



Asamblea General

Distr. general
17 de mayo de 2010
Español
Original: inglés

Consejo de Derechos Humanos

14º período de sesiones

Tema 3 de la agenda

Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*

Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión**

Resumen

El presente documento es una recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión; esta recopilación fue solicitada por el Consejo de Derechos Humanos y ha sido preparada por el Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo. La recopilación estuvo precedida por un proceso de consultas en el que participaron gobiernos, expertos y profesionales por diversos conceptos. En particular, se han tenido en cuenta las comunicaciones recibidas de los gobiernos hasta el plazo fijado del 1º de mayo de 2010. Las comunicaciones se incluirán en una adición (A/HRC/14/46/Add.1).

* Documento presentado con retraso.

** Dado que el informe supera con creces el número máximo de páginas prescrito actualmente por las resoluciones pertinentes de la Asamblea General, el anexo del informe y las notas se reproducen en el idioma del original.

Al término del proceso se identificaron 35 buenas prácticas, derivadas de prácticas arraigadas, o de reciente introducción, en una amplia variedad de Estados de todo el mundo. La recopilación se basa también en tratados internacionales, resoluciones de organizaciones internacionales y la jurisprudencia de los tribunales regionales.

En el comentario que acompaña a cada una de las 35 buenas prácticas presentadas se explican sus características sustanciales. El origen de las buenas prácticas se indica en las notas de pie de página a los comentarios, que incluyen referencias a los distintos Estados.

La noción de "buenas prácticas" está vinculada a los marcos jurídicos e institucionales que sirven para promover los derechos humanos y el respeto por el estado de derecho en la labor de los servicios de inteligencia. Este concepto no se limita a las prescripciones del derecho internacional, incluida la normativa de los derechos humanos, sino que va más allá de estas normas de obligado cumplimiento.

Las 35 buenas prácticas incluidas en la recopilación se dividen en cuatro ámbitos de aplicación, a saber, base jurídica (prácticas 1 a 5), supervisión y rendición de cuentas (prácticas 6 a 10 y 14 a 18), observancia de los derechos humanos sustantivos (prácticas 11 a 13 y 19 y 20) y cuestiones relacionadas con las funciones específicas de los organismos de inteligencia (prácticas 21 a 35).

Índice

	<i>Párrafos</i>	<i>Página</i>
I. Introducción	1–8	4
II. Recopilación de las buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional para los servicios de inteligencia y su supervisión	9–50	5
A. Mandato y base jurídica.....	9–12	5
B. Instituciones de supervisión.....	13–15	8
C. Denuncias y reparación efectiva.....	16–17	11
D. Imparcialidad y no discriminación	18–20	13
E. Responsabilidad del Estado respecto de la acción de los servicios de inteligencia.....	21	14
F. Responsabilidad individual y rendición de cuentas	22–25	15
G. Profesionalidad	26	18
H. Salvaguardias de los derechos humanos	27–33	19
I. Recopilación de información.....	34–36	21
J. Gestión y utilización de datos personales	37–40	23
K. El ejercicio de las facultades de arresto y detención.....	41–44	26
L. Intercambio de información y cooperación	45–50	29
 Anexo		
Good practices on legal and institutional frameworks for intelligence services and their oversight		33

I. Introducción*

1. La presente recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional para los servicios de inteligencia, particularmente en lo respecta a su supervisión, es resultado de un proceso de consulta encomendado por el Consejo de Derechos Humanos que, en su resolución 10/15, pidió al Relator Especial que, en consulta con los Estados y otros interesados, hiciera una recopilación de las buenas prácticas referentes a los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión.

2. Los servicios de inteligencia¹ desempeñan un papel fundamental en la protección de los Estados y sus poblaciones contra las amenazas a la seguridad nacional, incluido el terrorismo. Gracias a estos servicios los Estados pueden cumplir su obligación de salvaguardar los derechos humanos de todos los individuos bajo su jurisdicción. De ahí que un funcionamiento eficaz y la protección de los derechos humanos puedan ser objetivos mutuamente complementarios de los servicios de inteligencia.

3. La recopilación se ha derivado de prácticas arraigadas, o de reciente introducción, en una amplia variedad de Estados de todo el mundo. Esas prácticas se han extraído principalmente de las leyes nacionales, los modelos institucionales y la jurisprudencia y las recomendaciones de las instituciones nacionales de supervisión y de un cierto número de organizaciones de la sociedad civil. La recopilación se ha basado también en los tratados internacionales, las resoluciones de las organizaciones internacionales y la jurisprudencia de los tribunales nacionales. En este contexto, la noción de "buenas prácticas" está vinculada a los marcos jurídicos e institucionales que sirven para promover los derechos humanos y el respeto al estado de derecho en la labor de los servicios de inteligencia. Este concepto no se limita a las prescripciones del derecho internacional, incluida la normativa de los derechos humanos, sino que va más allá de estas normas de obligado cumplimiento.

4. Muy pocos Estados han incluido todas las prácticas que se describen a continuación en sus marcos jurídicos e institucionales para los servicios de inteligencia y su supervisión. Algunos Estados constatarán que ya aplican la mayoría de las 35 buenas prácticas indicadas. Otros podrán comprometerse en un principio a aplicar unas pocas prácticas que consideren esenciales para promover la observancia de los derechos humanos por parte de los servicios de inteligencia y sus órganos de supervisión.

5. La presente recopilación no tiene por objeto promulgar un conjunto de normas reglamentarias que sean de aplicación en todo momento y lugar. Por esta razón las buenas prácticas descritas en el presente informe no se formulan en términos normativos, sino

* El Relator Especial desea expresar su reconocimiento por la contribución de Hans Born y Aidan Wills, del Centro de Ginebra para el Control Democrático de las Fuerzas Armadas, que realizaron un estudio de referencia y contribuyeron a la preparación de la presente recopilación. Además, el Relator Especial expresa su gratitud a los gobiernos, a los miembros de instituciones de supervisión de los servicios de inteligencia, a (ex) funcionarios de inteligencia, a expertos en inteligencia y derechos humanos y a miembros de organizaciones de la sociedad civil, por su participación en el proceso de consulta que precedió a la presente recopilación.

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

descriptivos. No obstante, es posible identificar las prácticas comunes que contribuyen al respeto del estado de derecho y los derechos humanos por los servicios de inteligencia.

6. El Consejo de Derechos Humanos encargó la realización de la presente recopilación de buenas prácticas en relación con la lucha que libran los servicios de inteligencia contra el terrorismo. Sin embargo, debe observarse que no cabe hacer una distinción entre los marcos jurídicos e institucionales aplicables a las actividades de lucha contra el terrorismo de los servicios de inteligencia, y los que rigen para las actividades de esos servicios más en general. Aunque el terrorismo internacional ha cambiado las condiciones en que funcionan los organismos de inteligencia desde 2001, los efectos de este cambio van más allá de la lucha contra el terrorismo.

7. La recopilación contiene ejemplos de buenas prácticas extraídos de numerosas leyes nacionales y modelos institucionales. Empero, es importante observar que la cita de disposiciones concretas de leyes generales o de modelos institucionales no entraña la aceptación general de esas leyes o instituciones como buenas prácticas para la protección de los derechos humanos en la lucha contra el terrorismo. Además, el Relator Especial desea recalcar que la existencia de marcos jurídicos o institucionales que representen buenas prácticas es una condición fundamental, pero no suficiente, para garantizar el respeto de los derechos humanos por los servicios de inteligencia en sus actividades de lucha contra el terrorismo.

8. Las 35 buenas prácticas descritas a continuación se dividen en cuatro ámbitos de aplicación, a saber, base jurídica (1 a 5), supervisión y rendición de cuentas (6 a 10, 14 a 18), observancia de los derechos humanos sustantivos (11 a 13, 19 y 20) y cuestiones relacionadas con las funciones específicas de los organismos de inteligencia (21 a 35). Con miras a mejorar la presentación, las buenas prácticas se han agrupado bajo un número algo mayor de epígrafes.

II. Recopilación de las buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional para los servicios de inteligencia y su supervisión

A. Mandato y base jurídica

Práctica 1. Los servicios de inteligencia desempeñan un papel importante en la protección de la seguridad nacional y la defensa del estado de derecho. Su principal objetivo consiste en recopilar, analizar y difundir información que ayude a los responsables de las políticas y a otras entidades públicas a tomar disposiciones de protección de la seguridad nacional; en este último concepto está incluida la protección de la población y de sus derechos humanos.

9. Los servicios de inteligencia no desempeñan las mismas funciones en todos los países. Con todo, la recopilación, análisis y difusión de información pertinente para la protección de la seguridad nacional es una tarea fundamental de la mayor parte de estos servicios², y muchos Estados limitan la función de sus servicios de inteligencia a esta tarea.

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

Esto supone una buena práctica, porque impide que los servicios de inteligencia se dediquen a actividades relacionadas con la seguridad que ya son de la incumbencia de otros organismos públicos y que, si corrieran por cuenta de los mencionados servicios, podrían poner en peligro los derechos humanos. Además de definir los tipos de actividades que sus servicios de inteligencia pueden llevar a cabo, muchos Estados limitan la justificación de esas actividades a la protección de la seguridad nacional. Aunque no todos los Estados tienen una misma idea de la seguridad nacional, es de buena práctica que la seguridad nacional y sus valores constitutivos se definan con claridad en las leyes que aprueba el parlamento³. Esto es importante para garantizar que los servicios de inteligencia limiten sus actividades a la salvaguardia de los valores enunciados en la definición pública de la seguridad nacional. En muchos casos, la salvaguardia de la seguridad nacional incluye necesariamente la protección de la población y sus derechos humanos⁴; es más, algunos Estados incluyen explícitamente la protección de los derechos humanos entre las funciones principales de sus servicios de inteligencia⁵.

