United Nations A/HRC/14/46

General Assembly

Distr.: General
17 May 2010

Original: English

Human Rights Council
Fourteenth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*

Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight**

Summary

The present document is a compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, as requested by the Human Rights Council and prepared by the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism. The compilation is the outcome of a consultation process where Governments, experts and practitioners in various ways provided their input. In particular, written submissions received from Governments by a deadline of 1 May 2010 have been taken into account. The submissions will be reproduced in the form of an addendum (A/HRC/14/46/Add.1).

The outcome of the process is the identification of 35 elements of good practice. The elements of good practice were distilled from existing and emerging practices in a broad range of States throughout the world. The compilation also draws upon international treaties, resolutions of international organizations and the jurisprudence of regional courts.

The substance of the elements of good practice is explained in the commentary, usually presented separately for each of the 35 elements. The sources of good practice are

* Late submission.

** Given that the report greatly exceeds the page limitations currently imposed by the relevant General Assembly resolutions, the annex to the report and the footnotes are reproduced as received, in the language of submission only.

Please recycle

identified in the footnotes to the commentary, which include references to individual States.

The notion of "good practice" refers to legal and institutional frameworks that serve to promote human rights and the respect for the rule of law in the work of intelligence services. Good practice not only refers to what is required by international law, including human rights law, but goes beyond these legally-binding obligations.

The 35 areas of good practice included in the compilation are grouped into four "baskets", namely legal basis (practices 1–5), oversight and accountability (practices 6–10 and 14–18), substantive human rights compliance (practices 11–13 and 19–20) and issues related to specific functions of intelligence agencies (practices 21–35).

Contents

I. Introduction*

1. The present compilation of good practice on legal and institutional frameworks for intelligence services and their oversight is the outcome of a consultation process mandated by the Human Rights Council, which, in its resolution 10/15, called upon the Special Rapporteur to prepare, working in consultation with States and other relevant stakeholders, a compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight.

2. Intelligence services[1] play a critical role in protecting the State and its population against threats to national security, including terrorism. They help to enable States to fulfil their positive obligation to safeguard the human rights of all individuals under their jurisdiction. Hence, effective performance and the protection of human rights can be mutually complementary goals for intelligence services.

3. The compilation is distilled from existing and emerging practice from a broad range of States throughout the world. These practices are primarily derived from national laws, institutional models, as well as the jurisprudence and recommendations of national oversight institutions and a number of civil society organizations. The compilation also draws upon international treaties, resolutions of international organizations and the jurisprudence of regional courts. In this context, the notion of "good practice" refers to legal and institutional frameworks which serve to promote human rights and the respect for the rule of law in the work of intelligence services. "Good practice" not only refers to what is required by international law, including human rights law, but goes beyond these legally binding obligations.

4. Very few States have included all of the practices outlined below in their legal and institutional frameworks for intelligence services and their oversight. Some States will be able to identify themselves as following the majority of the 35 elements of good practice. Other States may start by committing themselves to a small number of these elements which they consider as essential to promoting human rights compliance by intelligence services and their oversight bodies.

5. It is not the purpose of this compilation to promulgate a set of normative standards that should apply at all times and in all parts of the world. Hence, the elements of good practice presented in this report are formulated in descriptive, rather than normative, language. It is nevertheless possible to identify common practices that contribute to the respect for the rule of law and human rights by intelligence services.

6. The Human Rights Council mandated the present compilation of good practices within the context of the role of intelligence services in counter-terrorism. However, it should be noted that the legal and institutional frameworks which apply to intelligence services' counter-terrorism activities cannot be separated from those which apply to their

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

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

activities more generally. While international terrorism has, since 2001, changed the landscape for the operation of intelligence agencies, the effects of that change go beyond the field of counter-terrorism.

7. The compilation highlights examples of good practice from numerous national laws and institutional models. It is, however, important to note that the citation of specific provisions from national laws or institutional models does not imply a general endorsement of these laws and institutions as good practice in protecting human rights in the context of counter-terrorism. Additionally, the Special Rapporteur wishes to emphasize that the existence of legal and institutional frameworks which represent good practice is essential, but not sufficient for ensuring that intelligence services respect human rights in their counter-terrorism activities.

8. The 35 areas of good practice presented below are grouped into four different "baskets", namely legal basis (1–5), oversight and accountability (6–10 and 14–18), substantive human rights compliance (11–13 and 19–20) and issues relating to specific functions of intelligence agencies (21–35). For reasons of presentation, the elements are grouped under a somewhat higher number of subheadings.

II. Compilation of good practices on legal and institutional frameworks for intelligence services and their oversight

A. Mandate and legal basis

> **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.

9. The functions of intelligence services differ from one country to another; however, the collection, analysis and dissemination of information relevant to the protection of national security is the core task performed by most intelligence services:[2] indeed, many States limit the role of their intelligence services to this task. This represents good practice, because it prevents intelligence services from undertaking additional security-related activities already performed by other public bodies and which may represent particular threats to human rights if performed by intelligence services. In addition to defining the types of activities their intelligence services may perform, many States also limit the rationale for these activities to the protection of national security. While the understanding of national security varies among States, it is good practice for national security and its constituent values to be clearly defined in legislation adopted by parliament.[3] This is important for ensuring that intelligence services confine their activities to helping to safeguard values that are enshrined in a public definition of national security. In many areas, safeguarding national security necessarily includes the protection of the population

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

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

and its human rights;[4] indeed, a number of States explicitly include the protection of human rights as one of the core functions of their intelligence services.[5]

> **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.

