notamment énoncées dans l'Ensemble de principes pour la protection de toutes les personnes soumises à une forme quelconque de détention ou d'emprisonnement, le Code de conduite pour les responsables de l'application des lois et les Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois.

Si les services de renseignement sont dotés de pouvoirs d'arrestation et de détention, ils sont tenus d'observer les normes internationales applicables à la privation de liberté (voir également ci-dessus pratique n° 28).[147] Ces normes sont précisées par divers codes de conduite internationaux et régionaux à l'usage des responsables de l'application des lois, qui contiennent une gamme de bonnes pratiques pouvant s'appliquer aux services de renseignement dotés de pouvoirs d'arrestation et de détention.[148] En dehors de l'obligation légale (concernant l'examen judiciaire de la légalité de la détention) définie ci-dessus dans le cadre de la pratique n° 28, il existe trois autres ensembles de normes applicables à l'utilisation des pouvoirs d'arrestation et de détention par les services de renseignement. Premièrement, les services secrets sont tenus de respecter l'interdiction absolue du recours à la torture et aux autres traitements inhumains ou dégradants.[149] Deuxièmement, le recours legal à la force pendant l'arrestation et la détention doit être conforme à des normes internationales telles que celles imposant que le recours à la force soit strictement nécessaire, proportionné au danger perçu et dûment signalé.[150] Troisièmement, le fait que les services de renseignement se conforment aux normes internationales suivantes relatives à l'arrestation et la détention des personnes constitue une bonne pratique: toutes les arrestations, détentions et tous les interrogatoires font l'objet d'un procès-verbal dès le moment de l'arrestation;[151] les agents chargés d'exécuter l'arrestation s'identifient auprès de la personne concernée et l'informent des motifs et des fondements juridiques de son arrestation/détention;[152] les personnes détenues par les services de renseignement ont accès à un conseiller juridique.[153]

Pratique 30

Les services de renseignement ne sont pas autorisés à administrer leurs propres centres de détention ni à faire usage d'un quelconque centre de détention non reconnu administré par des tiers.

Le fait que la législation nationale interdise explicitement que les services de renseignement administrent leurs propres centres de détention constitue une bonne pratique.[154] Si les services de renseignement sont autorisés à exercer des pouvoirs d'arrestation et de détention, les personnes concernées sont placées en détention provisoire dans des centres de détention officiels administrés par les services répressifs.[155] De même, les services de renseignement ne sont pas autorisés à faire usage de centres de détention non reconnus administrés par des tiers, par exemple des entrepreneurs privés. Il s'agit de garanties essentielles contre la détention arbitraire par les services de renseignement et/ou le risque de voir apparaître un régime carcéral parallèle dans lequel les personnes seraient détenues dans des conditions non conformes aux normes internationales, et sans garantie de bénéficier d'une procédure régulière.

Partage de renseignements et coopération

Pratique 31

Le partage de renseignements entre différents services de renseignement d'un même État ou avec les autorités d'un autre État est fondé sur une loi nationale qui définit les paramètres de l'échange de renseignements, et notamment les conditions devant être réunies pour que des informations puissent être partagées, les instances avec lesquelles le partage de renseignement est permis et les garanties entourant l'échange de renseignements.

C'est une bonne pratique que de s'assurer que toute forme de partage de renseignements entre des services de renseignement et d'autres instances étrangères est clairement fondée sur la législation nationale. Celle-ci précise les critères concernant les fins auxquelles

les renseignements peuvent être partagés, les instances avec lesquelles le partage de renseignements est permis, et contient des garanties procédurales applicables au partage de renseignements.[156] L'existence d'un fondement juridique autorisant le partage de renseignements est un préalable important pour le respect de la légalité, en particulier lorsqu'il s'agit d'échanger des données personnelles, parce que cela enfreint directement le droit au respect de la vie privée et peut affecter plusieurs autres droits et libertés fondamentales. Outre le fait de s'assurer que le partage de renseignements est fondé en droit interne, une bonne pratique largement admise consiste à s'assurer que ledit partage repose sur des accords ou des mémorandums conclus entre les parties qui sont conformes à des directives énoncées par les lois nationales.[157] Parmi les éléments communément inclus dans ce type d'accords se trouvent des règles régissant l'utilisation des renseignements partagés, une déclaration des parties sur le respect des droits de l'homme et la protection des données, et une disposition permettant au service qui fournit des renseignements de demander des informations en retour sur l'usage fait desdits renseignements.[158] Les accords de partage de renseignements contribuent à établir des normes mutuellement acceptables, à définir ce que l'on peut attendre du partage de renseignements et à limiter le champ du partage informel de renseignements, difficilement contrôlable par les institutions de contrôle.

Pratique 32

La législation nationale définit la procédure d'autorisation des accords de partage de renseignements, ainsi que la procédure applicable au partage ad hoc de renseignements. Tout accord de partage de renseignements avec une entité étrangère doit être approuvé par l'exécutif, de même que tout partage de renseignements pouvant avoir des conséquences importantes pour les droits de l'homme.

Le fait que la législation nationale contienne des directives concernant l'autorisation de la transmission ad hoc de renseignements et la conclusion d'accords de partage de renseignements constitue une bonne pratique.[159] Ceci permet de garantir que le partage de renseignements suit des voies officielles responsables, et que les personnes concernées pourront rendre compte de toute décision prise en la matière. Dans de nombreux États, le partage de renseignements de routine sur le plan national est autorisé au niveau interne (par les services de renseignement eux-mêmes). Cependant, quand des informations partagées par des services de renseignement peuvent être utilisées dans un procès, c'est une bonne pratique que le partage en question soit soumis à l'autorisation de l'exécutif; l'utilisation de tels renseignements dans un procès peut être lourde de conséquences pour les droits de la ou des personne(s) concernée(s), mais aussi pour les activités des services de renseignement eux-mêmes.[160] De surcroît, de nombreuses législations nationales imposent que le partage de renseignements et l'établissement d'accords de partage de renseignements avec des entités étrangères soient soumis à l'approbation de l'exécutif.[161]

Pratique 33

Avant de conclure un accord de partage de renseignements ou de procéder à un partage ad hoc de renseignements, les services de renseignement évaluent les résultats de leurs homologues dans le domaine des droits de l'homme et de la protection des données, ainsi que les garanties légales et les contrôles institutionnels auxquels ils sont soumis. Avant de transmettre des informations, les services de renseignement s'assurent que toutes les données partagées sont pertinentes eu égard au mandat du récepteur, qu'elles seront utilisées conformément aux conditions stipulées et qu'elles ne seront pas utilisées à des fins contraires aux droits de l'homme.