Práctica 2. Los mandatos de los servicios de inteligencia deben estar definidos con rigor y precisión en una ley a la que el público tenga acceso. Los mandatos deben limitarse estrictamente a proteger los intereses legítimos de la seguridad nacional, definidos en leyes o políticas de seguridad nacional a las que el público tenga acceso y a identificar las amenazas a la seguridad nacional que los servicios de inteligencia tienen que combatir. Si el terrorismo figura entre estas amenazas, deberá definirse con rigor y precisión.

10. El mandato de los servicios de inteligencia es uno de los instrumentos principales para garantizar que las actividades de esos servicios (incluidas las de la lucha contra el terrorismo) sirven a los intereses del país y de su población y no representan una amenaza para el orden constitucional ni para los derechos humanos. En la mayoría de los Estados, el mandato de los servicios de inteligencia está claramente definido en una ley promulgada por el Parlamento, a la que el público tiene acceso⁶. Es de buena práctica que el mandato estén formulados con rigor y precisión, y enumeren todas las amenazas contra la seguridad nacional que los servicios de inteligencia tienen la responsabilidad de combatir⁷. Un mandato claro y preciso facilita los procesos de responsabilización y permite que los servicios de inteligencia rindan cuenta del desempeño de sus funciones específicas a los organismos encargados de la supervisión o el examen. Por último, una definición clara de las amenazas es especialmente oportuna en el contexto de la lucha contra el terrorismo;

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

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

⁵ 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).

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

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

muchos Estados han adoptado leyes que contienen definiciones precisas del terrorismo, así como de los grupos y actividades terroristas⁸.

Práctica 3. Las facultades y competencias de los servicios de inteligencia han de estar definidas de modo claro y exhaustivo en la legislación nacional. Estos servicios están obligados a ejercer sus facultades con la finalidad exclusiva para la que les fueron conferidas. En particular, todas las facultades conferidas a los servicios de inteligencia para los fines de la lucha contra el terrorismo deben ejercerse exclusivamente con esos fines.

11. Un principio fundamental del estado de derecho es que todas las facultades y competencias de los servicios de inteligencia han de estar definidas en la legislación⁹. Una enumeración exhaustiva de las facultades y competencias de los servicios de inteligencia favorece la transparencia y permite que la población prevea cuáles de esas facultades podrían utilizarse en su contra. Esto es especialmente importante, porque muchas de las facultades conferidas a los servicios de inteligencia encierran el potencial necesario para vulnerar los derechos humanos y las libertades fundamentales¹⁰. Esta práctica está estrechamente relacionada con la práctica 2, porque el mandato de los servicios de inteligencia sirve para definir el marco en el cual esos servicios podrán ejercer las facultades que les ha conferido el poder legislativo¹¹. Las leyes de muchos Estados prohíben implícitamente la desviación de poder al autorizar a los servicios de inteligencia a ejercer sus facultades con fines muy específicos. Éste es el caso de las actividades de la lucha contra el terrorismo, porque muchos servicios de inteligencia han recibido mayores facultades con esos fines.

Práctica 4. Todos los servicios de inteligencia están constituidos en virtud de leyes a las que el público tiene acceso y que respetan las disposiciones de la Constitución y la normativa internacional de derechos humanos, y funcionan con arreglo a esas leyes. Los servicios de inteligencia sólo pueden emprender actividades, o recibir instrucciones de emprenderlas, que estén contempladas en la legislación nacional y sean conformes con ella. La aplicación de reglamentos subsidiarios está estrictamente limitada y sujeta a las disposiciones de leyes a las que sí tiene acceso el público. Los reglamentos que no se pongan en conocimiento del público no sirven de base para ninguna actividad que coarte los derechos humanos.

Práctica 5. Los servicios de inteligencia tienen prohibido explícitamente emprender cualquier actividad contraria a la Constitución o a la normativa internacional de los derechos humanos. Esta prohibición rige no sólo para el comportamiento de los servicios de inteligencia en el territorio nacional, sino también para sus actividades en el extranjero.

12. Los servicios de inteligencia son órganos del Estado y, en consecuencia, deben cumplir, al igual que otros organismos ejecutivos, las disposiciones pertinentes del derecho

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

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

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

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

nacional e internacional, y en particular la normativa de los derechos humanos¹². Esto significa que estos servicios están basados en leyes a las que el público tiene acceso y que son conformes con la Constitución y con las obligaciones internacionales del Estado en materia de derechos humanos, entre otras, y que su funcionamiento es acorde con esas leyes. Los Estados no pueden invocar el derecho interno para justificar violaciones de la normativa internacional de los derechos humanos ni, evidentemente, de cualquier otra obligación jurídica internacional¹³. El estado de derecho exige que las actividades de los servicios de inteligencia, y cualquier instrucción que les imparta el poder ejecutivo, cumplan esos conjuntos normativos¹⁴. En consecuencia, los servicios de inteligencia tienen prohibido emprender cualquier acción que vulnere las leyes nacionales, la Constitución o las obligaciones del Estado en materia de derechos humanos, y también está prohibido darles instrucciones en este sentido. En muchos Estados estas prescripciones son implícitas. Sin embargo, es evidentemente de buena práctica que la legislación nacional haga referencia explícita a estas obligaciones jurídicas más amplias y, en particular, a la obligación de respetar los derechos humanos¹⁵. A veces los reglamentos subsidiarios relativos a procesos internos y a actividades de los servicios de inteligencia no se dan a conocer al público, para proteger los métodos de trabajo de esos servicios. Estos reglamentos no han de servir de base para actividades que vulnere los derechos humanos. Es de buena práctica que toda reglamentación subsidiaria se base en leyes vigentes a las que el público tenga acceso, y cumpla dichas leyes¹⁶.

B. Instituciones de supervisión

Práctica 6. Los servicios de inteligencia están supervisados por un conjunto de instituciones de supervisión internas, ejecutivas, parlamentarias, judiciales y especializadas, cuyos mandatos y facultades se basan en leyes a las que el público tiene acceso. Un sistema efectivo de supervisión de los servicios de inteligencia incluye por lo menos una institución civil independiente de los servicios de inteligencia y del poder ejecutivo. El mandato combinado de las instituciones de supervisión abarca todos los aspectos de la labor de los servicios de inteligencia, con inclusión de su observancia de la ley, la eficacia y eficiencia de sus actividades, su situación financiera y sus prácticas administrativas.

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

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

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

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

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

13. Al igual que los servicios de inteligencia, las instituciones que supervisan las actividades de éstos están basadas en la ley, y en algunos casos en la Constitución¹⁷. No hay un modelo único para la supervisión de los servicios de inteligencia; no obstante, los elementos que se indican a continuación suelen formar parte de los sistemas más amplios de supervisión¹⁸: mecanismos de gestión y control internos en los servicios de inteligencia¹⁹; supervisión del poder ejecutivo²⁰; supervisión de los organismos parlamentarios²¹, y órganos de supervisión especializados y/o judiciales²². Es de buena práctica que este sistema de supervisión a múltiples niveles incluya al menos una institución que sea plenamente independiente de los servicios de inteligencia y del poder ejecutivo. Este principio garantiza la separación de los poderes en la supervisión de los servicios de inteligencia: las instituciones que encargan y realizan las actividades de inteligencia, y reciben sus resultados, no son las únicas que supervisan estas actividades. Todas las dimensiones de la labor de los servicios de inteligencia están sujetas a la supervisión de una institución externa, o un conjunto de instituciones externas. Una de las funciones primordiales de un sistema de supervisión consiste en verificar que los servicios de inteligencia cumplan las leyes vigentes, así como las normas de derechos humanos. Las instituciones de supervisión piden cuentas a los servicios de inteligencia y a sus empleados por cualquier violación de la ley²³; además, esas instituciones evalúan el rendimiento de los servicios de inteligencia²⁴. En el contexto de esta última actividad, las instituciones de supervisión verifican si los servicios de inteligencia utilizan de manera eficiente y eficaz los

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

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

¹⁹ For an elaboration on internal management and control mechanisms, see South African Ministerial Review Committee, p. 204; European Commission for Democracy through Law, report on the democratic oversight of the security services, CDL-AD(2007), point 131 (hereafter Venice Commission (2007)); OECD DAC handbook on security system reform: supporting security and justice; United Kingdom, Intelligence Security Committee, annual report 2001–2002, p. 46. See also The former Yugoslav Republic of Macedonia (reply).

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

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

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

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

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

fondos públicos que se les asignan²⁵. Un sistema eficaz de supervisión es especialmente importante para los servicios de inteligencia, porque gran parte de la labor de esos servicios es secreta y, por consiguiente, no se presta fácilmente a la verificación pública. Las instituciones de supervisión de los servicios de inteligencia mejoran la confianza del público en la labor de estos servicios, al garantizar que respeten el estado de derecho y los derechos humanos en el desempeño de sus funciones reglamentarias²⁶:

Práctica 7. Las instituciones de supervisión disponen de las facultades, recursos y conocimientos técnicos suficientes para iniciar y llevar a cabo sus propias investigaciones, así como un acceso completo y sin trabas a la información, los funcionarios y las instalaciones necesarias para cumplir sus mandatos, y gozan de la plena cooperación de los servicios de inteligencia y las autoridades encargadas de hacer cumplir la ley en el interrogatorio de los testigos, así como para obtener documentación y otros elementos probatorios.

