

Distr.: General  
17 May 2010  
Arabic  
Original: English



## مجلس حقوق الإنسان

الدورة الرابعة عشرة

البند ٣ من جدول الأعمال

تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية

تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، مارتين شاينين\*

تجميع الممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية التي تضمن احترام حقوق الإنسان من جانب وكالات الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك ما يتعلق بالرقابة على هذه الوكالات\*\*

موجز

هذا التقرير تجميع للممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية التي تضمن احترام حقوق الإنسان من جانب وكالات الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك ما يتعلق بالرقابة على هذه الوكالات، وقد طلبه مجلس حقوق الإنسان وأعدده المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب. والتجميع حصيلة عملية تشاور قدمت فيها الحكومات إسهاماتها، كما قدم فيها الخبراء والممارسون إسهاماتهم، بطرق مختلفة. ويذكر على وجه الخصوص أن الإفادات الكتابية، التي تم تلقيها من الحكومات بحلول الموعد النهائي وهو

\* تأخر تقديم هذا التقرير.

\*\* نظراً لتجاوز هذا التقرير كثيراً الحد المفروض حالياً لعدد الصفحات بموجب قرارات الجمعية العامة الصادرة بهذا الشأن، يُستنسخ مرفق التقرير والحواشي كما وردا، باللغة التي قدما بها فقط.

١ أيار/مايو ٢٠١٠، وضعت في الاعتبار. وسيجري استنساخ الإفادات في شكل إضافة (A/HRC/14/46/Add.1).

وحصيلة العملية هي تحديد ٣٥ عنصر ممارسة جيدة. وقد استخلصت عناصر الممارسة الجيدة من الممارسات القائمة والمستجدة في مجموعة كبيرة من الدول في جميع أرجاء العالم. ويستند التجميع أيضاً إلى المعاهدات الدولية وقرارات المنظمات الدولية والاجتهاد القضائي للمحاكم الإقليمية.

ويوضح جوهر عناصر الممارسة الجيدة في التعليق، ويعرض عادة على نحو منفصل فيما يتعلق بكل عنصر من العناصر الخمسة والثلاثين. ومصادر الممارسة الجيدة محددة في حواشي التعليق، التي تتضمن إشارات إلى آحاد الدول.

ويشير مفهوم "الممارسة الجيدة" إلى الأطر القانونية والمؤسسية التي تكفل تعزيز حقوق الإنسان واحترام سيادة القانون في عمل أجهزة الاستخبارات. ولا تشير الممارسة الجيدة إلى ما يقتضيه القانون الدولي، بما في ذلك قانون حقوق الإنسان، فحسب، ولكنها تتجاوز نطاق هذه الالتزامات الملزمة قانوناً.

ومجالات الممارسة الجيدة الخمسة والثلاثون المدرجة في التجميع مصنفة في أربع "مجموعات"، هي الأساس القانوني (الممارسات ١-٥)، والرقابة والمساءلة (الممارسات ٦-١٠ و ١٤-١٨)، والامتثال لحقوق الإنسان الجوهرية (الممارسات ١١-١٣ و ١٩-٢٠)، والمسائل المتعلقة بالوظائف المحددة لوكالات الاستخبارات (الممارسات ٢١-٣٥).

## المحتويات

الصفحة	الفقرات		
٤	٨-١	.....	مقدمة - أولاً -
		.....	تجميع الممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية لأجهزة الاستخبارات والرقابة عليها - ثانياً -
٥	٥٠-٩	.....	الاستخبارات والرقابة عليها
٥	١٢-٩	.....	ألف - الولاية والأساس القانوني
٩	١٥-١٣	.....	باء - مؤسسات الرقابة
١٢	١٧-١٦	.....	جيم - الشكاوى وسبيل الانتصاف الفعال
١٤	٢٠-١٨	.....	دال - النزاهة وعدم التمييز
١٦	٢١	.....	هاء - مسؤولية الدول عن أجهزة الاستخبارات
١٧	٢٥-٢٢	.....	واو - مسؤولية الأفراد ومساءلتهم
٢٠	٢٦	.....	زاي - الحس المهني
٢١	٣٣-٢٧	.....	حاء - ضمانات حقوق الإنسان
٢٣	٣٦-٣٤	.....	طاء - جمع المعلومات الاستخباراتية
٢٦	٤٠-٣٧	.....	ياء - إدارة البيانات الشخصية واستخدامها
٣٠	٤٤-٤١	.....	كاف - استخدام سلطات التوقيف والاحتجاز
٣٣	٥٠-٤٥	.....	لام - تبادل المعلومات الاستخباراتية والتعاون في مجال الاستخبارات

Page

Annex

Good practices on legal and institutional frameworks for intelligence services and their oversight 38

## أولاً - مقدمة\*

- ١- هذا التجميع للممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية التي تضمن احترام حقوق الإنسان من جانب وكالات الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك ما يتعلق بالرقابة على هذه الوكالات، هو حصيلة عملية تشاور أجريت بتكليف من مجلس حقوق الإنسان الذي دعا، في قراره ١٥/١٠، المقرر الخاص إلى أن يعيد، بالتشاور مع الدول وأصحاب المصلحة ذوي الصلة الآخرين، تجميعاً للممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية التي تضمن احترام حقوق الإنسان من جانب وكالات الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك ما يتعلق بالرقابة على هذه الوكالات.
- ٢- وتضطلع أجهزة الاستخبارات<sup>(١)</sup> بدور حاسم في حماية الدولة وسكانها من المخاطر التي تهدد الأمن الوطني، بما في ذلك الإرهاب. وهي تساعد الدول على الوفاء بالتزامها الإيجابي بصون حقوق الإنسان لجميع الأفراد الخاضعين لولايتها. ومن ثم، فمن الممكن أن يكون الأداء الفعال وحماية حقوق الإنسان هدفين لأجهزة الاستخبارات يكمل كل منهما الآخر.
- ٣- والتجميع مستخلص من الممارسات القائمة والمستجدة في مجموعة كبيرة من الدول في جميع أرجاء العالم. وهذه الممارسات مستمدة في المقام الأول من القوانين الوطنية والنماذج المؤسسية، وكذلك من اجتهاد وتوصيات المؤسسات الوطنية للرقابة وعدد من منظمات المجتمع المدني. ويستند التجميع أيضاً إلى المعاهدات الدولية وقرارات المنظمات الدولية والاجتهاد القضائي للمحاكم الإقليمية. وفي هذا السياق، يشير مفهوم "الممارسة الجيدة" إلى الأطر القانونية والمؤسسية التي تكفل تعزيز حقوق الإنسان واحترام سيادة القانون في عمل أجهزة الاستخبارات. ولا تشير "الممارسة الجيدة" إلى ما يقتضيه القانون الدولي، بما في ذلك قانون حقوق الإنسان، فحسب، ولكنها تتجاوز نطاق هذه الالتزامات الملزمة قانوناً.
- ٤- وقد أدرجت بلدان قليلة جداً جميع الممارسات المبينة أدناه في أطرها القانونية والمؤسسية لأجهزة الاستخبارات والرقابة عليها. وستكون بعض البلدان قادرة على تبيان أنفسها على أنها تتبع أغلب عناصر الممارسة الجيدة الخمسة والثلاثين. وقد تبدأ بلدان أخرى

\* 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.

<sup>1</sup> 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.

بإلزام أنفسها بعدد صغير من هذه العناصر ترى أنه ضروري لتعزيز الامتثال لحقوق الإنسان من جانب أجهزة الاستخبارات وهيئاتها الرقابية.

٥- وليس الغرض من هذا التجميع تعميم مجموعة معايير قياسية ينبغي أن تطبق في جميع الأوقات وفي جميع أرجاء العالم. ومن ثم، فإن العناصر المعروضة في هذا التقرير مصاغة بلغة وصفية لا بلغة معيارية. ومع ذلك، فإن من الممكن تحديد ممارسات شائعة تسهم في احترام سيادة القانون وحقوق الإنسان من جانب أجهزة الاستخبارات.

٦- وقد أصدر مجلس حقوق الإنسان تكليفاً بإعداد هذا التجميع للممارسات الجيدة في سياق دور أجهزة الاستخبارات في مكافحة الإرهاب. بيد أنه ينبغي ملاحظة أن الأطر القانونية والمؤسسية التي تنطبق على أنشطة أجهزة الاستخبارات في مجال مكافحة الإرهاب لا يمكن فصلها عن الأطر السياسية والقانونية التي تنطبق على أنشطتها بوجه أعم. ولئن كان الإرهاب الدولي قد غير، منذ عام ٢٠٠١، مشهد عمليات وكالات الاستخبارات، فإن آثار هذا التغيير تتجاوز مجال مكافحة الإرهاب.

٧- ويسلط التجميع الضوء على أمثلة للممارسات الجيدة من قوانين وطنية ونماذج مؤسسية عديدة. بيد أن من المهم ملاحظة أن الاستشهاد بأحكام محددة من القوانين الوطنية أو النماذج المؤسسية لا يعني ضمناً إقراراً عاماً بأن هذه القوانين والمؤسسات تشكل ممارسة جيدة في حماية حقوق الإنسان في سياق مكافحة الإرهاب. وبالإضافة إلى ذلك، يود المقرر الخاص أن يشدد على أن وجود الأطر القانونية والمؤسسية التي تمثل الممارسة الجيدة ضروري، ولكنه غير كاف لضمان احترام أجهزة الاستخبارات لحقوق الإنسان في أنشطتها المتعلقة بمكافحة الإرهاب.

٨- ومجالات الممارسة الجيدة الخمسة والثلاثون المعروضة أدناه مصنفة في أربع "مجموعات"، هي الأساس القانوني (١-٥)، والرقابة والمساءلة (٦-١٠ و ١٤-١٨)، والامتثال لحقوق الإنسان الجوهرية (١١-١٣ و ١٩-٢٠)، والمسائل المتعلقة بالوظائف المحددة لوكالات الاستخبارات (٢١-٣٥). ولأسباب تتعلق بالعرض، جرى تصنيف العناصر تحت عناوين فرعية أكبر عدداً إلى حد ما.

## ثانياً - تجميع الممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية لأجهزة الاستخبارات والرقابة عليها

### ألف - الولاية والأساس القانوني

الممارسة ١- تضطلع أجهزة الاستخبارات بدور حاسم في حماية الأمن الوطني ودعم سيادة القانون. والغرض الرئيسي هو جمع وتحليل ونشر المعلومات التي تساعد

راسمي السياسات والكيانات الأخرى في اتخاذ التدابير اللازمة لحماية الأمن الوطني. ويتضمن هذا حماية السكان وحقوق الإنسان الخاصة بهم.

٩- تختلف وظائف أجهزة الاستخبارات من بلد إلى آخر؛ بيد أن جمع وتحليل ونشر المعلومات ذات الصلة بحماية الأمن الوطني تشكل المهمة الأساسية التي تؤديها معظم أجهزة الاستخبارات: (٢) تقصر دول كثيرة، في الواقع، دور أجهزة الاستخبارات التابعة لها على هذه المهمة. ويشكل هذا ممارسة جيدة لأنه يمنع أجهزة الاستخبارات من الاضطلاع بأنشطة إضافية متعلقة بالأمن تؤديها فعلاً هيئات عامة أخرى وقد تشكل مخاطر خاصة تهدد حقوق الإنسان إذا اضطلعت بها أجهزة الاستخبارات. وتقوم أيضاً دول كثيرة، بالإضافة إلى تحديد أنواع الأنشطة التي يمكن أن تؤديها أجهزة الاستخبارات التابعة لها، بقصر الأساس المنطقي للاضطلاع بهذه الأنشطة على حماية الأمن الوطني. ولئن كان فهم الأمن الوطني يتفاوت بين البلدان، فإن التعريف الواضح للأمن الوطني والقيم المكونة له في تشريع يعتمد على البرلمان يشكل ممارسة جيدة (٣). وهذا مهم لضمان أن تقصر أجهزة الاستخبارات أنشطتها على المساعدة في صون القيم المكرسة في تعريف عام للأمن الوطني. وفي مناطق كثيرة يتضمن صون الأمن الوطني بالضرورة حماية السكان وحقوق الإنسان الخاصة بهم (٤)؛ والواقع أن بعض الدول تدرج صراحة حماية حقوق الإنسان باعتبارها إحدى الوظائف الأساسية لأجهزة الاستخبارات التابعة لها (٥).

الممارسة ٢- تحدد ولايات أجهزة الاستخبارات تحديداً ضيقاً ودقيقاً في قانون يتوافر على نطاق عام. والولايات تقصر بشكل دقيق على مصالح الأمن الوطني المشروعة كما هي محددة في التشريعات المتوافرة على نطاق عام أو سياسات الأمن الوطني، وتحدد الأخطار التي تهدد الأمن الوطني والتي تكلف أجهزة الاستخبارات بالتصدي لها. وإذا أدرج الإرهاب ضمن هذه الأخطار، فإنه يجري تعريفه بعبارات ضيقة ودقيقة.