10. The mandates of intelligence services are one of the primary instruments for ensuring that their activities (including in the context of counter-terrorism) serve the interests of the country and its population, and do not present a threat to the constitutional order and/or human rights. In the majority of States, intelligence services' mandates are clearly delineated in a publicly available law, promulgated by parliament.[6] It is good practice for mandates to be narrowly and precisely formulated, and to enumerate all of the threats to national security that intelligence services are responsible for addressing.[7] Clear and precise mandates facilitate accountability processes, enabling oversight and review bodies to hold intelligence services to account for their performance of specific functions. Finally, a clear definition of threats is particularly relevant in the context of counter-terrorism; many States have adopted legislation that provides precise definitions of terrorism, as well as of terrorist groups and activities.[8]

> **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.

11. It is a fundamental tenet of the rule of law that all powers and competences of intelligence services are outlined in law.[9] An exhaustive enumeration of the powers and competences of intelligence services promotes transparency and enables people to foresee

---

[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 equité et réconciliation, rapport final, Vol. I, Vérité, equité et réconciliation, 2005, chapitre IV, 8-3 (hereafter Morocco – ER Report); European Commission for Democracy Through Law, Internal Security Services in Europe, CDL-INF(1998)006, I, B (b) and (c) (hereafter Venice Commission (1998)).

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

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

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

what powers may be used against them. This is particularly important given that many of the powers held by intelligence services have the potential to infringe upon human rights and fundamental freedoms.[10] This practice is closely connected to practice 2, because the mandates of intelligence services serve to define the framework within which they can use the powers given by the legislature.[11] A prohibition of *détournement de pouvoir* is implicit in the legislation of many States as intelligence services are only permitted to use their powers for very specific purposes. This is particularly in the context of counter-terrorism, because many intelligence services have been endowed with greater powers 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.

12. Intelligence services are organs of the State and thus, in common with other executive bodies, are bound by relevant provisions of national and international law, and in particular human rights law.[12] This implies that they are based upon and operate in accordance with publicly available laws that comply with the Constitution of the State, as well as, inter alia, the State's international human rights obligations. States cannot rely upon domestic law to justify violations of international human rights law or indeed any other international legal obligations.[13] The rule of law requires that the activities of intelligence services and any instructions issued to them by the political executive comply with these bodies of law in all of their work.[14] Accordingly, intelligence services are prohibited from undertaking, or being asked to undertake, any action that would violate national statutory law, the Constitution or the State's human rights obligations. In many States, these requirements are implicit; however, it is notably good practice for national legislation to make explicit reference to these broader legal obligations and, in particular, to the obligation to respect human rights.[15] Subordinate regulations pertaining to the internal

---

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

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

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

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

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

[15] Argentina (footnote 2), art. 3; Bulgaria, Law on State Agency for National Security, art. 3 (1) 1–2;

processes and activities of intelligence services are sometimes withheld from the public in order to protect their working methods. These types of regulations do not serve as the basis for activities that infringe human rights. It is good practice for any subordinate regulation to be based on and comply with applicable public legislation.[16]

B. Oversight institutions

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.

13. In common with intelligence services, the institutions that oversee their activities are based on law and, in some cases, founded on the Constitution.[17] There is no single model for the oversight intelligence services; however, the following components are commonly included in comprehensive systems of oversight:[18] internal management and control mechanisms within intelligence services;[19] executive oversight;[20] oversight by parliamentary bodies;[21] as well as specialized and/or judicial oversight bodies.[22] It is good

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

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

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

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

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

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

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

[22] For specialized intelligence oversight bodies, see Norway, Act on Monitoring of Intelligence, Surveillance and Security Services, art. 1; Canada (footnote 6), sects. 34–40; Netherlands (footnote

practice for this multilevel system of oversight to include at least one institution that is fully independent of both the intelligence services and the political executive. This approach ensures that there is a separation of powers in the oversight of intelligence services; the institutions that commission, undertake and receive the outputs of intelligence activities are not the only institutions that oversee these activities. All dimensions of the work of intelligence services are subject to the oversight of one or a combination of external institutions. One of the primary functions of a system of oversight is to scrutinize intelligence services' compliance with applicable law, including human rights. Oversight institutions are mandated to hold intelligence services and their employees to account for any violations of the law.[23] In addition, oversight institutions assess the performance of intelligence services.[24] This includes examining whether intelligence services make efficient and effective use of the public funds allocated to them.[25] An effective system of oversight is particularly important in the field of intelligence because these services conduct much of their work in secret and hence cannot be easily overseen by the public. Intelligence oversight institutions serve to foster public trust and confidence in the work of intelligence services by ensuring that they perform their statutory functions in accordance with respect for the rule of law and human rights.[26]

> **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.