14. Las instituciones de supervisión gozan de facultades específicas para el desempeño de sus funciones. En particular, están facultadas a iniciar sus propias investigaciones sobre los aspectos de la labor de los servicios de inteligencia que están incluidos en sus mandatos, y tienen acceso a toda la información necesaria para ello. Entre estas facultades de acceso a la información figura la autoridad legal para consultar todos los archivos y documentos pertinentes²⁷, inspeccionar los locales de los servicios de inteligencia²⁸ y convocar a cualquier miembro de estos servicios para que testimonie bajo juramento²⁹. Gracias a estas facultades, los supervisores pueden examinar eficazmente las actividades de los servicios de inteligencia e investigar en detalle los posibles incumplimientos de la ley. Varios Estados han tomado las disposiciones necesarias para reforzar las competencias investigadoras de las instituciones de supervisión, tipificando como delito la no colaboración con las mismas³⁰. Esto significa que las instituciones de supervisión recurren a las autoridades judiciales para obtener la cooperación de las personas pertinentes³¹. Si bien la posesión de facultades bien definidas en el plano jurídico es esencial para llevar a cabo una supervisión eficaz, conviene que esas facultades estén complementadas con los recursos humanos y financieros necesarios para ejercerlas, a fin de que las instituciones puedan cumplir su mandato. En consecuencia, muchas instituciones de supervisión cuentan con su propio presupuesto independiente que les facilita directamente el parlamento³², y disponen de la capacidad de emplear a personal especializado³³ y contratar a expertos externos³⁴.

²⁵ Romania (footnote 2), art. 42.

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

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

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

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

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

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

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

³³ Canada (footnote 6), sect. 36.

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

Práctica 8. Las instituciones de supervisión toman todas las medidas necesarias para proteger la información confidencial y los datos personales a los que tengan acceso en el ejercicio de sus funciones. Se prevén sanciones para los miembros de las instituciones de supervisión que incumplan estos requisitos.

15. En el ejercicio de sus funciones, las instituciones de supervisión de los servicios de inteligencia tienen acceso a información confidencial y de carácter delicado. Por consiguiente, se han arbitrado diversos mecanismos para garantizar que estas instituciones, y sus miembros, no revelen esta información, deliberadamente o por inadvertencia. En primer lugar, en casi todos los casos, los miembros y el personal de las instituciones de supervisión tienen prohibido hacer revelaciones no autorizadas de información; el incumplimiento de estas disposiciones suele sancionarse con penas civiles y/o penales³⁵. En segundo lugar, muchas instituciones de supervisión aplican a sus miembros y al personal procedimientos de control de la seguridad antes de darles acceso a información confidencial³⁶. Otro procedimiento opcional, practicado comúnmente en las instituciones parlamentarias de supervisión, es que los miembros firmen un acuerdo comprometiéndose a no revelar la información³⁷. Por último, el manejo adecuado de la información confidencial por las instituciones de supervisión también depende de la profesionalidad de los miembros de esas instituciones.

C. Denuncias y reparación efectiva

Práctica 9. Toda persona que crea que sus derechos han sido vulnerados por un servicio de inteligencia puede presentar una denuncia ante un tribunal o una institución de supervisión como el defensor del pueblo, el comisionado de derechos humanos o una institución nacional de derechos humanos. Las personas afectadas por acciones ilegales de un servicio de inteligencia pueden elevar un recurso a una institución en condiciones de proporcionarle una reparación efectiva, como la plena compensación por los daños sufridos.

16. Es un hecho ampliamente reconocido que toda medida que coarte los derechos humanos debe ir acompañada de las adecuadas salvaguardias; entre éstas se cuentan las instituciones independientes por conducto de las cuales las personas pueden buscar reparación cuando se hayan vulnerado sus derechos³⁸. Los servicios de inteligencia poseen una variedad de facultades —de vigilancia, arresto y detención, entre otras— que, si se ejercen indebidamente, pueden violar derechos humanos. En consecuencia, existen instituciones encargadas de tramitar las denuncias de personas que creen que sus derechos han sido violados por los servicios de inteligencia y, cuando sea menester, proporcionar a

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

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

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

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

las víctimas de estos actos una reparación efectiva. A este respecto pueden distinguirse dos amplios planteamientos³⁹. El primero es el de los Estados que han establecido una serie de instituciones no judiciales encargadas de tramitar las denuncias contra los servicios de inteligencia, a saber: el Defensor del Pueblo⁴⁰; comisiones nacionales de derechos humanos⁴¹; auditoría nacional⁴²; organismos parlamentarios de supervisión⁴³; inspección general⁴⁴; organismos especializados de supervisión de los servicios de inteligencia⁴⁵, y comisiones de reclamaciones a los servicios de inteligencia⁴⁶. Estas instituciones están facultadas a recibir e investigar denuncias; sin embargo, dado que por lo general no pueden dictar órdenes de obligado cumplimiento ni proporcionar reparaciones, las víctimas de violaciones de derechos humanos tienen que recurrir a los tribunales para obtener estas reparaciones. El segundo consiste en que las instituciones judiciales pueden recibir denuncias contra los servicios de inteligencia. Estas instituciones, que pueden ser organismos judiciales creados con este fin específico⁴⁷ o formar parte del sistema judicial general, de ordinario están facultadas a ordenar medidas de reparación.

Práctica 10. Las instituciones encargadas de tramitar las denuncias o las solicitudes de una reparación efectiva como consecuencia de actividades de los servicios de inteligencia son independientes de estos servicios y del poder ejecutivo. Estas instituciones tienen un acceso pleno y sin trabas a toda la información pertinente y disponen de los recursos y servicios técnicos necesarios para realizar las investigaciones, y de la capacidad de dictar órdenes de obligado cumplimiento.

17. Para que pueda proporcionar una reparación efectiva a las violaciones de los derechos humanos, una institución ha de ser independiente de las instituciones participantes en las actividades denunciadas, ser capaz de garantizar la equidad procesal, disponer de capacidades y técnicas de investigación suficientes, y estar facultada a dictar decisiones de obligado cumplimiento⁴⁸. Por este motivo, los Estados han dotado a esas instituciones de las facultades jurídicas necesarias para investigar las denuncias y proporcionar reparación a las víctimas de las violaciones de los derechos humanos cometidas por los servicios de inteligencia. Entre estas facultades figuran el acceso pleno y sin trabas a toda la información pertinente, la capacidad de convocar a testigos en el curso de la investigación y de recibir testimonio bajo juramento⁴⁹, la facultad de determinar sus propios procedimientos

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

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

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

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

⁴³ Romania (footnote 15), art. 16.

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

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

⁴⁶ Kenya (footnote 16), arts. 24-26.

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

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

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

en relación con cualquier actuación y la capacidad de dictar órdenes de obligado cumplimiento⁵⁰.

D. Imparcialidad y no discriminación

Práctica 11. En el desempeño de sus actividades, los servicios de inteligencia contribuyen a la promoción y la protección de los derechos humanos y las libertades fundamentales de todas las personas bajo la jurisdicción del Estado. Los servicios de inteligencia no discriminan a personas o grupos por motivos de sexo, raza, color, idioma, religión, opiniones políticas o de cualquier índole, origen nacional o social o cualquier otra condición social.

18. Los servicios de inteligencia forman parte integrante del aparato estatal que contribuye a salvaguardar los derechos humanos de todas las personas bajo la jurisdicción del Estado. Estos servicios están obligados por el bien conocido principio de no discriminación, de la normativa internacional de los derechos humanos. Este principio exige que los Estados respeten los derechos y libertades de las personas sin discriminación alguna por cualquier motivo prohibido⁵¹. Muchos Estados han enunciado este principio en sus leyes nacionales, y exigen a sus servicios de inteligencia que cumplan sus mandatos de modo que sirvan a los intereses del Estado y de la sociedad en general. Los servicios de inteligencia tienen prohibido explícitamente actuar o ser utilizados de un modo que promueva los intereses de cualquier grupo étnico, religioso, político o de otra índole⁵². Además, los Estados deben asegurar que las actividades de sus servicios de inteligencia (en particular en el contexto de la lucha contra el terrorismo) se basan en el comportamiento de los individuos, y no en su etnia, religión u otro criterio análogo⁵³. Algunos Estados han prohibido explícitamente a sus servicios de inteligencia la constitución de archivos individuales, sobre esta base⁵⁴.

Práctica 12. Las leyes nacionales prohíben a los servicios de inteligencia dedicarse a cualquier actividad política o tomar medidas destinadas a promover o proteger los intereses de cualquier grupo político, religioso, lingüístico, étnico, social o económico.

19. Los servicios de inteligencia están dotados de facultades que podrían beneficiar, o bien dañar, los intereses de ciertos grupos políticos. A fin de garantizar la neutralidad política de los servicios de inteligencia, las leyes nacionales prohíben a esos servicios actuar en interés de cualquier grupo político⁵⁵. Esta obligación es válida no sólo para los servicios de inteligencia sino también para los poderes ejecutivos a los que sirven. Varios Estados han adoptado disposiciones para prohibir o limitar la participación de los servicios de inteligencia en la política de partidos, como por ejemplo la prohibición de que los empleados de los servicios de inteligencia sean miembros de partidos políticos, acepten

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

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

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

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

⁵⁴ Argentina (footnote 2), art. 4.

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

instrucciones o dinero de un partido político⁵⁶, o actúen en favor de los intereses de un partido político en particular⁵⁷. Además, varios Estados han tomado disposiciones para salvaguardar la neutralidad de los directores de los servicios de inteligencia, previendo entre otras cosas que el nombramiento del director de un servicio de inteligencia pueda ser verificado por instancias ajenas al poder ejecutivo⁵⁸; y que haya disposiciones jurídicas que regulen la duración del mandato y especifiquen los motivos para la destitución del titular, así como salvaguardias contra la aplicación de presiones indebidas a los directores de los servicios de inteligencia⁵⁹.

