unicef australia

Mr Dan Tehan MP
Committee Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

10 December 2015

Dear Chair,

Counter-Terrorism Legislation Amendment Bill (No. 1) 2015

UNICEF Australia is grateful for the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security regarding the *Counter-Terrorism Legislation Amendment Bill (No. 1) 2015.*

1. About UNICEF Australia

UNICEF is a multilateral organisation that works in over 190 countries to promote and protect the rights of children. UNICEF supports child health and nutrition, clean water and sanitation, quality basic education for all boys and girls, and the protection of children from violence, exploitation, abuse and HIV. UNICEF is unique among world organisations and unique in our rights based and participatory approach to working with children and young people. UNICEF Australia is the national committee for UNICEF in Australia and has a dual mandate of raising funds to advance the rights of all children and support governments to deliver quality outcomes for children, consistent with Australia's human rights obligations.

UNICEF is committed to protect children from all forms of violence, regardless of where they are in the world. UNICEF Australia recognises the complexity of the challenges facing governments as they seek to keep all people, including children, safe, and respond to terrorist or extremist related activities that pose threats of violence or harm to the community. UNICEF Australia believes that safety and security can be pursued in a framework that respects the human rights of all people, especially children, by ensuring that responses are reasonable, necessary and proportionate. International human rights treaties, such as the *Convention on the Rights of the Child*, provide a framework in which national security measures can be pursued through means which also protect the rights of all those affected, including children.

2. UNICEF Australia's core observations re the *Counter-Terrorism Legislation Amendment Bill (No. 1) 2015*

UNICEF Australia notes with specific concern the proposal included in the Bill which would lower the age that control orders can be used against children from 16 years to 14 years. UNICEF Australia is particularly concerned that:

- Coercive mechanisms such as control orders may significantly interfere with multiple human rights of children affected including, but not limited to, freedom of movement, freedom of speech, right to privacy, right to education, right to a fair trial and the presumption of innocence;

Australian Committee for UNICEF Limited
Level 4, 280 Pitt Street, Sydney NSW 2000
P +61 2 9261 2811 **F** +61 2 9261 2844 **E** unicef@unicef.org.au
PO Box 488, Queen Victoria Building, NSW 1230 | ABN 35 060 581 437
www.unicef.org.au | **Donation Hotline: 1300 884 233**

- Control orders are applied to individuals (including children) outside of the safeguards which apply in the context of a criminal prosecution;
- The Bill does not explicitly require that the best interests of the child be a "primary consideration" as required by article 3 of the *Convention on the Rights of the Child*;
- As noted by the Parliamentary Joint Committee on Human Rights in the Thirty-second report of the 44th Parliament (1 December 2015), the Explanatory Memorandum does not explain with specific detail how the proposal to lower the age at which control orders can be applied to children is rationally connected to a legitimate objective or that such a measure is reasonable, necessary and proportionate; and
- The right of the child to be heard (in particular, through access to review, remedy or redress) is not adequately safeguarded in the proposal. For example:
    - the Bill does not require a child to be provided with 1) a minimum standard of information regarding the allegations against him or her; or 2) information regarding all review and appeal rights. In effect, this lack of information could limit a child's ability to express his or her view and also could practically limit the ability of the child to challenge the imposition of a control order and/or aspects of the obligations, prohibitions and restrictions imposed by the order; and
    - the court is not required to take the views of the child into consideration in determining the impact of the order on the child's circumstances or in the court's assessment of the child's best interests.

Although UNICEF Australia is not able to fully comment in detail on the extensive proposals in the timeframe provided, we wish to draw to the Committee's attention to a number of important resources which speak to issues raised by the proposals applying to children. Accordingly, please find **attached**:

1) United Nations Committee on the Rights of the Child – General Comment No. 10 (2007) Children's rights in juvenile justice – which outlines the rights of the child in the context of contact with the criminal justice system;
2) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Document A/63/223 (6 August 2008) - which speaks to the issue of a fair hearing, including representation and standard of proof;
3) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, UN Document A/HRC/13/37 (28 December 2009) - which speaks on the right to privacy; and
4) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, UN Document A/HRC/14/46 (17 May 2010) - which speaks on the frameworks for intelligence services and their oversight.

UNICEF Australia encourages the Committee to consider the proposals applying to children in the *Counter-Terrorism Legislation Amendment Bill (No. 1) 2015* in light of both the *Convention on the Rights of the Child* and the guidance provided in these documents.

3. Contact

If you have any questions, please contact Ms Alison Elliott, Legal Advisor, UNICEF Australia

UNITED
NATIONS

CRC

Convention on the
Rights of the Child

Distr.
GENERAL

CRC/C/GC/10
25 April 2007

Original: ENGLISH

COMMITTEE ON THE RIGHTS OF THE CHILD
Forty-fourth session
Geneva, 15 January-2 February 2007

GENERAL COMMENT No. 10 (2007)

Children's rights in juvenile justice

GE.07-41351 (E) 270407

CONTENTS

I. INTRODUCTION

1. In the reports they submit to the Committee on the Rights of the Child (hereafter: the Committee), States parties often pay quite detailed attention to the rights of children alleged as, accused of, or recognized as having infringed the penal law, also referred to as "children in conflict with the law". In line with the Committee's guidelines for periodic reporting, the implementation of articles 37 and 40 of the Convention on the Rights of the Child (hereafter: CRC) is the main focus of the information provided by the States parties. The Committee notes with appreciation the many efforts to establish an administration of juvenile justice in compliance with CRC. However, it is also clear that many States parties still have a long way to go in achieving full compliance with CRC, e.g. in the areas of procedural rights, the development and implementation of measures for dealing with children in conflict with the law without resorting to judicial proceedings, and the use of deprivation of liberty only as a measure of last resort.

2. The Committee is equally concerned about the lack of information on the measures that States parties have taken to prevent children from coming into conflict with the law. This may be the result of a lack of a comprehensive policy for the field of juvenile justice. This may also explain why many States parties are providing only very limited statistical data on the treatment of children in conflict with the law.

3. The experience in reviewing the States parties' performance in the field of juvenile justice is the reason for the present general comment, by which the Committee wants to provide the States parties with more elaborated guidance and recommendations for their efforts to establish an administration of juvenile justice in compliance with CRC. This juvenile justice, which should promote, inter alia, the use of alternative measures such as diversion and restorative justice, will provide States parties with possibilities to respond to children in conflict with the law in an effective manner serving not only the best interests of these children, but also the short- and long-term interest of the society at large.

II. THE OBJECTIVES OF THE PRESENT GENERAL COMMENT

4. At the outset, the Committee wishes to underscore that CRC requires States parties to develop and implement a comprehensive juvenile justice policy. This comprehensive approach should not be limited to the implementation of the specific provisions contained in articles 37 and 40 of CRC, but should also take into account the general principles enshrined in articles 2, 3, 6 and 12, and in all other relevant articles of CRC, such as articles 4 and 39. Therefore, the objectives of this general comment are:

- To encourage States parties to develop and implement a comprehensive juvenile justice policy to prevent and address juvenile delinquency based on and in compliance with CRC, and to seek in this regard advice and support from the Interagency Panel on Juvenile Justice, with representatives of the Office of the United Nations High Commissioner for Human Rights (OHCHR), the United Nations Children's Fund (UNICEF), the United Nations Office on Drugs and Crime (UNODC) and non-governmental organizations (NGO's), established by ECOSOC resolution 1997/30;

- To provide States parties with guidance and recommendations for the content of this comprehensive juvenile justice policy, with special attention to prevention of juvenile delinquency, the introduction of alternative measures allowing for responses to juvenile delinquency without resorting to judicial procedures, and for the interpretation and implementation of all other provisions contained in articles 37 and 40 of CRC;

- To promote the integration, in a national and comprehensive juvenile justice policy, of other international standards, in particular, the United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the "Beijing Rules"), the United Nations Rules for the Protection of Juveniles Deprived of their Liberty (the "Havana Rules"), and the United Nations Guidelines for the Prevention of Juvenile Delinquency (the "Riyadh Guidelines").

III. JUVENILE JUSTICE: THE LEADING PRINCIPLES OF A COMPREHENSIVE POLICY

5. Before elaborating on the requirements of CRC in more detail, the Committee will first mention the leading principles of a comprehensive policy for juvenile justice. In the administration of juvenile justice, States parties have to apply systematically the general principles contained in articles 2, 3, 6 and 12 of CRC, as well as the fundamental principles of juvenile justice enshrined in articles 37 and 40.