١٠- ولايات أجهزة الاستخبارات إحدى الوسائل الأساسية لضمان أن أنشطتها (بما في ذلك أنشطتها في سياق مكافحة الإرهاب) تحقق مصالح البلد وسكانه، ولا تشكل تهديداً للنظام الدستوري و/أو حقوق الإنسان. وفي غالبية الدول، تحدد ولايات أجهزة

<sup>2</sup> 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).

<sup>3</sup> Australia, Security Intelligence Organisation Act, sect. 4.

<sup>4</sup> 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.

<sup>5</sup> Croatia (footnote 2), art. 1.1; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, art. 1; Brazil (footnote 2), art. 1(1).

الاستخبارات تحديداً واضحاً في قانون يصدره البرلمان ويتاح على نطاق عام<sup>(٦)</sup>. وتتمثل ممارسة جيدة في أن تصاغ الولايات صياغة ضيقة ودقيقة وأن تبين كل المخاطر التي تهدد الأمن الوطني والتي تتولى أجهزة الاستخبارات المسؤولية عن التصدي لها<sup>(٧)</sup>. وتيسر الولايات الواضحة والدقيقة التحديد عمليات المساءلة، وتمكن هيئات الرقابة والمراجعة من مساءلة أجهزة الاستخبارات عن أدائها لوظائف محددة. وأخيراً، فإن التحديد الدقيق للأخطار المهددة مهم بشكل خاص في سياق مكافحة الإرهاب؛ وقد اعتمدت دول كثيرة تشريعات تنص على تعريف دقيقة للإرهاب، وكذلك للجماعات والأنشطة الإرهابية<sup>(٨)</sup>.

**الممارسة ٣-** تحدد سلطات واختصاصات أجهزة الاستخبارات تحديداً واضحاً وشاملاً في القانون الوطني. ويقتضى منها أن تستخدم هذه السلطات على نحو حصري للأغراض التي عهد بها إليها. وعلى وجه الخصوص، فإن أية سلطات ممنوحة لأجهزة الاستخبارات لأغراض مكافحة الإرهاب يجب أن تستخدم على وجه الحصر لهذه الأغراض.

١١- تحديد جميع سلطات واختصاصات أجهزة الاستخبارات في القانون مبدأً أساسياً من مبادئ سيادة القانون<sup>(٩)</sup>. والتبيان الشامل لسلطات واختصاصات أجهزة الاستخبارات يعزز الشفافية ويمكن الناس من توقع السلطات التي قد تستخدم ضدهم. وهذا مهم بشكل خاص بالنظر إلى أن الكثير من السلطات المخولة لأجهزة الاستخبارات ينطوي على احتمال انتهاك حقوق الإنسان والحريات الأساسية<sup>(١٠)</sup>. وهذه الممارسة وثيقة الصلة بالممارسة ٢ لأن ولايات أجهزة الاستخبارات تحدد الإطار الذي يمكنها أن تستخدم فيه السلطات الممنوحة من الهيئة التشريعية<sup>(١١)</sup>. وحظر تجاوز السلطة يرد ضمناً في تشريعات دول كثيرة حيث إن

<sup>6</sup> 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)).

<sup>7</sup> 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).

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

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

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

<sup>11</sup> Canada, MacDonald Commission, pp. 432, 1067.

أجهزة الاستخبارات لا يسمح لها باستخدام سلطاتها إلا لأغراض محددة جداً. ويكون هذا بشكل خاص في سياق مكافحة الإرهاب لأنه جرى منح أجهزة استخبارات كثيرة سلطات أوسع نطاقاً لهذه الأغراض.

**الممارسة ٤-** تشكل جميع أجهزة الاستخبارات من خلال، وتعمل بموجب، قوانين متوافرة على نطاق عام تمثل للدستور والقانون الدولي لحقوق الإنسان. ولا يمكن أن تضطلع أجهزة الاستخبارات، أو أن يجري تكليفها بالاضطلاع، إلا بأنشطة منصوص عليها في القانون الوطني ووفقاً لهذا القانون. واستخدام اللوائح الفرعية غير المتوافرة على نطاق عام مقيد تماماً، وهذه اللوائح ترخص بها معايير القوانين المتوافرة على نطاق عام وتبقى في نطاق هذه المعايير. ولا تصلح اللوائح غير المعلنة على نطاق عام لأن تكون أساس أية أنشطة تقيد حقوق الإنسان.

**الممارسة ٥-** يحظر صراحة على أجهزة الاستخبارات أن تضطلع بأي عمل يخالف الدستور أو القانون الدولي لحقوق الإنسان. ولا يمتد هذا الحظر إلى تصرفات أجهزة الاستخبارات على أراضيها الوطنية فحسب وإنما يمتد أيضاً إلى أنشطتها في الخارج.

١٢- أجهزة الاستخبارات هيئات تابعة للدولة ومن ثم، فإنها ملتزمة، مثل الهيئات التنفيذية الأخرى، بالأحكام ذات الصلة المنصوص عليها في القوانين الوطنية والدولية، وبصفة خاصة قوانين حقوق الإنسان<sup>(١٢)</sup>. ويعني هذا ضمناً أنها تركز على القوانين المتوافرة على نطاق عام - التي تمثل لدستور الدولة وكذلك، ضمن أمور أخرى، للالتزامات الدولية المتعلقة بحقوق الإنسان الدولية - وتعمل وفقاً لها. ولا يمكن للدولة أن تعتمد على القانون الداخلي لتبرير انتهاكات القانون الدولي لحقوق الإنسان أو، في الواقع، أي التزامات قانونية دولية أخرى<sup>(١٣)</sup>. وتقتضي سيادة القانون أن تمثل أنشطة أجهزة الاستخبارات وأي تعليمات تصدرها إليها السلطة السياسية التنفيذية لمجموعات القوانين هذه في جميع أعمالها<sup>(١٤)</sup>. وبناء على ذلك، يحظر أن تقوم أجهزة الاستخبارات، أو أن يطلب منها أن تقوم، بأي عمل ينتهك القانون التشريعي الوطني أو الدستور أو التزامات الدولة المتعلقة بحقوق الإنسان. وهذه المقتضيات ضمنية في دول كثيرة؛ بيد أن الممارسة الجيدة بشكل خاص هي أن تشير

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

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

<sup>14</sup> 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.

التشريعات الوطنية صراحة إلى هذه الالتزامات القانونية الأوسع نطاقاً، وبصفة خاصة إلى الالتزام باحترام حقوق الإنسان<sup>(١٥)</sup>. وأحياناً ما تحجب اللوائح الفرعية المتعلقة بعمليات أجهزة الاستخبارات وأنشطتها الداخلية عن الجمهور من أجل حماية أساليب عملها. وهذه الأنواع من اللوائح لا تصلح لأن تكون أساس الأنشطة التي تنتهك حقوق الإنسان. والممارسة الجيدة هي أن تركز أية لائحة فرعية على التشريعات العامة الواجبة التطبيق وتمثل لها<sup>(١٦)</sup>.

## باء - مؤسسات الرقابة

**الممارسة ٦ -** تتولى الرقابة على أجهزة الاستخبارات مجموعة من المؤسسات الرقابية الداخلية والتنفيذية والبرلمانية والقضائية والمتخصصة تستند ولاياتها وسلطاتها إلى القانون المتوافق على نطاق عام. ويتضمن نظام فعال للرقابة على الاستخبارات ما لا يقل عن مؤسسة مدنية مستقلة عن كل من أجهزة الاستخبارات والسلطة التنفيذية. وتغطي المهمة المشتركة لمؤسسات الرقابة جميع جوانب عمل أجهزة الاستخبارات، بما في ذلك امتثالها للقانون؛ وفعالية أنشطتها وكفاءتها، ومواردها المالية؛ وممارساتها الإدارية.

**١٣ -** تركز المؤسسات التي ترافق أنشطة أجهزة الاستخبارات، شأنها في ذلك شأن هذه الأجهزة، على القانون، وترتكز، في بعض الحالات، على الدستور<sup>(١٧)</sup>. ولا يوجد نموذج وحيد للرقابة على أجهزة الاستخبارات؛ بيد أن من الشائع إدراج المكونات التالية في النظم الرقابية الشاملة<sup>(١٨)</sup>: آليات الإدارة الداخلية والتحكم ضمن أجهزة الاستخبارات<sup>(١٩)</sup>؛ والرقابة من

<sup>15</sup> 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).

<sup>16</sup> 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.

<sup>17</sup> Germany, Basic Law for the Federal Republic of Germany, art. 45d; South Africa, Constitution, arts. 209-210.

<sup>18</sup> 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.

<sup>19</sup> 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).

جانب السلطة التنفيذية<sup>(٢٠)</sup>؛ والرقابة من جانب الهيئات البرلمانية<sup>(٢١)</sup>؛ وكذلك الرقابة من جانب الهيئات الرقابية المتخصصة و/أو القضائية<sup>(٢٢)</sup>. وثمة ممارسة جيدة هي أن يتضمن هذا النظام الرقابي المتعدد المستويات ما لا يقل عن مؤسسة واحدة مستقلة تماماً عن كل من أجهزة الاستخبارات والسلطة السياسية التنفيذية. ويضمن هذا النهج أن يكون هناك فصل بين السلطات في الرقابة على أجهزة الاستخبارات؛ وألا تكون المؤسسات التي تصدر التكاليف بهذه الأنشطة وتضطلع بها وتتلقى نتائجها المؤسسات الوحيدة التي تراقب هذه الأنشطة. وتخضع كل أبعاد عمل أجهزة الاستخبارات لرقابة مؤسسة خارجية أو مجموعة مؤسسات خارجية. وتمثل إحدى الوظائف الأساسية لنظام رقابي في التحقق من امتثال أجهزة الاستخبارات للقانون الواجب التطبيق، بما في ذلك حقوق الإنسان. وتكلف مؤسسات الرقابة بمساءلة أجهزة الاستخبارات وموظفيها عن أي انتهاكات للقانون<sup>(٢٣)</sup>. وبالإضافة إلى ذلك، تضطلع مؤسسات الرقابة بتقييم أداء أجهزة الاستخبارات<sup>(٢٤)</sup>. ويتضمن هذا بحث ما إذا كانت أجهزة الاستخبارات تستخدم بفعالية وكفاءة الأموال العامة المخصصة لها<sup>(٢٥)</sup>. ونظام الرقابة الفعال مهم بشكل خاص في مجال الاستخبارات لأن أجهزة الاستخبارات تضطلع بكثير من أعمالها في سرية، وبالتالي لا يمكن للجمهور أن يراقبها بسهولة. وتعزز مؤسسات الرقابة على الاستخبارات ثقة الجمهور في عمل أجهزة الاستخبارات واطمئنانه إليه وذلك بالعمل على ضمان أن تؤدي هذه الأجهزة وظائفها القانونية وفقاً لمقتضيات احترام سيادة القانون وحقوق الإنسان<sup>(٢٦)</sup>.

<sup>20</sup> 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.

<sup>21</sup> 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.

<sup>22</sup> 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.

<sup>23</sup> 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.

<sup>24</sup> 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.

<sup>25</sup> Romania (footnote 2), art. 42.

<sup>26</sup> 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.

الممارسة ٧- لدى مؤسسات الرقابة ما يلزم من سلطة وموارد وخبرات لاستهلال وإجراء تحقيقاتها وكذلك إمكانية الوصول على نحو تام وبلا عوائق إلى ما يلزم من معلومات وموظفين ومنشآت للاضطلاع بولايتها. وتحظى مؤسسات الرقابة بالتعاون التام من جانب أجهزة الاستخبارات وسلطات إنفاذ القوانين فيما يتعلق بالاستماع إلى الشهود والحصول على الوثائق وغيرها من الأدلة.

١٤- تتمتع مؤسسات الرقابة بسلطات محددة تمكنها من أداء وظائفها. وعلى وجه الخصوص، فإن لديها سلطة استهلال التحقيقات الخاصة بها في مجالات عمل أجهزة الاستخبارات التي تدرج في نطاق ولاياتها، وهي مخولة في الحصول على جميع المعلومات التي تلزمها للقيام بذلك. وتشمل هذه السلطات المتعلقة بالحصول على المعلومات السلطة القانونية للاطلاع على جميع الملفات والوثائق ذات الصلة<sup>(٢٧)</sup>، وتفتيش مباني أجهزة الاستخبارات<sup>(٢٨)</sup>، واستدعاء أي عضو من أعضاء أجهزة الاستخبارات لتقديم أدلة مشفوعة بيمين<sup>(٢٩)</sup>. وتساعد هذه السلطات على ضمان أن يتسنى للمراقبين فحص أنشطة الاستخبارات بفعالية والتحقيق بشكل كامل في المخالفات المحتملة للقانون. وقد اتخذ عدد من الدول خطوات لتعزيز صلاحيات مؤسسات الرقابة في مجال التحقيق وذلك بتجريم أي حالة عدم تعاون معها<sup>(٣٠)</sup>. ويعني هذا ضمناً أن مؤسسات الرقابة يمكنها اللجوء إلى سلطات إنفاذ القانون لتأمين تعاون جميع الأشخاص المعنيين<sup>(٣١)</sup>. ولئن كانت السلطات القانونية القوية ضرورية للرقابة الفعالة، فإن الممارسة الجيدة تقتضي أن تكون هذه السلطات مصحوبة بالموارد البشرية والمالية اللازمة لاستخدام هذه السلطات وبالتالي للاضطلاع بمؤسسات الرقابة بولاياتها. وبناء على ذلك، فإن لدى مؤسسات رقابية كثيرة ميزانيتها الخاصة بها والتي يوفرها لها البرلمان بشكل مباشر<sup>(٣٢)</sup>، والقدرة على تعيين موظفين متخصصين<sup>(٣٣)</sup>، والاستعانة بخبراء خارجيين<sup>(٣٤)</sup>.