14. Oversight institutions enjoy specific powers to enable them to perform their functions. In particular, they have the power to initiate their own investigations into areas of the intelligence service's work that fall under their mandates, and are granted access to all information necessary to do so. These powers of access to information encompass the legal authority to view all relevant files and documents,[27] inspect the premises of intelligence services,[28] and to summon any member of the intelligence services to give evidence under oath.[29] These powers help to ensure that overseers can effectively scrutinize the activities of intelligence services and fully investigate possible contraventions of the law. A number of States have taken steps to reinforce the investigative competences of oversight institutions

20), chapter 6; Belgium, Law on the Control of Police and Intelligence Services and the Centre for Threat Analysis, chapter 3.

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

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

[25] Romania (footnote 2), art. 42.

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

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

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

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

by criminalizing any failure to cooperate with them.[30] This implies that oversight institutions have recourse to law enforcement authorities in order to secure the cooperation of relevant individuals.[31] While strong legal powers are essential for effective oversight, it is good practice for these to be accompanied by the human and financial resources needed to make use of these powers, and, thus, to fulfil their mandates. Accordingly, many oversight institutions have their own independent budget provided directly by parliament,[32] the capacity to employ specialized staff,[33] and to engage the services of external experts.[34]

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.

15. Intelligence oversight institutions have access to classified and sensitive information during the course of their work. Therefore, a variety of mechanisms are put in place to ensure that oversight institutions and their members do not disclose such information either inadvertently or deliberately. Firstly, in almost all cases, members and staffers of oversight institutions are prohibited from making unauthorized disclosure of information; failure to comply with these proscriptions is generally sanctioned through civil and/or criminal penalties.[35] Secondly, many oversight institutions also subject members and staff to security clearance procedures before giving them access to classified information.[36] An alternative to this approach, most commonly seen in parliamentary oversight institutions, is for members to be required to sign a non-disclosure agreement.[37] Ultimately, the appropriate handling of classified information by oversight institutions also relies upon the professional behaviour of the members of the oversight institutions.

C. Complaints and effective remedy

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.

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

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

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

[33] Canada (footnote 6), sect. 36.

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

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

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

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

16. It is widely acknowledged that any measure restricting human rights must be accompanied by adequate safeguards, including independent institutions, through which individuals can seek redress in the event that their rights are violated.[38] Intelligence services possess a range of powers – including powers of surveillance, arrest and detention, which, if misused, may violate human rights. Accordingly, institutions exist to handle complaints raised by individuals who believe their rights have been violated by intelligence services and, where necessary, to provide victims of human rights violations with an effective remedy. Two broad approaches can be distinguished in this regard.[39] First, States have established a range of non-judicial institutions to handle complaints pertaining to intelligence services. These include the ombudsman,[40] the national human rights commission,[41] the national audit office,[42] the parliamentary oversight body,[43] the inspector general,[44] the specialized intelligence oversight body[45] and the complaints commission for intelligence services.[46] These institutions are empowered to receive and investigate complaints; however, since they cannot generally issue binding orders or provide remedies, victims of human rights violations have to seek remedies through the courts. Second, judicial institutions may receive complaints pertaining to intelligence services. These institutions may be judicial bodies set up exclusively for this purpose,[47] or part of the general judicial system; they are usually empowered to order remedial action.

> **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.

17. In order for an institution to provide effective remedies for human rights violations, it must be independent of the institutions involved in the impugned activities, able to ensure procedural fairness, have sufficient investigative capacity and expertise, and the capacity to issue binding decisions.[48] For this reason, States have endowed such institutions with the requisite legal powers to investigate complaints and provide remedies to victims of human rights violations perpetrated by intelligence services. These powers include full and

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

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

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

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

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

[43] Romania (footnote 15), art. 16.

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

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

[46] Kenya (footnote 16), arts. 24–26.

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

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

unhindered access to all relevant information, investigative powers to summon witnesses and to receive testimony under oath,[49] the power to determine their own procedures in relation to any proceedings, and the capacity to issue binding orders.[50]

D. Impartiality and non-discrimination

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.

18. Intelligence services are an integral part of the State apparatus that contributes to safeguarding the human rights of all individuals under the jurisdiction of the State. They are bound by the well-established principle of international human rights law of non-discrimination. This principle requires States to respect the rights and freedoms of individuals without discrimination on any prohibited ground.[51] Many States have enshrined the principle in national law, requiring their intelligence services to fulfil their mandates in a manner that serves the interests of the State and society as a whole. Intelligence services are explicitly prohibited from acting or being used to further the interests of any ethnic, religious, political or other group.[52] In addition, States ensure that the activities of their intelligence services (in particular in the context of counter-terrorism) are undertaken on the basis of individuals' behaviour, and not on the basis of their ethnicity, religion or other such criteria.[53] Some States have also explicitly proscribed their intelligence services from establishing files on individuals on this basis.[54]

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.

19. Intelligence services are endowed with powers that have the potential to promote or damage the interest of particular political groups. In order to ensure that intelligence services remain politically neutral, national laws prohibit intelligence services from acting in the interest of any political group.[55] This obligation is not only incumbent upon the intelligence services but also upon the political executives whom they serve. A number of States have also passed measures to prohibit or limit intelligence services' involvement in party politics. Examples of these measures include prohibitions on employees of intelligence services being members of political parties; accepting instructions or money from a political party;[56] or from acting to further the interests of any political

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

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

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

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

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

[54] Argentina (footnote 2), art. 4.