Non-discrimination (art. 2)

6. States parties have to take all necessary measures to ensure that all children in conflict with the law are treated equally. Particular attention must be paid to de facto discrimination and disparities, which may be the result of a lack of a consistent policy and involve vulnerable groups of children, such as street children, children belonging to racial, ethnic, religious or linguistic minorities, indigenous children, girl children, children with disabilities and children who are repeatedly in conflict with the law (recidivists). In this regard, training of all professionals involved in the administration of juvenile justice is important (see paragraph 97 below), as well as the establishment of rules, regulations or protocols which enhance equal treatment of child offenders and provide redress, remedies and compensation.

7. Many children in conflict with the law are also victims of discrimination, e.g. when they try to get access to education or to the labour market. It is necessary that measures are taken to prevent such discrimination, inter alia, as by providing former child offenders with appropriate support and assistance in their efforts to reintegrate in society, and to conduct public campaigns emphasizing their right to assume a constructive role in society (art. 40 (1)).

8. It is quite common that criminal codes contain provisions criminalizing behavioural problems of children, such as vagrancy, truancy, runaways and other acts, which often are the result of psychological or socio-economic problems. It is particularly a matter of concern that girls and street children are often victims of this criminalization. These acts, also known as Status Offences, are not considered to be such if committed by adults. The Committee recommends that the States parties abolish the provisions on status offences in order to establish

an equal treatment under the law for children and adults. In this regard, the Committee also refers to article 56 of the Riyadh Guidelines which reads: "In order to prevent further stigmatization, victimization and criminalization of young persons, legislation should be enacted to ensure that any conduct not considered an offence or not penalized if committed by an adult is not considered an offence and not penalized if committed by a young person."

9. In addition, behaviour such as vagrancy, roaming the streets or runaways should be dealt with through the implementation of child protective measures, including effective support for parents and/or other caregivers and measures which address the root causes of this behaviour.

Best interests of the child (art. 3)

10. In all decisions taken within the context of the administration of juvenile justice, the best interests of the child should be a primary consideration. Children differ from adults in their physical and psychological development, and their emotional and educational needs. Such differences constitute the basis for the lesser culpability of children in conflict with the law. These and other differences are the reasons for a separate juvenile justice system and require a different treatment for children. The protection of the best interests of the child means, for instance, that the traditional objectives of criminal justice, such as repression/retribution, must give way to rehabilitation and restorative justice objectives in dealing with child offenders. This can be done in concert with attention to effective public safety.

The right to life, survival and development (art. 6)

11. This inherent right of every child should guide and inspire States parties in the development of effective national policies and programmes for the prevention of juvenile delinquency, because it goes without saying that delinquency has a very negative impact on the child's development. Furthermore, this basic right should result in a policy of responding to juvenile delinquency in ways that support the child's development. The death penalty and a life sentence without parole are explicitly prohibited under article 37 (a) of CRC (see paragraphs 75-77 below). The use of deprivation of liberty has very negative consequences for the child's harmonious development and seriously hampers his/her reintegration in society. In this regard, article 37 (b) explicitly provides that deprivation of liberty, including arrest, detention and imprisonment, should be used only as a measure of last resort and for the shortest appropriate period of time, so that the child's right to development is fully respected and ensured (see paragraphs 78-88 below).[1]

The right to be heard (art. 12)

12. The right of the child to express his/her views freely in all matters affecting the child should be fully respected and implemented throughout every stage of the process of juvenile

[1] Note that the rights of a child deprived of his/her liberty, as recognized in CRC, apply with respect to children in conflict with the law, and to children placed in institutions for the purposes of care, protection or treatment, including mental health, educational, drug treatment, child protection or immigration institutions.

justice (see paragraphs 43-45 below). The Committee notes that the voices of children involved in the juvenile justice system are increasingly becoming a powerful force for improvements and reform, and for the fulfilment of their rights.

Dignity (art. 40 (1))

13. CRC provides a set of fundamental principles for the treatment to be accorded to children in conflict with the law:

- *Treatment that is consistent with the child's sense of dignity and worth.* This principle reflects the fundamental human right enshrined in article 1 of UDHR, which stipulates that all human beings are born free and equal in dignity and rights. This inherent right to dignity and worth, to which the preamble of CRC makes explicit reference, has to be respected and protected throughout the entire process of dealing with the child, from the first contact with law enforcement agencies and all the way to the implementation of all measures for dealing with the child;

- *Treatment that reinforces the child's respect for the human rights and freedoms of others.* This principle is in line with the consideration in the preamble that a child should be brought up in the spirit of the ideals proclaimed in the Charter of the United Nations. It also means that, within the juvenile justice system, the treatment and education of children shall be directed to the development of respect for human rights and freedoms (art. 29 (1) (b) of CRC and general comment No. 1 on the aims of education). It is obvious that this principle of juvenile justice requires a full respect for and implementation of the guarantees for a fair trial recognized in article 40 (2) (see paragraphs 40-67 below). If the key actors in juvenile justice, such as police officers, prosecutors, judges and probation officers, do not fully respect and protect these guarantees, how can they expect that with such poor examples the child will respect the human rights and fundamental freedom of others?;

- *Treatment that takes into account the child's age and promotes the child's reintegration and the child's assuming a constructive role in society.* This principle must be applied, observed and respected throughout the entire process of dealing with the child, from the first contact with law enforcement agencies all the way to the implementation of all measures for dealing with the child. It requires that all professionals involved in the administration of juvenile justice be knowledgeable about child development, the dynamic and continuing growth of children, what is appropriate to their well-being, and the pervasive forms of violence against children;

- *Respect for the dignity of the child requires that all forms of violence in the treatment of children in conflict with the law must be prohibited and prevented.* Reports received by the Committee show that violence occurs in all phases of the juvenile justice process, from the first contact with the police, during pretrial detention and during the stay in treatment and other facilities for children sentenced to deprivation of liberty. The committee urges the States parties to take effective measures to prevent such violence and to make sure that the perpetrators are brought to justice and to give effective follow-up to the recommendations made in the report on the United Nations Study on Violence Against Children presented to the General Assembly in October 2006 (A/61/299).

14. The Committee acknowledges that the preservation of public safety is a legitimate aim of the justice system. However, it is of the opinion that this aim is best served by a full respect for and implementation of the leading and overarching principles of juvenile justice as enshrined in CRC.

IV. JUVENILE JUSTICE: THE CORE ELEMENTS OF A COMPREHENSIVE POLICY

15. A comprehensive policy for juvenile justice must deal with the following core elements: the prevention of juvenile delinquency; interventions without resorting to judicial proceedings and interventions in the context of judicial proceedings; the minimum age of criminal responsibility and the upper age-limits for juvenile justice; the guarantees for a fair trial; and deprivation of liberty including pretrial detention and post-trial incarceration.

A. Prevention of juvenile delinquency

16. One of the most important goals of the implementation of CRC is to promote the full and harmonious development of the child's personality, talents and mental and physical abilities (preamble, and articles 6 and 29). The child should be prepared to live an individual and responsible life in a free society (preamble, and article 29), in which he/she can assume a constructive role with respect for human rights and fundamental freedoms (arts. 29 and 40). In this regard, parents have the responsibility to provide the child, in a manner consistent with his evolving capacities, with appropriate direction and guidance in the exercise of her/his rights as recognized in the Convention. In the light of these and other provisions of CRC, it is obviously not in the best interests of the child if he/she grows up in circumstances that may cause an increased or serious risk of becoming involved in criminal activities. Various measures should be taken for the full and equal implementation of the rights to an adequate standard of living (art. 27), to the highest attainable standard of health and access to health care (art. 24), to education (arts. 28 and 29), to protection from all forms of physical or mental violence, injury or abuse (art. 19), and from economic or sexual exploitation (arts. 32 and 34), and to other appropriate services for the care or protection of children.

17. As stated above, a juvenile justice policy without a set of measures aimed at preventing juvenile delinquency suffers from serious shortcomings. States parties should fully integrate into their comprehensive national policy for juvenile justice the United Nations Guidelines for the Prevention of Juvenile Delinquency (the Riyadh Guidelines) adopted by the General Assembly in its resolution 45/112 of 14 December 1990.