Práctica 13. Los servicios de inteligencia tienen prohibido ejercer sus facultades en relación con una actividad política legítima u otra manifestación legal de los derechos a la libertad de asociación, reunión pacífica y expresión.

20. Las actividades de recopilación de información de los servicios de inteligencia pueden interferir en la acción política legítima y en otras manifestaciones de las libertades de expresión, asociación y reunión⁶⁰. Estos derechos son fundamentales para el funcionamiento de una sociedad libre, en el que participan los partidos políticos, los medios de comunicación y la sociedad civil. Por consiguiente, los Estados han adoptado disposiciones para reducir la medida en que los servicios de inteligencia pueden elegir como blanco de sus operaciones (o la medida en que se les puede pedir que lo hagan) a personas o grupos dedicados a estas actividades. Estas disposiciones comprenden la prohibición absoluta de centrar sus operaciones en actividades legítimas, y limitaciones estrictas al uso de medidas de recopilación de información (véase la práctica 21) y a la retención y el uso de los datos personales recopilados por los servicios de inteligencia (véase la práctica 23)⁶¹. En vista del papel fundamental que desempeñan los medios de comunicación en cualquier sociedad, algunos Estados han arbitrado medidas concretas para proteger a los periodistas de la acción de los servicios de inteligencia⁶².

E. Responsabilidad del Estado respecto de la acción de los servicios de inteligencia

Práctica 14. Los Estados son internacionalmente responsables de las actividades de sus servicios y agentes de inteligencia y cualquier contratista privado que contraten, independientemente del lugar en que tengan lugar estas actividades o de quien sea la víctima de un hecho internacionalmente ilícito. Por consiguiente, el poder ejecutivo

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

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

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

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

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

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

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

se hace responsable de la acción de los servicios de inteligencia, y ejerce el control general de estos servicios.

21. Con arreglo al derecho internacional, los Estados son responsables de las actividades de sus servicios y agentes de inteligencia en cualquier lugar del mundo en que realicen sus operaciones. Esta responsabilidad comprende la acción de los contratistas privados que los Estados contraten para llevar a cabo actividades de inteligencia⁶³. Los Estados están legalmente obligados a garantizar que sus servicios de inteligencia no violen los derechos humanos, y a proporcionar reparaciones a las víctimas de estas violaciones⁶⁴. En consecuencia, los Estados toman disposiciones para regular y gestionar sus servicios de inteligencia de un modo que promueva el respeto por el estado de derecho y, en particular, el cumplimiento de la normativa internacional de los derechos humanos⁶⁵. El control de los servicios de inteligencia por parte del poder ejecutivo es esencial con este fin y, muchas leyes nacionales lo enuncian en consecuencia⁶⁶.

F. Responsabilidad individual y rendición de cuentas

Práctica 15. Las disposiciones de la Constitución, los reglamentos y el derecho penal internacional rigen para los miembros de los servicios de inteligencia como para cualquier otro funcionario público. Toda excepción que permita a los funcionarios de los servicios de inteligencia tomar medidas que en condiciones normales violarían la legislación nacional está estrictamente limitada y claramente definida por la ley. Estas excepciones no permiten en ningún caso vulnerar las normas imperativas del derecho internacional o las obligaciones del Estado en materia de derechos humanos.

22. Aunque las responsabilidades institucionales de los servicios de inteligencia revisten gran importancia, los miembros de estos servicios también son responsables a título individual y deben responder de sus acciones⁶⁷. Por regla general, la Constitución, los reglamentos y el derecho penal internacional rigen para los miembros de los servicios de inteligencia como para cualquier otra persona⁶⁸. Muchos Estados han decretado la responsabilidad civil de todo miembro de un servicio de inteligencia que viole a sabiendas la Constitución o la ley civil u ordene o solicite la adopción de una medida que las viole, o han tipificado como delito esta violación⁶⁹. De esta manera se promueve el respeto por el estado de derecho en los servicios de inteligencia, y se combate la impunidad. Muchos

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

⁶⁴ Croatia (footnote 2), art. 87(1); Human Rights Committee, general comment no. 31 on the nature of the general legal obligations imposed on States parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 4; Michael Defeo, "What international law controls exist or should exist on intelligence operations and their intersects 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.

⁶⁵ E/CN.4/2005/102/Add.1, art. 36.

⁶⁶ See also practice 6.

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

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

⁶⁹ Morton Halperin, "Controlling the intelligence agencies", *First Principles*, vol. 1, No. 2, October 1975.

Estados autorizan a los miembros de sus servicios de inteligencia a realizar actividades que, si las llevasen a cabo los ciudadanos comunes, serían constitutivas de delito⁷⁰. Es de buena práctica que estas autorizaciones se limiten estrictamente, sean prescritas por la ley y estén sujetas a las salvaguardias pertinentes⁷¹. Las disposiciones legales que autorizan a los funcionarios de los servicios de inteligencia a llevar a cabo actos que en condiciones normales y con arreglo a la legislación nacional serían ilegales no pueden hacerse extensivas a ninguna acción que viole la Constitución o la normativa internacional no derogable de los derechos humanos⁷².

Práctica 16. La legislación nacional prevé sanciones penales, civiles o de otro tipo para cualquier miembro de los servicios de inteligencia, o persona que actúe en nombre de estos servicios, que viole la legislación nacional o la normativa internacional de los derechos humanos, o que ordene una medida que las viole. Las leyes prevén además procedimientos para que las personas puedan responder de estas violaciones.

23. Los Estados se aseguran de que los empleados de los servicios de inteligencia respondan de las violaciones de la ley, previendo y aplicando sanciones para determinados delitos. Esto contribuye a promover el respeto por el estado de derecho y los derechos humanos en los servicios de inteligencia. Muchas leyes nacionales que regulan los servicios de inteligencia prevén sanciones específicas para los empleados que violen esas leyes u otras disposiciones aplicables de la legislación nacional o el derecho internacional⁷³. Dado que muchas de las actividades de los servicios de inteligencia son de carácter secreto, es posible que las autoridades judiciales competentes no detecten los delitos (cometidos por empleados). Por consiguiente, es de buena práctica que la legislación nacional exija a la administración de los servicios de inteligencia que someta los casos de posibles actos delictivos a las autoridades judiciales⁷⁴. Cuando miembros de los servicios de inteligencia cometan violaciones graves de los derechos humanos, como torturas, los Estados tienen la obligación legal internacional de procesar a estas personas⁷⁵. La responsabilidad penal de los empleados de los servicios de inteligencia no sólo se deriva de su participación directa en las actividades de que se trate, sino también de que hayan ordenado tales actividades, o hayan sido cómplices en las mismas por otros conceptos⁷⁶.

Práctica 17. Los miembros de los servicios de inteligencia están legalmente obligados a negarse a obedecer las órdenes de sus superiores que violarían la legislación nacional o la normativa internacional de los derechos humanos. Se prevé la protección adecuada para los miembros de los servicios de inteligencia que se nieguen a obedecer órdenes en estos casos.

24. Es de buena práctica que la legislación nacional exija a los miembros de los servicios de inteligencia que se nieguen a obedecer órdenes que, a su juicio, violarían la

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

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

⁷² Netherlands (footnote 20), annex.

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

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

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

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

legislación nacional o la normativa internacional de derechos humanos⁷⁷. Si bien esta disposición es más habitual en las leyes aplicables a las fuerzas armadas, varios Estados la han incluido en los reglamentos de sus servicios de inteligencia⁷⁸. La obligación de los miembros de los servicios de inteligencia de negarse a obedecer órdenes ilegales es una salvaguardia importante contra posibles abusos de los derechos humanos, así como contra las órdenes que imparten los gobiernos en ejercicio para promover o proteger sus intereses propios. Un principio acreditado del derecho internacional es que los individuos no están exentos de responsabilidad penal por las violaciones graves de los derechos humanos que hayan cometido en cumplimiento de la orden de un superior⁷⁹. Por consiguiente, para eludir la responsabilidad penal individual, los miembros de los servicios de inteligencia están obligados a negarse a obedecer cualquier orden que, a su leal saber y entender, sea manifiestamente ilegítima. Esto pone de relieve la importancia de la formación en derechos humanos de los funcionarios de los servicios de inteligencia, que han de ser conscientes de los derechos y obligaciones que les incumben en virtud del derecho internacional (véase la práctica 19). Para promover la no tolerancia de los abusos de los derechos humanos, los Estados ofrecen protección jurídica contra represalias a los miembros de los servicios de inteligencia que se nieguen a obedecer órdenes ilegales⁸⁰. La obligación de negarse a obedecer órdenes ilegales está estrechamente vinculada con la existencia de mecanismos internos o externos que permitan a los empleados de los servicios de inteligencia dar a conocer sus temores acerca de las eventuales órdenes ilegales (véase la práctica 18 *infra*).

Práctica 18. Existen procedimientos internos para que los miembros de los servicios de inteligencia puedan denunciar los hechos ilícitos. Estos procedimientos están complementados por la acción de un organismo independiente que tiene el mandato de investigar a fondo los hechos ilícitos y tomar disposiciones para repararlos cuando los procedimientos internos hayan resultado inadecuados, y el acceso a la información necesaria para ello. Los miembros de los servicios de inteligencia que, actuando de buena fe, denuncien un hecho ilícito, están protegidos legalmente de cualquier forma de represalia. Esta protección se hace extensiva a las revelaciones a los medios de comunicación o al público en general, si se hicieran como último recurso y se referían a cuestiones de gran interés público.

