



Assemblée générale

Distr. générale
17 mai 2010
Français
Original: anglais

Conseil des droits de l'homme

Quatorzième session

Point 3 de l'ordre du jour

**Promotion et protection de tous les droits de l'homme,
civils, politiques, économiques, sociaux et culturels,
y compris le droit au développement**

Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte antiterroriste, Martin Scheinin*

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 la lutte antiterroriste**

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 1^{er} mai 2010 ont été pris en compte. Ces documents seront reproduits sous la forme d'un addendum (A/HRC/14/46/Add.1).

Cette procédure a permis d'identifier 35 bonnes pratiques, obtenues à partir de pratiques existantes ou émergentes dans un vaste ensemble de pays à travers le monde.

* Soumission tardive

** Le présent rapport excédant largement les limites actuellement imposées par les résolutions pertinentes de l'Assemblée générale, l'annexe et les notes de bas de page sont reproduites telles qu'elles ont été reçues, uniquement dans la langue du texte original.

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

Le contenu des dites 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 de renseignement (pratiques 21 à 35).

Table des matières

	<i>Paragraphes</i>	<i>Page</i>
I. Introduction.....	1–8	4
II. Compilation de bonnes pratiques en matière de cadres juridiques et institutionnels pour le contrôle des services de renseignement.....	9–50	5
A. Mandats et fondements juridiques.....	9–12	5
B. Institutions de contrôle.....	13–15	8
C. Plaintes et recours effectifs.....	16–17	11
D. Impartialité et non-discrimination.....	18–20	13
E. Responsabilité des États à l’égard des services de renseignement.....	21	14
F. Responsabilité individuelle.....	22–25	15
G. Professionnalisme.....	26	18
H. Protection des droits de l’homme.....	27–33	19
I. Recherche du renseignement.....	34–36	21
J. Gestion et utilisation des données personnelles.....	37–40	23
K. Recours au pouvoir d’arrestation et de détention.....	41–44	26
L. Partage de renseignements et coopération.....	45–50	28
 Annexe		
Good practices on legal and institutional frameworks for intelligence services and their oversight.....		33

I. Introduction*

1. 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.

2. Les services de renseignement¹ 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.

3. Cette compilation tire sa substance de pratiques existantes et émergentes 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.

4. 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.

5. 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.

* 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.

6. 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.

7. 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.

8. 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.

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

A. Mandats et fondements juridiques

Pratique n° 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.

9. 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 renseignement². 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

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).

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 parlement³. 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 fondamentaux⁴. De fait, plusieurs États mentionnent spécifiquement la protection des droits de l'homme comme étant l'une des fonctions essentielles de leurs services de renseignement⁵.

Pratique n° 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.

10. 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 parlement⁶. 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 pratique⁷. 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

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 équité 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).

adopté des lois qui donnent une définition précise du terrorisme, ainsi que des groupes et des actes terroristes⁸.

Pratique n° 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.

11. Un principe fondamental de l'état de droit veut que tous les pouvoirs et compétences dévolus aux services de renseignement proviennent de la loi⁹. 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 rencontre. 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 fondamentales¹⁰. 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 législateur¹¹. 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 n° 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 n° 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.

12. 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 humanitaire¹². Ceci implique que leur existence

⁸ Roumanie, Law on Preventing and Countering Terrorism, art. 4; Norvège, Criminal Code, sect. 147a; Nouvelle-Zélande, Intelligence and Security Service Act, sect. 2.

⁹ Croatie (footnote 2), Arts. 25–37; Lituanie, Law on State Security Department, art. 3; Allemagne (footnote 2), sect. 8. Voir aussi: South African Ministerial Review Commission, p. 157; Canada, MacDonald Commission, p. 410; Maroc - IER report, 8-3; Malaisie, Royal Police Commission, 2.11.3 (p. 316).

¹⁰ Conseil de l'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

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 internationale¹³. 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 lois¹⁴. 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 notoire¹⁵. 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 pratique¹⁶.

B. Institutions de contrôle

Pratique n° 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.

13. À l'instar des services de renseignement, les institutions qui contrôlent leurs activités sont régies par les lois, ainsi, dans certains, que par la constitution¹⁷. Il n'existe pas

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.

de modèle unique en matière de contrôle des services secrets. Cependant, les éléments suivants sont communément inclus dans les systèmes exhaustifs de contrôle¹⁸: des mécanismes de gestion et de contrôle internes au sein des services de renseignement¹⁹; un contrôle exercé par l'exécutif²⁰; un contrôle exercé par des organes parlementaires²¹, et un autre par des organes spécialisés et/ou judiciaires²². 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 lois²³. De plus, elles évaluent les performances des services de renseignement²⁴. Ceci inclut le fait d'examiner si les services de renseignement font un usage efficace des fonds publics qui leur sont alloués²⁵. 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

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 (footnote 2), 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.