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

[56] Bosnia and Herzegovina (footnote 6), art. 45; Albania (footnote 21), art. 11; Kenya (footnote 16), art.

party.[57] In addition, various States have taken measures to safeguard the neutrality of the directors of intelligence services. For example, the appointment of the director of intelligence services is open to scrutiny from outside the executive;[58] there are legal provisions on the duration of tenure and specification of the grounds for the dismissal of directors, as well as safeguards against improper pressure being applied on directors of intelligence services.[59]

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.

20. Intelligence services have recourse to information-collection measures that may interfere with legitimate political activities and other manifestations of the freedoms of expression, association and assembly.[60] These rights are fundamental to the functioning of a free society, including political parties, the media and civil society. Therefore, States have taken measures to reduce the scope for their intelligence services to target (or to be asked to target) these individuals and groups engaged in these activities. Such measures include absolute prohibitions on targeting lawful activities, and strict limitations on both the use of intelligence collection measures (see practice 21) and the retention and use of personal data collected by intelligence services (see practice 23).[61] In view of the fact that the media plays a crucial role in any society, some States have instituted specific measures to protect journalists from being targeted by intelligence services.[62]

E. State responsibility for intelligence services

Practice 14. States are internationally responsible for the activities of their intelligence services and 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.

21. States are responsible under international law for the activities of their intelligence services and agents wherever they operate in the world. This responsibility extends to any private contractors that States engage to undertake intelligence functions.[63] States have a legal obligation to ensure that their intelligence services do not violate human rights and to

15 (1)a; Lithuania (footnote 9), art. 24.

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

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

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

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

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

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

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

provide remedies to the individuals concerned if such violations occur.[64] Accordingly, they take steps to regulate and manage their intelligence services in a manner that promotes respect for the rule of law and in particular, compliance with international human rights law.[65] Executive control of intelligence services is essential for these purposes and is therefore enshrined in many national laws.[66]

F. Individual responsibility and accountability

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.

22. While great emphasis is placed on the institutional responsibilities of intelligence services, individual members of intelligence services are also responsible and held to account for their actions.[67] As a general rule, constitutional, statutory and international criminal law applies to intelligence officers as much as it does to any other individual.[68] Many States have made it a cause for civil liability or a criminal offence for any member of an intelligence service to knowingly violate and/or order or request an action that would violate constitutional or statutory law.[69] This practice promotes respect for the rule of law within intelligence services, and helps to prevent impunity. Many States give members of their intelligence services the authority to engage in activities which, if undertaken by ordinary citizens, would constitute criminal offences.[70] It is good practice that any such authorizations be strictly limited, prescribed by law and subject to appropriate safeguards.[71] Statutory provisions that authorize intelligence officers to undertake acts that would normally be illegal under national law do not extend to any actions that would violate the Constitution or non-derogable international human rights standards. [72]

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

---

[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 intersect.s with criminal justice systems?", *Revue international de droit penal* 78, no.1 (2007), pp. 57–77; European Commission for Democracy through Law, opinion 363/2005 on the International Legal Obligations of Council of Europe Member States in Respect of Secret Detention Facilities and Inter-State Transport of Prisoners, p. 15.

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

[66] See also practice 6.

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

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

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

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

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

[72] Netherlands (footnote 20), annex.

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.

23. States ensure that employees of intelligence services are held to account for any violations of the law by providing and enforcing sanctions for particular offences. This serves to promote respect for the rule of law and human rights within intelligence services. Many national laws regulating intelligence services include specific sanctions for employees who violate these laws or other applicable provisions of national and international law.[73] Given that many of the activities of intelligence services take place in secret, criminal offences (perpetrated by employees) may not be detected by the relevant prosecutorial authorities. Therefore, it is good practice for national law to require the management of intelligence services to refer cases of possible criminal wrongdoing to prosecutorial authorities.[74] In cases of serious human rights violations, such as torture, States are under an international legal obligation to prosecute members of the intelligence services.[75] The criminal responsibility of employees of intelligence services may be engaged not only through their direct participation in the given activities, but also if they order or are otherwise complicit in such activities.[76]

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.

24. It is good practice for national laws to require members of intelligence services to refuse orders that they believe would violate national law or international human rights law.[77] While this provision is more common in laws regulating armed forces, several States have included it in statutes regulating their intelligence services.[78] A requirement for members of intelligence services to refuse illegal orders is an important safeguard against possible human rights abuses, as well as against incumbent Governments ordering intelligence services to take action to further or protect their own interests. It is a well-established principle of international law that individuals are not absolved of criminal responsibility for serious human rights violations by virtue of having been requested to undertake an action by a superior.[79] Hence, to avoid individual criminal liability, members of intelligence services are required to refuse to carry out any orders that they should understand to be manifestly unlawful. This underlines the importance of human rights training for intelligence officers because they need to be aware of their rights and duties under international law (see practice 19). In order to promote an environment in which human rights abuses are not tolerated, States provide legal protections against reprisals for members of intelligence services who refuse to carry out illegal orders.[80] The obligation to

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

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

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

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

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

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

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

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

refuse illegal orders is closely linked to the availability of internal and external mechanisms through which intelligence service employees can voice their concerns about illegal orders (see practice 18 below).

> **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.