الممارسة ٨- تتخذ مؤسسات الرقابة كل التدابير اللازمة لحماية المعلومات السرية والبيانات الشخصية التي يتسنى لها الوصول إليها أثناء عملها. وتفرض عقوبات فيما يتعلق بمخالفة هذه المتعضيات من جانب أعضاء مؤسسات الرقابة.

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

<sup>28</sup> 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.

<sup>29</sup> Croatia (footnote 2), art. 105; Lithuania (footnote 23), art. 23.

<sup>30</sup> South Africa (footnote 23), sect. 7a.

<sup>31</sup> Belgium (footnote 22), art. 48; The Netherlands (footnote 20), art. 74.6.

<sup>32</sup> Belgium (footnote 22), art. 66 bis.

<sup>33</sup> Canada (footnote 6), sect. 36.

<sup>34</sup> 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.

١٥ - يتسنى لمؤسسات الرقابة على الاستخبارات الوصول إلى المعلومات السرية والحساسة أثناء عملها. ولذلك توضع مجموعة متنوعة من الآليات لضمان عدم قيام مؤسسات الرقابة وأعضائها بالكشف عن هذه المعلومات سهواً أو عمداً. أولاً، يحظر على أعضاء وموظفي مؤسسات الرقابة، في حل الحالات، الكشف عن المعلومات دون تصريح؛ ويجازى عن عدم الامتثال لهذه المحظورات من خلال العقوبات المدنية و/أو الجنائية<sup>(٣٥)</sup>. ثانياً، تقوم أيضاً منظمات رقابية كثيرة بإخضاع الأعضاء والموظفين لإجراءات الحصول على الموافقة الأمنية قبل تمكينهم من الوصول إلى المعلومات السرية<sup>(٣٦)</sup>. وثمة بديل لهذا النهج، من الشائع إلى أبعد الحدود ملاحظته في مؤسسات الرقابة البرلمانية، هو اشتراط أن يوقع الأعضاء اتفاق عدم كشف<sup>(٣٧)</sup>. وأخيراً، فإن تناول الصحيح للمعلومات من جانب مؤسسات الرقابة يتوقف أيضاً على السلوك المهني لأعضاء مؤسسات الرقابة.

## جيم - الشكاوى وسبيل الانتصاف الفعال

٩ - الممارسة - يمكن لأي شخص يعتقد أن جهاز استخبارات انتهك حقوقه تقديم شكوى إلى محكمة أو مؤسسة رقابة، مثل أمين مظالم أو مفوض حقوق إنسان أو مؤسسة وطنية لحقوق الإنسان. ويلجأ الأشخاص المتضررون من الأعمال غير المشروعة التي يقوم بها جهاز استخبارات إلى مؤسسة يمكنها توفير سبيل انتصاف فعال، بما في ذلك الجبر الكامل للضرر المتكبد.

١٦ - من المسلم به على نطاق واسع أن أي تدبير مقيد لحقوق الإنسان يجب أن يكون مصحوباً بضوابط كافية، بما في ذلك وجود مؤسسات مستقلة يمكن من خلالها للأشخاص التماس الانتصاف في حالة انتهاك حقوقهم<sup>(٣٨)</sup>. ولدى أجهزة الاستخبارات طائفة من السلطات - بما في ذلك سلطات المراقبة والتوقيف والاحتجاز - التي قد تنتهك حقوق الإنسان إذا أسيء استخدامها. وبناء على ذلك، توجد مؤسسات لمعالجة الشكاوى التي يثيرها أشخاص يعتقدون أن أجهزة الاستخبارات انتهكت حقوقهم وكذلك، حسب

<sup>35</sup> 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.

<sup>36</sup> 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).

<sup>37</sup> 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).

<sup>38</sup> 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.

الاقتضاء، لتزويد ضحايا انتهاكات حقوق الإنسان بسبيل انتصاف فعال. ويمكن تمييز نهجين عريضين في هذا الصدد<sup>(٣٩)</sup>. أولاً، أنشأت الدول مجموعة متنوعة من المؤسسات غير القضائية لمعالجة الشكاوى المتعلقة بأجهزة الاستخبارات. وتتضمن هذه المؤسسات أمين المظالم<sup>(٤٠)</sup>، واللجنة الوطنية لحقوق الإنسان<sup>(٤١)</sup>، والمكتب الوطني لمراجعة الحسابات<sup>(٤٢)</sup>، وهيئة الرقابة البرلمانية<sup>(٤٣)</sup>، والمفتش العام<sup>(٤٤)</sup>، وهيئة المتخصصة للرقابة على الاستخبارات<sup>(٤٥)</sup>، واللجنة المعنية بالشكاوى المتعلقة بأجهزة الاستخبارات<sup>(٤٦)</sup>. وهذه المؤسسات مخولة سلطة تلقي الشكاوى والتحقيق فيها؛ ولكن، بالنظر إلى أنه لا يمكنها بوجه عام إصدار أوامر ملزمة أو توفير سبل الانتصاف، يتعين على ضحايا انتهاكات حقوق الإنسان التماس سبل الانتصاف عن طريق المحاكم. ثانياً، يمكن للمؤسسات القضائية تلقي الشكاوى المتعلقة بأجهزة الاستخبارات. وقد تكون هذه المؤسسات هيئات قضائية منشأة لهذا الغرض على وجه الحصر<sup>(٤٧)</sup>، أو جزءاً من النظام القضائي العام؛ وعادة ما يتم تحويلها سلطة الأمر باتخاذ إجراءات الانتصاف.

**الممارسة ١٠ - المؤسسات المسؤولة عن معالجة الشكاوى والمطالبات المتعلقة بالانتصاف الفعال، الناجمة عن أنشطة أجهزة الاستخبارات، مستقلة عن أجهزة الاستخبارات والسلطة السياسية التنفيذية.** ويتسنى لهذه المؤسسات الوصول على نحو تام وبلا عوائق إلى جميع المعلومات ذات الصلة، والموارد والخبرات الضرورية لإجراء التحقيقات، والقدرة اللازمة لإصدار الأوامر الملزمة.

١٧ - لكي توفر مؤسسة ما سبل الانتصاف الفعالة من انتهاكات حقوق الإنسان، يجب أن تكون مستقلة عن المؤسسات المنخرطة في الأنشطة المطعون فيها، وقادرة على ضمان النزاهة الإجرائية، ولديها ما يكفي من القدرات والخبرات التحقيقية، وذات قدرة على إصدار أوامر ملزمة<sup>(٤٨)</sup>. ولهذا السبب، منحت الدول هذه المؤسسات السلطات القانونية اللازمة للتحقيق

<sup>39</sup> 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.

<sup>40</sup> 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).

<sup>41</sup> Jordan, Law on the National Centre for Human Rights.

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

<sup>43</sup> Romania (footnote 15), art. 16.

<sup>44</sup> South Africa (footnote 23), sect. 7(7).

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

<sup>46</sup> Kenya (footnote 16), arts. 24-26.

<sup>47</sup> United Kingdom, Regulation of Investigatory Powers Act, arts. 65-70; Sierra Leone (footnote 14), arts. 24-25.

<sup>48</sup> 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.

في الشكاوى وتوفير سبل الانتصاف لضحايا انتهاكات حقوق الإنسان التي ترتكبها أجهزة الاستخبارات. وتتضمن هذه السلطات الوصول على نحو تام وبلا عوائق إلى جميع المعلومات ذات الصلة، والسلطات التحقيقية لاستدعاء الشهود والحصول على شهادة مشفوعة بيمين<sup>(٤٩)</sup>، وسلطة تحديد الإجراءات الخاصة بما يتعلق بأي دعاوى، والقدرة على إصدار الأوامر الملزمة<sup>(٥٠)</sup>.

## دال - التראה وعدم التمييز

الممارسة ١١ - تضطلع أجهزة الاستخبارات بعملها بطريقة تسهم في تعزيز وحماية حقوق الإنسان والحريات الأساسية لجميع الأفراد الخاضعين لولاية الدولة. ولا تميز أجهزة الاستخبارات ضد الأفراد أو الجماعات على أساس نوع الجنس أو العرق أو اللون أو اللغة أو الدين، أو الرأي السياسي أو أي رأي آخر، أو الأصل القومي أو الاجتماعي، أو أي وضع آخر.

١٨ - أجهزة الاستخبارات جزء لا يتجزأ من جهاز الدولة الذي يسهم في صون حقوق الإنسان لجميع الأفراد الخاضعين لولاية الدولة. وهي ملزمة بالمبدأ الراسخ تماماً المنصوص عليه في القانون الدولي لحقوق الإنسان وهو عدم التمييز. ويتقضي هذا المبدأ من الدول احترام حقوق الأفراد وحرّياتهم دون تمييز على أي أساس محظور<sup>(٥١)</sup>. وقد كرست دول كثيرة المبدأ في القانون الوطني، الذي يقتضي من أجهزة الاستخبارات التابعة لها أن تضطلع بولاياتها على نحو يحقق مصالح الدولة والمجتمع بأسره. ويحظر على أجهزة الاستخبارات صراحة أن تعمل أو أن يجري استخدامها لتعزيز مصالح أية جماعة عرقية أو دينية أو سياسية أو أية جماعة أخرى<sup>(٥٢)</sup>. وبالإضافة إلى ذلك، فإن الدول تضمن الاضطلاع بأنشطة أجهزة الاستخبارات التابعة لها (وبصفة خاصة في سياق مكافحة الإرهاب) على أساس سلوك الأفراد وليس على أساس أصلهم العرقي أو دينهم أو أي معايير أخرى من هذا القبيل<sup>(٥٣)</sup>. وقد حظرت بعض الدول أيضاً صراحة على أجهزة الاستخبارات التابعة لها إعداد ملفات بشأن الأفراد على هذا الأساس<sup>(٥٤)</sup>.

<sup>49</sup> Kenya (footnote 16), art. 26; Sierra Leone (footnote 14), art. 27.

<sup>50</sup> United Kingdom (footnote 47), art. 68.

<sup>51</sup> 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).

<sup>52</sup> Ottawa Principles on Anti-Terrorism and Human Rights, art. 1.1.3.

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

<sup>54</sup> Argentina (footnote 2), art. 4.

**الممارسة ١٢ -** يحظر القانون الوطني على أجهزة الاستخبارات الانخراط في أي أنشطة سياسية أو العمل على تعزيز أو حماية مصالح أية جماعة سياسية أو دينية أو لغوية أو عرقية أو اجتماعية أو اقتصادية بعينها.

١٩ - أجهزة الاستخبارات مخولة سلطات تنطوي على إمكانية تعزيز أو تفويض مصالح جماعات سياسية معينة. ولضمان أن تظل أجهزة الاستخبارات محايدة سياسياً، تحظر القوانين الوطنية على أجهزة الاستخبارات العمل لصالح أية جماعة سياسية<sup>(٥٥)</sup>. ولا يقع هذا الالتزام على أجهزة الاستخبارات فحسب ولكنه يقع أيضاً على المسؤولين التنفيذيين السياسيين الذين تخدمهم. وقد أقر عدد من الدول أيضاً تدابير لحظر أو تقييد انخراط أجهزة الاستخبارات في الأحزاب السياسية. وتتضمن أمثلة هذه التدابير الإجراءات التي تحظر على العاملين في أجهزة الاستخبارات أن يكونوا أعضاء في أحزاب سياسية، أو أن يتلقوا تعليمات أو أموالاً من حزب سياسي<sup>(٥٦)</sup>، أو أن يعملوا على تعزيز مصالح أي حزب سياسي<sup>(٥٧)</sup>. وبالإضافة إلى ذلك، اتخذت دول شتى تدابير لضمان حياد مديري أجهزة الاستخبارات. وعلى سبيل المثال، فإن تعيين مديري أجهزة الاستخبارات قابل للتدقيق من خارج السلطة التنفيذية<sup>(٥٨)</sup>؛ وتوجد أحكام قانونية بشأن مدة ولاية المديرين وتحديد أسس فصل المديرين وبشأن الضوابط ضد ممارسة ضغط غير مناسب على مديري أجهزة الاستخبارات<sup>(٥٩)</sup>.

**الممارسة ١٣ -** يحظر على أجهزة الاستخبارات استخدام سلطاتها لاستهداف نشاط سياسي مشروع أو مظاهر مشروعة أخرى للحقوق في حرية تكوين الجمعيات والتجمع السلمي والتعبير.