Aussi bien la transmission que la réception de renseignements peuvent avoir des conséquences importantes pour les droits de l'homme et les libertés fondamentales. Les informations transmises à un gouvernement ou des services de renseignement étrangers peuvent servir de base à la limitation légitime des droits fondamentaux d'une personne, mais elles peuvent aussi être à l'origine d'une violation des droits de l'homme. De même, des renseignements reçus d'une entité étrangère peuvent être obtenus d'une manière

contraire au droit international humanitaire. Aussi, avant de conclure un accord de partage de renseignements et avant tout partage de renseignements, une bonne pratique consiste, pour les services de renseignement, à procéder à une évaluation générale des résultats des services partenaires en matière de protection des droits de l'homme et des données personnelles, mais aussi de garanties légales et institutionnelles (par exemple en matière de contrôle) régissant ces services.[162] Avant de partager des informations sur des personnes ou des groupes spécifiques, les services de renseignement prennent des mesures pour évaluer les conséquences possibles pour les personnes concernées.[163] C'est une bonne pratique que d'interdire absolument le partage de tout renseignement s'il est vraisemblable que ledit partage pourrait entraîner une violation des droits de la ou des personne(s) concernée(s).[164] Dans certaines circonstances, un partage de renseignements qui contribuerait à entraîner des violations graves des droits de l'homme pourrait engager la responsabilité de l'État. De plus, de nombreuses lois nationales imposent aux États d'évaluer la nécessité de partager des renseignements particuliers en se référant à leur propre mandat et à celui de leurs homologues.[165] Évaluer la nécessité du partage de renseignements et sa pertinence à l'égard du mandat du destinataire permet aux services de renseignement d'appliquer le principe du partage minimum, selon lequel les services de renseignement qui partagent des informations limitent au strict minimum la quantité de données personnelles transférées.[166] Cette garantie contribue à prévenir les partages de renseignement abusifs ou arbitraires.

Vu les conséquences possibles du partage de renseignements sous l'angle des droits de l'homme, c'est une bonne pratique que les services de renseignement contrôlent toutes les informations à transférer pour s'assurer de leur exactitude et de leur pertinence avant de les adresser à des entités étrangères.[167] En cas de doute quant à la fiabilité d'informations à transférer, celles-ci sont soit soustraites à la communication, soit accompagnées d'une estimation du risque d'erreur.[168] Enfin, le fait que tout partage de renseignements se fasse sous forme écrite et soit enregistré constitue également une bonne pratique; ceci pour faciliter l'examen ultérieur des institutions de contrôle.[169]

Pratique 34

Les institutions indépendantes de contrôle sont en mesure d'examiner les accords de partage de renseignements, ainsi que toute information adressée par des services de renseignement à des entités étrangères.

C'est une bonne pratique que de mandater les institutions de contrôle pour examiner les accords servant de fondement au partage de renseignements, ainsi que tout arrangement basé sur ces accords.[170] Les institutions indépendantes de contrôle peuvent examiner le cadre juridique et les aspects procéduraux des accords de partage de renseignements afin de s'assurer de leur conformité avec le droit interne et les normes de droit international pertinentes. En règle générale, les institutions de contrôle sont autorisées à accéder à toute information nécessaire à l'exercice de leurs fonctions, (voir ci-dessus pratique n° 7). Cependant, dans le contexte du partage international de renseignements, les règles applicables au tiers peuvent restreindre l'accès de l'institution de contrôle aux informations reçues d'entités étrangères. Les institutions de contrôle sont généralement considérées comme des tiers; aussi, normalement, elles ne peuvent pas accéder aux informations transmises aux services de renseignement par des entités étrangères. Nonobstant, les institutions de contrôle ont le droit d'examiner les renseignements adressés à des entités étrangères, et elles exercent ce droit dans le cadre de leurs attributions, consistant à contrôler tous les aspects des activités des services de renseignement (voir pratique n° 7 ci-dessus). Dans ce contexte, le fait que la législation nationale exige explicitement des services de renseignement qu'ils signalent tout partage de renseignements à une institution de contrôle indépendante constitue une bonne pratique.[171] Ceci permet de vérifier la légalité des pratiques de partage de renseignements; c'est une garantie importante contre des partages de données personnelles qui pourraient avoir des conséquences graves sur les droits fondamentaux des personnes concernées.

Pratique 35

Il est expressément interdit aux services de renseignement de recourir à l'assistance de services de renseignement étrangers de quelque manière que ce soit, si cela a pour conséquence de circonvenir les normes du droit interne et les contrôles institutionnels applicables à leurs activités. Si les États demandent à des services de renseignement étrangers de mener des activités en leur nom, ils imposent à ces services de se conformer aux mêmes normes légales que celles qui seraient applicables si lesdites activités étaient menées par leurs propres services de renseignement.

Les lois nationales régissant les activités des services de renseignement contiennent des garanties légales et institutionnelles destinées à protéger les droits de l'homme et l'ordre juridique et constitutionnel dans le cadre des activités desdits services. Pour cette raison, il serait contraire au respect de la légalité que des États ou leurs services de renseignement demandent à des entités étrangères de mener des actions sur le territoire sous leur juridiction qu'ils ne seraient pas autorisés à mener eux-mêmes. Une bonne pratique serait que la législation nationale interdise absolument que les services de renseignement coopèrent avec des entités étrangères pour échapper aux obligations juridiques encadrant leurs propres activités.[172] De plus, il importe de rappeler que les États sont dans l'obligation internationale de protéger les droits de toutes les personnes relevant de leur juridiction. Ceci implique qu'ils ont le devoir de s'assurer que les services de renseignement étrangers ne se livrent sur leur territoire à aucune activité contraire aux droits de l'homme, et qu'ils doivent s'interdire de participer à une telle activité.[173] En effet, les États engagent leur responsabilité au niveau international s'ils aident un autre État à violer les droits fondamentaux de qui que ce soit.[174]

Notes

* The Special Rapporteur would like to acknowledge the contribution of Hans Born and Aidan Wills of the Geneva Centre for the Democratic Control of Armed Forces for conducting a background study and assisting in the preparation of this compilation. Furthermore, the Special Rapporteur is grateful to Governments, as well as members of intelligence oversight institutions, (former) intelligence officials, intelligence and human rights experts as well as members of civil society organizations for their participation in the consultation process which led to this compilation.