25. Employees of intelligence services are often first, and best, placed to identify wrongdoing within intelligence services, such as human rights violations, financial malpractice and other contraventions of statutory law. Accordingly, it is good practice for national law to outline specific procedures for members of intelligence services to disclose concerns about wrongdoing.[81] These provisions aim to encourage members of intelligence services to report wrongdoing, while at the same time ensuring that disclosures of potentially sensitive information are made and investigated in a controlled manner. State practice demonstrates that there are several channels for such disclosures, including internal mechanisms to receive and investigate disclosures made by members of intelligence services,[82] external institutions to receive and investigate disclosures, and members of intelligence services making disclosures directly to these institutions.[83] In some systems, members of intelligence services may only approach the external institution if the internal body has failed to address adequately their concerns.[84] In some States, members of intelligence services are permitted to make public disclosures as a last resort or when such disclosures concern particularly grave matters, such as a threat to life.[85] Regardless of the precise nature of the channels for disclosure, it is good practice for national law to afford individuals who make disclosures authorized by law to protection against reprisals.[86]

---

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

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

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

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

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

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

G. Professionalism

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.

26. The institutional culture of an intelligence service refers to widely shared or dominant values, attitudes and practices of employees. It is one of the main factors defining the attitude of intelligence officials towards the rule of law and human rights.[87] Indeed, legal and institutional frameworks alone cannot ensure that members of intelligence services comply with human rights and the rule of law. A number of States and their intelligence services have formulated codes of ethics or principles of professionalism in order to promote an institutional culture that values and fosters respect for human rights and the rule of law.[88] Codes of conduct typically include provisions on appropriate behaviour, discipline and ethical standards that apply to all members of intelligence services.[89] In some States, the minister responsible for intelligence services promulgates such documents; this ensures political accountability for their content.[90] It is good practice for codes of conduct (and similar documents) to be subject to the scrutiny of internal and external oversight institutions.[91] Training is a second key instrument for the promotion of a professional institutional culture within intelligence services. Many intelligence services have initiated training programmes that emphasize professionalism and educate employees on relevant constitutional standards, statutory law and international human rights law.[92] It is good practice for these training programmes to be both required and regulated by law, and to include all (prospective) members of intelligence services.[93] Finally, a professional culture can be reinforced by internal personnel management policies that reward ethical and professional conduct.

H. Human rights safeguards

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;

---

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

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

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

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

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

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

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

(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**.**

27. Under national law, most intelligence services are permitted to undertake activities that restrict human rights. These powers are primarily found in the area of intelligence collection but also include law enforcement measures, the use of personal data and the sharing of personal information. National laws contain human rights safeguards for two main reasons: to limit interference with the rights of individuals to what is permissible under international human rights law; and to prevent the arbitrary or unfettered use of these measures.[94]

28. Any measure restricting human rights must be prescribed by a law that is compatible with international human rights standards and in force at the time the measure is taken.[95] Such a law outlines these measures in narrow and precise terms, sets out strict conditions for their use and establishes that their use must be directly linked to the mandate of an intelligence service.[96]

29. Many national laws also include the requirement that any intelligence measures restricting human rights must be necessary in a democratic society.[97] Necessity entails that the use of any measures is clearly and rationally linked to the protection of legitimate national security interests as defined in national law.[98]

30. The principle of proportionality is enshrined in laws of many States and requires that any measures that restrict human rights must be proportionate to the specified (and legally permissible) aims.[99] In order to ensure that measures taken by intelligence services are proportionate, many States require their intelligence services to use the least intrusive means possible for the achievement of a given objective.[100]

31. Intelligence services are prohibited by national law from using any measures that would violate international human rights standards and/or peremptory norms of

[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.

international law. Some States have included explicit prohibitions on serious human rights violations in their laws on intelligence services.[101] While non-derogable human rights may be singled out as inviolable, every human right includes an essential core that is beyond the reach of permissible limitations.

32. States ensure that intelligence measures that restrict human rights are subject to a legally prescribed process of authorization, as well as ex post oversight and review (see practices 6, 7, 21, 22, 28 and 32).

33. It is a fundamental requirement of international human rights law that victims of human rights violations be able to seek redress and remedy. Many States have procedures in place to ensure that individuals have access to an independent institution that can adjudicate on such claims (see practices 9 and 10 above).[102]

I. Intelligence collection

> **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.

34. In most States, intelligence services have recourse to intrusive measures, such as covert surveillance and the interception of communications, in order to collect information necessary to fulfil their mandates. It is a fundamental requirement of the rule of law that individuals must be aware of measures that public authorities may use to restrict their rights and be able to foresee which activities may give rise to their use.[103] National law outlines the categories of persons and activities that may be subject to intelligence collection,[104] as well as the threshold of suspicion required for particular collection measures to be initiated.[105] Some national laws also impose specific limitations on the use of intrusive collection measures against particular categories of individuals, notably journalists and lawyers.[106] These measures are designed to protect professional privileges deemed to be essential to the functioning of a free society, such as the right of journalists not to disclose their sources, or lawyer-client privilege. Strict limitations on the use of intrusive collection

---

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

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

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

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

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

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

methods help to ensure that intelligence collection is both necessary and limited to individuals and groups that are likely to be involved in activities posing a threat to national security. National law also includes guidelines on the permissible duration of the use of intrusive collection measures, after which time intelligence services are required to seek reauthorization in order to continue using them.[107] Similarly, it is good practice for national law to require that intelligence collection measures are ceased as soon as the purpose for which they were used has been fulfilled or if it becomes clear that that purpose cannot be met.[108] These provisions serve to minimize infringements on the rights of individuals concerned and help to ensure that intelligence-collection measures meet the requirement of proportionality.