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'homme²⁶.

Pratique n° 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.

14. 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 pertinents²⁷, inspecter les locaux des services de renseignement²⁸ et obtenir que tout membre desdits services témoigne sous serment²⁹. 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 elles³⁰. Ceci implique que les institutions de contrôle puissent recourir aux services répressifs pour obtenir la coopération des personnes concernées³¹. 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 œuvre 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 parlement³², sont habilitées à recruter un personnel spécialisé³³ et à faire appel aux services d'experts externes³⁴.

Pratique n° 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

²⁶ Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, a new review mechanism for the RCMP'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.

l'encontre des membres des institutions de contrôle qui enfreignent ces prescriptions.

15. 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 pénales³⁵. 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 classés³⁶. Alternativement, une approche souvent adoptée par les institutions de contrôle parlementaire consiste à faire signer aux membres un accord³⁷ de non-divulgateur. En définitive, le traitement approprié des renseignements classés par les institutions de contrôle repose aussi sur le professionnalisme des membres desdites institutions.

C. Plaintes et recours effectifs

Pratique n° 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.

16. 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 droits³⁸. 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

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.

recours effectif. Globalement, on peut distinguer deux approches à cet égard³⁹. 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 médiation⁴⁰, de la commission nationale des droits de l'homme⁴¹, de l'office national de vérification⁴², de l'organe parlementaire de contrôle⁴³, de l'inspection générale⁴⁴, de l'organe spécialisé de contrôle des services de renseignement⁴⁵ et de la commission de recours contre les actes des services de renseignement⁴⁶. 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 exclusives⁴⁷ ou d'entités faisant partie du système judiciaire général. Ces institutions sont généralement habilitées à ordonner des sanctions.

Pratique n° 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.

17. 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 contraignantes⁴⁸. 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 serment⁴⁹, de définir leurs propres procédures en relation avec tout procès et de délivrer des ordonnances contraignantes⁵⁰.

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.

D. Impartialité et non-discrimination

Pratique n° 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.

18. 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 proscrits⁵¹. 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 autre⁵². 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 critères⁵³. Certains États ont aussi expressément interdit à leurs services de renseignement de fichier des personnes pour ce type de motifs⁵⁴.

Pratique n° 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.

19. 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 politique⁵⁵. 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'argent⁵⁶ ou d'agir en sa

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.

faveur⁵⁷ 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 exécutifs⁵⁸; 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 induite⁵⁹.

Pratique n° 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.

20. 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 rassemblement⁶⁰. 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 mesures⁶¹. 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 journalistes⁶².

E. Responsabilité des États à l'égard des services de renseignement

Pratique n° 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.

21. 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 renseignement⁶³. Les États sont légalement tenus de

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

garantir que leurs services de renseignement respectent les droits de l'homme et de remédier à ce type de violations subies par des particuliers⁶⁴. 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 humanitaire⁶⁵. Le contrôle des services de renseignement par l'exécutif est essentiel à ces fins, c'est pourquoi il est consacré par de nombreuses lois nationales⁶⁶.

F. Responsabilité individuelle

Pratique n° 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.

22. 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 actes⁶⁷. En règle générale, le droit constitutionnel, législatif et le droit pénal international s'appliquent aux agents secrets comme à toute autre personne physique⁶⁸. 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 pénale⁶⁹. 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 pénales⁷⁰. Que toute autorisation de cette nature soit strictement limitée, énoncée par la loi et assortie de garanties adéquates est une bonne pratique⁷¹. Les dispositions législatives qui autorisent les agents des services de renseignement à accomplir des actes normalement interdits par les

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 n° 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 internationale de droit penal* 78, n° 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); Intiaz 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.

lois nationales ne sauraient autoriser des actes contraires à la constitution ou à des normes impératives du droit international⁷².

Pratique n° 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.

23. 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 pénale⁷⁴. 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 concernés⁷⁵. 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 complices⁷⁶.

Pratique n° 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.

24. 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 pratique⁷⁷. 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 renseignement⁷⁸. 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

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).

d'actes constituant des violations graves du droit international humanitaire⁷⁹. 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 illégaux⁸⁰. 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 ci-dessous pratique n° 18).

Pratique n° 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.

25. 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 abus⁸¹. 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 sujet⁸² ou des institutions externes remplissant les mêmes fonctions, et prévoir la communication des informations à ces institutions directement par les agents des services de renseignement⁸³. 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

⁷⁹ Rome Statute, art. 33; Geneva Conventions I–IV; Commission on Human Rights (footnote 65), principe 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.

leur préoccupation⁸⁴. 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 jeu⁸⁵. 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 pratique⁸⁶.

G. Professionnalisme

Pratique n° 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.