1 For the purposes of the present study, the term 'intelligence services' refers to all state institutions that undertake intelligence activities pertaining to national security. Within this context, this compilation of good practice applies to all internal, external, and military intelligence services.

2 Germany, Federal Act on Protection of the Constitution, sect. 5(1); Croatia, Act on the Security Intelligence System, art. 23 (2); Argentina, National Intelligence Law, art. 2 (1); Brazil, Act 9 883, arts. 1(2) and 2(1); Romania, Law on the Organisation and Operation of the Romanian Intelligence Service, art. 2; South Africa, National Strategic Intelligence Act, sect. 2 (1).

3 Australia, Security Intelligence Organisation Act, sect. 4.

4 General Assembly resolutions 54/164 and 60/288; Council of the European Union, European Union Counter-Terrorism Strategy, doc. no 14469/4/05; para. 1; Inter-American Convention Against Terrorism, AG/RES. 1840 (XXXII-O/02), preamble; Council of Europe, Committee of Ministers, Guidelines on human rights in the fight against terrorism, art. I.

5 General Assembly resolutions 54/164 and 60/288; Council of the European Union, European Union Counter-Terrorism Strategy, doc. no 14469/4/05; para. 1; Inter-American Convention Against Terrorism, AG/RES. 1840 (XXXII-O/02), preamble; Council of Europe, Committee of Ministers, Guidelines on human rights in the fight against terrorism, art. I.

6 Norway, Act relating to the Norwegian Intelligence Service, sect. 8; Bosnia and Herzegovina, Law on the Intelligence and Security Agency, arts. 5–6; Brazil (footnote 2), art. 4; Canada, Security Intelligence Service Act, sects. 12–16; Australia (footnote 3), sect. 17. This practice was also recommended in Morocco, Instance equité et réconciliation, rapport final, Vol. I, Vérité, équité et réconciliation, 2005, chapitre IV, 8-3 (hereafter Morocco – ER Report); European Commission for Democracy Through Law, Internal Security Services in Europe, CDL-INF(1998)006, I, B (b) and (c) (hereafter Venice Commission (1998)).

7 Canada (footnote 6), sect. 2; Malaysia, report of the Royal Commission to enhance the operation and management of the Royal Malaysia Police of 2005, (hereafter Malaysia – Royal Police Commission), 2.11.3 (p. 316); Croatia (footnote 2), art. 23(1); Australia (footnote 3), sect. 4; Germany (footnote 2), sects. 3(1) and 4; United States of America, Executive Order 12333, art. 1.4 (b).

8 Romania, Law on Preventing and Countering Terrorism, art. 4; Norway, Criminal Code, sect. 147a; New Zealand, Intelligence and Security Service Act, sect. 2.

9 Croatia (footnote 2), Arts. 25–37; Lithuania, Law on State Security Department, art. 3; Germany (footnote 2), sect. 8. See also: South African Ministerial Review Commission, p. 157; Canada, MacDonald Commission, p. 410; Morocco - IER report, 8-3; Malaysia, Royal Police Commission, 2.11.3 (p. 316).

10 Council of Europe (footnote 4), art. V (i); European Court of Human Rights, Malone v. The United Kingdom, para. 67.

11 Canada, MacDonald Commission, pp. 432, 1067.

12 General Assembly resolution 56/83, annex, art. 4 (1); Dieter Fleck, "Individual and State responsibility for intelligence gathering", Michigan Journal of International Law 28, (2007), pp. 692-698.

13 General Assembly resolution 56/83, annex, art. 3.

14 Brazil (footnote 2), art. 1(1); Sierra Leone, National Security and Central Intelligence Act, art. 13(c); United States Senate, Intelligence activities and the rights of Americans¸ Book II, final report of the select committee to study governmental operations with respect to intelligence (hereafter: Church Committee), p. 297; Canada, MacDonald Commission, pp. 45, 408; Economic Community of West African States Draft Code of Conduct for the Armed Forces and Security Services in West Africa (hereafter ECOWAS Code of Conduct), art. 4; Committee of Intelligence and Security Services of Africa, memorandum of understanding on the establishment of the Committee of Intelligence and Security Services of Africa (hereafter CISSA MoU), art. 6.

15 Argentina (footnote 2), art. 3; Bulgaria, Law on State Agency for National Security, art. 3 (1) 1–2; Bosnia and Herzegovina (footnote 6), art. 1; Brazil (footnote 2), art. 1(1); Croatia (footnote 2), art. 2(2); Ecuador, State and Public Safety Act, art. 3; Lithuania (footnote 9), art. 5; Romania, Law on the National Security of Romania, arts. 5, 16; Mexico (reply).

16 Argentina (footnote 2), art. 24; Venice Commission (1998), I, B (b) and (c); Malaysia, Royal Police Commission 2.11.3 (p. 316); Kenya, National Security Intelligence Act, art. 31; South Africa, Truth and Reconciliation Commission of South Africa, report, vol. 5, chap. 8, p. 328.

17 Germany, Basic Law for the Federal Republic of Germany, art. 45d; South Africa, Constitution, arts. 209–210.

18 See S/2008/39, para. 6. While not included in the present compilation, it should be underlined that civil society organizations also play an important role in the public oversight of intelligence services; see reply of Madagascar.