> **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.

35. It is common practice for national laws to include detailed provisions on the process for authorizing all intelligence collection measures that restrict human rights.[109] Authorization processes require intelligence services to justify the proposed use of intelligence-collection measures in accordance with a clearly defined legal framework (see practices 20 and 21 above). This is a key mechanism for ensuring that collection measures are used in accordance with the law. It is good practice for intrusive collection measures to be authorized by an institution that is independent of the intelligence services, i.e., a politically accountable member of the executive[110] or a (quasi) judicial body.[111] Judicial bodies are independent of the intelligence process and therefore best placed to conduct an independent and impartial assessment of an application to use intrusive collection powers.[112] Furthermore, it is notably good practice for the authorization of the most intrusive intelligence collection methods (e.g. the interception of the content of communications, the interception of mail and surreptitious entry into property) to include

---

[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.

senior managers in intelligence services, the politically accountable executive and a (quasi) judicial body.[113]

36. States also ensure that intelligence collection is subject to ongoing oversight by an institution that is external to the intelligence services. It is good practice for intelligence services to be required to report on the use of collection measures on an ongoing basis and for the external oversight institution to have the power to order the termination of collection measures.[114] In many States, external oversight bodies also conduct ex post oversight of the use of intelligence-collection measures to ascertain whether or not they are authorized and used in compliance with the law.[115] This is particularly important in view of the fact that the individuals whose rights are affected by intelligence collection are unlikely to be aware of the fact and, thus, have limited opportunity to challenge its legality.

J. Management and use of personal data

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.

37. There is a number of general principles that apply to the protection of personal data that are commonly included in national laws[116] as well as in international instruments.[117] These include the following requirements: that personal data be collected and processed in a lawful and fair manner; that the use of personal data be limited and confined to its original specified purpose; that steps be taken to ensure that records of personal data are accurate; that personal data files be deleted when no longer required; and that individuals have the right to have access to and correct their personal data file.[118] In the context of personal data use by intelligence services, the opening, retention and disposal of personal data files can have serious human rights implications; therefore, guidelines for the management and use of personal data by intelligence services are set out in public statutory law. This is a legal safeguard against giving the executive or the intelligence services unchecked powers over these matters.[119] A second safeguard is that legal guidelines are established to specify and

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

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

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

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

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

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

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

limit the reasons for opening and keeping personal data files by intelligence services.[120] Third, it is established practice in various States that the intelligence services inform the general public about the type of personal data kept by an intelligence service; this includes information on the type and scope of personal data that may be retained, as well as permissible grounds for the retention of personal information by an intelligence service.[121] Fourth, various States have made it a criminal offence for intelligence officers to disclose or use personal data outside the established legal framework.[122] A final safeguard is that States have explicitly stipulated that intelligence services are not allowed to store personal data on discriminatory grounds.[123]

> **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.

38. States have taken steps to ensure that intelligence services regularly check whether personal data files are accurate and relevant to their mandate.[124] Safeguards on the relevance and accuracy of personal data help to ensure that any ongoing infringement of the right to privacy is minimized. In some States, the intelligence services have not only the legal obligation to destroy files that are no longer relevant[125] but also files that are incorrect or have been processed incorrectly.[126] While intelligence services are ordinarily obliged to delete data that are no longer relevant to their mandate, it is important that this is not to the detriment of the work of oversight bodies or possible legal proceedings. Information held by intelligence services may constitute evidence in legal proceedings with significant implications for the individuals concerned; the availability of such material may be important for guaranteeing due process rights. Therefore, it is good practice for intelligence services to be obliged to retain all records (including original transcripts and operational notes) in cases that may lead to legal proceedings, and that the deletion of any such information be supervised by an external institution (see practice 25 below).[127]

> **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.

39. In many States, the management of personal data files is subject to regular and continuous oversight by independent institutions.[128] These institutions are mandated to conduct regular inspection visits and random checks of personal data files of current and

---

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

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

[122] Romania (footnote 15), art. 21.

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

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

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

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

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

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

past operations.[129] States have also mandated independent oversight institutions to check whether the internal directives on file management comply with the law.[130] States have acknowledged that oversight institutions need to be autonomous in their working and inspection methods, and have sufficient resources and capacities to conduct regular inspections of the management and use of personal data by intelligence services.[131] Intelligence services have a legal duty to cooperate fully with the oversight institution responsible for scrutinizing their management and use of personal data.[132]

> **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.