25. Sucede con frecuencia que los empleados de los servicios de inteligencia son los que están en mejores condiciones para detectar antes que nadie los hechos ilícitos cometidos por los servicios, como violaciones de los derechos humanos, malversaciones financieras y otras infracciones de la ley civil. En consecuencia, es de buena práctica que la legislación nacional prevea procedimientos específicos para que los miembros de los servicios de inteligencia puedan dar a conocer sus temores respecto de la comisión de hechos ilícitos⁸¹. Estas disposiciones tienen por objeto alentar a los miembros de estos servicios a denunciar los hechos ilícitos, garantizando al propio tiempo que la revelación de información potencialmente delicada, y la investigación de la misma, se hagan de manera controlada. La práctica de los Estados muestra que hay varios cauces posibles para esas revelaciones, como mecanismos internos encargados de recibir e investigar las revelaciones de miembros de los servicios de inteligencia⁸², instituciones externas encargadas de lo mismo, y

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

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

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

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

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

⁸² United Kingdom, Intelligence and Security Committee, annual report 2007–2008, paras. 66–67

miembros de servicios de inteligencia que hagan directamente las revelaciones a las mencionadas instituciones⁸³. En algunos sistemas, los miembros de los servicios de inteligencia sólo pueden dirigirse a la institución externa si el órgano interno no ha tenido debidamente en cuenta los temores expresados⁸⁴. Algunos Estados autorizan a los miembros de los servicios de inteligencia a hacer revelaciones públicas como último recurso, o cuando esas revelaciones tengan que ver con cuestiones especialmente graves, como una amenaza a la vida humana⁸⁵. Independientemente de la naturaleza concreta de los cauces utilizados para hacer la revelación, es de buena práctica que la legislación nacional proporcione protección contra las represalias a los individuos que hagan revelaciones autorizadas por la ley⁸⁶.

G. Profesionalidad

Práctica 19. Los servicios de inteligencia y sus instituciones de supervisión toman disposiciones para promover una cultura institucional de profesionalidad, basada en el respeto por el estado de derecho y los derechos humanos. En particular, los servicios de inteligencia deben impartir formación a sus miembros respecto de las disposiciones pertinentes de la legislación nacional y el derecho internacional, incluida la normativa internacional de los derechos humanos.

26. Por cultura institucional de un servicio de inteligencia se entiende un conjunto de valores, actitudes y prácticas predominantes o ampliamente compartidas por los empleados del servicio. Es uno de los principales factores que define la actitud de los funcionarios de los servicios de inteligencia frente al estado de derecho o a los derechos humanos⁸⁷. En efecto, los marcos jurídicos e institucionales por sí solos no pueden garantizar que los miembros de los servicios de inteligencia respeten los derechos humanos o el estado de derecho. Varios Estados y sus servicios de inteligencia han formulado códigos deontológicos o principios profesionales para promover una cultura institucional que valore y realce el respeto por los derechos humanos y el estado de derecho⁸⁸. Los códigos de

(reference to the position of an “ethical counsellor” within the British Security Service); United States of America, Department of Justice, Whistleblower Protection for Federal Bureau of Investigation Employees, Federal Register, vol. 64, No. 210 (Inspector General and the Office of Professional Responsibility).

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

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

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

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

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

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

conducta suelen incluir disposiciones sobre el comportamiento adecuado, la disciplina y las normas éticas que deben observar todos los miembros de los servicios de inteligencia⁸⁹. En algunos Estados, el ministerio encargado de los servicios de inteligencia publica estos documentos, con lo que se responsabiliza políticamente su contenido⁹⁰. Es de buena práctica que los códigos de conducta (y otros documentos similares) sean sometidos al examen pormenorizado de instituciones internas y externas de supervisión⁹¹. La formación es otro instrumento clave para la promoción de una cultura institucional y profesional en los servicios de inteligencia: muchos servicios de inteligencia han organizado programas de formación que prestan especial atención a la profesionalidad y enseñan a los empleados las normas constitucionales pertinentes, la ley civil y la normativa internacional de los derechos humanos⁹². Es de buena práctica que estos programas de formación sean exigidos y regulados por la ley, y se apliquen a todos los miembros presentes y futuros de los servicios de inteligencia⁹³. Por último, la adopción de políticas internas de personal que premien las conductas éticas y profesionales puede reforzar la cultura de la profesionalidad.

H. Salvaguardias de los derechos humanos

Práctica 20. Todas las medidas adoptadas por los servicios de inteligencia que coarten los derechos humanos y las libertades fundamentales cumplen los siguientes criterios:

- a) Están contempladas en leyes a las que el público tiene acceso y que son conformes con las normas internacionales de derechos humanos.
- b) Son estrictamente necesarias para el desempeño del mandato legal de los servicios de inteligencia.
- c) Guardan proporción con el objetivo. Con esta finalidad, los servicios de inteligencia seleccionan las medidas que menos coarten los derechos humanos y procuran muy en especial reducir al mínimo los efectos desfavorables de estas medidas en los derechos de las personas, incluidos los particulares de los que no se sospeche que han cometido ningún hecho ilícito.
- d) Ninguna de esas medidas vulnera las normas imperativas del derecho internacional ni los elementos esenciales de todo derecho humano.
- e) Existe un sistema bien definido y completo para autorizar, vigilar y supervisar la aplicación de cualquier medida que coarte los derechos humanos.
- f) Las personas cuyos derechos hayan sido eventualmente coartados por los servicios de inteligencia pueden presentar denuncias a una institución independiente y tratar de obtener una reparación efectiva.

27. Las leyes nacionales permiten a la mayoría de los servicios de inteligencia realizar actividades que coarten los derechos humanos. Estas facultades se ejercen principalmente

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

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

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

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

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

en el ámbito de la recopilación de información, pero pueden incluir también medidas para hacer cumplir la ley, el empleo de datos personales y la utilización compartida de información personal. La legislación de los países prevé salvaguardias de los derechos humanos por dos razones principales: para limitar las injerencias en el derecho de los individuos a realizar actos permisibles de conformidad con la normativa internacional y los derechos humanos, y para impedir el uso arbitrario o ilimitado de esas medidas⁹⁴.

28. Toda medida que coarte los derechos humanos debe estar prescrita por una ley que sea compatible con la normativa internacional de los derechos humanos y esté en vigor en el momento en que se adopte la medida⁹⁵. Esta ley ha de definir las medidas en términos concretos y precisos, establecer condiciones estrictas para su aplicación y exigir que su aplicación tenga que ver directamente con el mandato del servicio de inteligencia⁹⁶.

29. Muchas legislaciones nacionales prevén el requisito de que todas las medidas de los servicios de inteligencia que coarten los derechos humanos han de ser necesarias en una sociedad democrática⁹⁷. Por necesarias se entiende que la aplicación de cualquier medida ha de estar vinculada de manera clara y racional con la protección de los intereses legítimos de la seguridad nacional, según se definen en la legislación nacional⁹⁸.

30. Con arreglo al principio de proporcionalidad, que está enunciado en las leyes de muchos Estados, cualquier medida que coarte los derechos humanos ha de guardar proporción con el objetivo previsto (y legalmente permisible)⁹⁹. Con objeto de garantizar la proporcionalidad de las medidas adoptadas por los servicios de inteligencia, muchos Estados exigen que sus servicios de inteligencia utilicen los medios menos invasivos posibles para el logro de un determinado objetivo¹⁰⁰.

31. Las legislaciones nacionales prohíben a los servicios de inteligencia aplicar cualquier medida que incumpla la normativa internacional de los derechos humanos y/o las normas imperativas del derecho internacional. Algunos Estados han incluido prohibiciones explícitas de violaciones graves de los derechos humanos en las leyes que regulan los servicios de inteligencia¹⁰¹. Aunque podría destacarse el carácter inviolable de los derechos humanos no derogables, en cada derecho humano hay un elemento esencial que no se presta a limitación alguna.

32. Los Estados se aseguran de que las medidas de los servicios de inteligencia que coartan los derechos humanos están sujetas a autorización previa con arreglo a un proceso legalmente prescrito, así como a la supervisión y examen posteriores (véanse las prácticas 6, 7, 21, 22, 28 y 32).

33. Un requisito fundamental de la normativa internacional de los derechos humanos es que las víctimas de violaciones de esos derechos puedan pedir reparación y compensación.

⁹⁴ Siracusa Principles (footnote 38).

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

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

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

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

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

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

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

En muchos Estados hay procedimientos para garantizar el acceso de los individuos a una institución independiente que pueda zanjar estas reclamaciones (véanse las prácticas 9 y 10)¹⁰².

I. Recopilación de información

Práctica 21. La legislación nacional define los tipos de medidas de recopilación que pueden emplear los servicios de inteligencia, los objetivos permisibles de la recopilación de información; las clases de personas y actividades respecto de las cuales puede recopilarse información; el grado de sospecha que justifica la recopilación de información; los plazos dentro de las cuales puede recopilarse la información; y los procedimientos para actualizar, supervisar y examinar las medidas de recopilación de información.