19 For an elaboration on internal management and control mechanisms, see South African Ministerial Review Committee, p. 204; European Commission for Democracy through Law, report on the democratic oversight of the

security services, CDL-AD(2007), point 131 (hereafter Venice Commission (2007)); OECD DAC handbook on security system reform: supporting security and justice; United Kingdom, Intelligence Security Committee, annual report 2001–2002, p. 46. See also The former Yugoslav Republic of Macedonia (reply).

20 On executive control of intelligence services, see Croatia (footnote 2), art. 15; United Kingdom, Security Services Act, sects. 2(1), 4(1); Argentina (footnote 2), art. 14; Netherlands, Intelligence and Security Services Act, art. 20(2); Sierra Leone (footnote 14), art. 24; Bulgaria (footnote 15), art. 131; Azerbaijan, Law on Intelligence and Counter-Intelligence Activities, art. 22.2.

21 For legislation on parliamentary oversight of intelligence services, see Albania, Law on National Intelligence Service, art. 7; Brazil (footnote 2), art. 6; Romania (footnote 2), art. 1; Ecuador (footnote 14), art. 24; Botswana, Intelligence and Security Act, sect. 38; Croatia (footnote2), art. 104; Switzerland (footnote 5), art. 25, Loi sur l'Assemblée fédérale, art. 53(2); Germany (footnote 17), art. 45d; Bulgaria (footnote 15), art. 132; The former Yugoslav Republic of Macedonia (reply). See also Morocco, IER Report, p. 11. In Latvia, the National Security Committee of the parliament (Saeima) is responsible for parliamentary oversight of the intelligence service (reply); Georgia, Law on Intelligence Activity, art. 16.

22 For specialized intelligence oversight bodies, see Norway, Act on Monitoring of Intelligence, Surveillance and Security Services, art. 1; Canada (footnote 6), sects. 34–40; Netherlands (footnote 20), chapter 6; Belgium, Law on the Control of Police and Intelligence Services and the Centre for Threat Analysis, chapter 3.

23 For mandates to oversee intelligence services' compliance with the law, see Lithuania, Law on Operational Activities, art. 23(2)1–2; Croatia (footnote 2), art. 112; Norway (footnote 22), sect. 2. In South Africa, the Inspector-General for intelligence examines intelligence services' compliance with the law and Constitution; see South Africa, Intelligence Services Oversight Act, sect. 7(7) a-b.

24 South African Ministerial Review Commission report, p. 56; Hans Born and Ian Leigh, Making Intelligence Accountable, Oslo, Publishing House of the Parliament of Norway, 2005, pp. 16–20.

25 Romania (footnote 2), art. 42.

26 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, a new review mechanism for the RMCP's national security activities (hereafter the Arar Commission), p. 469.

27 Sweden, Act on Supervision of Certain Crime-Fighting Activities, art. 4; Netherlands (footnote 20), art. 73; Canada (footnote 6), sect. 38(c).

28 South Africa (footnote 23), sect. 8(a) goes beyond the intelligence community to allowing the Inspector-General access any premises, if necessary. According to sect. 8 (8) c, the Inspector-General can obtain warrants under the Criminal Procedure Act.

29 Croatia (footnote 2), art. 105; Lithuania (footnote 23), art. 23.

30 South Africa (footnote 23), sect. 7a.

31 Belgium (footnote 22), art. 48; The Netherlands (footnote 20), art. 74.6.

32 Belgium (footnote 22), art. 66 bis.

33 Canada (footnote 6), sect. 36.

34 Concerning the assistance of external experts, see Netherlands (footnote 20), art. 76; Lithuania (footnote 23), art. 23 (2); Luxembourg, Law concerning the organization of the State intelligence service, art. 14 (4). On having the disposition of independent legal staff and advice: United Kingdom, Joint Committee on Human Rights, 25 March 2010, paras. 110–111.

35 Lithuania (footnote 23), art. 23.4. In South Africa, the law prescribes criminal sanctions for any unauthorized disclosure by members of the parliamentary oversight body; see South Africa (footnote 23), sect. 7a (a); United States of America Code, General congressional oversight provisions, sect. 413 (d); Norway (footnote 22), art. 9.

36 For example, the staff of the German Parliamentary Control Panel undergo strict security checks; see Germany, Parliamentary Control Panel Act, sects. 11 (1) and 12 (1).

37 As elected representatives of the people, the members of the Parliamentary Control Panel are not obliged to undergo a vetting and clearing procedure, see Germany (footnote 36), sect. 2; United States of America (footnote 35), sect. 413 (d).

38 American Convention on Human Rights, art. 25; Arab Charter on Human Rights, art. 23; Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, annex (E/CN.4/1984/4), art. 8; European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 13; International Covenant on Civil and Political Rights, art. 2.

39 Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, Oslo, Publishing House of the Parliament of Norway, 2005, p. 105.

40 Netherlands (footnote 20), art. 83; in Finland: with regard to data stored by the intelligence service, the Data Protection Ombudsman (reply); Greece: Ombudsman (reply); Estonia: Legal Chancellor (reply).

41 Jordan, Law on the National Centre for Human Rights.

42 For control of the budget of the intelligence service: Costa Rica, Organic Act of the Republic's General Audit.

43 Romania (footnote 15), art. 16.

44 South Africa (footnote 23), sect. 7(7).

45 Norway (footnote 22), art. 3; Canada (footnote 6), sects. 41, 42, 46 and 50.

46 Kenya (footnote 16), arts. 24–26.

47 United Kingdom, Regulation of Investigatory Powers Act, arts. 65–70; Sierra Leone (footnote 14), arts. 24–25.

48 Iain Cameron, National security and the European Convention on Human Rights: Trends and patterns, presented at the Stockholm international symposium on national security and the European Convention on Human Rights, p. 50.

49 Kenya (footnote 16), art. 26; Sierra Leone (footnote 14), art. 27.

50 United Kingdom (footnote 47), art. 68.

51 International Covenant on Civil and Political Rights, art. 26; American Convention on Human Rights, art. 1; Arab Charter on Human Rights, art. 3.1. For case law by the Human Rights Committee see, in particular, Ibrahima Gueye et al. v. France (communication No. 196/1985) and Nicholas Toonen v. Australia (communication 488/1992).