٢٠ - وتلجأ أجهزة الاستخبارات إلى تدابير لجمع المعلومات قد تنطوي على تدخل في الأنشطة السياسية المشروعة وغيرها من مظاهر حريات التعبير وتكوين الجمعيات والتجمع<sup>(٦٠)</sup>. وهذه الحقوق أساسية لأداء مجتمع حر، بما في ذلك الأحزاب السياسية ووسائل الإعلام والمجتمع المدني. ولذلك اتخذت الدول تدابير لتضييق نطاق استهداف أجهزة الاستخبارات التابعة لها (أو مطالبتها باستهداف) المتخربين في هذه الأنشطة من هؤلاء الأفراد وهذه الجماعات. وتتضمن هذه التدابير الحظر المطلق لاستهداف الأنشطة المشروعة،

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

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

<sup>57</sup> 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).

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

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

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

وفرض قيود صارمة على كل من استخدام تدابير جمع المعلومات الاستخباراتية (انظر الممارسة ٢١) والاحتفاظ بالبيانات الشخصية التي تجمعها أجهزة الاستخبارات واستخدامها (انظر الممارسة ٢٣)<sup>(٦١)</sup>. وبالنظر إلى حقيقة أن وسائل الإعلام تضطلع بدور حاسم في أي مجتمع، فقد وضعت بعض الدول تدابير محددة لحماية الصحفيين من استهدافهم من جانب أجهزة الاستخبارات<sup>(٦٢)</sup>.

## هاء - مسؤولية الدول عن أجهزة الاستخبارات

**الممارسة ١٤ -** الدول مسؤولة دولياً عن أنشطة أجهزة وعناصر الاستخبارات التابعة لها، وأنشطة أي مقاولين تستخدمهم من القطاع الخاص، بصرف النظر عن المكان الذي تنفذ فيه هذه الأنشطة وعن هوية ضحية التصرف الخاطيء دولياً. ولذلك تتخذ السلطة التنفيذية التدابير اللازمة لضمان ممارسة السيطرة الشاملة على أجهزة الاستخبارات التابعة لها وتحمل المسؤولية الكلية عن هذه الأجهزة.

**٢١ -** الدول مسؤولة بموجب القانون الدولي عن أنشطة أجهزة وعناصر الاستخبارات التابعة لها أينما تعمل في العالم. وتمتد هذه المسؤولية إلى أي مقاولين من القطاع الخاص تستخدمهم الدول لأداء مهام استخباراتية<sup>(٦٣)</sup>. وعلى الدول التزام قانوني بضمان عدم انتهاك أجهزة الاستخبارات التابعة لها لحقوق الإنسان وتوفير سبل الانتصاف للأفراد المعنيين إذا حدثت انتهاكات من هذا القبيل<sup>(٦٤)</sup>. وبناء على ذلك، تتخذ الدول الخطوات اللازمة لتنظيم وإدارة أجهزة الاستخبارات التابعة لها على نحو يعزز احترام سيادة القانون، وبصفة خاصة الامتثال للقانون الدولي لحقوق الإنسان<sup>(٦٥)</sup>. وسيطرة السلطة التنفيذية على أجهزة الاستخبارات ضرورية لهذه الأغراض وهي مكرسة بالتالي في كثير من القوانين الوطنية<sup>(٦٦)</sup>.

<sup>61</sup> 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.

<sup>62</sup> 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.

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

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

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

<sup>66</sup> See also practice 6.

## واو - مسؤولية الأفراد ومساءلتهم

**الممارسة ١٥-** تسري القوانين الدستورية والتشريعية والقانون الجنائي الدولي على أعضاء أجهزة الاستخبارات بقدر ما تسري على أي مسؤول عام آخر. ويقيد القانون على نحو صارم، وينص بوضوح على حظر، أي استثناءات تسمح لمسؤولي الاستخبارات باتخاذ إجراءات تنطوي عادة على انتهاك القانون الوطني. ولا تجيز هذه الاستثناءات على الإطلاق انتهاك القواعد القطعية للقانون الدولي أو التزامات الدولة المتعلقة بحقوق الإنسان.

٢٢- لئن كان التشديد ينصب على المسؤوليات المؤسسية لأجهزة الاستخبارات، فإن آحاد أعضاء أجهزة الاستخبارات أيضاً مسؤولون عن أفعالهم ويخضعون للمساءلة عنها<sup>(٦٧)</sup>. وكقاعدة عامة، تسري القوانين الدستورية والتشريعية والقانون الجنائي الدولي على مسؤولي الاستخبارات بقدر ما تسري على أي فرد آخر<sup>(٦٨)</sup>. وقد حددت دول كثيرة أن يكون قيام أي عضو في جهاز استخبارات، عن علم، بانتهاك قانون دستوري أو تشريعي، و/أو بالأمر باتخاذ إجراء أو طلب اتخاذ إجراء ينتهك هذا القانون، سبباً يتم تحميله المسؤولية المدنية عنه أو فعلاً إجرامياً يحاسب عليه<sup>(٦٩)</sup>. وتعزز هذه الممارسة احترام سيادة القانون داخل أجهزة الاستخبارات، وتساعد على منع الإفلات من العقاب. وتفوض دول كثيرة أعضاء أجهزة الاستخبارات التابعة لها سلطة القيام بأنشطة تشكل، إذا اضطلع بها مواطنون عاديون، أفعالاً إجرامية<sup>(٧٠)</sup>. وتقتضي الممارسة الجيدة أن تكون أي تفويضات من هذا القبيل مقيدة على نحو صارم ومنصوصاً عليها بموجب القانون وخاضعة لضوابط ملائمة<sup>(٧١)</sup>. ولا تمتد الأحكام التشريعية، التي ترخص لمسؤولي الاستخبارات بالاضطلاع بأي أعمال يعتبرها القانون الوطني عادة غير مشروعة، إلى أي إجراءات تنطوي على انتهاك الدستور أو المعايير الدولية لحقوق الإنسان، التي لا يجوز الحيد عنها<sup>(٧٢)</sup>.

**الممارسة ١٦-** تنص القوانين الوطنية على جزاءات جنائية أو مدنية أو جزاءات أخرى ضد أي عضو في جهاز استخبارات، أو أي فرد يعمل نيابة عن جهاز

<sup>67</sup> ECOWAS Code of Conduct, arts. 4 and 6.

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

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

<sup>70</sup> 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.

<sup>71</sup> South African Ministerial Review Commission, pp. 157-158.

<sup>72</sup> Netherlands (footnote 20), annex.

استخبارات، ينتهك، أو يأمر بإجراء ينتهك، القانون الوطني أو القانون الدولي لحقوق الإنسان. وتضع هذه القوانين أيضاً إجراءات لمساءلة الأفراد عن هذه الانتهاكات.

٢٣- تكفل الدول مساءلة موظفي أجهزة الاستخبارات عن أي انتهاكات للقانون وذلك بالنص على جزاءات متعلقة بجرائم معينة وإنفاذ هذه الجزاءات. ويساعد هذا على تعزيز احترام سيادة القانون وحقوق الإنسان داخل أجهزة الاستخبارات. ويتضمن كثير من القوانين الوطنية المنظمة لأجهزة الاستخبارات جزاءات محددة توقع على الموظفين الذين ينتهكون هذه القوانين أو أحكام القانون الوطني والقانون الدولي الأخرى الواجبة التطبيق<sup>(٧٣)</sup>. وبالنظر إلى أن الكثير من أنشطة أجهزة الاستخبارات يحدث سراً، فإن الجرائم (التي يرتكبها الموظفون) قد لا تكتشفها سلطات الادعاء المعنية. ومن ثم، فإن الممارسة الجيدة تتمثل في أن يقضي القانون الوطني بأن تحيل إدارة أجهزة الاستخبارات حالات الأعمال الإجرامية المحتملة إلى سلطات الادعاء<sup>(٧٤)</sup>. وفي حالات الانتهاكات الجسيمة لحقوق الإنسان، مثل التعذيب، يقع على الدول التزام قانوني دولي بمحاكمة أعضاء أجهزة الاستخبارات<sup>(٧٥)</sup>. وقد تترتب المسؤولية الجنائية على موظفي أجهزة الاستخبارات لا من خلال مشاركتهم المباشرة في الأنشطة المحددة فحسب ولكنها تترتب عليهم أيضاً إذا أمروا بهذه الأنشطة أو تواطؤوا بشكل آخر فيها<sup>(٧٦)</sup>.

**الممارسة ١٧- أعضاء أجهزة الاستخبارات ملزمون قانوناً برفض الأوامر العليا التي تنتهك القانون الوطني أو القانون الدولي لحقوق الإنسان. وتوفر حماية ملائمة لأعضاء أجهزة الاستخبارات الذين يرفضون الأوامر في الحالات من هذا القبيل.**

٢٤- تتمثل ممارسة جيدة في أن تقضي القوانين الوطنية بأن يرفض أعضاء أجهزة الاستخبارات الأوامر التي يعتقدون أنها تنتهك القانون الوطني أو القانون الدولي لحقوق الإنسان<sup>(٧٧)</sup>. ولئن كان هذا الحكم أكثر شيوعاً في القوانين المنظمة للقوات المسلحة، فإن عدة دول أدرجته في القوانين التي تنظم أجهزة الاستخبارات التابعة لها<sup>(٧٨)</sup>. ويشكل وجود حكم يقضي بأن يرفض أعضاء أجهزة الاستخبارات الأوامر غير القانونية ضماناً هاماً ضد الانتهاكات المحتملة لحقوق الإنسان، وكذلك ضد أن تأمر الحكومات القائمة أجهزة

<sup>73</sup> 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.

<sup>74</sup> Canada (footnote 6), sect. 20 (2–4).

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

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

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

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

الاستخبارات باتخاذ إجراء لتعزيز أو حماية مصالحها. ويتمثل مبدأ راسخ تماماً من مبادئ القانون الدولي في عدم إعفاء الأفراد من المسؤولية الجنائية عن الانتهاكات الجسيمة لحقوق الإنسان على أساس أن رئيساً أمرهم باتخاذ إجراء ما<sup>(٧٩)</sup>. ومن ثم، فإنه يقتضى من أعضاء أجهزة الاستخبارات، لتجنب المسؤولية الجنائية الفردية، أن يرفضوا تنفيذ أي أوامر يدركون أنها مخالفة للقانون بشكل واضح. ويبرز هذا أهمية تدريب ضباط الاستخبارات في مجال حقوق الإنسان لأن من الضروري أن يكونوا على دراية بحقوقهم وواجباتهم بموجب القانون الدولي (انظر الممارسة ١٩). ولتهيئة بيئة لا يجري فيها التسامح إزاء انتهاكات حقوق الإنسان، توفر الدول حماية قانونية من الأعمال الانتقامية لأعضاء أجهزة الاستخبارات الذين يرفضون تنفيذ الأوامر غير القانونية<sup>(٨٠)</sup>. ويرتبط الالتزام برفض الأوامر غير القانونية ارتباطاً وثيقاً بتوافر آليات داخلية وخارجية يمكن من خلالها أن يعرب موظفو أجهزة الاستخبارات عن شواغلهم بخصوص الأوامر غير القانونية (انظر الممارسة ١٨ أدناه).

**الممارسة ١٨ -** توجد إجراءات داخلية موضوعة لكي يستخدمها أعضاء أجهزة الاستخبارات للإبلاغ عن الإساءات. وتجري تكملة هذه الإجراءات ببيئة مستقلة تتمثل ولايتها في أن تحقق بشكل كامل في الإساءات وأن تتخذ الإجراءات اللازمة للتصدي لها، عندما يثبت عدم كفاية الإجراءات الداخلية، ويتسنى لها الحصول على المعلومات اللازمة لذلك. وتوفر لأعضاء أجهزة الاستخبارات الذين يبلغون، بحسن نية، عن الإساءات حماية من أي شكل من أشكال الأعمال الانتقامية. وتمتد هذه الحماية إلى أعمال الكشف لوسائل الإعلام أو لعامة الجماهير إذا اضطلع بها كملاذ أخير وتعلقت بمسائل محل انشغال عام واسع النطاق.

٢٥ - كثيراً ما يكون موظفو أجهزة الاستخبارات مجهزين على أفضل وجه لتحديد الإساءات داخل أجهزة الاستخبارات، مثل انتهاكات حقوق الإنسان وسوء التصرف المالي والمخالفات الأخرى للقانون التشريعي. وبناء على ذلك، فإن الممارسة الجيدة هي أن ينص القانون الوطني على إجراءات محددة كيما يستخدمها أعضاء أجهزة الاستخبارات للكشف عن شواغلهم بخصوص الإساءات<sup>(٨١)</sup>. وتهدف هذه الأحكام إلى أن تشجع أعضاء أجهزة الاستخبارات على الإبلاغ عن الإساءات، وأن تضمن، في الوقت نفسه، القيام بأعمال الكشف عن المعلومات ذات الحساسية المحتملة والتحقيق فيها بطريقة خاضعة للسيطرة. وتوضح ممارسة الدول أنه توجد عدة قنوات لأعمال الكشف هذه، بما في ذلك آليات داخلية

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

<sup>80</sup> Bosnia and Herzegovina (footnote 6), art. 42.