40. Many States have given individuals the right to have access to their personal data held by intelligence services. This right may be exercised by addressing a request to the intelligence service,[133] a relevant minister,[134] or an independent oversight institution.[135] The right of individuals to have access to their personal data files should be understood in the context of safeguards for privacy rights and the freedom of access to information. This safeguard is important not only because it allows individuals to check whether their personal data file is accurate and lawful, but also because it is a safeguard against abuse, mismanagement and corruption. Indeed, an individual's right to have access to personal data held by intelligence services serves to enhance transparency and accountability of the decision-making processes of the intelligence services and, therefore, assists in developing citizens' trust in Government actions.[136] States may restrict access to personal data files, for reasons such as safeguarding ongoing investigations and protecting sources and methods of the intelligence services. However, it is good practice for such restrictions to be outlined in law, and that they meet the requirements of proportionality and necessity.[137]

---

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

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

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

[132] Hungary (footnote 77), sect. 52.

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

[134] Netherlands (footnote 20), art. 47.

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

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

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

K. The use of powers of arrest and detention

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.

41. It is widely accepted as good practice for intelligence services to be prohibited explicitly from exercising powers of arrest and detention if their legal mandate does not require them to exercise law enforcement functions in relation to national security offences, such as terrorism.[138] Strong arguments have been made against combining intelligence and law enforcement functions.[139] However, if national law provides intelligence services with powers of arrest and detention, it is good practice for this to be explicitly within the context of a mandate that gives them the responsibility for performing law enforcement functions pertaining to specified threats to national security, such as terrorism.[140] If national or regional law enforcement bodies have a mandate to enforce criminal law in relation to national security offences, there is no legitimate reason for a separate intelligence service to be given powers of arrest and detention for the same activities. There is a risk of the development of a parallel enforcement system, whereby intelligence services exercise powers of arrest and detention in order to circumvent legal safeguards and oversight that apply to the law enforcement agencies.[141]

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.

42. If intelligence services are given powers of arrest and detention, national law outlines the purposes of such powers and circumstances under which they may be used.[142] It is good practice for the use of these powers to be strictly limited to cases where there is reasonable suspicion that a crime (falling under the mandate of the intelligence services) has been, or is about to be, committed. It follows that intelligence services are not permitted to use these powers for the mere purpose of intelligence collection.[143] The apprehension and detention of individuals when there is no reasonable suspicion that they have committed or are about to commit a criminal offence, or other internationally accepted ground for

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

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

[140] Norway, Criminal Procedure Act.

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

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

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

detention, is not permissible under international human rights law.[144] If national law permits intelligence services to apprehend and detain individuals, it is good practice for the exercise of these powers to be subject to the same degree of oversight applying to the use of these powers by law enforcement authorities.[145] Most importantly, international human rights law requires that individuals have the right to challenge the lawfulness of their detention before a court.[146]

> **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.

43. If intelligence services are given powers of arrest and detention, they are required to comply with international standards applying to the deprivation of liberty (see also practice 28 above).[147] These standards are further elaborated in several international and regional codes of conduct of law enforcement officials codifying a range of good practices that can be applied to intelligence services with powers of arrest and detention.[148] In addition to the legal obligation (pertaining to the judicial review of detention) outlined in practice 28 above, there are three additional sets of standards that apply the use of powers of arrest and detention by intelligence services. First, intelligence services are bound by the absolute prohibition on the use of torture and inhuman and degrading treatment.[149] Second, any use of force during arrest and detention must comply with international standards, including the requirements that any use of force be strictly necessary, proportionate to the perceived danger and properly reported.[150] Third, it is good practice for intelligence services to comply with the following international standards on the apprehension and detention of individuals: that all arrests, detentions and interrogations are recorded from the moment of apprehension;[151] that officers making an arrest identify themselves to the individual concerned and inform them of the reasons and legal basis for their

---

144 Venice Commission (1998), sect. E.

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

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

147 Venice Commission (1998), sect. E.

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

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

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

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

apprehension/detention;[152] and that individuals detained by intelligence services have access to legal representation.[153]

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.

44. It is good practice for intelligence services to be explicitly prohibited in national law from operating their own detention facilities.[154] If intelligence services are permitted to exercise powers of arrest and detention, the individuals concerned are remanded in regular detention centres administered by law enforcement agencies.[155] Equally, intelligence services are not permitted to make use of unacknowledged detention facilities run by third parties, such as private contractors. These are essential safeguards against arbitrary detention by intelligence services and/or the possible development of a parallel detention regime in which individuals could be held in conditions that do not meet international standards of detention and due process.

L. Intelligence-sharing and cooperation

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.

45. It is good practice for all forms of information-sharing between intelligence services and other domestic or foreign entities to have a clear basis in national law. National law includes criteria on the purposes for which intelligence may be shared, the entities with which it may be shared, and the procedural safeguards that apply to intelligence-sharing.[156] A legal basis for intelligence-sharing is an important requirement of the rule of law, and is particularly important when personal data are exchanged, because this directly infringes the right to privacy and may affect a range of other rights and fundamental freedoms. In addition to ensuring that intelligence-sharing is based on national law, it is widely accepted as good practice that intelligence-sharing be based on written agreements or memoranda between the parties, which comply with guidelines laid down in national law.[157] The elements that are commonly included in such agreements include rules governing the use of shared information, a statement of the parties' compliance with human rights and data protection, and the provision that the sending service may request feedback on the use of

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

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

[154] Romania (footnote 2), art. 13.

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

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

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

the shared information.[158] Intelligence-sharing agreements help to establish mutually agreed standards and expectations about shared information, and reduce the scope for informal intelligence-sharing, which cannot be easily reviewed by oversight institutions.