52 Ottawa Principles on Anti-Terrorism and Human Rights, art. 1.1.3.

53 Australia (footnote 3), sect. 17A; Ecuador (footnote 14), art. 22; Canada, Macdonald Commission, p. 518.

54 Argentina (footnote 2), art. 4.

55 Australia (footnote 3), sect. 11, (2A); Sierra Leone (footnote 14), art. 13 (d); Romania (footnote 2), art. 36.

56 Bosnia and Herzegovina (footnote 6), art. 45; Albania (footnote 21), art. 11; Kenya (footnote 16), art. 15 (1)a; Lithuania (footnote 9), art. 24.

57 Botswana (footnote 21), sect. 5(2); Sierra Leone (footnote 14), sect. 13 (d); United Kingdom (footnote 20), sect. 2 (2); South Africa (footnote 17), sect. 199(7).

58 For the involvement of parliament, see Belgium (footnote 22), art. 17; and Australia (footnote 3), sect. 17(3).

59 Poland, Internal Security Agency and Foreign Intelligence Act, art. 16; Croatia (footnote 2), art. 15(2).

60 Canada, MacDonald Commission, p. 514; South African Ministerial Review Commission, pp. 168-169, 174–175; Venice Commission (1998), p. 25.

61 Canada (footnote 6), sect. 2; Switzerland (footnote 5), art. 3 (1); Japan, Act Regarding the Control of Organizations having Committed Indiscriminate Mass Murder, art. 3(1) and (2); United Republic of Tanzania, Intelligence and Security Act, art. 5 (2)b.

62 Netherlands, Security and Intelligence Review Commission, Supervisory Report no. 10 on the investigation by the General Intelligence and Security Service (GISS) into the leaking of State secrets, 2006, point 11.5.

63 Montreux document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict, pp. 12, 35.

64 Croatia (footnote 2), art. 87(1); Human Rights Committee, general comment no 31 on the nature of the general legal obligations imposed on States parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 4; Michael Defeo, "What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?", Revue international de droit penal 78, no 1 (2007), pp. 57–77; European Commission for Democracy through Law, opinion 363/2005 on the International Legal Obligations of Council of Europe Member States in Respect of Secret Detention Facilities and Inter-State Transport of Prisoners, p. 15.

65 E/CN.4/2005/102/Add.1, art. 36.

66 See also practice 6.

67 ECOWAS Code of Conduct, arts. 4 and 6.

68 International Commission of Jurists, "Assessing damage, urging action", report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, pp. 85–89 (hereafter ICJ-EJP report); Imtiaz Fazel, "Who shall guard the guards?: civilian operational oversight and Inspector General of Intelligence", in "To spy or not to spy? Intelligence and Democracy in South Africa", p. 31.

69 Morton Halperin, "Controlling the intelligence agencies", First Principles, vol. I, No. 2, October 1975.

70 United Kingdom (footnote 47), arts. 1, 4; United Kingdom (footnote 20), sect. 7. With regard to engaging in criminal activities as part of intelligence collection, see Netherlands (footnote 20), art. 21 (3); United Kingdom (footnote 47), arts. 1, 4; United Kingdom (footnote 20), sect. 7.

71 South African Ministerial Review Commission, pp. 157–158.

72 Netherlands (footnote 20), annex.

73 Croatia (footnote 2), arts. 88–92; Romania (footnote 15), arts. 20–22, Argentina (footnote 2), art. 42; Bulgaria (footnote 15), art. 88(1), 90 & 91; South Africa (footnote 23), arts. 18, 26.

74 Canada (footnote 6), sect. 20 (2–4).

75 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, arts. 4 and 6.

76 Rome Statute, art. 25 (3) (b-d), Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 1.

77 Hungary, Act on the National Security Services, sect. 27; Lithuania (footnote 9), art. 18; ECOWAS Code of Conduct, art. 16.

78 Bosnia and Herzegovina (footnote 6), art. 42; South Africa (footnote 23), art. 11 (1).

79 Rome Statute, art. 33; Geneva Conventions I–IV; Commission on Human Rights (footnote 65), principle 27; see also Lithuania (footnote 9), art. 18.

80 Bosnia and Herzegovina (footnote 6), art. 42.

81 New Zealand, Protected Disclosures Act, sect. 12; Bosnia and Herzegovina (footnote 6), art. 42; Canada, Security of Information Act, sect. 15.

82 United Kingdom, Intelligence and Security Committee, annual report 2007–2008, paras. 66–67 (reference to the position of an "ethical counsellor" within the British Security Service); United States of America, Department of Justice, Whistleblower Protection for Federal Bureau of Investigation Employees, Federal Register, vol. 64, No. 210 (Inspector General and the Office of Professional Responsibility).

83 Germany (footnote 36), sect. 8(1); New Zealand (footnote 81), sect. 12. It should be noted that, in New Zealand, the Inspector-General is the only designated channel for protected disclosures.

84 United States of America (footnote 35), title 50, sect. 403(q), 5; Canada (footnote 6), sect. 15 (5); Australia, Inspector-General of Intelligence and Security Act 1986, sect.s 8 (1)a,(2)a,(3)a and 9(5).

85 Canada (footnote 81), sect. 15; Germany, Criminal Code, sects. 93(2), 97a and 97b. The importance of public disclosures as a last resort was also highlighted in the report "Whistleblower protection: a comprehensive scheme for the Commonwealth public sector" House of Representatives Standing Committee on Legal and Constitutional Affaires on the inquiry into whistleblowing protection within the Australian Government public sector, pp. 163–164; see also National Commission on Terrorist Attacks Upon the United States, "The 911 Commission Report", chapter 3.

86 Netherlands, Government Decree of 15 December 2009 Laying Down a Procedure for Reporting Suspected Abuses in the Police and Government Sectors, art. 2; United States of America, title 5, US Code, sect. 2303(a); Bosnia and Herzegovina (footnote 6), art. 42; Australia (footnote footnote 84), sect. 33; Parliamentary Assembly of the Council of Europe, Draft Resolution on the protection of whistleblowers, doc. 12006, paras. 6.2.2 and 6.2.5.