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

لتلقي المعلومات التي يكشف عنها أعضاء أجهزة الاستخبارات والتحقيق فيها<sup>(٨٢)</sup>، ومؤسسات خارجية لتلقي المعلومات المكشوف عنها والتحقيق فيها، وأن أعضاء أجهزة الاستخبارات يكشفون لهذه المؤسسات بشكل مباشر عن الإساءات<sup>(٨٣)</sup>. وفي بعض النظم، قد لا يلجأ أعضاء أجهزة الاستخبارات إلى المؤسسة الخارجية إلا إذا أخفقت الهيئة الداخلية في معالجة شواغلهم على نحو كاف<sup>(٨٤)</sup>. وفي بعض الدول، يسمح لأعضاء أجهزة الاستخبارات بالكشف العلني عن الإساءات كملاد أخير أو عندما تتعلق أعمال الكشف بمسائل خطيرة، مثل وجود تهديد للحياة<sup>(٨٥)</sup>. وبصرف النظر عن الطابع المحدد لقنوات الكشف، فإن الممارسة الجيدة هي أن يوفر القانون الوطني للأفراد الذين يقومون بأعمال الكشف، التي يصرح بها القانون، حماية من الأعمال الانتقامية<sup>(٨٦)</sup>.

## زاي - الحس المهني

**الممارسة ١٩ -** تتخذ أجهزة الاستخبارات ومؤسساتها الرقابية الخطوات اللازمة لتهيئة ثقافة حس مهني مؤسسية، تركز على احترام سيادة القانون وحقوق الإنسان. وأجهزة الاستخبارات مسؤولة، على وجه الخصوص، عن تدريب أعضائها في مجال الأحكام ذات الصلة التي ينص عليها القانون الوطني والقانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان.

٢٦ - تشير الثقافة المؤسسية لجهاز الاستخبارات إلى قيم الموظفين ومواقفهم وممارساتهم المشتركة أو السائدة على نطاق واسع. وهي أحد العوامل الرئيسية التي تحدد موقف مسؤولي

<sup>82</sup> 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).

<sup>83</sup> 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.

<sup>84</sup> 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).

<sup>85</sup> 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 911 Commission Report”, chapter 3.

<sup>86</sup> 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.

الاستخبارات تجاه سيادة القانون وحقوق الإنسان<sup>(٨٧)</sup>. والواقع أن الأطر القانونية والمؤسسية وحدها لا يمكن أن تضمن امتثال أعضاء أجهزة الاستخبارات لحقوق الإنسان وسيادة القانون. وقد وضع عدد من الدول وأجهزة الاستخبارات التابعة لها مدونات أخلاقيات أو مبادئ حس مهني من أجل تهيئة ثقافة مؤسسية تثن وتغزز احترام حقوق الإنسان وسيادة القانون<sup>(٨٨)</sup>. وتشتمل مدونات قواعد السلوك بشكل نمطي على أحكام بشأن السلوك اللائق والانضباط والمعايير الأخلاقية تسري على جميع أعضاء أجهزة الاستخبارات<sup>(٨٩)</sup>. وفي بعض الدول، يصدر الوزير المسؤول عن أجهزة الاستخبارات هذه الوثائق؛ ويكفل هذا المساءلة السياسية عن محتوياتها<sup>(٩٠)</sup>. وتمثل الممارسة الجيدة في أن تخضع مدونات قواعد السلوك (والوثائق المشابهة) للتدقيق من جانب المؤسسات الرقابية الداخلية والخارجية<sup>(٩١)</sup>. والتدريب وسيلة رئيسية ثانية لتهيئة ثقافة مؤسسية مهنية داخل أجهزة الاستخبارات. وقد استهلت أجهزة استخبارات كثيرة برامج تدريبية تشدد على الحس المهني وتثقف الموظفين بشأن المعايير الدستورية ذات الصلة والقانون التشريعي والقانون الدولي لحقوق الإنسان<sup>(٩٢)</sup>. والممارسة الجيدة هي أن يقضي القانون بتوفير هذه البرامج التدريبية وينظمها، وأن تشمل هذه البرامج جميع أعضاء أجهزة الاستخبارات (المرتقنين)<sup>(٩٣)</sup>. وأخيراً، فإن الثقافة المهنية يمكن تعزيزها بسياسات داخلية لإدارة شؤون الموظفين تكافئ على السلوك الأخلاقي والمهني.

## حاء - ضمانات حقوق الإنسان

الممارسة ٢٠ - تتمثل أي تدابير تتخذها أجهزة الاستخبارات، وتنطوي على تقييد حقوق الإنسان والحريات الأساسية، للمعايير التالية:

(أ) ينص عليها قانون متوافر على نطاق عام، يمثل للمعايير الدولية لحقوق الإنسان؛

<sup>87</sup> South African Ministerial Review Commission on Intelligence, p. 233.

<sup>88</sup> 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).

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

<sup>90</sup> United Republic of Tanzania (footnote 61), art. 8(3).

<sup>91</sup> 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.

<sup>92</sup> South African Ministerial Review Commission on Intelligence, pp. 209 and 211.

<sup>93</sup> Argentina (footnote 2), arts. 26-30; South Africa (footnote 23), art. 5(2)(a).

(ب) يجب أن تكون كل هذه التدابير ضرورية تماماً لااضطلاع جهاز الاستخبارات بولايته المنصوص عليها قانوناً؛

(ج) يجب أن تكون التدابير المتخذة متناسبة مع الهدف. ويقتضي هذا أن تختار أجهزة الاستخبارات التدبير الأقل تقييداً لحقوق الإنسان، وتتوخى عناية خاصة للتقليل إلى أدنى حد من التأثير السلبي لأي تدابير على حقوق الأفراد، بمن فيهم، على وجه الخصوص، الأشخاص غير المشتبه في ارتكابهم أية إساءة؛

(د) لا يجوز أن ينتهك أي تدبير تتخذه أجهزة الاستخبارات القواعد القطعية للقانون الدولي أو جوهر أي حق من حقوق الإنسان؛

(هـ) يوجد نظام واضح وشامل للتصريح باستخدام أي تدبير يقيد حقوق الإنسان ولرصد هذا الاستخدام ومراقبته؛

(و) يمكن للأشخاص الذين قد تكون أجهزة الاستخبارات قيدت حقوقهم أن يقدموا شكاوى إلى مؤسسة مستقلة ويلتمسوا الحصول على سبيل انتصاف فعال.

٢٧- يسمح لأجهزة الاستخبارات، بموجب القانون الوطني، بالاضطلاع بأنشطة تقييد حقوق الإنسان. وتوجد هذه السلطات في المقام الأول في مجال جمع المعلومات الاستخباراتية ولكنها أيضاً تتضمن تدابير إنفاذ القانون، واستخدام البيانات الشخصية، وتبادل المعلومات الشخصية. وتحتوي القوانين الوطنية على ضمانات لحقوق الإنسان لسببين رئيسيين: قصر التدخل فيما يتعلق بحقوق الأفراد على ما هو مسموح به بموجب القانون الدولي لحقوق الإنسان؛ ومنع الاستخدام التعسفي أو غير المقيد لهذه التدابير<sup>(٩٤)</sup>.

٢٨- وأي تدبير مقيد لحقوق الإنسان يجب أن ينص عليه قانون متوافق مع المعايير الدولية لحقوق الإنسان، وساري المفعول في الوقت الذي يتخذ فيه التدبير<sup>(٩٥)</sup>. ويحدد هذا القانون هذه التدابير تحديداً ضيق النطاق ودقيقاً، وينص على شروط صارمة لاستخدامها، ويقضي بوجوب أن يكون استخدامها مرتبطاً ارتباطاً مباشراً بولاية جهاز الاستخبارات<sup>(٩٦)</sup>.

٢٩- كما تتضمن قوانين وطنية كثيرة اشتراط وجوب أن تكون أي تدابير استخباراتية مقيدة لحقوق الإنسان ضرورية في مجتمع ديمقراطي<sup>(٩٧)</sup>. وتستتبع الضرورة أن يكون استخدام

<sup>94</sup> Siracusa Principles (footnote 38).

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

<sup>96</sup> MacDonald Commission, p. 423; Morton Halperin (footnote 69).

<sup>97</sup> 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.

أي تدابير مرتبطاً ارتباطاً واضحاً ورشيداً بحماية مصالح الأمن الوطني المشروعة كما هي محددة في القانون الوطني<sup>(٩٨)</sup>.

٣٠- ومبدأ التناسب مكرس في قوانين دول كثيرة ويقضي بوجوب أن تكون أي تدابير مقيدة لحقوق الإنسان متناسبة مع الأهداف المحددة (والمسموح بها قانوناً)<sup>(٩٩)</sup>. ولضمان أن تكون التدابير التي تتخذها أجهزة الاستخبارات متناسبة، تقتضي دول كثيرة من أجهزة الاستخبارات التابعة لها استخدام أقل الوسائل تدخلاً قدر الإمكان لتحقيق هدف معين<sup>(١٠٠)</sup>.

٣١- ويحظر القانون على أجهزة الاستخبارات استخدام أي تدابير تنتهك المعايير الدولية لحقوق الإنسان و/أو القواعد القطعية للقانون الدولي. وقد أدرجت بعض الدول محظورات صريحة بشأن الانتهاكات الجسيمة لحقوق الإنسان في قوانينها المتعلقة بأجهزة الاستخبارات<sup>(١٠١)</sup>. ولئن كان من الممكن أن تخص حقوق الإنسان غير القابلة للانتقاص منها بالذكر باعتبارها حقوقاً مصنوعة، فإن كل حق من حقوق الإنسان يتضمن جوهرًا أساسياً يتجاوز نطاق القيود المسموح بها.

٣٢- وتضمن الدول أن تخضع التدابير الاستخباراتية التي تقيد حقوق الإنسان لعملية تصريح محددة قانوناً ولرقابة ومراجعة لاحقتين (انظر الممارسات ٦ و٧ و٢١ و٢٢ و٢٨ و٣٢).

٣٣- ويشترط القانون الدولي لحقوق الإنسان اشتراطاً أساسياً مؤداه أن يكون ضحايا انتهاكات حقوق الإنسان قادرين على التماس الجبر والانتصاف. ولدى دول كثيرة إجراءات معمول بها لضمان أن يتسنى للأفراد الوصول إلى مؤسسة مستقلة يمكنها الفصل في هذه المطالبات (انظر الممارستين ٩ و١٠ أعلاه)<sup>(١٠٢)</sup>.

## طاء - جمع المعلومات الاستخباراتية

٢١- يحدد القانون الوطني أنواع التدابير المتاحة لأجهزة الاستخبارات لجمع المعلومات الاستخباراتية؛ والأهداف المسموح بها لجمع المعلومات الاستخباراتية؛ وفئات الأشخاص والأنشطة التي يمكن أن تخضع لجمع المعلومات

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

<sup>99</sup> 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.

<sup>100</sup> 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.

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

<sup>102</sup> 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.

الاستخباراتية؛ وعتبة الشك اللازمة لتبرير استخدام تدابير الجمع؛ والقيود المفروضة على المدة التي يمكن خلالها استخدام تدابير الجمع؛ وإجراءات التصريح باستخدام تدابير جمع المعلومات الاستخباراتية والرقابة على هذا الاستخدام ومراجعته.

٣٤- تلجأ أجهزة الاستخبارات، في معظم الدول، إلى تدابير تدخلية، مثل المراقبة السرية واعتراض الاتصالات، من أجل جمع المعلومات اللازمة لاضطلاعها بولاياتها. وثمة متطلب أساسي لسيادة القانون هو وجوب أن يكون الأفراد على دراية بالتدابير التي قد تستخدمها السلطات العامة لتقييد حقوقهم وقادرين على التنبؤ بالأنشطة التي قد تتسبب في استخدامها<sup>(١٠٣)</sup>. ويحدد القانون فئات الأشخاص والأنشطة التي يمكن أن تخضع لجمع المعلومات الاستخباراتية<sup>(١٠٤)</sup>، وكذلك عتبة الشك اللازمة لتبرير تدابير معينة لجمع هذه المعلومات<sup>(١٠٥)</sup>. وتفرض بعض القوانين الوطنية قيوداً محددة على استخدام تدابير الجمع التدخلية ضد فئات معينة من الأفراد، ولا سيما الصحفيين والمحامين<sup>(١٠٦)</sup>. والغرض من هذه التدابير حماية الامتيازات المهنية التي تعتبر ضرورية لأداء مجتمع حر، مثل حق الصحفيين في عدم الكشف عن مصادرهم، أو خصوصية العلاقة بين المحامي وموكله. وتساعد القيود المفروضة على استخدام طرق الجمع التدخلية في ضمان أن يكون جمع المعلومات الاستخباراتية ضرورياً ومقتصراً على أفراد وجماعات يحتمل أن يكونوا منخرطين في أنشطة تشكل تهديداً للأمن الوطني. ويتضمن القانون الوطني أيضاً مبادئ توجيهية بشأن المدة المسموح بها لاستخدام تدابير الجمع التدخلية، والتي يلزم على أجهزة الاستخبارات بعدها التماس إعادة التصريح بهذه التدابير من أجل مواصلة استخدامها<sup>(١٠٧)</sup>. وبالمثل، فإن الممارسة الجيدة هي أن يقضي القانون الوطني بوقف استخدام تدابير جمع المعلومات الاستخباراتية حالما يتحقق الغرض الذي استخدمت من أجله أو إذا أصبح واضحاً أنه لا يمكن تحقيق هذا

<sup>103</sup> 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).