18. The Committee fully supports the Riyadh Guidelines and agrees that emphasis should be placed on prevention policies that facilitate the successful socialization and integration of all children, in particular through the family, the community, peer groups, schools, vocational training and the world of work, as well as through voluntary organizations. This means, inter alia that prevention programmes should focus on support for particularly vulnerable families, the involvement of schools in teaching basic values (including information about the rights and responsibilities of children and parents under the law), and extending special care and attention to young persons at risk. In this regard, particular attention should also be given to children who drop out of school or otherwise do not complete their education. The use of peer group support and a strong involvement of parents are recommended. The States parties should also develop

community-based services and programmes that respond to the special needs, problems, concerns and interests of children, in particular of children repeatedly in conflict with the law, and that provide appropriate counselling and guidance to their families.

19. Articles 18 and 27 of CRC confirm the importance of the responsibility of parents for the upbringing of their children, but at the same time CRC requires States parties to provide the necessary assistance to parents (or other caretakers), in the performance of their parental responsibilities. The measures of assistance should not only focus on the prevention of negative situations, but also and even more on the promotion of the social potential of parents. There is a wealth of information on home- and family-based prevention programmes, such as parent training, programmes to enhance parent-child interaction and home visitation programmes, which can start at a very young age of the child. In addition, early childhood education has shown to be correlated with a lower rate of future violence and crime. At the community level, positive results have been achieved with programmes such as Communities that Care (CTC), a risk-focused prevention strategy.

20. States parties should fully promote and support the involvement of children, in accordance with article 12 of CRC, and of parents, community leaders and other key actors (e.g. representatives of NGOs, probation services and social workers), in the development and implementation of prevention programmes. The quality of this involvement is a key factor in the success of these programmes.

21. The Committee recommends that States parties seek support and advice from the Interagency Panel on Juvenile Justice in their efforts to develop effective prevention programmes.

B. Interventions/diversion (see also section E below)

22. Two kinds of interventions can be used by the State authorities for dealing with children alleged as, accused of, or recognized as having infringed the penal law: measures without resorting to judicial proceedings and measures in the context of judicial proceedings. The Committee reminds States parties that utmost care must be taken to ensure that the child's human rights and legal safeguards are thereby fully respected and protected.

23. Children in conflict with the law, including child recidivists, have the right to be treated in ways that promote their reintegration and the child's assuming a constructive role in society (art. 40 (1) of CRC). The arrest, detention or imprisonment of a child may be used only as a measure of last resort (art. 37 (b)). It is, therefore, necessary - as part of a comprehensive policy for juvenile justice - to develop and implement a wide range of measures to ensure that children are dealt with in a manner appropriate to their well-being, and proportionate to both their circumstances and the offence committed. These should include care, guidance and supervision, counselling, probation, foster care, educational and training programmes, and other alternatives to institutional care (art. 40 (4)).

Interventions without resorting to judicial proceedings

24. According to article 40 (3) of CRC, the States parties shall seek to promote measures for dealing with children alleged as, accused of, or recognized as having infringed the penal law

without resorting to judicial proceedings, whenever appropriate and desirable. Given the fact that the majority of child offenders commit only minor offences, a range of measures involving removal from criminal/juvenile justice processing and referral to alternative (social) services (i.e. diversion) should be a well-established practice that can and should be used in most cases.

25. In the opinion of the Committee, the obligation of States parties to promote measures for dealing with children in conflict with the law without resorting to judicial proceedings applies, but is certainly not limited to children who commit minor offences, such as shoplifting or other property offences with limited damage, and first-time child offenders. Statistics in many States parties indicate that a large part, and often the majority, of offences committed by children fall into these categories. It is in line with the principles set out in article 40 (1) of CRC to deal with all such cases without resorting to criminal law procedures in court. In addition to avoiding stigmatization, this approach has good results for children and is in the interests of public safety, and has proven to be more cost-effective.

26. States parties should take measures for dealing with children in conflict with the law without resorting to judicial proceedings as an integral part of their juvenile justice system, and ensure that children's human rights and legal safeguards are thereby fully respected and protected (art. 40 (3) (b)).

27. It is left to the discretion of States parties to decide on the exact nature and content of the measures for dealing with children in conflict with the law without resorting to judicial proceedings, and to take the necessary legislative and other measures for their implementation. Nonetheless, on the basis of the information provided in the reports from some States parties, it is clear that a variety of community-based programmes have been developed, such as community service, supervision and guidance by for example social workers or probation officers, family conferencing and other forms of restorative justice including restitution to and compensation of victims. Other States parties should benefit from these experiences. As far as full respect for human rights and legal safeguards is concerned, the Committee refers to the relevant parts of article 40 of CRC and emphasizes the following:

- Diversion (i.e. measures for dealing with children, alleged as, accused of, or recognized as having infringed the penal law without resorting to judicial proceedings) should be used only when there is compelling evidence that the child committed the alleged offence, that he/she freely and voluntarily admits responsibility, and that no intimidation or pressure has been used to get that admission and, finally, that the admission will not be used against him/her in any subsequent legal proceeding;

- The child must freely and voluntarily give consent in writing to the diversion, a consent that should be based on adequate and specific information on the nature, content and duration of the measure, and on the consequences of a failure to cooperate, carry out and complete the measure. With a view to strengthening parental involvement, States parties may also consider requiring the consent of parents, in particular when the child is below the age of 16 years;

- The law has to contain specific provisions indicating in which cases diversion is possible, and the powers of the police, prosecutors and/or other agencies to make decisions in this regard should be regulated and reviewed, in particular to protect the child from discrimination;

- The child must be given the opportunity to seek legal or other appropriate assistance on the appropriateness and desirability of the diversion offered by the competent authorities, and on the possibility of review of the measure;

- The completion of the diversion by the child should result in a definite and final closure of the case. Although confidential records can be kept of diversion for administrative and review purposes, they should not be viewed as "criminal records" and a child who has been previously diverted must not be seen as having a previous conviction. If any registration takes place of this event, access to that information should be given exclusively and for a limited period of time, e.g. for a maximum of one year, to the competent authorities authorized to deal with children in conflict with the law.

Interventions in the context of judicial proceedings

28. When judicial proceedings are initiated by the competent authority (usually the prosecutor's office), the principles of a fair and just trial must be applied (see section D below). At the same time, the juvenile justice system should provide for ample opportunities to deal with children in conflict with the law by using social and/or educational measures, and to strictly limit the use of deprivation of liberty, and in particular pretrial detention, as a measure of last resort. In the disposition phase of the proceedings, deprivation of liberty must be used only as a measure of last resort and for the shortest appropriate period of time (art. 37 (b)). This means that States parties should have in place a well-trained probation service to allow for the maximum and effective use of measures such as guidance and supervision orders, probation, community monitoring or day report centres, and the possibility of early release from detention.

29. The Committee reminds States parties that, pursuant to article 40 (1) of CRC, reintegration requires that no action may be taken that can hamper the child's full participation in his/her community, such as stigmatization, social isolation, or negative publicity of the child. For a child in conflict with the law to be dealt with in a way that promotes reintegration requires that all actions should support the child becoming a full, constructive member of his/her society.

C. Age and children in conflict with the law

The minimum age of criminal responsibility

30. The reports submitted by States parties show the existence of a wide range of minimum ages of criminal responsibility. They range from a very low level of age 7 or 8 to the commendable high level of age 14 or 16. Quite a few States parties use two minimum ages of criminal responsibility. Children in conflict with the law who at the time of the commission of the crime are at or above the lower minimum age but below the higher minimum age are assumed to be criminally responsible only if they have the required maturity in that regard. The assessment of this maturity is left to the court/judge, often without the requirement of involving a psychological expert, and results in practice in the use of the lower minimum age in cases of

serious crimes. The system of two minimum ages is often not only confusing, but leaves much to the discretion of the court/judge and may result in discriminatory practices. In the light of this wide range of minimum ages for criminal responsibility the Committee feels that there is a need to provide the States parties with clear guidance and recommendations regarding the minimum age of criminal responsibility.