87 South African Ministerial Review Commission on Intelligence, p. 233.

88 South Africa, Five principles of intelligence service professionalism, South African Intelligence Services; South Africa, Ministerial Regulations of the Intelligence Services, chapter 1(3)(d), 1(4)(d); see also Bulgaria (footnote 15), art. 66 (with regard to application of the Ethical Code of Behaviour for Civil Servants to members of the intelligence services).

89 United Republic of Tanzania (footnote 61), art. 8(3); South Africa, Five principles of intelligence service professionalism, South African Intelligence Services.

90 United Republic of Tanzania (footnote 61), art. 8(3).

91 Netherlands, Supervisory Committee on Intelligence and Security Services, On the Supervisory Committee's investigation into the deployment by the GISS of informers and agents, especially abroad, see sect. 4; for the role of Inspectors-General in these matters, see South African Ministerial Review Commission, p. 234.

92 South African Ministerial Review Commission on Intelligence, pp. 209 and 211.

93 Argentina (footnote 2), arts. 26–30; South Africa (footnote 23), art. 5(2)(a).

94 Siracusa Principles (footnote 38).

95 See practices nos. 3 and 4; Croatia (footnote 2), art. 33; Lithuania (footnote 9), art. 5; Council of Europe (footnote 4), para. 5.

96 MacDonald Commission, p. 423; Morton Halperin (footnote 69).

97 Sierra Leone (footnote 14), art. 22 (b); United Republic of Tanzania (footnote 61), art. 14 (1); Japan (footnote 61), art. 3(1); Botswana (footnote 21), sect. 22(4) a-b.

98 Johannesburg Principles on National Security, Freedom of Expression and Access to Information, principle 2(b); Ottawa Principles, principle 7.4.1.

99 Germany (footnote 2), sect. 8(5); Germany, Act on the Federal Intelligence Service, sect. 2(4); Council of Europe (footnote 4), art. V (ii); MacDonald Commission report, p. 513.

100 Croatia (footnote 2), art. 33(2); Hungary (footnote 77), sect. 53(2); United States of America, Executive Order No. 12333, sect. 2.4. Federal Register vol. 40, No. 235, sect. 2; Germany (footnote 2), Sect. 8(5); Germany (footnote 99), Sect. 2(4); A/HRC/13/37, paras. 17 (f) and 49.

101 Botswana (footnote 21), sect. 16 (1)(b)(i) related to the prohibition of torture and similar treatment.

102 American Convention on Human Rights, art. 25; Arab Charter, art. 9; Siracusa principles, art. 8; European Court of Human Rights, Klass v. Germany, A 28 (1979-80), 2 EHHR 214, para. 69. See also practices 9 and10.

103 European Court of Human Rights, Liberty v. UK, para 63; Malone v. The United Kingdom, 2 August 1984, para.67; Council of Europe (footnote 4), art. V (i); Huvig v. France, para. 32; Kenya (footnote 16), art. 22 (4); Romania (footnote 8), art. 20. This recommendation is also made in the Moroccan TRC Report, vol. 1, chap. IV, 8-4; Hungary (footnote 77), sects. 54, 56; Croatia (footnote 2), art. 33 (3-6).

104 European Court of Human Rights, Weber & Saravia v. Germany, decision on admissibility, para. 95; European Court of Human Rights, Huvig v France, 24 April 1990, para. 34; United Republic of Tanzania (footnote 61), art. 15(1).

105 Kenya (footnote 16), art. 22 (1); Sierra Leone (footnote 14), art. 22; Tanzania (footnote 61), art. 14 (1), 15 (1); Canada (footnote 6), sect. 21 (all reasonable grounds); Netherlands (footnote 20), art. 6(a) (serious suspicion); Germany (footnote 2), sect. 9(2); Germany, Constitutional Court, Judgement on Provisions in North-Rhine Westphalia Constitution Protection Act, 27 February 2008.

106 Germany, G10 Act, sect. 3b; Germany (footnote 85), sects. 53 and 53a.

107 Germany (footnote 106), sect. 10 (5); Kenya (footnote 16), art. 22 (6); Romania (footnote 8), art. 21(10); South Africa (footnote 23), sect. 11(3)a; Croatia (footnote 2), art. 37; Canada (footnote 6), sect. 21 (5); Hungary (footnote 77), sect. 58(4), sect. 60 (termination); European Court of Human Rights, Weber & Saravia v. Germany, para. 95.

108 United Kingdom (footnote 47), sect. 9; Germany (footnote 106), sect. 11(2); Germany (footnote 2), sect. 9 (1); European Court of Human Rights, Huvig v France, para. 34.

109 Germany (footnote 106), sects. 9–10; Canada (footnote 6), sect. 21; Netherlands (footnote 20), arts. 20(4) and 25(4); Kenya (footnote 16), art. 22.

110 Australia (footnote 3), arts. 25, 25a; Netherlands (footnote 20), arts. 19, 20(3–4), 22 (4), 25; United Kingdom (footnote 47), sects. 5–7.

111 Argentina (footnote 2), arts. 18 and 19; Kenya (footnote 16), art. 22; Sierra Leone (footnote 14), art. 22; Croatia (footnote 2), arts. 36–38; Romania (footnote 8), arts. 21 and 22; Canada (footnote 6), sect. 21 (1–2); South Africa (footnote 23), sect. 11. See also European Court of Human Rights, Klass v. Germany (footnote 102), para. 56.

112 The European Court of Human Rights has indicated its preference for judicial control for the use of intrusive collection methods, see Klass v. Germany (footnote 102), paras. 55–56. See also Parliamentary Assembly of the

Council of Europe, recommendation 1402, ii. The South African Ministerial Review Commission argues that all intrusive methods should require judicial authorizations; see p. 175; Cameron (footnote 48), pp. 151, 156–158.

113 Canada (footnote 6), sect. 21; Germany (footnote 106), sects. 9–11 and 15(5). See also Canada, MacDonald Commission, pp. 516–528.

114 Croatia (footnote 2), art. 38 (2); United Kingdom (footnote 47), sect. 9(3–4); Germany (footnote 106), sect. 12 (6). See also Canada, MacDonald Commission, p. 522.