<sup>104</sup> 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).

<sup>105</sup> 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.

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

<sup>107</sup> 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.

الغرض<sup>(١٠٨)</sup>. وتفيد هذه الأحكام في التقليل إلى أدنى حد من انتهاكات حقوق الأفراد المعنيين وتساعد على ضمان أن تفي تدابير جمع المعلومات الاستخباراتية بشرط التناسب.

**الممارسة ٢٢-** تقوم مؤسسة واحدة على الأقل من خارج أجهزة الاستخبارات ومستقلة عنها بالتصريح بتدابير جمع المعلومات الاستخباراتية، التي تفرض قيوداً شديدة على حقوق الإنسان، وبمراقبة هذه التدابير. ولهذه المؤسسة سلطة الأمر بتعديل أو تعليق أو إنهاء تدابير الجمع هذه. وتخضع تدابير جمع المعلومات الاستخباراتية التي تفرض قيوداً شديدة على حقوق الإنسان لعملية تصريح متعددة المستويات تتضمن الإقرار داخل أجهزة الاستخبارات، ومن جانب السلطة السياسية التنفيذية، ومن قبل مؤسسة مستقلة عن أجهزة الاستخبارات والسلطة التنفيذية.

**٣٥-** تتمثل ممارسة شائعة في أن تتضمن القوانين الوطنية أحكاماً تفصيلية بشأن عملية التصريح بجميع تدابير جمع المعلومات الاستخباراتية التي تقيّد حقوق الإنسان<sup>(١٠٩)</sup>. وعمليات التصريح تقتضي من أجهزة الاستخبارات تبرير الاستخدام المقترح لتدابير جمع المعلومات الاستخباراتية وفقاً لإطار قانوني واضح التحديد (انظر الممارستين ٢٠ و ٢١ أعلاه). وهذه آلية أساسية لضمان استخدام تدابير الجمع طبقاً للقانون. والممارسة الجيدة هي أن ترخص بتدابير الجمع التدخلية مؤسسة مستقلة عن أجهزة الاستخبارات، أي مؤسسة عضو في السلطة التنفيذية خاضعة للمساءلة السياسية<sup>(١١٠)</sup> أو هيئة (شبه) قضائية<sup>(١١١)</sup>. والهيئات القضائية مستقلة عن العملية الاستخباراتية وبالتالي فإنها الأقدر على إجراء تقييم مستقل ومحيد لطلب مقدم لاستخدام صلاحيات جمع تدخلية<sup>(١١٢)</sup>. وفضلاً عن هذا، فإن الممارسة الجيدة بشكل خاص هي أن يشمل التصريح بأشد أساليب جمع المعلومات الاستخباراتية تدخلاً (مثل اعتراض محتويات الاتصالات، واعتراض البريد، ودخول الممتلكات خلسة) كبار

<sup>108</sup> 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.

<sup>109</sup> 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.

<sup>110</sup> Australia (footnote 3), arts. 25, 25a; Netherlands (footnote 20), arts. 19, 20(3-4), 22 (4), 25; United Kingdom (footnote 47), sects. 5-7.

<sup>111</sup> 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.

<sup>112</sup> 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.

المديرين في أجهزة الاستخبارات، والسلطة التنفيذية التي يمكن مساءلتها سياسياً، وهيئة (شبه) قضائية<sup>(١١٣)</sup>.

٣٦- وتكفل الدول أيضاً أن يخضع جمع المعلومات الاستخباراتية لرقابة مستمرة من جانب مؤسسة من خارج أجهزة الاستخبارات. والممارسة الجيدة هي أن يقتضى من أجهزة الاستخبارات الإبلاغ على أساس مستمر عن استخدام تدابير الجمع وأن تكون للمؤسسة الرقابية الخارجية سلطة الأمر بإلغاء تدابير الجمع<sup>(١١٤)</sup>. وفي دول كثيرة، تقوم الهيئات الرقابية الخارجية أيضاً بالرقابة اللاحقة على استخدام تدابير جمع المعلومات الاستخباراتية بغية التحقق مما إذا كانت، أم لم تكن، مصرحاً بها ومستخدمة وفقاً للقانون<sup>(١١٥)</sup>. وهذا مهم بشكل خاص بالنظر إلى أن من غير المرجح أن يكون الأفراد الذين تنتصر حقوقهم من جراء جمع المعلومات الاستخباراتية على دراية بهذه الحقيقة وبالتالي تكون الفرصة المتاحة لهم للطعن في مشروعيته محدودة.

## ياء - إدارة البيانات الشخصية واستخدامها

الممارسة ٢٣- يحدد القانون المتوافر على نطاق عام أنواع البيانات الشخصية التي يجوز أن تحتفظ بها أجهزة الاستخبارات، والمعايير التي تطبق على استخدام هذه البيانات والاحتفاظ بها وحذفها والكشف عنها. ويسمح لأجهزة الاستخبارات بالاحتفاظ بالبيانات الشخصية التي توجد ضرورة قصوى للجوء إليها لأغراض الاضطلاع بولايتها.

٣٧- هناك عدد من المبادئ العامة التي تطبق على حماية البيانات الشخصية والتي تدرج عادة في القوانين الوطنية<sup>(١١٦)</sup> وكذلك في الصكوك الدولية<sup>(١١٧)</sup>. وتشتمل هذه على المتطلبات التالية: أن يجري جمع البيانات الشخصية ومعالجتها بطريقة مشروعة ونزيهة؛ وأن يقتصر استخدام البيانات الشخصية على، وينحصر في، غرضه المحدد الأصلي؛ وأن تتخذ الخطوات

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

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

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

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

<sup>117</sup> 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).

اللازمة لضمان دقة سجلات البيانات الشخصية؛ وأن تحذف ملفات البيانات الشخصية عندما لا تعد هناك حاجة إليها؛ وأن يكون للأفراد الحق في الوصول إلى ملفات بياناتهم الشخصية وتصحيحها<sup>(١١٨)</sup>. وفي سياق استخدام أجهزة الاستخبارات للبيانات الشخصية، يمكن أن تكون لفتح ملفات البيانات الشخصية والاحتفاظ بها والتخلص منها تأثيرات خطيرة على حقوق الإنسان؛ ولذلك ينص في القانون التشريعي العام على مبادئ توجيهية لإدارة البيانات الشخصية واستخدامها من جانب أجهزة الاستخبارات. ويشكل هذا ضماناً قانونية ضد إعطاء السلطة التنفيذية أو أجهزة الاستخبارات صلاحيات لا حدود لها على هذه المسائل<sup>(١١٩)</sup>. وثمة ضمانات ثانية هي أنه توضع مبادئ توجيهية قانونية لتحديد وتقييد دواعي قيام أجهزة الاستخبارات بفتح وحفظ ملفات البيانات الشخصية<sup>(١٢٠)</sup>. والضمانة الثالثة هي أن هناك ممارسة راسخة في دول مختلفة هي أن أجهزة الاستخبارات تبلغ الجمهور عموماً بنوع البيانات الشخصية التي يحتفظ بها جهاز الاستخبارات؛ ويتضمن هذا المعلومات المتعلقة بنوع ونطاق البيانات الشخصية التي يمكن الاحتفاظ بها، وكذلك الأسس المسموح بها لاحتفاظ جهاز الاستخبارات بالمعلومات الشخصية<sup>(١٢١)</sup>. والضمانة الرابعة هي أن دولاً مختلفة جرمت كشف موظفي الاستخبارات عن البيانات الشخصية أو استخدام هذه البيانات خارج الإطار القانوني المنشأ<sup>(١٢٢)</sup>. والضمانة الأخيرة هي أن الدول قضت صراحة بأن من غير المسموح لأجهزة الاستخبارات أن تحفظ بيانات شخصية على أسس تمييزية<sup>(١٢٣)</sup>.

**الممارسة ٢٤ -** تجري أجهزة الاستخبارات تقييمات منتظمة لمدى مناسبة ودقة البيانات الشخصية التي تحتفظ بها. ويقتضى منها قانوناً حذف أو تحديث أي معلومات يجري تقييمها على أنها غير دقيقة أو لم تعد ذات صلة بولايتها أو بعمل مؤسسات الرقابة أو بالإجراءات القضائية المحتملة.

<sup>118</sup> 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.

<sup>119</sup> European Court of Human Rights, *Weber and Saravia v. Germany*, no. 54934/00, 29 June 2006, paras. 93-95.

<sup>120</sup> MacDonal Inquiry, p. 519; Netherlands (footnote 20), art. 13.

<sup>121</sup> 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>).

<sup>122</sup> Romania (footnote 15), art. 21.

<sup>123</sup> 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.

٣٨- اتخذت الدول خطوات لضمان أن تتحقق أجهزة الاستخبارات بانتظام مما إذا كانت ملفات البيانات الشخصية دقيقة أو ذات صلة بولايتها<sup>(١٢٤)</sup>. وتساعد الضمانات المتعلقة بمناسبة ودقة البيانات الشخصية على التقليل إلى أدنى حد من أي انتهاك جاز للحق في الخصوصية. وفي بعض الدول، لا يقتصر الالتزام القانوني لأجهزة الاستخبارات على إتلاف الملفات التي لم تعد ذات صلة<sup>(١٢٥)</sup> فحسب وإنما يشمل أيضاً إتلاف الملفات غير الصحيحة أو التي عولجت على نحو غير صحيح<sup>(١٢٦)</sup>. ولئن كانت أجهزة الاستخبارات ملزمة عادة بحذف البيانات التي لم تعد ذات صلة بولايتها، فإن من المهم ألا يضر هذا بعمل هيئات الرقابة أو بالإجراءات القضائية المحتملة. وقد تشكل المعلومات التي تحتفظ بها أجهزة الاستخبارات أدلة في الإجراءات القضائية ذات تأثيرات كبيرة بالنسبة للأفراد المعنيين؛ وقد يكون توافر هذه المواد مهما لضمان الحقوق المتعلقة بالإجراءات القانونية الواجبة. ومن ثم، فإن الممارسة الجيدة تقضي بإلزام أجهزة الاستخبارات بالاحتفاظ بجميع السجلات (بما في ذلك المدونات الأصلية والمذكرات الأصلية) في الحالات التي قد تفضي إلى إجراءات قضائية، وبخضوع حذف أي معلومات من هذا القبيل للرقابة من جانب مؤسسة خارجية (انظر الممارسة ٢٥ أدناه)<sup>(١٢٧)</sup>.

**الممارسة ٢٥-** توجد مؤسسة خارجية للرقابة على استخدام أجهزة الاستخبارات للبيانات الشخصية. ويتسنى لهذه المؤسسة الوصول إلى جميع الملفات التي تحتفظ بها أجهزة الاستخبارات ولها سلطة الأمر بالكشف عن المعلومات للأفراد المعنيين، وإتلاف الملفات أو المعلومات الشخصية الواردة فيها.

٣٩- تخضع إدارة ملفات البيانات الشخصية، في دول كثيرة، لرقابة منتظمة ومستمرة من جانب مؤسسات مستقلة<sup>(١٢٨)</sup>. وتحويل هذه المؤسسات ولاية إجراء زيارات تفتيشية منتظمة ومراجعات عشوائية لملفات البيانات الشخصية المتعلقة بالعمليات الجارية والسابقة<sup>(١٢٩)</sup>. كما عهدت الدول إلى المؤسسات الرقابية المستقلة بولاية التحقق مما إذا كانت التوجيهات الداخلية بشأن إدارة الملفات مطابقة للقانون<sup>(١٣٠)</sup>. وسلمت الدول بحاجة مؤسسات الرقابة

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

<sup>125</sup> Germany (footnote 2), sect. 12 (2); Kenya (footnote 16), sect. 28(1).

<sup>126</sup> Netherlands (footnote 20), art. 43; Croatia (footnote 2), art. 41(1).

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

<sup>128</sup> Sweden (footnote 27), art. 1; Hungary (footnote 77), sect. 52. See also practices 6-8.

<sup>129</sup> 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).

<sup>130</sup> 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.

إلى أن تكون مستقلة في طرق العمل والتفتيش التي تتبعها، وأن تتوفر لها موارد وقدرات كافية لإجراء عمليات تفتيش منتظمة على إدارة واستخدام البيانات الشخصية من جانب أجهزة الاستخبارات<sup>(١٣١)</sup>. وعلى أجهزة الاستخبارات واجب قانوني يقتضي منها التعاون التام مع مؤسسة الرقابة المسؤولة عن فحص إدارتها واستخدامها للبيانات الشخصية<sup>(١٣٢)</sup>.