31. Article 40 (3) of CRC requires States parties to seek to promote, inter alia, the establishment of a minimum age below which children shall be presumed not to have the capacity to infringe the penal law, but does not mention a specific minimum age in this regard. The committee understands this provision as an obligation for States parties to set a minimum age of criminal responsibility (MACR). This minimum age means the following:

- Children who commit an offence at an age below that minimum cannot be held responsible in a penal law procedure. Even (very) young children do have the capacity to infringe the penal law but if they commit an offence when below MACR the irrefutable assumption is that they cannot be formally charged and held responsible in a penal law procedure. For these children special protective measures can be taken if necessary in their best interests;

- Children at or above the MACR at the time of the commission of an offence (or: infringement of the penal law) but younger than 18 years (see also paragraphs 35-38 below) can be formally charged and subject to penal law procedures. But these procedures, including the final outcome, must be in full compliance with the principles and provisions of CRC as elaborated in the present general comment.

32. Rule 4 of the Beijing Rules recommends that the beginning of MACR shall not be fixed at too low an age level, bearing in mind the facts of emotional, mental and intellectual maturity. In line with this rule the Committee has recommended States parties not to set a MACR at a too low level and to increase the existing low MACR to an internationally acceptable level. From these recommendations, it can be concluded that a minimum age of criminal responsibility below the age of 12 years is considered by the Committee not to be internationally acceptable. States parties are encouraged to increase their lower MACR to the age of 12 years as the absolute minimum age and to continue to increase it to a higher age level.

33. At the same time, the Committee urges States parties not to lower their MACR to the age of 12. A higher MACR, for instance 14 or 16 years of age, contributes to a juvenile justice system which, in accordance with article 40 (3) (b) of CRC, deals with children in conflict with the law without resorting to judicial proceedings, providing that the child's human rights and legal safeguards are fully respected. In this regard, States parties should inform the Committee in their reports in specific detail how children below the MACR set in their laws are treated when they are recognized as having infringed the penal law, or are alleged as or accused of having done so, and what kinds of legal safeguards are in place to ensure that their treatment is as fair and just as that of children at or above MACR.

34. The Committee wishes to express its concern about the practice of allowing exceptions to a MACR which permit the use of a lower minimum age of criminal responsibility in cases where

the child, for example, is accused of committing a serious offence or where the child is considered mature enough to be held criminally responsible. The Committee strongly recommends that States parties set a MACR that does not allow, by way of exception, the use of a lower age.

35. If there is no proof of age and it cannot be established that the child is at or above the MACR, the child shall not be held criminally responsible (see also paragraph 39 below).

The upper age-limit for juvenile justice

36. The Committee also wishes to draw the attention of States parties to the upper age-limit for the application of the rules of juvenile justice. These special rules - in terms both of special procedural rules and of rules for diversion and special measures - should apply, starting at the MACR set in the country, for all children who, at the time of their alleged commission of an offence (or act punishable under the criminal law), have not yet reached the age of 18 years.

37. The Committee wishes to remind States parties that they have recognized the right of every child alleged as, accused of, or recognized as having infringed the penal law to be treated in accordance with the provisions of article 40 of CRC. This means that every person under the age of 18 years at the time of the alleged commission of an offence must be treated in accordance with the rules of juvenile justice.

38. The Committee, therefore, recommends that those States parties which limit the applicability of their juvenile justice rules to children under the age of 16 (or lower) years, or which allow by way of exception that 16 or 17-year-old children are treated as adult criminals, change their laws with a view to achieving a non-discriminatory full application of their juvenile justice rules to all persons under the age of 18 years. The Committee notes with appreciation that some States parties allow for the application of the rules and regulations of juvenile justice to persons aged 18 and older, usually till the age of 21, either as a general rule or by way of exception.

39. Finally, the Committee wishes to emphasize the fact that it is crucial for the full implementation of article 7 of CRC requiring, inter alia, that every child shall be registered immediately after birth to set age-limits one way or another, which is the case for all States parties. A child without a provable date of birth is extremely vulnerable to all kinds of abuse and injustice regarding the family, work, education and labour, particularly within the juvenile justice system. Every child must be provided with a birth certificate free of charge whenever he/she needs it to prove his/her age. If there is no proof of age, the child is entitled to a reliable medical or social investigation that may establish his/her age and, in the case of conflict or inconclusive evidence, the child shall have the right to the rule of the benefit of the doubt.

D. The guarantees for a fair trial

40. Article 40 (2) of CRC contains an important list of rights and guarantees that are all meant to ensure that every child alleged as or accused of having infringed the penal law receives fair treatment and trial. Most of these guarantees can also be found in article 14 of the International Covenant on Civil and Political Rights (ICCPR), which the Human Rights Committee elaborated and commented on in its general comment No. 13 (1984) (Administration of justice) which is

currently in the process of being reviewed. However, the implementation of these guarantees for children does have some specific aspects which will be presented in this section. Before doing so, the Committee wishes to emphasize that a key condition for a proper and effective implementation of these rights or guarantees is the quality of the persons involved in the administration of juvenile justice. The training of professionals, such as police officers, prosecutors, legal and other representatives of the child, judges, probation officers, social workers and others is crucial and should take place in a systematic and ongoing manner. These professionals should be well informed about the child's, and particularly about the adolescent's physical, psychological, mental and social development, as well as about the special needs of the most vulnerable children, such as children with disabilities, displaced children, street children, refugee and asylum-seeking children, and children belonging to racial, ethnic, religious, linguistic or other minorities (see paragraphs 6-9 above). Since girls in the juvenile justice system may be easily overlooked because they represent only a small group, special attention must be paid to the particular needs of the girl child, e.g. in relation to prior abuse and special health needs. Professionals and staff should act under all circumstances in a manner consistent with the child's dignity and worth, which reinforces the child's respect for the human rights and fundamental freedoms of others, and which promotes the child's reintegration and his/her assuming a constructive role in society (art. 40 (1)). All the guarantees recognized in article 40 (2), which will be dealt with hereafter, are minimum standards, meaning that States parties can and should try to establish and observe higher standards, e.g. in the areas of legal assistance and the involvement of the child and her/his parents in the judicial process.

No retroactive juvenile justice (art. 40 (2) (a))

41. Article 40 (2) (a) of CRC affirms that the rule that no one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence, under national or international law, at the time it was committed is also applicable to children (see also article 15 of ICCPR). It means that no child can be charged with or sentenced under the penal law for acts or omissions which at the time they were committed were not prohibited under national or international law. In the light of the fact that many States parties have recently strengthened and/or expanded their criminal law provisions to prevent and combat terrorism, the Committee recommends that States parties ensure that these changes do not result in retroactive or unintended punishment of children. The Committee also wishes to remind States parties that the rule that no heavier penalty shall be imposed than the one that was applicable at the time when the criminal offence was committed, as expressed in article 15 of ICCPR, is in the light of article 41 of CRC, applicable to children in the States parties to ICCPR. No child shall be punished with a heavier penalty than the one applicable at the time of his/her infringement of the penal law. But if a change of law after the act provides for a lighter penalty, the child should benefit from this change.

The presumption of innocence (art. 40 (2) (b) (i))

42. The presumption of innocence is fundamental to the protection of the human rights of children in conflict with the law. It means that the burden of proof of the charge(s) brought against the child is on the prosecution. The child alleged as or accused of having infringed the penal law has the benefit of doubt and is only guilty as charged if these charges have been proven beyond reasonable doubt. The child has the right to be treated in accordance with this presumption and it is the duty of all public authorities or others involved to refrain from

prejudging the outcome of the trial. States parties should provide information about child development to ensure that this presumption of innocence is respected in practice. Due to the lack of understanding of the process, immaturity, fear or other reasons, the child may behave in a suspicious manner, but the authorities must not assume that the child is guilty without proof of guilt beyond any reasonable doubt.

The right to be heard (art. 12)

43. Article 12 (2) of CRC requires that a child be provided with the opportunity to be heard in any judicial or administrative proceedings affecting the child, either directly or through a representative or an appropriate body in a manner consistent with the procedural rules of national law.

44. It is obvious that for a child alleged as, accused of, or recognized as having infringed the penal law, the right to be heard is fundamental for a fair trial. It is equally obvious that the child has the right to be heard directly and not only through a representative or an appropriate body if it is in her/his best interests. This right must be fully observed at all stages of the process, starting with pretrial stage when the child has the right to remain silent, as well as the right to be heard by the police, the prosecutor and the investigating judge. But it also applies to the stages of adjudication and of implementation of the imposed measures. In other words, the child must be given the opportunity to express his/her views freely, and those views should be given due weight in accordance with the age and maturity of the child (art. 12 (1)), throughout the juvenile justice process. This means that the child, in order to effectively participate in the proceedings, must be informed not only of the charges (see paragraphs 47-48 below), but also of the juvenile justice process as such and of the possible measures.