26. 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'homme⁸⁷. 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 légalité⁸⁸. 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 renseignement⁸⁹. 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 contenu⁹⁰. Que les codes de conduite (et les documents assimilés) soient soumis à la surveillance d'institutions internes

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 Affairs 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 9/11 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).

et externes de contrôle constitue une bonne pratique⁹¹. 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 pertinentes⁹². 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 renseignement⁹³. Enfin, la culture du professionnalisme peut être renforcée par des mesures internes de gestion du personnel qui récompensent les conduites éthiques et professionnelles.

H. Protection des droits de l'homme

Pratique n° 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.

27. 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

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).

international humanitaire, et pour prévenir le recours arbitraire ou discrétionnaire à ce type de mesures⁹⁴.

28. 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 adoptée⁹⁵. 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 renseignement⁹⁶.

29. 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 démocratique⁹⁷. 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 nationale⁹⁸.

30. 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) visées⁹⁹. 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 ciblé¹⁰⁰.

31. 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 humanitaire¹⁰¹. 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.

32. 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).

33. 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 grief¹⁰² (voir pratiques n^{os} 9 et 10 ci-dessus).

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 and 10.

I. Recherche du renseignement

Pratique n° 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.

34. 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 emploi¹⁰³. La législation nationale indique les catégories de personnes et d'activités susceptibles d'être soumises à des mesures de recherche du renseignement¹⁰⁴, et le niveau de suspicion requis pour déclencher le recours à une mesure particulière¹⁰⁵. 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 avocats¹⁰⁶. 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 proroger¹⁰⁷. 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 atteint¹⁰⁸. Ces dispositions servent à minimiser les ingérences dans les

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.

droits des personnes ciblées et contribuent à garantir que les mesures de recherche du renseignement sont conformes au principe de proportionnalité.

Pratique n° 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.

35. 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'homme¹⁰⁹. 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°s 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'exécutif¹¹⁰ ou par une instance quasi-judiciaire constitue une bonne pratique¹¹¹. 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 intrusives¹¹². 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 pratique¹¹³.

36. 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 mesures¹¹⁴. Dans de nombreux États, les organes de contrôle externe conduisent aussi le contrôle externe des mesures de recherche du renseignement

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.

pour s'assurer qu'elles sont autorisées et que leur emploi est conforme à la loi¹¹⁵. 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.

J. Gestion et utilisation des données personnelles

Pratique n° 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.

37. Un certain nombre de principes généraux concernant la protection des données personnelles est communément intégré aux lois nationales¹¹⁶ et aux instruments internationaux¹¹⁷. 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 corriger¹¹⁸. 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 domaine¹¹⁹. 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 renseignement¹²⁰. 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

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.

légalement que de telles données soient conservées par les services de renseignement¹²¹. 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 loi¹²². 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 discriminatoires¹²³.

Pratique n° 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.

38. 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 mandat¹²⁴. 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 pertinents¹²⁵, mais également ceux qui sont inexacts ou dont le traitement est inadéquat¹²⁶. 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 n° 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.

39. Dans de nombreux États, la gestion des fichiers personnels est soumise à la supervision régulière et continue d'institutions indépendantes¹²⁸. Ces institutions sont mandatées pour conduire des visites d'inspection régulières et des contrôles aléatoires des

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.

fichiers personnels concernant les opérations en cours et passées¹²⁹. Les États ont en outre mandaté des institutions de contrôle indépendantes pour vérifier si les directives internes concernant la gestion des fichiers sont conformes à la loi¹³⁰. 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 renseignement¹³¹. 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 personnelles¹³².

Pratique n° 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.

40. 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 renseignement¹³³, au ministre compétent¹³⁴ ou à une institution de contrôle indépendante¹³⁵. 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 gouvernement¹³⁶. 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

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.

loi et à s'assurer qu'elles sont conformes aux principes de proportionnalité et de nécessité¹³⁷.

K. Recours au pouvoir d'arrestation et de détention

Pratique n° 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.

41. 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 terrorisme¹³⁸. Des arguments convaincants ont été avancés contre l'association des fonctions de renseignement et de répression¹³⁹. 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 terrorisme¹⁴⁰. 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'ordre¹⁴¹.

Pratique n° 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.

42. 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

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.

pouvoirs peuvent être utilisés¹⁴². 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 renseignements¹⁴³. 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 humanitaire¹⁴⁴. 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'ordre¹⁴⁵. 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 justice¹⁴⁶.

Pratique n° 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.

43. 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 détention¹⁴⁸. 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 dégradants¹⁴⁹. Deuxièmement, le recours

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

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 signalé¹⁵⁰. 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'arrestation¹⁵¹; 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/détention¹⁵²; les personnes détenues par les services de renseignement ont accès à un conseiller juridique¹⁵³.

Pratique n° 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.