**الممارسة ٢٦-** تتوفر للأفراد إمكانية طلب الوصول إلى بياناتهم الشخصية التي تحتفظ بها أجهزة الاستخبارات. ويجوز للأفراد ممارسة هذا الحق بتقديم طلب إلى سلطة معنية أو من خلال مؤسسة مستقلة لحماية البيانات أو الرقابة على استخدامها. ويحق للأفراد تصحيح المعلومات غير الدقيقة التي تتضمنها البيانات الشخصية. وتكون أي استثناءات من هذه القواعد العامة منصوصاً عليها بموجب القانون ومحدودة للغاية وضرورية لاضطلاع جهاز الاستخبارات بولايته. ويتعين على جهاز الاستخبارات أن يبرر لمؤسسة رقابية مستقلة أي قرار يتخذه بعدم إصدار معلومات شخصية.

٤٠- أعطت دول كثيرة الأفراد الحق في الوصول إلى بياناتهم الشخصية التي تحتفظ بها أجهزة الاستخبارات. ويمكن ممارسة هذا الحق بتقديم طلب إلى جهاز الاستخبارات<sup>(١٣٣)</sup>، أو وزير مختص<sup>(١٣٤)</sup>، أو مؤسسة رقابية مستقلة<sup>(١٣٥)</sup>. وينبغي أن يفهم حق الأفراد في الوصول إلى ملفات بياناتهم الشخصية في سياق الضمانات المتعلقة بحقوق الخصوصية وحرية الوصول إلى المعلومات. وهذه الضمانة مهمة لا لأنها تسمح للأفراد بالتحقق مما إذا كان ملف بياناتهم الشخصية دقيقاً ومشروعاً فحسب، وإنما أيضاً لأنها ضمانات ضد الانتهاك وسوء الإدارة والفساد. والواقع أن حق الفرد في الوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات يفيد في زيادة الشفافية والمساءلة في عمليات اتخاذ القرارات التي تضطلع بها أجهزة الاستخبارات ويساعد بالتالي على تعزيز ثقة المواطنين في الإجراءات الحكومية<sup>(١٣٦)</sup>. وقد تقيّد الدول الوصول إلى ملفات البيانات الشخصية، لأسباب مثل صون التحقيقات الجارية وحماية مصادر وطرق أجهزة الاستخبارات. بيد أن الممارسة الجيدة في هذا الصدد هي أن تحدد هذه التقييدات في القانون وأن تفي باشتراطات التناسب والضرورة<sup>(١٣٧)</sup>.

<sup>131</sup> 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).

<sup>132</sup> Hungary (footnote 77), sect. 52.

<sup>133</sup> Croatia (footnote 2), art. 40 (1).

<sup>134</sup> Netherlands (footnote 20), art. 47.

<sup>135</sup> Sweden (footnote 27), art. 3; Switzerland (footnote 5), art. 18 (1).

<sup>136</sup> 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.

<sup>137</sup> Netherlands (footnote 20), arts. 53-56; Croatia (footnote 2), art. 40 (2) (3); Germany (footnote 2), sect. 15(2).

## كاف - استخدام سلطات التوقيف والاحتجاز

الممارسة ٢٧- لا يسمح لأجهزة الاستخبارات باستخدام سلطات التوقيف والاحتجاز إذا لم تكن لها ولاية لأداء مهام إنفاذ القانون. ولا تعطى لها سلطات التوقيف والاحتجاز إذا كان من شأن هذا أن يشكل ازدواجية مع سلطات وكالات إنفاذ القانون المخولة ولاية الاضطلاع بالأنشطة ذاتها.

٤١- ثمة ممارسة جيدة مسلم بها على نطاق واسع هي أن تحظر صراحة على أجهزة الاستخبارات ممارسة سلطات التوقيف والاحتجاز إذا لم تكن ولايتها القانونية تقتضي منها ممارسة مهام إنفاذ القانون فيما يتعلق بالجرائم التي تمس الأمن الوطني، مثل الإرهاب<sup>(١٣٨)</sup>. وقد سبقت حجج قوية ضد الجمع بين مهام الاستخبارات ومهام إنفاذ القانون<sup>(١٣٩)</sup>. بيد أنه إذا كان القانون الوطني ينص على منح أجهزة الاستخبارات سلطات التوقيف والاحتجاز، فإن الممارسة الجيدة تقتضي أن يكون هذا صراحة في سياق ولاية تعطي هذه الأجهزة المسؤولية عن أداء مهام إنفاذ القانون فيما يتعلق بأخطار محددة تهدد الأمن الوطني، مثل الإرهاب<sup>(١٤٠)</sup>. وإذا كانت للهيئات الوطنية أو الإقليمية لإنفاذ القانون ولاية لإنفاذ القانون الجنائي فيما يتعلق بالجرائم التي تمس الأمن الوطني، فإنه لا يوجد سبب مشروع لإعطاء جهاز استخبارات منفصل سلطات التوقيف والاحتجاز فيما يتصل بالأنشطة ذاتها. وهناك خطر محتمل يتمثل في إنشاء نظام إنفاذ مواز، تمارس بموجبه أجهزة الاستخبارات سلطات التوقيف والاحتجاز للتحايل على الضمانات القانونية والرقابة التي تختص بها وكالات إنفاذ القانون<sup>(١٤١)</sup>.

الممارسة ٢٨- إذا كانت لأجهزة الاستخبارات سلطات التوقيف والاحتجاز، فإن هذه السلطات تستند إلى قانون متوافر على نطاق عام. وتقتصر ممارسة هذه السلطات على الحالات التي يوجد فيها شك معقول في احتمال أن يكون شخص قد ارتكب، أو يوشك أن يرتكب، جريمة محددة. ولا يسمح لأجهزة الاستخبارات بمجرمان أشخاص من حريتهم لغرض وحيد هو جمع معلومات استخباراتية. ويخضع استخدام أجهزة الاستخبارات لأي سلطات توقيف واحتجاز لدرجة الرقابة ذاتها

<sup>138</sup> 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).

<sup>139</sup> 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.

<sup>140</sup> Norway, Criminal Procedure Act.

<sup>141</sup> International Commission of Jurists, "Assessing damage, urging action", pp. 73-78.

التي يخضع لها استخدام هيئات إنفاذ القانون لهذه السلطات، بما في ذلك المراجعة القضائية لمشروعية أي حرمان من الحرية.

٤٢- إذا أعطيت أجهزة الاستخبارات سلطات التوقيف والاحتجاز، فإن القانون الوطني يحدد أغراض هذه السلطات والظروف التي يجوز فيها استخدامها<sup>(١٤٢)</sup>. والممارسة الجيدة هي القصر التام لاستخدام هذه السلطات على الحالات التي يوجد فيها شك معقول في احتمال أن تكون جريمة (تندرج في نطاق ولاية أجهزة الاستخبارات) قد ارتكبت أو على وشك أن ترتكب. وبالتالي، فإن أجهزة الاستخبارات لا يسمح لها باستخدام هذه السلطات لغرض وحيد هو جمع معلومات استخباراتية<sup>(١٤٣)</sup>. ولا يسمح بموجب القانون الدولي لحقوق الإنسان باعتقال واحتجاز أفراد عندما لا يكون هناك شك معقول في أنهم ارتكبوا، أو على وشك أن يرتكبوا، جريمة، أو أي مبرر آخر مقبول دولياً للاحتجاز<sup>(١٤٤)</sup>. والممارسة الجيدة هي أن يخضع استخدام أجهزة الاستخبارات لهذه السلطات لدرجة الرقابة ذاتها التي يخضع لها استخدامها من جانب هيئات إنفاذ القانون<sup>(١٤٥)</sup>. وأهم شيء في هذا الصدد هو أن القانون الدولي لحقوق الإنسان يقضي بأن للأفراد حق الطعن في مشروعية احتجازهم أمام محكمة<sup>(١٤٦)</sup>.

**الممارسة ٢٩-** إذا كانت أجهزة الاستخبارات تملك سلطات التوقيف والاحتجاز، فإنها تمثل للمعايير الدولية لحقوق الإنسان بشأن الحق في الحرية والحق في محاكمة عادلة، وحظر التعذيب والمعاملة اللاإنسانية والمهينة. وعند ممارسة هذه السلطات، تمثل أجهزة الاستخبارات للمعايير الدولية المنصوص عليها في صكوك من بينها مجموعة المبادئ المتعلقة بحماية جميع الأشخاص الذين يتعرضون لأي شكل من أشكال الاحتجاز أو السجن ومدونة قواعد سلوك موظفي إنفاذ القانون والمبادئ الأساسية المتعلقة باستخدام القوة والأسلحة النارية من قبل موظفي إنفاذ القانون.

٤٣- إذا أعطيت أجهزة الاستخبارات سلطات التوقيف والاحتجاز، فإنه يلزم عليها أن تمثل للمعايير الدولية التي تنطبق على الحرمان من الحرية (انظر أيضاً الممارسة ٢٨ أعلاه)<sup>(١٤٧)</sup>. وهذه المعايير يجري تناولها بمزيد من التوسع في عدة مدونات دولية وإقليمية

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

<sup>143</sup> 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).

<sup>144</sup> Venice Commission (1998), sect. E.

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

<sup>146</sup> 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.

<sup>147</sup> Venice Commission (1998), sect. E.

لقواعد سلوك موظفي إنفاذ القانون تدون طائفة من الممارسات الجيدة التي يمكن تطبيقها على أجهزة الاستخبارات المخولة سلطات التوقيف والاحتجاز<sup>(١٤٨)</sup>. وبالإضافة إلى الالتزام القانوني (المتعلق بالمراجعة القضائية للاحتجاز) المحدد في الممارسة ٢٨ أعلاه، توجد ثلاث مجموعات إضافية من المعايير التي تسري على استخدام سلطات التوقيف والاحتجاز من جانب أجهزة الاستخبارات. أولاً، أجهزة الاستخبارات ملزمة بالحظر التام لاستخدام التعذيب والمعاملة اللاإنسانية والمهينة<sup>(١٤٩)</sup>. ثانياً، يجب أن يمثل أي استخدام للقوة أثناء التوقيف والاحتجاز للمعايير الدولية، بما في ذلك المقتضيات المتعلقة بأن يكون أي استخدام للقوة ضرورياً تماماً ومتناسباً مع الخطر المتوجس منه وأن يجري الإبلاغ عنه على النحو الواجب<sup>(١٥٠)</sup>. ثالثاً، تتمثل ممارسة جيدة في أن تمثل أجهزة الاستخبارات للمعايير الدولية التالية بشأن اعتقال الأفراد واحتجازهم: أن تسجل كل حالات التوقيف والاحتجاز والاستجواب من لحظة الاعتقال<sup>(١٥١)</sup>؛ وأن يعرف الضباط القائمون بالتوقيف الأفراد المعنيين بأنفسهم ويبلغوهم بأسباب اعتقالهم/احتجازهم والأساس القانوني لذلك<sup>(١٥٢)</sup>؛ وأن يتسنى للأفراد الذين تحتجزهم أجهزة الاستخبارات أن يكون لهم تمثيل قانوني<sup>(١٥٣)</sup>.

**الممارسة ٣٠-** لا يسمح لأجهزة الاستخبارات بتشغيل مرافق الاحتجاز الخاصة بها أو استخدام أي مرافق احتجاز غير معترف بها تقوم بتشغيلها أطراف ثالثة.

**٤٤-** تتمثل ممارسة جيدة في أن يحظر القانون الوطني صراحة على أجهزة الاستخبارات أن تقوم بتشغيل مرافق الاحتجاز الخاصة بها<sup>(١٥٤)</sup>. وفي حالة السماح لأجهزة الاستخبارات بممارسة سلطات التوقيف والاحتجاز، يودع الأفراد المعنيون في مراكز احتجاز نظامية تديرها

<sup>148</sup> 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).

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

<sup>150</sup> 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.

<sup>151</sup> 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.

<sup>152</sup> 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.

<sup>153</sup> 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.

<sup>154</sup> Romania (footnote 2), art. 13.

وكالات إنفاذ القانون<sup>(١٥٥)</sup>. وبالتساوي مع هذا، لا يسمح لأجهزة الاستخبارات باستخدام مرافق احتجاز غير معترف بها تديرها أطراف ثالثة، مثل مقاولي القطاع الخاص. وهذه ضمانات ضرورية ضد الاحتجاز التعسفي من جانب أجهزة الاستخبارات و/أو إقامة نظام احتجاز مواز يمكن فيه حجز الأفراد في أوضاع لا تفي بالمعايير الدولية للاحتجاز والإجراءات القانونية الواجبة.

## لام - تبادل المعلومات الاستخباراتية والتعاون في مجال الاستخبارات

**الممارسة ٣١-** يستند تبادل المعلومات بين وكالات الاستخبارات في الدولة نفسها أو مع سلطات دولة أجنبية إلى القانون الوطني الذي يحدد معايير واضحة لتبادل المعلومات الاستخباراتية، بما في ذلك الشروط التي يجب الوفاء بها لتبادل المعلومات، والكيانات التي يمكن تبادل المعلومات الاستخباراتية معها، والضوابط التي تطبق على عمليات تبادل المعلومات الاستخباراتية.