45. The child should be given the opportunity to express his/her views concerning the (alternative) measures that may be imposed, and the specific wishes or preferences he/she may have in this regard should be given due weight. Alleging that the child is criminally responsible implies that he/she should be competent and able to effectively participate in the decisions regarding the most appropriate response to allegations of his/her infringement of the penal law (see paragraph 46 below). It goes without saying that the judges involved are responsible for taking the decisions. But to treat the child as a passive object does not recognize his/her rights nor does it contribute to an effective response to his/her behaviour. This also applies to the implementation of the measure(s) imposed. Research shows that an active engagement of the child in this implementation will, in most cases, contribute to a positive result.

The right to effective participation in the proceedings (art 40 (2) (b) (iv))

46. A fair trial requires that the child alleged as or accused of having infringed the penal law be able to effectively participate in the trial, and therefore needs to comprehend the charges, and possible consequences and penalties, in order to direct the legal representative, to challenge witnesses, to provide an account of events, and to make appropriate decisions about evidence, testimony and the measure(s) to be imposed. Article 14 of the Beijing Rules provides that the proceedings should be conducted in an atmosphere of understanding to allow the child to participate and to express himself/herself freely. Taking into account the child's age and maturity may also require modified courtroom procedures and practices.

Prompt and direct information of the charge(s) (art. 40 (2) (b) (ii))

47. Every child alleged as or accused of having infringed the penal law has the right to be informed promptly and directly of the charges brought against him/her. Prompt and direct means as soon as possible, and that is when the prosecutor or the judge initially takes procedural steps against the child. But also when the authorities decide to deal with the case without resorting to judicial proceedings, the child must be informed of the charge(s) that may justify this approach. This is part of the requirement of article 40 (3) (b) of CRC that legal safeguards should be fully respected. The child should be informed in a language he/she understands. This may require a presentation of the information in a foreign language but also a "translation" of the formal legal jargon often used in criminal/juvenile charges into a language that the child can understand.

48. Providing the child with an official document is not enough and an oral explanation may often be necessary. The authorities should not leave this to the parents or legal guardians or the child's legal or other assistance. It is the responsibility of the authorities (e.g. police, prosecutor, judge) to make sure that the child understands each charge brought against him/her. The Committee is of the opinion that the provision of this information to the parents or legal guardians should not be an alternative to communicating this information to the child. It is most appropriate if both the child and the parents or legal guardians receive the information in such a way that they can understand the charge(s) and the possible consequences.

Legal or other appropriate assistance (art. 40 (2) (b) (ii))

49. The child must be guaranteed legal or other appropriate assistance in the preparation and presentation of his/her defence. CRC does require that the child be provided with assistance, which is not necessarily under all circumstances legal but it must be appropriate. It is left to the discretion of States parties to determine how this assistance is provided but it should be free of charge. The Committee recommends the State parties provide as much as possible for adequate trained legal assistance, such as expert lawyers or paralegal professionals. Other appropriate assistance is possible (e.g. social worker), but that person must have sufficient knowledge and understanding of the various legal aspects of the process of juvenile justice and must be trained to work with children in conflict with the law.

50. As required by article 14 (3) (b) of ICCPR, the child and his/her assistant must have adequate time and facilities for the preparation of his/her defence. Communications between the child and his/her assistance, either in writing or orally, should take place under such conditions that the confidentiality of such communications is fully respected in accordance with the guarantee provided for in article 40 (2) (b) (vii) of CRC, and the right of the child to be protected against interference with his/her privacy and correspondence (art. 16 of CRC). A number of States parties have made reservations regarding this guarantee (art. 40 (2) (b) (ii) of CRC), apparently assuming that it requires exclusively the provision of legal assistance and therefore by a lawyer. That is not the case and such reservations can and should be withdrawn.

Decisions without delay and with involvement of parents (art. 40 (2) (b) (iii))

51. Internationally there is a consensus that for children in conflict with the law the time between the commission of the offence and the final response to this act should be as short as

possible. The longer this period, the more likely it is that the response loses its desired positive, pedagogical impact, and the more the child will be stigmatized. In this regard, the Committee also refers to article 37 (d) of CRC, where the child deprived of liberty has the right to a prompt decision on his/her action to challenge the legality of the deprivation of his/her liberty. The term "prompt" is even stronger - and justifiably so given the seriousness of deprivation of liberty - than the term "without delay" (art. 40 (2) (b) (iii) of CRC), which is stronger than the term "without undue delay" of article 14 (3) (c) of ICCPR.

52. The Committee recommends that the States parties set and implement time limits for the period between the commission of the offence and the completion of the police investigation, the decision of the prosecutor (or other competent body) to bring charges against the child, and the final adjudication and decision by the court or other competent judicial body. These time limits should be much shorter than those set for adults. But at the same time, decisions without delay should be the result of a process in which the human rights of the child and legal safeguards are fully respected. In this decision-making process without delay, the legal or other appropriate assistance must be present. This presence should not be limited to the trial before the court or other judicial body, but also applies to all other stages of the process, beginning with the interviewing (interrogation) of the child by the police.

53. Parents or legal guardians should also be present at the proceedings because they can provide general psychological and emotional assistance to the child. The presence of parents does not mean that parents can act in defence of the child or be involved in the decision-making process. However, the judge or competent authority may decide, at the request of the child or of his/her legal or other appropriate assistance or because it is not in the best interests of the child (art. 3 of CRC), to limit, restrict or exclude the presence of the parents from the proceedings.

54. The Committee recommends that States parties explicitly provide by law for the maximum possible involvement of parents or legal guardians in the proceedings against the child. This involvement shall in general contribute to an effective response to the child's infringement of the penal law. To promote parental involvement, parents must be notified of the apprehension of their child as soon as possible.

55. At the same time, the Committee regrets the trend in some countries to introduce the punishment of parents for the offences committed by their children. Civil liability for the damage caused by the child's act can, in some limited cases, be appropriate, in particular for the younger children (e.g. below 16 years of age). But criminalizing parents of children in conflict with the law will most likely not contribute to their becoming active partners in the social reintegration of their child.

Freedom from compulsory self-incrimination (art. 40 (2) (b) (iii))

56. In line with article 14 (3) (g) of ICCPR, CRC requires that a child be not compelled to give testimony or to confess or acknowledge guilt. This means in the first place - and self-evidently - that torture, cruel, inhuman or degrading treatment in order to extract an admission or a confession constitutes a grave violation of the rights of the child (art. 37 (a) of CRC) and is wholly unacceptable. No such admission or confession can be admissible as evidence (article 15 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment).

57. There are many other less violent ways to coerce or to lead the child to a confession or a self-incriminatory testimony. The term "compelled" should be interpreted in a broad manner and not be limited to physical force or other clear violations of human rights. The age of the child, the child's development, the length of the interrogation, the child's lack of understanding, the fear of unknown consequences or of a suggested possibility of imprisonment may lead him/her to a confession that is not true. That may become even more likely if rewards are promised such as: "You can go home as soon as you have given us the true story", or lighter sanctions or release are promised.

58. The child being questioned must have access to a legal or other appropriate representative, and must be able to request the presence of his/her parent(s) during questioning. There must be independent scrutiny of the methods of interrogation to ensure that the evidence is voluntary and not coerced, given the totality of the circumstances, and is reliable. The court or other judicial body, when considering the voluntary nature and reliability of an admission or confession by a child, must take into account the age of the child, the length of custody and interrogation, and the presence of legal or other counsel, parent(s), or independent representatives of the child. Police officers and other investigating authorities should be well trained to avoid interrogation techniques and practices that result in coerced or unreliable confessions or testimonies.

Presence and examination of witnesses (art. 40 (2) (b) (iv))

59. The guarantee in article 40 (2) (b) (iv) of CRC underscores that the principle of equality of arms (i.e. under conditions of equality or parity between defence and prosecution) should be observed in the administration of juvenile justice. The term "to examine or to have examined" refers to the fact that there are distinctions in the legal systems, particularly between the accusatorial and inquisitorial trials. In the latter, the defendant is often allowed to examine witnesses although he/she rarely uses this right, leaving examination of the witnesses to the lawyer or, in the case of children, to another appropriate body. However, it remains important that the lawyer or other representative informs the child of the possibility to examine witnesses and to allow him/her to express his/her views in that regard, views which should be given due weight in accordance with the age and maturity of the child (art. 12).