> **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.

46. It is good practice for national law to set out guidelines for the authorization of the sending of information on an ad hoc basis, as well as for the establishment of agreements for intelligence-sharing.[159] This serves to ensure that there are established channels of responsibility for intelligence-sharing and that relevant individuals can be held to account for any decisions they make in this regard. In many States, routine intelligence-sharing at the domestic level is authorized internally (within the intelligence services). However, when information shared by intelligence services may be used in court proceedings, it is good practice for executive authorization to be required; the use of intelligence in such proceedings may have profound implications for the rights of the individuals concerned, as well as for the activities of the intelligence services themselves.[160] Additionally, many national laws require executive authorization for the sharing of intelligence or establishment of sharing agreements with foreign entities.[161]

> **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.

47. Both the sending and receipt of intelligence can have important implications for human rights and fundamental freedoms. Information sent to a foreign Government or intelligence service may not only contribute to legal limitations on the rights of an individual, but could also serve as the basis for human rights violations. Similarly, intelligence received from a foreign entity may have been obtained in violation of international human rights law. Therefore, before entering into a sharing agreement or sharing any information, it is good practice for intelligence services to conduct a general assessment of a foreign counterpart's record on human rights and the protection of personal data, as well as the legal and institutional safeguards (such as oversight) that apply to those services.[162] Before sharing information on specific individuals or groups, intelligence services take steps to assess the possible impact on the individuals concerned.[163] It is good

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

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

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

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

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

[163] Croatia (footnote 2), art. 60 (1); Germany (footnote 2), sect. 19; Switzerland (footnote 5), art. 17 (4);

practice to maintain an absolute prohibition on the sharing of any information if there is a reasonable belief that sharing information could lead to the violation of the rights of the individual(s) concerned.[164] In some circumstances, State responsibility may be triggered through the sharing of intelligence that contributes to the commission of grave human rights violations. Additionally, many national laws require States to evaluate the necessity of sharing particular information from the point of view of their own mandate and that of their counterparts.[165] An assessment of whether information-sharing is necessary and relevant to the mandate of the recipient allows intelligence services to uphold the principle of minimization when sharing information, i.e., intelligence services minimize the amount of personal data shared to the greatest extent possible.[166] These safeguards help to prevent excessive or arbitrary intelligence-sharing.

48. In view of the possible implications of intelligence-sharing for human rights, it is good practice for intelligence services to screen all outgoing information for accuracy and relevance before sending it to foreign entities.[167] Where there are doubts about the reliability of outgoing intelligence, it is either withheld or accompanied by error estimates.[168] Finally, it is good practice for all intelligence-sharing to take place in writing and to be recorded; this facilitates subsequent review by oversight institutions.[169]

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

49. It is good practice for oversight institutions to be mandated to review the agreements upon which intelligence-sharing is based, as well as any arrangements based on such agreements.[170] Independent oversight institutions can scrutinize the legal framework and procedural dimensions of intelligence-sharing agreements to ensure that they comply with national laws and relevant international legal standards. As a general rule, oversight institutions are authorized to have access to all information necessary to fulfil their mandate (see practice 7 above). However, within the context of international intelligence-sharing, the third party rule may entail restrictions on oversight institutions' access to incoming information provided by foreign entities. Oversight institutions are generally considered to be third parties; therefore, they cannot normally have access to information shared with intelligence services by foreign entities. Nevertheless, oversight institutions have a right to scrutinize information sent to foreign entities, and they exercise this right as part of a mandate to oversee all aspects of an intelligence service's activities (see practice 7 above). Within this context, it is good practice for national law to explicitly require intelligence services to report intelligence-sharing to an independent oversight institution.[171] This

Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with foreign intelligence and/or security services, p. 24.

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

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

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

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

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

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

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

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

provides a check on the legality of intelligence-sharing practices, and is an important safeguard against the sharing of personal data that may have serious human rights implications for the individuals concerned.

> **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.

50. National laws regulating the activities of intelligence services provide legal and institutional safeguards to protect human rights and the constitutional legal order within the context of intelligence activities. In view of this, it would be contrary to the rule of law for States or their intelligence services to request a foreign entity to undertake activities in their jurisdiction that they could not lawfully undertake themselves. It would be good practice for national law to contain an absolute prohibition on intelligence services cooperating with foreign entities in order to evade legal obligations that apply to their own activities.[172] In addition, it is important to recall that States have an international legal obligation to safeguard the rights of all individuals under their jurisdiction. This implies that they have a duty to ensure that foreign intelligence services do not engage in activities that violate human rights on their territory, as well as to refrain from participating in any such activities.[173] Indeed, States are internationally responsible if they aid or assist another State to violate the human rights of individuals.[174]

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

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

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

Annex

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) They are prescribed by publicly available law that complies with international human rights standards;

(b) All such measures must be strictly necessary for an intelligence service to fulfil its legally prescribed mandate;

(c) Measures taken must be proportionate to the objective. This requires that intelligence services select the measure that least restricts human rights, and take special care to minimize the adverse impact of any measures on the rights of individuals, including, in particular, persons who are not suspected of any wrongdoing;

(d) No measure taken by intelligence services may violate peremptory norms of international law or the essence of any human right;

(e) There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights;

(f) Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy**.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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