115 United Kingdom (footnote 47), sect. 57(2); Norway, Parliamentary Intelligence Oversight Committee; Netherlands (footnote 20), art. 64(2)(a).

116 Japan, Act on the Protection of Personal Information held by Administrative organs; Switzerland, Loi fédérale sur la protection des données.

117 A/HRC/13/37, paras. 11–13. For specific examples of international principles, see the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108); the Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); The Guidelines for the Regulation of Computerized Personal data Files (General Assembly resolution 45/95 and E/CN.4/1990/72).

118 It should be acknowledged that international agreements permit derogation from basic principles for data protection when such derogation is provided for by law and constitutes a necessity in the interest of, inter alia, national security. See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), art. 9.

119 European Court of Human Rights, Weber and Saravia v. Germany, no. 54934/00, 29 June 2006, paras. 93–95.

120 MacDonald Inquiry, p. 519; Netherlands (footnote 20), art. 13.

121 Canada, Privacy Act, sect. 10. An overview of personal information banks maintained by the Canadian Security and Intelligence Services can be found on the website of the Government of Canada (http://www.infosource.gc.ca/inst/csi/fed07-eng.asp).

122 Romania (footnote 15), art. 21.

123 For example, in Ecuador, intelligence services are not allowed to store personal data on the basis of ethnicity, sexual orientation, religious belief, political position or of adherence to or membership in political, social, union, communitarian, cooperative, welfare, cultural or labour organizations; see Ecuador (footnote 15), art. 22.

124 Germany (footnote 2), sect. 14 (2); Germany (footnote 106), sect. 4 (1), sect. (5); Switzerland (footnote 5), art. 15 (1) (5).

125 Germany (footnote 2), sect. 12 (2); Kenya (footnote 16), sect. 28(1).

126 Netherlands (footnote 20), art. 43; Croatia (footnote 2), art. 41(1).

127 Charkaoui v. Canada (Citizenship and Immigration), [2008] 2 S.C.R. 326, 2008 SCC 38, para. 64.

128 Sweden (footnote 27), art. 1; Hungary (footnote 77), sect. 52. See also practices 6–8.

129 In Norway, the Parliamentary Intelligence Oversight Commission is obliged to carry out six inspections per year of the Norwegian Police Security Service, involving at least 10 random checks in archives in each inspection and a review of all current surveillance cases at least twice per year; see Norway, Instructions for monitoring of intelligence, surveillance and security services, arts. 11.1 (c) and 11.2 (d).

130 See Germany (footnote 2), sect. 14 (1), according to which the Federal Commissioner for Data Protection and Freedom of Information should be heard prior to issuing a directive on file management.

131 Sweden, Ordinance containing Instructions for the Swedish Commission on Security and Integrity Protection, paras. 4–8 (on management and decision-making), 12 and 13 (on resources and support).

132 Hungary (footnote 77), sect. 52.

133 Croatia (footnote 2), art. 40 (1).

134 Netherlands (footnote 20), art. 47.

135 Sweden (footnote 27), art. 3; Switzerland (footnote 5), art. 18 (1).

136 David Banisar, Public oversight and national security: Comparative approaches to freedom of information, Marina Caparini and Hans Born (eds.), Democratic control of intelligence services: Containing the rogue elephant, p. 217.

137 Netherlands (footnote 20), arts. 53–56; Croatia (footnote 2), art. 40 (2) (3); Germany (footnote 2), sect. 15(2).

138 Albania (footnote 21), art. 9; United Republic of Tanzania (footnote 61), art. 4 (2)a; Argentina (footnote 2), art. 4 (1); New Zealand (footnote 8), sect. 4(2); Germany (footnote 2), art. 2(1).

139 A/HRC/10/3, paras. 31, 69; Secretary-General of the Council of Europe, report under art. 52 of the European Convention of Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies, SG/Inf (2006) 5, para. 41; Parliamentary Assembly of the Council of Europe, recommendation 1402, paras. 5–6; International Commission of Jurists, "Assessing damage, urging action", pp. 73–78, 89; Canada, MacDonald Commission, pp. 422–423 and 613–614.

140 Norway, Criminal Procedure Act.

141 International Commission of Jurists, "Assessing damage, urging action", pp. 73–78.

142 Hungary (footnote 77), art. 32; Bulgaria (footnote 15), arts. 121(2)3, 125 and 128; Norway (footnote 140), sects. 171–190.

143 Norway, Criminal Procedure Act (footnote 140), sects. 171–173 (implied); Hungary (footnote 77), art. 32 (implied); Lithuania (footnote 9), art. 18 (implied); Switzerland (footnote 5), art. 14 (3).

144 Venice Commission (1998), sect. E.

145 Cyprus, Reply; Norway (footnote 140), sects. 183–185; Bulgaria (footnote 15), art. 125(5); Mexico, reply.

146 International Covenant on Civil and Political Rights, art. 9(4); OSCE-ODIHR, Countering Terrorism, Protecting Human Rights, pp. 158–160; Arab Charter on Human Rights, art. 8; American Convention on Human Rights, art. 7(6); Council of Europe (footnote 4), arts. VII (3) and VIII; General Assembly resolution A/RES/43/173, annex, principle 4.

147 Venice Commission (1998), sect. E

148 See Code of Conduct for Law Enforcement Officials in General Assembly resolution 34/169; Basic Principles on the Use of Force and Firearms by Law Enforcement Officials; General Assembly resolution 43/173, annex. See also Committee of Ministers of the Council of Europe, European Code of Police Ethics, recommendation (2001)10 (hereafter, European Code of Police Ethics).

149 Convention against Torture, art. 1; African Charter on Human and People's Rights, art. 5; Code of Conduct for Law Enforcement Officials, art. 5; European Code of Police Ethics, arts. 35 and 36; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, principle 6.

150 Code of Conduct for Law Enforcement Officials, art. 3; European Code of Police Ethics, art. 37; Council of Europe (footnote 4), art. VI (2); Morocco, IER Report, vol. 1, chap. IV, 8–6.