The right to appeal (art. 40 (2) (b) (v))

60. The child has the right to appeal against the decision by which he is found guilty of the charge(s) brought against him/her and against the measures imposed as a consequence of this guilty verdict. This appeal should be decided by a higher, competent, independent and impartial authority or judicial body, in other words, a body that meets the same standards and requirements as the one that dealt with the case in the first instance. This guarantee is similar to the one expressed in article 14 (5) of ICCPR. This right of appeal is not limited to the most serious offences.

61. This seems to be the reason why quite a few States parties have made reservations regarding this provision in order to limit this right of appeal by the child to the more serious offences and/or imprisonment sentences. The Committee reminds States parties to the ICCPR

that a similar provision is made in article 14 (5) of the Covenant. In the light of article 41 of CRC, it means that this article should provide every adjudicated child with the right to appeal. The Committee recommends that the States parties withdraw their reservations to the provision in article 40 (2) (b) (v).

Free assistance of an interpreter (art. 40 (2) (vi))

62. If a child cannot understand or speak the language used by the juvenile justice system, he/she has the right to get free assistance of an interpreter. This assistance should not be limited to the court trial but should also be available at all stages of the juvenile justice process. It is also important that the interpreter has been trained to work with children, because the use and understanding of their mother tongue might be different from that of adults. Lack of knowledge and/or experience in that regard may impede the child's full understanding of the questions raised, and interfere with the right to a fair trial and to effective participation. The condition starting with "if", "if the child cannot understand or speak the language used", means that a child of a foreign or ethnic origin for example, who - besides his/her mother tongue - understands and speaks the official language, does not have to be provided with the free assistance of an interpreter.

63. The Committee also wishes to draw the attention of States parties to children with speech impairment or other disabilities. In line with the spirit of article 40 (2) (vi), and in accordance with the special protection measures provided to children with disabilities in article 23, the Committee recommends that States parties ensure that children with speech impairment or other disabilities are provided with adequate and effective assistance by well-trained professionals, e.g. in sign language, in case they are subject to the juvenile justice process (see also in this regard general comment No. 9 (The rights of children with disabilities) of the Committee on the Rights of the Child.

Full respect of privacy (arts. 16 and 40 (2) (b) (vii))

64. The right of a child to have his/her privacy fully respected during all stages of the proceedings reflects the right to protection of privacy enshrined in article 16 of CRC. "All stages of the proceedings" includes from the initial contact with law enforcement (e.g. a request for information and identification) up until the final decision by a competent authority, or release from supervision, custody or deprivation of liberty. In this particular context, it is meant to avoid harm caused by undue publicity or by the process of labelling. No information shall be published that may lead to the identification of a child offender because of its effect of stigmatization, and possible impact on his/her ability to have access to education, work, housing or to be safe. It means that a public authority should be very reluctant with press releases related to offences allegedly committed by children and limit them to very exceptional cases. They must take measures to guarantee that children are not identifiable via these press releases. Journalists who violate the right to privacy of a child in conflict with the law should be sanctioned with disciplinary and when necessary (e.g. in case of recidivism) with penal law sanctions.

65. In order to protect the privacy of the child, most States parties have as a rule - sometimes with the possibility of exceptions - that the court or other hearings of a child accused of an

infringement of the penal law should take place behind closed doors. This rule allows for the presence of experts or other professionals with a special permission of the court. Public hearings in juvenile justice should only be possible in well-defined cases and at the written decision of the court. Such a decision should be open for appeal by the child.

66. The Committee recommends that all States parties introduce the rule that court and other hearings of a child in conflict with the law be conducted behind closed doors. Exceptions to this rule should be very limited and clearly stated in the law. The verdict/sentence should be pronounced in public at a court session in such a way that the identity of the child is not revealed. The right to privacy (art. 16) requires all professionals involved in the implementation of the measures taken by the court or another competent authority to keep all information that may result in the identification of the child confidential in all their external contacts. Furthermore, the right to privacy also means that the records of child offenders should be kept strictly confidential and closed to third parties except for those directly involved in the investigation and adjudication of, and the ruling on, the case. With a view to avoiding stigmatization and/or prejudgements, records of child offenders should not be used in adult proceedings in subsequent cases involving the same offender (see the Beijing Rules, rules 21.1 and 21.2), or to enhance such future sentencing.

67. The Committee also recommends that the States parties introduce rules which would allow for an automatic removal from the criminal records of the name of the child who committed an offence upon reaching the age of 18, or for certain limited, serious offences where removal is possible at the request of the child, if necessary under certain conditions (e.g. not having committed an offence within two years after the last conviction).

E. Measures (see also chapter IV, section B, above)

Pretrial alternatives

68. The decision to initiate a formal criminal law procedure does not necessarily mean that this procedure must be completed with a formal court sentence for a child. In line with the observations made above in section B, the Committee wishes to emphasize that the competent authorities - in most States the office of the public prosecutor - should continuously explore the possibilities of alternatives to a court conviction. In other words, efforts to achieve an appropriate conclusion of the case by offering measures like the ones mentioned above in section B should continue. The nature and duration of these measures offered by the prosecution may be more demanding, and legal or other appropriate assistance for the child is then necessary. The performance of such a measure should be presented to the child as a way to suspend the formal criminal/juvenile law procedure, which will be terminated if the measure has been carried out in a satisfactory manner.

69. In this process of offering alternatives to a court conviction at the level of the prosecutor, the child's human rights and legal safeguards should be fully respected. In this regard, the Committee refers to the recommendations set out in paragraph 27 above, which equally apply here.

Dispositions by the juvenile court/judge

70. After a fair and just trial in full compliance with article 40 of CRC (see chapter IV, section D, above), a decision is made regarding the measures which should be imposed on the child found guilty of the alleged offence(s). The laws must provide the court/judge, or other competent, independent and impartial authority or judicial body, with a wide variety of possible alternatives to institutional care and deprivation of liberty, which are listed in a non-exhaustive manner in article 40 (4) of CRC, to assure that deprivation of liberty be used only as a measure of last resort and for the shortest possible period of time (art. 37 (b) of CRC).

71. The Committee wishes to emphasize that the reaction to an offence should always be in proportion not only to the circumstances and the gravity of the offence, but also to the age, lesser culpability, circumstances and needs of the child, as well as to the various and particularly long-term needs of the society. A strictly punitive approach is not in accordance with the leading principles for juvenile justice spelled out in article 40 (1) of CRC (see paragraphs 5-14 above). The Committee reiterates that corporal punishment as a sanction is a violation of these principles as well as of article 37 which prohibits all forms of cruel, inhuman and degrading treatment or punishment (see also the Committee's general comment No. 8 (2006) (The right of the child to protection from corporal punishment and other cruel or degrading forms of punishment)). In cases of severe offences by children, measures proportionate to the circumstances of the offender and to the gravity of the offence may be considered, including considerations of the need of public safety and sanctions. In the case of children, such considerations must always be outweighed by the need to safeguard the well-being and the best interests of the child and to promote his/her reintegration.

72. The Committee notes that if a penal disposition is linked to the age of a child, and there is conflicting, inconclusive or uncertain evidence of the child's age, he/she shall have the right to the rule of the benefit of the doubt (see also paragraphs 35 and 39 above).

73. As far as alternatives to deprivation of liberty/institutional care are concerned, there is a wide range of experience with the use and implementation of such measures. States parties should benefit from this experience, and develop and implement these alternatives by adjusting them to their own culture and tradition. It goes without saying that measures amounting to forced labour or to torture or inhuman and degrading treatment must be explicitly prohibited, and those responsible for such illegal practices should be brought to justice.

74. After these general remarks, the Committee wishes to draw attention to the measures prohibited under article 37 (a) of CRC, and to deprivation of liberty.

Prohibition of the death penalty

75. Article 37 (a) of CRC reaffirms the internationally accepted standard (see for example article 6 (5) of ICCPR) that the death penalty cannot be imposed for a crime committed by a person who at that time was under 18 years of age. Although the text is clear, there are States parties that assume that the rule only prohibits the execution of persons below the age of 18 years. However, under this rule the explicit and decisive criteria is the age at the time of the

commission of the offence. It means that a death penalty may not be imposed for a crime committed by a person under 18 regardless of his/her age at the time of the trial or sentencing or of the execution of the sanction.