34. En la mayoría de los Estados, los servicios de inteligencia recurren a medidas invasivas, como la vigilancia encubierta y la interceptación de comunicaciones, a fin de recopilar la información necesaria para el desempeño de sus mandatos. Un requisito fundamental del estado de derecho es que los individuos han de ser conscientes de las medidas que puedan tomar las autoridades para coartar sus derechos, y ser capaces de prever las actividades que puedan dar lugar a la aplicación de esas medidas¹⁰³. La legislación nacional define las clases de personas y actividades respecto de las cuales puede recopilarse información¹⁰⁴, así como el grado de sospecha que justifica la aplicación de determinadas medidas de recopilación de información¹⁰⁵. Algunas leyes nacionales imponen limitaciones específicas a la aplicación de medidas invasivas de recopilación de información sobre determinadas categorías de personas, en particular periodistas y abogados¹⁰⁶. Esta protección tiene por objeto salvaguardar privilegios profesionales que se consideran esenciales para el funcionamiento de una sociedad libre, como el derecho de los periodistas a no revelar sus fuentes o relación de privilegio entre el abogado y su cliente. Una limitación estricta del uso de métodos invasivos de recopilación de información contribuye a garantizar que estas operaciones sean a la vez necesarias y limitadas a individuos y grupos que probablemente participan en actividades que ponen en peligro la seguridad nacional. La legislación nacional también prevé normas sobre la duración permisible de las medidas invasivas de recopilación de información; una vez concluido el plazo los servicios de inteligencia deben solicitar autorización para poder continuar

¹⁰² American Convention on Human Rights, art. 25; Arab Charter, art. 9; Siracusa principles, art. 8; European Court of Human Rights, *Klass v. Germany*, A 28 (1979-80), 2 EHHR 214, para. 69. See also practices 9 and 10.

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

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

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

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

aplicándolas¹⁰⁷. Asimismo, es de buena práctica que la legislación nacional exija que las medidas de recopilación de información dejen de aplicarse en cuanto se haya alcanzado el objetivo para el que se utilizaron, o cuando esté claro que este objetivo no puede alcanzarse¹⁰⁸. Estas disposiciones sirven para minimizar la vulneración de los derechos de los afectados, y contribuyen a garantizar que las medidas de recopilación de información cumplan el requisito de proporcionalidad.

Práctica 22. Las medidas de recopilación de información que coartan de manera significativa los derechos humanos son autorizadas y supervisadas por una institución, por lo menos, que es externa a los servicios de inteligencia e independiente de ellos. Esta institución tiene poderes para ordenar la revisión, suspensión o terminación de esas medidas. Las medidas de recopilación de información que coarten de manera significativa los derechos humanos deben pasar por un procedimiento previo de autorización a múltiples niveles, que comprende la aprobación del propio servicio de inteligencia, del poder ejecutivo y de una institución que sea independiente de los servicios de inteligencia y del poder ejecutivo.

35. De ordinario las legislaciones nacionales incluyen disposiciones detalladas sobre el procedimiento de autorización de todas las medidas de recopilación de información que coarten los derechos humanos¹⁰⁹. Para conceder la autorización es menester que los servicios de inteligencia justifiquen la utilización propuesta de las medidas de recopilación de información, de conformidad con un marco jurídico claramente definido (véanse las prácticas 20 y 21 *supra*). Este mecanismo es fundamental para garantizar la conformidad con la ley de estas medidas. Es de buena práctica que las medidas invasivas de recopilación de información sean autorizadas por una institución independiente de los servicios de inteligencia, por ejemplo un miembro del poder ejecutivo que asuma la responsabilidad política¹¹⁰ o un organismo (cuasi) judicial¹¹¹. Los organismos judiciales son independientes del proceso de inteligencia y por ello están en mejores condiciones de efectuar una evaluación independiente e imparcial de una solicitud de aplicación de medidas invasivas de recopilación de información¹¹². Además, una práctica especialmente aconsejable es que los métodos de recopilación de información más invasivos (por ejemplo, la interceptación del contenido de comunicaciones, la interceptación de la correspondencia, y el allanamiento

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

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

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

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

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

¹¹² The European Court of Human Rights has indicated its preference for judicial control for the use of intrusive collection methods, see *Klass v. Germany* (footnote 102), paras. 55–56. See also Parliamentary Assembly of the Council of Europe, recommendation 1402, ii. The South African Ministerial Review Commission argues that all intrusive methods should require judicial authorizations; see p. 175; Cameron (footnote 48), pp. 151, 156–158.

de morada) sean autorizados por los principales directivos de los servicios de inteligencia, el poder ejecutivo que asuma la responsabilidad política y un organismo (cuasi) judicial¹¹³.

36. Los Estados garantizan la supervisión constante de la recopilación de información por una institución externa a los servicios de inteligencia. Es de buena práctica que los servicios de inteligencia deban informar constantemente de la aplicación de las medidas de recopilación de información, y que la institución externa de supervisión tenga facultades para ordenar el cese de esas medidas¹¹⁴. En muchos Estados hay organismos externos que se encargan de la supervisión *ex post facto* de las medidas de recopilación de información, para determinar si han sido autorizadas y aplicadas de conformidad con la ley¹¹⁵. Esto es especialmente importante, porque no es probable que los individuos cuyos derechos hayan resultado afectados por la recopilación de información sean conscientes de ello y, por consiguiente, esas personas tienen pocas oportunidades de impugnar la legalidad de las medidas.

J. Gestión y utilización de datos personales

Práctica 23. Una ley a la que el público tiene acceso define los tipos de datos personales que pueden retener los servicios de inteligencia, y los criterios que rigen la utilización, retención, supresión y revelación de estos datos. Los servicios de inteligencia están autorizados a retener los datos personales que sean estrictamente necesarios para el cumplimiento de su mandato.

37. Hay un cierto número de principios generales que regulan la protección de los datos personales; habitualmente estos principios están enunciados en la legislación nacional¹¹⁶ y en instrumentos internacionales¹¹⁷. Se trata de los siguientes requisitos: que la recopilación y el procesamiento de los datos personales se hagan de manera legal y equitativa; que el uso de los datos personales se limite y circunscriba a su finalidad original indicada; que se tomen medidas para garantizar la exactitud de los registros de datos personales; que los archivos de datos personales se supriman cuando ya no sean necesarios, y que los particulares tengan derecho de acceder a sus archivos de datos personales y corregirlos¹¹⁸. En el contexto de la utilización de los datos personales por los servicios de inteligencia, la apertura, retención o eliminación de archivos de datos personales pueden tener graves consecuencias para los derechos humanos. Por consiguiente, la legislación civil prevé normas para la gestión y el uso de los datos personales por los servicios de inteligencia, a

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

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

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

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

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

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

modo de salvaguardia legal contra la atribución de facultades incontroladas al poder ejecutivo o a los servicios de inteligencia a este respecto¹¹⁹. Una segunda salvaguardia consiste en el establecimiento de directrices legales que especifican y limitan los motivos por los cuales los servicios de inteligencia están autorizados a abrir y mantener archivos de datos personales¹²⁰. En tercer lugar, es práctica establecida en varios Estados que los servicios de inteligencia informen al público en general de la clase de datos personales que tienen en archivo, el tipo de datos personales que pueden retener en el archivo, el alcance de los datos y los motivos que justifican la retención de información personal en el servicio¹²¹. En cuarto lugar, varios Estados han tipificado como delito la revelación o utilización de datos personales por funcionarios de los servicios de inteligencia, fuera del marco jurídico establecido¹²². Una última salvaguardia es que los Estados han dispuesto de manera explícita que los servicios de inteligencia no están autorizados a almacenar datos personales con criterios discriminatorios¹²³.

Práctica 24. Los servicios de inteligencia llevan a cabo evaluaciones regulares de la pertinencia y la exactitud de los datos personales en su poder. Estos servicios están legalmente obligados a suprimir o actualizar cualquier información que se haya determinado que no es exacta o que ya no sea pertinente para su mandato, la labor de las instituciones de supervisión o posibles actuaciones judiciales.

38. Diversos Estados han tomado disposiciones para que los servicios de inteligencia comprueben regularmente la exactitud de los datos personales de sus archivos, y su pertinencia para el mandato del servicio¹²⁴. Las salvaguardias relativas a la pertinencia y la exactitud de los datos personales contribuyen a minimizar la vulneración permanente del derecho a la intimidad. En algunos Estados la ley obliga a los servicios de inteligencia a destruir no sólo los archivos que ya no sean pertinentes¹²⁵, sino también los que no sean correctos o hayan sido procesados inadecuadamente¹²⁶. Aunque los servicios de inteligencia están obligados de ordinario a suprimir los datos que dejen de ser pertinentes para su mandato, es importante que esto no vaya en detrimento de la labor de los organismos de supervisión o de las posibles actuaciones judiciales. La información en poder de los servicios de inteligencia puede constituir una prueba en las actuaciones judiciales, con importantes consecuencias para las personas afectadas; además, la disponibilidad de este material puede ser importante para la garantía de los derechos procesales. Por lo tanto, es de buena práctica que los servicios de inteligencia estén obligados a retener todos los registros (incluidas las transcripciones originales y las notas operativas) cuando pueda haber lugar a actuaciones judiciales, y que la supresión de estas informaciones sea supervisada por una institución externa (véase la práctica 25 *infra*)¹²⁷.

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

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

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

¹²² Romania (footnote 15), art. 21.

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

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

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

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

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

Práctica 25. Existe una institución independiente encargada de supervisar la utilización de datos personales por los servicios de inteligencia. Esta institución tiene acceso a todos los archivos de los servicios de inteligencia y está facultada a ordenar la revelación de información a las personas afectadas, así como la destrucción de archivos o de la información personal contenida en ellos.

39. En muchos Estados la gestión de los archivos de datos personales es objeto de supervisión regular y continua por parte de instituciones independientes¹²⁸. Estas instituciones tienen el mandato de realizar visitas regulares de inspección y comprobaciones aleatorias de los archivos de datos personales de operaciones presentes y pasadas¹²⁹. Asimismo, algunos Estados han encomendado a instituciones independientes de supervisión que verifiquen si las directrices internas relativas a la gestión de los archivos son conformes a derecho¹³⁰. Los Estados han reconocido que las instituciones de supervisión tienen que ser autónomas en sus métodos de trabajo/inspección, y disponer de los recursos y las capacidades suficientes para llevar a cabo inspecciones regulares de la gestión y utilización de datos personales por los servicios de inteligencia¹³¹. Los servicios de inteligencia están obligados por ley a cooperar plenamente con la institución de supervisión encargada de examinar sus prácticas de gestión y utilización de datos personales¹³².