**٤٥-** تتمثل ممارسة جيدة في أن يكون لجميع أشكال تبادل المعلومات بين أجهزة الاستخبارات والكيانات المحلية والأجنبية الأخرى أساس واضح في القانون الوطني. ويتضمن القانون الوطني معايير بشأن الأغراض التي يمكن من أجلها تبادل المعلومات الاستخباراتية، والكيانات التي يمكن تبادلها معها، والضوابط الإجرائية التي تطبق على تبادل المعلومات الاستخباراتية<sup>(١٥٦)</sup>. والأساس القانوني لتبادل المعلومات الاستخباراتية متطلب مهم لسيادة القانون ويتسم بأهمية خاصة عند تبادل البيانات الشخصية لأن هذا ينتهك بشكل مباشر الحق في الخصوصية وقد يؤثر على مجموعة متنوعة من الحقوق والحريات الأساسية الأخرى. وبالإضافة إلى ضمان أن يستند تبادل المعلومات الاستخباراتية إلى القانون الوطني، فإن من المسلم على نطاق واسع بأنه ممارسة جيدة أن يستند تبادل المعلومات الاستخباراتية إلى اتفاقات أو مذكرات خطية بين الأطراف، تنطوي على الامتثال للمبادئ التوجيهية المنصوص عليها في القانون الوطني<sup>(١٥٧)</sup>. وتشتمل العناصر التي تدرج عادة في هذه الاتفاقات على قواعد تحكم استخدام المعلومات المتبادلة، وبيان بامتثال الأطراف لحقوق الإنسان وحماية البيانات، والبند الذي يقضي بأنه يجوز للجهاز المرسل طلب تعليقات بشأن استخدام المعلومات

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

<sup>156</sup> 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.

<sup>157</sup> Canada, Arar Commission, pp. 321-322; Venice Commission (2007), p. 182.

المتبادلة<sup>(١٥٨)</sup>. واتفاقات تبادل المعلومات الاستخباراتية تساعد على وضع معايير وتوقعات متفق عليها بين الأطراف بخصوص المعلومات المتبادلة، وتقلص نطاق التبادل غير الرسمي للمعلومات الاستخباراتية، الذي لا يمكن أن تراجعه مؤسسات الرقابة بسهولة.

**الممارسة ٣٢-** يحدد القانون الوطني عملية التصريح بالاتفاقات التي يستند إليها تبادل المعلومات الاستخباراتية وكذلك بتبادل المعلومات الاستخباراتية على أساس مخصص. وتلزم موافقة السلطة التنفيذية على أي اتفاقات لتبادل المعلومات الاستخباراتية مع كيانات أجنبية وعلى تبادل المعلومات الاستخباراتية التي قد تكون لها تأثيرات كبيرة على حقوق الإنسان

٤٦- تتمثل ممارسة جيدة في أن ينص القانون الوطني على مبادئ توجيهية للتصريح بإرسال المعلومات على أساس مخصص وإبرام اتفاقات لتبادل المعلومات الاستخباراتية<sup>(١٥٩)</sup>. ويساعد هذا على ضمان أن تكون هناك قنوات مسؤولية راسخة لتبادل المعلومات الاستخباراتية وأن يكون من الممكن مساءلة الأفراد عن أي قرارات يتخذونها في هذا الصدد. وفي دول كثيرة، يصرح بالتبادل الروتيني للمعلومات الاستخباراتية على الصعيد المحلي داخلياً (في أجهزة الاستخبارات). بيد أن الممارسة الجيدة تستلزم، عندما يكون من الممكن أن تستخدم المعلومات الاستخباراتية في إجراءات المحاكم، الحصول على تصريح من السلطة التنفيذية؛ وقد تكون لاستخدام المعلومات الاستخباراتية في هذه الإجراءات تأثيرات عميقة على حقوق الأفراد المعنيين وكذلك على أنشطة أجهزة الاستخبارات ذاتها<sup>(١٦٠)</sup>. وبالإضافة إلى ذلك، تقضي قوانين وطنية كثيرة بوجوب الحصول على تصريح من السلطة التنفيذية لتبادل المعلومات الاستخباراتية أو لإبرام اتفاقات تبادل مع كيانات أجنبية<sup>(١٦١)</sup>.

**الممارسة ٣٣-** قبل إبرام اتفاق لتبادل المعلومات الاستخباراتية، أو تبادل المعلومات الاستخباراتية على أساس مخصص، تجري أجهزة الاستخبارات تقييماً لسجل الكيان النظير بشأن حقوق الإنسان وحماية البيانات، وكذلك للضمانات القانونية والضوابط المؤسسية المنظمة للكيان النظير. وقبل تسليم المعلومات، تتأكد أجهزة الاستخبارات من أن أي معلومات استخباراتية متبادلة ذات صلة بولاية المتلقي، وأنها ستستخدم وفقاً للشروط المرفقة، ولن تستخدم لأغراض تنتهك حقوق الإنسان

<sup>158</sup> 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).

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

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

<sup>161</sup> 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).

٤٧- يمكن أن تكون لكل من إرسال المعلومات الاستخباراتية وتلقيها تأثيرات هامة بالنسبة لحقوق الإنسان والحريات الأساسية. والمعلومات المرسلّة إلى حكومة أجنبية أو جهاز استخبارات أجنبي قد لا تزيد فقط من القيود القانونية الواقعة على حقوق الفرد، ولكنها يمكن أيضاً أن تشكل أساس انتهاكات حقوق الإنسان. وبالمثل، فإن المعلومات الاستخباراتية المتلقاة من كيان أجنبي ربما يكون قد تم الحصول عليها بصورة تنتهك القانون الدولي لحقوق الإنسان. ومن ثم، فإن الممارسة الجيدة هي أن تجري أجهزة الاستخبارات تقييماً عاماً لسجل الكيان الأجنبي النظير بشأن حقوق الإنسان وحماية البيانات الشخصية، وكذلك للضمانات القانونية والمؤسسية (مثل الرقابة) التي تطبق على هذه الأجهزة<sup>(١٦٢)</sup>. وقبل تبادل المعلومات المتعلقة بأفراد محددين أو جماعات محددة، تتخذ أجهزة الاستخبارات الخطوات اللازمة لتقييم التأثير الممكن على الأفراد المعنيين<sup>(١٦٣)</sup>. والممارسة الجيدة هي الإبقاء على الحظر التام لتبادل أي معلومات إذا كان هناك اعتقاد معقول أن تبادل المعلومات يمكن أن يؤدي إلى انتهاك حقوق الشخص المعني (الأشخاص المعنيين)<sup>(١٦٤)</sup>. وفي بعض الظروف، قد تطلق مسؤولية الدولة من خلال تبادل المعلومات الاستخباراتية التي تسهم في ارتكاب انتهاكات جسيمة لحقوق الإنسان. وبالإضافة إلى ذلك، فإن الكثير من القوانين الوطنية يقتضي من الدول تقييم مدى ضرورة تبادل معلومات معينة من منظور ولايتها وولاية الدول النظيرة لها<sup>(١٦٥)</sup>. وتقييم ما إذا كان تبادل المعلومات الاستخباراتية ضرورياً وذا صلة بولاية المتلقي يتيح لأجهزة الاستخبارات دعم مبدأ التقليل إلى الحد الأدنى عند تبادل المعلومات، أي أن أجهزة الاستخبارات تقلل المعلومات التي يجري تبادلها إلى أقصى حد ممكن<sup>(١٦٦)</sup>. وتساعد هذه الضمانات على منع التبادل المفرط أو الاعتباطي للمعلومات الاستخباراتية.

٤٨- وبالنظر إلى التأثيرات الممكنة لتبادل المعلومات الاستخباراتية بالنسبة لحقوق الإنسان، فإن الممارسة الجيدة هي التدقيق في جميع المعلومات الصادرة للتحقق من دقتها ومناسبتها قبل إرسالها إلى كيانات أجنبية<sup>(١٦٧)</sup>. وحيثما تكون هناك شكوك في معولية المعلومات الاستخباراتية الصادرة، فإن هذه المعلومات إما تحجز وإما ترفق بما تقديرات للأخطاء<sup>(١٦٨)</sup>. وأخيراً، فإن الممارسة الجيدة هي أن تحدث كل تبادلات المعلومات

<sup>162</sup> 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.

<sup>163</sup> 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.

<sup>164</sup> Canada, Arar Commission, p. 346–347.

<sup>165</sup> 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).

<sup>166</sup> Canada, Arar Commission, pp. 338–339.

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

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

الاستخباراتية خطياً أو أن يجري تسجيلها؛ ويسر هذا المراجعة اللاحقة من جانب مؤسسات الرقابة<sup>(١٦٩)</sup>.

**الممارسة ٣٤-** المؤسسات الرقابية المستقلة قادرة على فحص ترتيبات تبادل المعلومات الاستخباراتية وأي معلومات ترسلها أجهزة الاستخبارات إلى كيانات أجنبية.

٤٩- تتمثل الممارسة الجيدة في تحويل أجهزة الاستخبارات ولاية مراجعة الاتفاقات التي يستند إليها تبادل المعلومات الاستخباراتية، وكذلك أي ترتيبات تركز على هذه الاتفاقات<sup>(١٧٠)</sup>. والمؤسسات الرقابية المستقلة يمكنها تمحيص الإطار القانوني والأبعاد الإجرائية لاتفاقات تبادل المعلومات الاستخباراتية للتحقق من امتثالها للقوانين الوطنية والمعايير القانونية الدولية ذات الصلة. وكقاعدة عامة، تخول المؤسسات الرقابية الوصول إلى جميع المعلومات الضرورية للاضطلاع بولايتها (انظر الممارسة ٧ أعلاه). بيد أن قاعدة الأطراف الثالثة قد تستتبع، في سياق التبادل الدولي للمعلومات الاستخباراتية، فرض قيود على وصول المؤسسات الرقابية إلى المعلومات الواردة التي تقدمها كيانات أجنبية. والمؤسسات الرقابية تعتبر بوجه عام أطرافاً ثالثة؛ ولذلك لا يمكنها عادة الوصول إلى المعلومات التي تتبادلها كيانات أجنبية مع أجهزة الاستخبارات. ومع ذلك، فإن المؤسسات الرقابية لها الحق في تمحيص المعلومات المرسله إلى كيانات أجنبية، وهي تمارس هذا الحق باعتباره جزءاً من ولايتها المتعلقة بمراقبة كل جوانب أنشطة جهاز الاستخبارات (انظر الممارسة ٧ أعلاه). وفي هذا السياق، تتمثل الممارسة الجيدة في أن يقضي القانون الوطني صراحة بأن تبلغ أجهزة الاستخبارات مؤسسة رقابية مستقلة بما يحدث من تبادل للمعلومات الاستخباراتية<sup>(١٧١)</sup>. ويتيح هذا التحقق من مشروعية ممارسات تبادل المعلومات الاستخباراتية ويشكل ضماناً هامة ضد تبادل البيانات الشخصية الذي قد تكون له تأثيرات خطيرة على حقوق الإنسان فيما يتعلق بالأفراد المعنيين.

**الممارسة ٣٥-** يحظر صراحة على أجهزة الاستخبارات الاستعانة بأجهزة الاستخبارات الأجنبية على أي نحو يسفر عن التحايل على المعايير القانونية الوطنية والضوابط المؤسسية المفروضة على أنشطتها. وعندما تطلب دول من أجهزة استخبارات أجنبية الاضطلاع بأنشطة لصالحها، فإنها تقتضي من هذه الأجهزة

<sup>169</sup> 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.

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

<sup>171</sup> Germany (footnote 106), sect. 7a (5-6); Croatia, Act on Personal Data Protection, art. 34.

الامتثال للمعايير القانونية نفسها التي تطبق في حالة اضطلاع أجهزة الاستخبارات التابعة لها بهذه الأنشطة.

٥٠ - تنص القوانين الوطنية المنظمة لأنشطة أجهزة الاستخبارات على ضمانات قانونية ومؤسسية لحماية حقوق الإنسان والنظام القانوني الدستوري في سياق الأنشطة الاستخباراتية. وبالنظر إلى هذا، فإن من المخالف لسيادة القانون أن تطلب الدول أو أجهزة الاستخبارات التابعة لها من كيان أجنبي الاضطلاع بأنشطة في نطاق ولايتها لا يمكنها هي ذاتها الاضطلاع بها على نحو مشروع. وستكون ممارسة جيدة أن يتضمن القانون الوطني فرض حظر تام على تعاون أجهزة الاستخبارات مع كيانات أجنبية بهدف تفادي الالتزامات القانونية التي تطبق على أنشطتها<sup>(١٧٣)</sup>. وعلاوة على ذلك، فإن من المهم الإشارة إلى أن الدول يقع عليها التزام قانوني دولي بضمان حقوق جميع الأفراد الخاضعين لولايتها. ويعني هذا ضمناً أن عليها واجباً يقتضي منها ضمان ألا تنخرط أجهزة الاستخبارات الأجنبية في أنشطة تنتهك حقوق الإنسان على أراضيها، وأن تجزم عن المشاركة في أي أنشطة من هذا القبيل<sup>(١٧٣)</sup>. والواقع أن الدول تتحمل المسؤولية دولياً إذا عاونت أو ساعدت دولة أخرى على انتهاك حقوق الإنسان المكفولة للأفراد<sup>(١٧٤)</sup>.

<sup>172</sup> 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.

<sup>173</sup> 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.

<sup>174</sup> 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.

## Annex

### **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.