76. The Committee recommends the few States parties that have not done so yet to abolish the death penalty for all offences committed by persons below the age of 18 years and to suspend the execution of all death sentences for those persons till the necessary legislative measures abolishing the death penalty for children have been fully enacted. The imposed death penalty should be changed to a sanction that is in full conformity with CRC.

No life imprisonment without parole

77. No child who was under the age of 18 at the time he or she committed an offence should be sentenced to life without the possibility of release or parole. For all sentences imposed upon children the possibility of release should be realistic and regularly considered. In this regard, the Committee refers to article 25 of CRC providing the right to periodic review for all children placed for the purpose of care, protection or treatment. The Committee reminds the States parties which do sentence children to life imprisonment with the possibility of release or parole that this sanction must fully comply with and strive for the realization of the aims of juvenile justice enshrined in article 40 (1) of CRC. This means inter alia that the child sentenced to this imprisonment should receive education, treatment, and care aiming at his/her release, reintegration and ability to assume a constructive role in society. This also requires a regular review of the child's development and progress in order to decide on his/her possible release. Given the likelihood that a life imprisonment of a child will make it very difficult, if not impossible, to achieve the aims of juvenile justice despite the possibility of release, the Committee strongly recommends the States parties to abolish all forms of life imprisonment for offences committed by persons under the age of 18.

F. Deprivation of liberty, including pretrial detention and post-trial incarceration

78. Article 37 of CRC contains the leading principles for the use of deprivation of liberty, the procedural rights of every child deprived of liberty, and provisions concerning the treatment of and conditions for children deprived of their liberty.

Basic principles

79. The leading principles for the use of deprivation of liberty are: (a) the arrest, detention or imprisonment of a child shall be in conformity with the law and shall be used only as a measure of last resort and for the shortest appropriate period of time; and (b) no child shall be deprived of his/her liberty unlawfully or arbitrarily.

80. The Committee notes with concern that, in many countries, children languish in pretrial detention for months or even years, which constitutes a grave violation of article 37 (b) of CRC. An effective package of alternatives must be available (see chapter IV, section B, above), for the States parties to realize their obligation under article 37 (b) of CRC to use deprivation of liberty only as a measure of last resort. The use of these alternatives must be carefully structured to reduce the use of pretrial detention as well, rather than "widening the net" of sanctioned children. In addition, the States parties should take adequate legislative and other measures to reduce the

use of pretrial detention. Use of pretrial detention as a punishment violates the presumption of innocence. The law should clearly state the conditions that are required to determine whether to place or keep a child in pretrial detention, in particular to ensure his/her appearance at the court proceedings, and whether he/she is an immediate danger to himself/herself or others. The duration of pretrial detention should be limited by law and be subject to regular review.

81. The Committee recommends that the State parties ensure that a child can be released from pretrial detention as soon as possible, and if necessary under certain conditions. Decisions regarding pretrial detention, including its duration, should be made by a competent, independent and impartial authority or a judicial body, and the child should be provided with legal or other appropriate assistance.

Procedural rights (art. 37 (d))

82. Every child deprived of his/her liberty has the right to prompt access to legal and other appropriate assistance, as well as the right to challenge the legality of the deprivation of his/her liberty before a court or other competent, independent and impartial authority, and to a prompt decision on any such action.

83. Every child arrested and deprived of his/her liberty should be brought before a competent authority to examine the legality of (the continuation of) this deprivation of liberty within 24 hours. The Committee also recommends that the States parties ensure by strict legal provisions that the legality of a pretrial detention is reviewed regularly, preferably every two weeks. In case a conditional release of the child, e.g. by applying alternative measures, is not possible, the child should be formally charged with the alleged offences and be brought before a court or other competent, independent and impartial authority or judicial body, not later than 30 days after his/her pretrial detention takes effect. The Committee, conscious of the practice of adjourning court hearings, often more than once, urges the States parties to introduce the legal provisions necessary to ensure that the court/juvenile judge or other competent body makes a final decision on the charges not later than six months after they have been presented.

84. The right to challenge the legality of the deprivation of liberty includes not only the right to appeal, but also the right to access the court, or other competent, independent and impartial authority or judicial body, in cases where the deprivation of liberty is an administrative decision (e.g. the police, the prosecutor and other competent authority). The right to a prompt decision means that a decision must be rendered as soon as possible, e.g. within or not later than two weeks after the challenge is made.

Treatment and conditions (art. 37 (c))

85. Every child deprived of liberty shall be separated from adults. A child deprived of his/her liberty shall not be placed in an adult prison or other facility for adults. There is abundant evidence that the placement of children in adult prisons or jails compromises their basic safety, well-being, and their future ability to remain free of crime and to reintegrate. The permitted exception to the separation of children from adults stated in article 37 (c) of CRC, "unless it is considered in the child's best interests not to do so", should be interpreted narrowly; the child's

best interests does not mean for the convenience of the States parties. States parties should establish separate facilities for children deprived of their liberty, which include distinct, child-centred staff, personnel, policies and practices.

86. This rule does not mean that a child placed in a facility for children has to be moved to a facility for adults immediately after he/she turns 18. Continuation of his/her stay in the facility for children should be possible if that is in his/her best interest and not contrary to the best interests of the younger children in the facility.

87. Every child deprived of liberty has the right to maintain contact with his/her family through correspondence and visits. In order to facilitate visits, the child should be placed in a facility that is as close as possible to the place of residence of his/her family. Exceptional circumstances that may limit this contact should be clearly described in the law and not be left to the discretion of the competent authorities.

88. The Committee draws the attention of States parties to the United Nations Rules for the Protection of Juveniles Deprived of their Liberty, adopted by the General Assembly in its resolution 45/113 of 14 December 1990. The Committee urges the States parties to fully implement these rules, while also taking into account as far as relevant the Standard Minimum Rules for the Treatment of Prisoners (see also rule 9 of the Beijing Rules). In this regard, the Committee recommends that the States parties incorporate these rules into their national laws and regulations, and make them available, in the national or regional language, to all professionals, NGOs and volunteers involved in the administration of juvenile justice.

89. The Committee wishes to emphasize that, inter alia, the following principles and rules need to be observed in all cases of deprivation of liberty:

- Children should be provided with a physical environment and accommodations which are in keeping with the rehabilitative aims of residential placement, and due regard must be given to their needs for privacy, sensory stimuli, opportunities to associate with their peers, and to participate in sports, physical exercise, in arts, and leisure time activities;

- Every child of compulsory school age has the right to education suited to his/her needs and abilities, and designed to prepare him/her for return to society; in addition, every child should, when appropriate, receive vocational training in occupations likely to prepare him/her for future employment;

- Every child has the right to be examined by a physician upon admission to the detention/correctional facility and shall receive adequate medical care throughout his/her stay in the facility, which should be provided, where possible, by health facilities and services of the community;

- The staff of the facility should promote and facilitate frequent contacts of the child with the wider community, including communications with his/her family, friends and other persons or representatives of reputable outside organizations, and the opportunity to visit his/her home and family;

- Restraint or force can be used only when the child poses an imminent threat of injury to him or herself or others, and only when all other means of control have been exhausted. The use of restraint or force, including physical, mechanical and medical restraints, should be under close and direct control of a medical and/or psychological professional. It must never be used as a means of punishment. Staff of the facility should receive training on the applicable standards and members of the staff who use restraint or force in violation of the rules and standards should be punished appropriately;

- Any disciplinary measure must be consistent with upholding the inherent dignity of the juvenile and the fundamental objectives of institutional care; disciplinary measures in violation of article 37 of CRC must be strictly forbidden, including corporal punishment, placement in a dark cell, closed or solitary confinement, or any other punishment that may compromise the physical or mental health or well-being of the child concerned;

- Every child should have the right to make requests or complaints, without censorship as to the substance, to the central administration, the judicial authority or other proper independent authority, and to be informed of the response without delay; children need to know about and have easy access to these mechanisms;

- Independent and qualified inspectors should be empowered to conduct inspections on a regular basis and to undertake unannounced inspections on their own initiative; they should place special emphasis on holding conversations with children in the facilities, in a confidential setting.

V. THE ORGANIZATION OF JUVENILE JUSTICE

90. In order to ensure the full implementation of the principles and rights elaborated in the previous paragraphs, it is necessary to establish an effective organization for the administration of juvenile justice, and a comprehensive juvenile justice system. As stated in article 40 (3) of CRC, States parties shall seek to promote the establishment of laws, procedures, authorities and institutions specifically applicable to children in conflict with the penal law.