Práctica 26. Los particulares tienen la posibilidad de pedir el acceso a sus datos personales que obren en poder de los servicios de inteligencia. Para ejercer este derecho deberán presentar una solicitud, directamente a una autoridad competente o por conducto de una institución independiente encargada de la protección de los datos o la supervisión. Los particulares tienen derecho a rectificar los elementos de sus datos personales que no sean exactos. Toda excepción a esta regla está prevista en las leyes, está estrictamente limitada, es proporcional y es necesaria para el desempeño del mandato del servicio de inteligencia. Los servicios de inteligencia deben justificar, ante una institución independiente de supervisión, toda decisión de no dar a conocer información personal.

40. Muchos Estados han reconocido a los particulares el derecho a acceder a sus datos personales que obran en poder de los servicios de inteligencia. Este derecho puede ejercerse dirigiendo una solicitud al servicio de inteligencia¹³³, a un ministerio competente¹³⁴, o a una institución independiente de supervisión¹³⁵. El derecho de los particulares a acceder a sus archivos de datos personales debe verse en el contexto de las salvaguardias de los derechos a la intimidad, y de la libertad de acceso a la información. Esta salvaguardia no sólo es importante porque permite que los particulares verifiquen si su archivo de datos personales es legal y no contiene inexactitudes, sino también porque protege del abuso, la mala

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

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

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

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

¹³² Hungary (footnote 77), sect. 52.

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

¹³⁴ Netherlands (footnote 20), art. 47.

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

administración y la corrupción. En efecto, el derecho del particular a acceder a sus datos personales que obran en poder de los servicios de inteligencia permite promover la transparencia del proceso de adopción de decisiones de los servicios de inteligencia y la rendición de cuentas de esos servicios, y, por consiguiente, contribuye a aumentar la confianza de los ciudadanos en la acción del gobierno¹³⁶. Los Estados pueden limitar el acceso a los archivos de datos personales por diversos motivos, como la protección de las investigaciones en curso y de sus fuentes y métodos. No obstante, es de buena práctica que estas restricciones estén contempladas en la ley, y cumplan los requisitos de proporcionalidad y necesidad¹³⁷.

K. El ejercicio de las facultades de arresto y detención

Práctica 27. Los servicios de inteligencia no están autorizados a ejercer las facultades de arresto y detención sin un mandato que les permita desempeñar las funciones reservadas a las fuerzas de seguridad. No se confieren facultades de arresto y detención a los servicios de inteligencia si estas facultades las ejercen ya las fuerzas de seguridad, que llevan a cabo estas actividades en virtud de su mandato.

41. Una buena práctica ampliamente aceptada es prohibir explícitamente a los servicios de inteligencia que ejerzan facultades de arresto y detención si su mandato legal no prevé que desempeñen funciones de policía en relación con los delitos contra la seguridad nacional, como el terrorismo¹³⁸. Se han esgrimido argumentos convincentes contra la conjunción de las funciones de inteligencia y de policía¹³⁹. No obstante, si la legislación nacional confiere a los servicios de inteligencia las facultades de arresto y detención, es de buena práctica que esto se haga explícitamente en el marco de un mandato que atribuya a estos servicios funciones de policía en relación con amenazas concretas a la seguridad nacional, como el terrorismo¹⁴⁰. Si las fuerzas de seguridad nacionales o regionales tienen el mandato de hacer cumplir la ley en relación con los delitos contra la seguridad nacional, no hay ninguna razón legítima para conferir a un servicio de inteligencia no perteneciente a esas fuerzas facultades de arresto y detención en relación con estas mismas actividades. Existe el peligro de que se cree un sistema de seguridad paralelo, con el cual los servicios de inteligencia ejercerían facultades de arresto y detención para eludir las salvaguardias legales y los sistemas de supervisión a que están sujetas las fuerzas de seguridad del Estado¹⁴¹.

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

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

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

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

¹⁴⁰ Norway, Criminal Procedure Act.

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

Práctica 28. Si los servicios de inteligencia ejercen facultades de arresto y detención, estas facultades se basan en leyes a las que el público tiene acceso. El ejercicio de estas facultades está limitado a los casos en que exista una sospecha razonable de que un individuo ha cometido o va a cometer un delito concreto. Los servicios de inteligencia no pueden privar de libertad a los individuos por la simple razón de que necesitan información. El ejercicio de las facultades de arresto y detención por los servicios de inteligencia está sujeto al mismo grado de supervisión que el aplicable a las fuerzas de seguridad, incluido el examen judicial de la legitimidad de cualquier medida de privación de libertad.

42. Si se confiere a los servicios de inteligencia facultades de arresto y detención, la legislación nacional ha de definir los objetivos de estas facultades y las circunstancias en que pueden ejercerse¹⁴². Es de buena práctica que el ejercicio de estas facultades esté estrictamente limitado a los casos en que haya una sospecha razonable de que se ha cometido un delito (comprendido en el mandato de los servicios de inteligencia), o se va a cometer en breve. De ello se sigue que los servicios de inteligencia no están autorizados a ejercer estas facultades con la mera finalidad de recoger información¹⁴³. El arresto y detención de individuos sin que medie una sospecha razonable de que han cometido o van a cometer un delito, o cualquier otra justificación internacionalmente aceptada de la detención, no es admisible de conformidad con la normativa internacional de los derechos humanos¹⁴⁴. Si la legislación nacional permite que los servicios de inteligencia arresten y detengan a individuos, es de buena práctica que el ejercicio de esas facultades esté sujeto al mismo grado de supervisión que se aplica a las fuerzas de seguridad en las mismas circunstancias¹⁴⁵. Y, lo que es más importante, la normativa internacional de los derechos humanos exige que los individuos tengan derecho a impugnar la legitimidad de su detención ante un tribunal¹⁴⁶.

Práctica 29. Si los servicios de inteligencia poseen facultades de arresto y detención, estas facultades deben ajustarse a la normativa internacional relativa a los derechos humanos, a la libertad y a un juicio equitativo, así como a la prohibición de la tortura y los tratos inhumanos y degradantes. En el ejercicio de estas facultades los servicios de inteligencia deberán atenerse a las normas internacionales establecidas en el Conjunto de Principios para la protección de todas las personas sometidas a cualquier forma de detención o prisión, el Código de Conducta para funcionarios y encargados de hacer cumplir la ley y los Principios Básicos sobre el empleo de la fuerza y armas de fuego por funcionarios encargados de hacer cumplir la ley, entre otros instrumentos.

43. Si se les confiere facultades de arresto y detención, los servicios de inteligencia están obligados a respetar las normas internacionales vigentes en materia de privación de libertad (véase también la práctica 28 *supra*)¹⁴⁷. Estas normas están explicitadas en varios

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

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

¹⁴⁴ Venice Commission (1998), sect. E.

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

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

¹⁴⁷ Venice Commission (1998), sect. E.

códigos de conducta internacionales y regionales de los funcionarios de las fuerzas de seguridad, que contienen una serie de buenas prácticas aplicables a los servicios de inteligencia cuando ejercen facultades de arresto y detención¹⁴⁸. Además de la obligación legal (correspondiente al examen judicial de la detención) descrita en la práctica 28 *supra*, hay otras tres series de normas que regulan el ejercicio de las facultades de arresto y detención por los servicios de inteligencia. En primer lugar, los servicios de inteligencia tienen terminantemente prohibido utilizar la tortura o los tratos inhumanos o degradantes¹⁴⁹. En segundo lugar, toda utilización de la fuerza durante el arresto y la detención debe ajustarse a las normas internacionales, incluido el requisito de que el uso de la fuerza ha de ser estrictamente necesario, guardar proporción con el peligro percibido y ser objeto del correspondiente informe¹⁵⁰. En tercer lugar, es de buena práctica que los servicios de inteligencia observen las siguientes normas internacionales por las que se rige el arresto y detención de las personas: todos los arrestos, detenciones e interrogatorios que se registren desde el momento del primer arresto¹⁵¹; que los funcionarios que procedan al arresto se den a conocer a la persona arrestada y la informen de los motivos y la base jurídica de su arresto/detención¹⁵²; y que las personas detenidas por los servicios de inteligencia tengan acceso a los servicios de un abogado que las represente¹⁵³.

Práctica 30. Los servicios de inteligencia no están autorizados a tener instalaciones de detención propias ni a utilizar ninguna instalación de detención de terceros que no esté reconocida.

44. Es de buena práctica que la legislación nacional prohíba explícitamente a los servicios de inteligencia tener de instalaciones propias de detención propias¹⁵⁴. Cuando se autoriza a los servicios de inteligencia a ejercer facultades de arresto y detención, las personas detenidas son trasladadas a centros regulares de detención administrados por organismos encargados de hacer cumplir la ley¹⁵⁵. Los servicios de inteligencia tampoco están autorizados a utilizar instalaciones de detención no reconocidas que administren terceros a título de contratistas privados. Estas salvaguardias son esenciales para evitar las detenciones arbitrarias por parte de los servicios de inteligencia y/o el posible establecimiento de un régimen paralelo de detención con el que pueda retenerse a las

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

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

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

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

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

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

¹⁵⁴ Romania (footnote 2), art. 13.

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

personas en condiciones que no cumplan las normas internacionales en materia de detención ni las garantías procesales.