44. Le fait que la législation nationale interdise explicitement que les services de renseignement administrent leurs propres centres de détention constitue une bonne pratique¹⁵⁴. 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 répressifs¹⁵⁵. 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.

L. Partage de renseignements et coopération

Pratique n° 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.

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.

45. 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 renseignements¹⁵⁶. 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 enfonce 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 nationales¹⁵⁷. 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 renseignements¹⁵⁸. 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 n° 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.

46. 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 pratique¹⁵⁹. 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-mêmes¹⁶⁰. De surcroît, de nombreuses législations nationales imposent que le partage

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).

de renseignements et l'établissement d'accords de partage de renseignements avec des entités étrangères soient soumis à l'approbation de l'exécutif¹⁶¹.

Pratique n° 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.

47. 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 services¹⁶². 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 concernées¹⁶³. 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 homologues¹⁶⁵. 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 transférées¹⁶⁶. Cette garantie contribue à prévenir les partages de renseignement abusifs ou arbitraires.

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.

48. 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 étrangères¹⁶⁷. 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'erreur¹⁶⁸. 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 contrôle¹⁶⁹.

Pratique n° 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.

49. 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 accords¹⁷⁰. 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 pratique¹⁷¹. 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 n° 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.

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.

50. 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 activités¹⁷². 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 activité¹⁷³. 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 soit¹⁷⁴.

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.

Annexe

Good practices on legal and institutional frameworks for intelligence services and their oversight

Practice 1. Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.

Practice 5. Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

Practice 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.

Practice 9. Any individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as

an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are independent of the intelligence services and the political executive. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

Practice 11. Intelligence services carry out their work in a manner that contributes to the promotion and protection of the human rights and fundamental freedoms of all individuals under the jurisdiction of the State. Intelligence services do not discriminate against individuals or groups on the grounds of their sex, race, colour, language, religion, political or other opinion, national or social origin, or other status.

Practice 12. National law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.

Practice 13. Intelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression.

Practice 14. States are internationally responsible for the activities of their intelligence services and their agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services.

Practice 15. Constitutional, statutory and international criminal law applies to members of intelligence services as much as it does to any other public official. Any exceptions allowing intelligence officials to take actions that would normally violate national law are strictly limited and clearly prescribed by law. These exceptions never allow the violation of peremptory norms of international law or of the human rights obligations of the State.

Practice 16. National laws provide for criminal, civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations.

Practice 17. Members of intelligence services are legally obliged to refuse superior orders that would violate national law or international human rights law. Appropriate protection is provided to members of intelligence services who refuse orders in such situations.

Practice 18. There are internal procedures in place for members of intelligence services to report wrongdoing. These are complemented by an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate. Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern.

Practice 19. Intelligence services and their oversight institutions take steps to foster an institutional culture of professionalism based on respect for the rule of law and human rights. In particular, intelligence services are responsible for training their members on relevant provisions of national and international law, including international human rights law.

Practice 20: Any measures by intelligence services that restrict human rights and fundamental freedoms comply with the following criteria:

- (a) They are prescribed by publicly available law that complies with international human rights standards;
- (b) All such measures must be strictly necessary for an intelligence service to fulfil its legally prescribed mandate;
- (c) Measures taken must be proportionate to the objective. This requires that intelligence services select the measure that least restricts human rights, and take special care to minimize the adverse impact of any measures on the rights of individuals, including, in particular, persons who are not suspected of any wrongdoing;
- (d) No measure taken by intelligence services may violate peremptory norms of international law or the essence of any human right;
- (e) There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights;
- (f) Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy.

Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorizing, overseeing and reviewing the use of intelligence-collection measures.

Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

Practice 25. An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

Practice 26. Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service. It is incumbent upon the

intelligence service to justify, to an independent oversight institution, any decision not to release personal information.

Practice 27. Intelligence services are not permitted to use powers of arrest and detention if they do not have a mandate to perform law enforcement functions. They are not given powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities.

Practice 28. If intelligence services have powers of arrest and detention, they are based on publicly available law. The exercise of these powers is restricted to cases in which there is reasonable suspicion that an individual has committed or is about to commit a specific criminal offence. Intelligence services are not permitted to deprive persons of their liberty simply for the purpose of intelligence collection. The use of any powers and arrest and detention by intelligence services is subject to the same degree of oversight as applies to their use by law enforcement authorities, including judicial review of the lawfulness of any deprivation of liberty.

Practice 29. If intelligence services possess powers of arrest and detention they comply with international human rights standards on the rights to liberty and fair trial, as well as the prohibition of torture and inhuman and degrading treatment. When exercising these powers, intelligence services comply with international standards set out in, inter alia, the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, the Code of Conduct for Law Enforcement Officials and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

Practice 30. Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

Practice 33. Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

Practice 35. Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.