151 Bulgaria (footnote 15), art. 125 (8); OSCE Guidebook on Democratic Policing, 2008, arts 55–64; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, principle 12.

152 American Convention on Human Rights, art. 7(4); European Convention on Human Rights, art. 5(2); European Code of Police Ethics, art. 45; Council of Europe (footnote 4), art. VII (1); OSCE-ODIHR, Countering Terrorism, Protecting Human Rights, p. 157; Fox, Campbell and Hartley v. UK, para. 40; Norway (footnote 140), sect. 177.

153 See also European Code of Police Ethics, arts. 48, 50, 54, 55 and 57; Bulgaria (footnote 15), art. 125(6); and Norway (footnote 140), sect. 186.

154 Romania (footnote 2), art. 13.

155 Australia (footnote 3), sect. 34G(3)(i)(iii); Lithuania (footnote 9), art. 19(4); Venice Commission (1998), sect. E.

156 Croatia (footnote 2), arts. 58, 60; Switzerland (footnote 5), art. 17; Netherlands (footnote 20), arts. 37, 41 and 42, 58–63; Albania (footnote 21), art. 19; Canada (footnote 6), arts. 17, 19; Germany (footnote 2), sects. 19, 20, Germany (footnote 99), sect. 9; Germany (footnote 106), sects. 4 (4–6), 7, 7a, 8 (6); Hungary (footnote 77), sects. 40, 44, 45. See also Canada, MacDonald Commission Report, p. 1080.

157 Canada, Arar Commission, pp. 321–322; Venice Commission (2007), p. 182.

158 Canada, Arar Commission, p. 339; Germany (footnote 2), sect. 19; Germany (footnote 106), sect. 7a(4); Netherlands (footnote 20), arts. 37, 59; Croatia (footnote 2), art. 60 (3).

159 Croatia (footnote 2), art. 59(2); United Republic of Tanzania (footnote 61), art. 15 (3) (4); Canada (footnote 6), art. 17.

160 Netherlands (footnote 20), arts. 38.1 and 61; Canada (footnote 6), art. 17.1 (a).

161 Netherlands (footnote 20), art. 59 (5–6); Croatia (footnote 2), art. 59(2); United Kingdom, Intelligence and Security Committee, p. 54; Canada (footnote 6), art. 17.1 (b); Germany (footnote 106), art. 7a; Germany (footnote 2), sect. 19(1).

162 Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with Foreign intelligence and/or security services, pp. 7–11, 43; Arar Commission pp. 345, 348.

163 Croatia (footnote 2), art. 60 (1); Germany (footnote 2), sect. 19; Switzerland (footnote 5), art. 17 (4); Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with foreign intelligence and/or security services, p. 24.

164 Canada, Arar Commission, p. 346–347.

165 Croatia (footnote 2), art. 60 (1)(3); Germany (footnote 2), sect. 19, Germany (footnote 106), sect. 7 a (1)1; Switzerland (footnote 2), art. 17 (3).

166 Canada, Arar Commission, pp. 338–339.

167 Netherlands (footnote 20), arts. 41, 59; Canada, Arar Commission pp. 332, 334–336.

168 Netherlands (footnote 20), art. 41. On this obligation in the context of domestic sharing, see South Africa (footnote 2), sect. 3(3).

169 Netherlands (footnote 20), art. 42; Germany (footnote 2), sect. 19 (3)(4); Germany (footnote 106), sect. 7 a (3); Croatia (footnote 2), art. 60(3); Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with foreign intelligence and/or security services, pp. 22–23.

170 Canada (footnote 6), art. 17(2); Canada, MacDonald Commission report, p. 1080; Canada, Arar Commission, p. 321; Venice Commission (2007), p. 182.

171 Germany (footnote 106), sect. 7a (5–6); Croatia, Act on Personal Data Protection, art. 34.

172 European Parliament Temporary Committee on the Echelon Interception System, report on the existence of a global system for the interception of private and commercial communications, A5-0264/2001, pp. 87–88 (hereafter European Parliament, Echelon report); Church Committee report, p. 306.

173 Human Rights Committee, general comment No. 31 on the nature of the general legal obligation imposed on States parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 10; European Parliament Echelon report, pp. 87–89.

174 Human Rights Committee, general comment No. 31; General Assembly resolution 56/83, annex, art. 16; Secretary-General of the Council of Europe, Secretary-General's report under art. 52 of the European Convention on Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies, SG/Inf (2006) 5, paras. 23 and 101.

مركز جنيف للرقابة الديموقراطية على القوات المسلحة
شارع المعارف ٣٤
رام الله / البيرة
الضفة الغربية
فلسطين

هاتف: ٦٢٩٧ ٢٩٥ (٢) ٩٧٢+
فاكس: ٦٢٩٥ ٢٩٥ (٢) ٩٧٢+

مركز جنيف للرقابة الديموقراطية على القوات المسلحة
مركز جيفنور – بلوك C – الطابق السادس
شارع كليمنسو
بيروت
لبنان

هاتف: ٤٠١ ١٧٣٨ (٠) ٩٦١+
فاكس: ٤٠٢ ١٧٣٨ (٠) ٩٦١+

DCAF Genève
Adresse postale:
Centre pour le Contrôle Démocratique des Forces Armées – Genève (DCAF)
P.O. Box 1360
CH-1211 Genève 1
Suisse

Pour les visiteurs:
Centre pour le Contrôle Démocratique des Forces Armées – Genève (DCAF)
Rue de Chantepoulet 11
CH-1201 Genève 1
Suisse
Tel: +41 (0) 22 741 77 00
Fax: +41 (0) 22 741 77 05

DCAF Beyrouth
Centre pour le Contrôle Démocratique des Forces Armées – Genève (DCAF)
Gefinor Center - Block C - 6th Floor
Clemenceau Street
Beyrouth
Liban
Tel: +961 (0) 1 738 401
Fax: +961 (0) 1 738 402

DCAF Ramallah
Centre pour le Contrôle Démocratique des Forces Armées – Genève (DCAF)
Al-Maaref Street 34
Ramallah / Al-Bireh
Cisjordanie
Palestine
Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

www.dcaf.ch