L. Intercambio de información y cooperación

Práctica 31. El intercambio de información entre organismos de inteligencia de un mismo Estado, o con las autoridades de un Estado extranjero, se basa en la legislación nacional que prevé normas bien definidas para esta operación, incluidas las condiciones que deben reunirse, las entidades con las que puede intercambiarse información y las salvaguardias aplicables a esos intercambios.

45. Es de buena práctica que todas las formas de intercambio de información entre los servicios de inteligencia y otras entidades nacionales o extranjeras estén basadas en términos inequívocos en la legislación nacional. La legislación nacional prevé criterios respecto de los fines admisibles del intercambio de información, las entidades con las que puede intercambiarse y las salvaguardias de procedimiento aplicables a estos intercambios¹⁵⁶. Un requisito importante en un estado de derecho es que exista una base legal para el intercambio de información, sobre todo cuando se intercambian datos personales, porque esto incide directamente en el derecho a la intimidad y puede afectar a toda una serie de derechos y libertades fundamentales. Además de garantizar que el intercambio de información se base en la legislación nacional, una buena práctica ampliamente aceptada es plasmar estas operaciones en acuerdos o memorandos escritos entre las partes, que se ajusten a las directrices establecidas por la legislación nacional¹⁵⁷. Estos acuerdos suelen contener normas que regulan el uso de la información intercambiada, una declaración de las partes en las que se comprometen a respetar los derechos humanos y proteger los datos, y una disposición según la cual el servicio que envíe la información puede pedir explicaciones sobre el uso de la información enviada¹⁵⁸. Los acuerdos de intercambio de información contribuyen a establecer normas y expectativas mutuamente convenidas sobre la información intercambiada, y a reducir el margen para realizar intercambios informales de información, que no se prestan fácilmente al examen de las instituciones de supervisión.

Práctica 32. La legislación nacional define el proceso por el que se autorizan los acuerdos en que se basa el intercambio de información y los intercambios ad hoc. Cualquier acuerdo de intercambio de información con entidades extranjeras ha de ser aprobado por el poder ejecutivo, y lo propio cabe decir de los intercambios de información que tengan consecuencias significativas para los derechos humanos.

46. Es de buena práctica que la legislación nacional establezca las directrices para autorizar el envío de información con carácter ad hoc, así como la concertación de acuerdos para el intercambio de información¹⁵⁹. De esta manera se establecen cauces de responsabilidad por el uso compartido de la información y se garantiza que se podrán pedir cuentas a las personas pertinentes por cualquier decisión que adopten al respecto.

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

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

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

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

En muchos Estados, los intercambios de información a nivel interno (dentro de los servicios de inteligencia) se autorizan corrientemente. No obstante, cuando una información intercambiada por los servicios de inteligencia puede utilizarse en actuaciones judiciales, es de buena práctica pedir la autorización del poder ejecutivo; el uso de la información en esas actuaciones puede tener graves consecuencias para los derechos de las personas interesadas, así como para las actividades de los servicios de inteligencia¹⁶⁰. Además, muchas legislaciones nacionales disponen que el intercambio de información o la concertación de acuerdos de intercambio de información con entidades extranjeras han de ser aprobados por el poder ejecutivo¹⁶¹.

Práctica 33. Antes de concertar un acuerdo de intercambio de información, o de proceder a un intercambio ad hoc, los servicios de inteligencia hacen una evaluación de los antecedentes de la otra parte en materia de derechos humanos y protección de los datos, así como de las salvaguardias jurídicas y los controles institucionales que rigen en esa parte. Antes de transmitir la información, los servicios de inteligencia se aseguran de que toda la información enviada es pertinente para el mandato del receptor, se utilizará de conformidad con las condiciones prescritas y no se destinará a fines contrarios a los derechos humanos.

47. Tanto el envío como la recepción de información pueden tener consecuencias importantes para los derechos humanos y las libertades fundamentales. La información enviada a un gobierno o un servicio de inteligencia extranjero no sólo puede contribuir a coartar legalmente los derechos de una persona, sino que también puede servir de base para cometer violaciones de los derechos humanos. Del mismo modo, la inteligencia recibida de una entidad extranjera puede haberse obtenido por un procedimiento que vulnere la normativa internacional de los derechos humanos. Así pues, antes de concertar un acuerdo de intercambio de información, o de intercambiar cualquier información, es de buena práctica que los servicios de inteligencia hagan una evaluación general de los antecedentes de la parte extranjera en materia de derechos humanos y protección de los datos personales, así como de las salvaguardias jurídicas e institucionales (como la supervisión) aplicables a esos servicios¹⁶². Antes de intercambiar información sobre personas o grupos específicos, los servicios de inteligencia tratan de determinar los posibles efectos en los interesados¹⁶³. Es de buena práctica mantener la prohibición absoluta de intercambiar cualquier información si existe la creencia bien fundada de que ese intercambio podría hacer que se vulnerasen los derechos de la persona interesada¹⁶⁴. En algunas circunstancias, la responsabilidad por el intercambio de información que contribuye a la comisión de graves violaciones de los derechos humanos puede recaer en el Estado. Además, muchas legislaciones nacionales exigen a los Estados que evalúen la necesidad de intercambiar determinadas informaciones desde el punto de vista de su propio mandato y el de sus interlocutores¹⁶⁵. Una evaluación de la necesidad y la pertinencia de la información para el

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

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

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

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

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

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

mandato del receptor permite a los servicios de inteligencia atenerse al principio de minimizar en lo posible el intercambio de datos personales¹⁶⁶. Estas salvaguardias contribuyen a impedir los intercambios excesivos o arbitrarios de información.

48. En vista de las posibles consecuencias de los intercambios de información para los derechos humanos, es de buena práctica que los servicios de inteligencia verifiquen la exactitud y la pertinencia de toda la información facilitada, antes de enviarla a entidades extranjeras¹⁶⁷. Cuando haya dudas acerca de la fiabilidad de la información que se vaya a transmitir, no se procederá al envío o bien la información irá acompañada de una fe de erratas¹⁶⁸. Por último, es de buena práctica que quede constancia escrita de todas las actividades de intercambio de información; esto facilitará su posterior examen por las instituciones de supervisión¹⁶⁹.

Práctica 34. Las instituciones independientes de supervisión pueden examinar los acuerdos de intercambio de información y cualquier información enviada por los servicios de inteligencia a entidades extranjeras.

49. Es de buena práctica que en el mandato de las instituciones de supervisión figure la obligación de examinar los acuerdos en que se basen los intercambios de información, así como cualquier disposición inspirada en esos acuerdos¹⁷⁰. Instituciones independientes de supervisión pueden examinar el marco jurídico y las cuestiones de procedimiento de los acuerdos de intercambio de información para asegurarse de que cumplen las leyes nacionales y las normas pertinentes del derecho internacional. Por regla general, las instituciones de supervisión tienen acceso a toda la información necesaria para cumplir su mandato (véase la práctica 7 *supra*). No obstante, en el contexto de los intercambios de información, la norma de la tercera parte puede entrañar restricciones al acceso de las instituciones de supervisión a la información procedente de entidades extranjeras. Las instituciones de supervisión se consideran en general terceras partes; por lo tanto, normalmente no tienen acceso a la información intercambiada entre los servicios de inteligencia y las entidades extranjeras. No obstante, estas instituciones tienen derecho a examinar la información enviada a las entidades extranjeras, y lo ejercen en el marco de su mandato de supervisar todos los aspectos de la actividad de los servicios de inteligencia (véase la práctica 7 *supra*). En este contexto, es de buena práctica que la legislación nacional exija explícitamente a los servicios de inteligencia que comuniquen las actividades de intercambio de información a una institución independiente de supervisión¹⁷¹. Esto servirá para verificar la legalidad de las prácticas de intercambio de información, y ofrecerá una importante salvaguardia contra el intercambio de datos personales, que podría tener graves consecuencias para los derechos humanos de los interesados.

Práctica 35. Los servicios de inteligencia tienen prohibido explícitamente recurrir a la asistencia de servicios de inteligencia extranjeros de cualquier manera que cause el incumplimiento de la norma jurídica nacional y el control institucional de sus propias actividades. Cuando pidan a servicios de inteligencia extranjeros que lleven

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

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

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

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

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

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

a cabo actividades en su nombre, los Estados exigirán a estos servicios que observen la misma normativa jurídica que regiría si las actividades las llevaran a cabo sus propios servicios de inteligencia.

50. Las leyes nacionales que regulan las actividades de los servicios de inteligencia prevén salvaguardias jurídicas e institucionales para proteger los derechos humanos y el orden constitucional en el contexto de las actividades de los servicios de inteligencia. En consecuencia, si los Estados o sus servicios de inteligencia pidieran a una entidad extranjera que llevase a cabo actividades en su jurisdicción que ellos mismos no podrían realizar legalmente, se produciría una contradicción en el estado de derecho. Sería de buena práctica que la legislación nacional prohibiera en términos taxativos a los servicios de inteligencia colaborar con entidades extranjeras con el fin de eludir las obligaciones jurídicas aplicables a sus propias actividades¹⁷². Además, es importante recordar que los Estados tienen la obligación legal internacional de salvaguardar los derechos de todos los individuos situados bajo su jurisdicción. Esto significa que están obligados a garantizar que los servicios de inteligencia extranjeros no emprendan actividades que violen los derechos humanos en su territorio, y a abstenerse de participar en cualquier actividad de este tipo¹⁷³. Es más, los Estados partes son internacionalmente responsables si ayudan o asisten a otro Estado a violar los derechos humanos de las personas¹⁷⁴.

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

¹⁷³ Human Rights Committee, general comment No. 31 on the nature of the general legal obligation imposed on States parties to the Covenant (CCPR/C/21/Rev1/Add.13), para. 10; European Parliament Echelon report, pp. 87-89.

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

Anexo

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.