91. What the basic provisions of these laws and procedures are required to be, has been presented in the present general comment. More and other provisions are left to the discretion of States parties. This also applies to the form of these laws and procedures. They can be laid down in special chapters of the general criminal and procedural law, or be brought together in a separate act or law on juvenile justice.

92. A comprehensive juvenile justice system further requires the establishment of specialized units within the police, the judiciary, the court system, the prosecutor's office, as well as specialized defenders or other representatives who provide legal or other appropriate assistance to the child.

93. The Committee recommends that the States parties establish juvenile courts either as separate units or as part of existing regional/district courts. Where that is not immediately feasible for practical reasons, the States parties should ensure the appointment of specialized judges or magistrates for dealing with cases of juvenile justice.

94. In addition, specialized services such as probation, counselling or supervision should be established together with specialized facilities including for example day treatment centres and, where necessary, facilities for residential care and treatment of child offenders. In this juvenile justice system, an effective coordination of the activities of all these specialized units, services and facilities should be promoted in an ongoing manner.

95. It is clear from many States parties' reports that non-governmental organizations can and do play an important role not only in the prevention of juvenile delinquency as such, but also in the administration of juvenile justice. The Committee therefore recommends that States parties seek the active involvement of these organizations in the development and implementation of their comprehensive juvenile justice policy and provide them with the necessary resources for this involvement.

VI. AWARENESS-RAISING AND TRAINING

96. Children who commit offences are often subject to negative publicity in the media, which contributes to a discriminatory and negative stereotyping of these children and often of children in general. This negative presentation or criminalization of child offenders is often based on misrepresentation and/or misunderstanding of the causes of juvenile delinquency, and results regularly in a call for a tougher approach (e.g. zero-tolerance, three strikes and you are out, mandatory sentences, trial in adult courts and other primarily punitive measures). To create a positive environment for a better understanding of the root causes of juvenile delinquency and a rights-based approach to this social problem, the States parties should conduct, promote and/or support educational and other campaigns to raise awareness of the need and the obligation to deal with children alleged of violating the penal law in accordance with the spirit and the letter of CRC. In this regard, the States parties should seek the active and positive involvement of members of parliament, NGOs and the media, and support their efforts in the improvement of the understanding of a rights-based approach to children who have been or are in conflict with the penal law. It is crucial for children, in particular those who have experience with the juvenile justice system, to be involved in these awareness-raising efforts.

97. It is essential for the quality of the administration of juvenile justice that all the professionals involved, inter alia, in law enforcement and the judiciary receive appropriate training on the content and meaning of the provisions of CRC in general, particularly those directly relevant to their daily practice. This training should be organized in a systematic and ongoing manner and should not be limited to information on the relevant national and international legal provisions. It should include information on, inter alia, the social and other causes of juvenile delinquency, psychological and other aspects of the development of children, with special attention to girls and children belonging to minorities or indigenous peoples, the culture and the trends in the world of young people, the dynamics of group activities, and the available measures dealing with children in conflict with the penal law, in particular measures without resorting to judicial proceedings (see chapter IV, section B, above).

VII. DATA COLLECTION, EVALUATION AND RESEARCH

98. The Committee is deeply concerned about the lack of even basic and disaggregated data on, inter alia, the number and nature of offences committed by children, the use and the average duration of pretrial detention, the number of children dealt with by resorting to measures other

than judicial proceedings (diversion), the number of convicted children and the nature of the sanctions imposed on them. The Committee urges the States parties to systematically collect disaggregated data relevant to the information on the practice of the administration of juvenile justice, and necessary for the development, implementation and evaluation of policies and programmes aiming at the prevention and effective responses to juvenile delinquency in full accordance with the principles and provisions of CRC.

99. The Committee recommends that States parties conduct regular evaluations of their practice of juvenile justice, in particular of the effectiveness of the measures taken, including those concerning discrimination, reintegration and recidivism, preferably carried out by independent academic institutions. Research, as for example on the disparities in the administration of juvenile justice which may amount to discrimination, and developments in the field of juvenile delinquency, such as effective diversion programmes or newly emerging juvenile delinquency activities, will indicate critical points of success and concern. It is important that children are involved in this evaluation and research, in particular those who have been in contact with parts of the juvenile justice system. The privacy of these children and the confidentiality of their cooperation should be fully respected and protected. In this regard, the Committee refers the States parties to the existing international guidelines on the involvement of children in research.

United Nations A/63/223

General Assembly

Distr.: General
6 August 2008

Original: English

Sixty-third session
Item 67 (c) of the provisional agenda*
Promotion and protection of human rights: human rights situations and reports of special rapporteurs and representatives

Protection of human rights and fundamental freedoms while countering terrorism

Note by the Secretary-General

The Secretary-General has the honour to transmit to the members of the General Assembly the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, submitted in accordance with General Assembly resolution 62/159 and Human Rights Council resolution 6/28.

* A/63/150.

08-45182 (E) 290808

A/63/223

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

Summary

Following the introduction, section II of the present report highlights two key activities of the Special Rapporteur, including a visit in December 2007 to Guantánamo Bay for the purposes of observing military commission hearings and a summary of an official country visit to Spain in May 2008. The main thematic focus of this report is the fundamental right to a fair trial in the specific context of prosecuting terrorist suspects.

Section III of the report provides an overview of the applicable legal framework as reflected in international human rights treaties, treaty and customary international law, and conventions to counter terrorism. Of particular relevance is Human Rights Committee, general comment No. 32 on article 14 of the International Covenant on Civil and Political Rights. The Special Rapporteur also emphasizes that fundamental principles of the right to a fair trial may not be subject to derogation and that any derogation must not circumvent the protection of non-derogable rights.

In section IV of the report, the Special Rapporteur analyses the key role of the judiciary both as a vehicle of legal recourse to ensure that terrorist suspects who are detained pursuant to criminal law provisions or subject to "administrative detention" or detained during the course of participating in hostilities have effective access to the courts. The Special Rapporteur reflects on the key elements of independence and impartiality that are required of a judicial institution in order that justice can be administered in a competent, fair and open manner. In this context, the jurisdiction of military or special courts is discussed. The Special Rapporteur also addresses a key area of concern regarding the broader issue of access to justice regarding the practice of listing and de-listing individuals and groups as terrorist or associated entities by intergovernmental bodies or by a national procedures of a State.

Various aspects of a fair hearing are outlined in section V of the report, which include: the privilege against self-incrimination; evidence obtained in breach of human rights or domestic law will render the trial unfair; the right to equal treatment and equality of arms; the right to disclosure of information and the right to representation; and applicable standards of proof.

Section VI of the report makes a reference to death penalty cases and reflects the concerns of the Special Rapporteur when a trial involving terrorism offences could lead to the imposition of capital punishment. All stages of the proceedings and the consideration of appeals on matters of fact and law must comply with all aspects of a fair trial.

In the concluding section, the Special Rapporteur emphasises a number of basic principles as elements of best practice in securing the right to a fair trial in terrorism cases.

Contents

I. Introduction

1. The present report is the fourth submitted to the General Assembly by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to Human Rights Council resolution 6/28 and Assembly resolution 62/159. It highlights activities from 1 November 2007 to 31 July 2008, including the visit of the Special Rapporteur to Guantánamo Bay in December 2007 for the purposes of observing the military commission hearings and an official visit to Spain in May 2008. The main thematic focus of this report is the right to a fair trial in the fight against terrorism.

2. In addition to his last report to the General Assembly,[1] the Special Rapporteur draws attention to his main report[2] and addenda[3] considered at the sixth session of the Human Rights Council in December 2007. The main report summarized the activities of the Special Rapporteur in 2007 and focused on the thematic issue of the effects of counter-terrorism measures in relation to economic, social and cultural rights. The addenda contained a communications report and reports on official missions to South Africa, the United States of America and Israel, including a visit to the Occupied Palestinian Territory.

3. Regarding future country visits, the Special Rapporteur accepted with appreciation the official invitation extended by the Government of Tunisia on 5 June 2008. At the time of submission of the present report, the dates of the mission had not been confirmed.

II. Activities related to the Special Rapporteur

4. General activities undertaken by the Special Rapporteur will be reflected in a forthcoming report to the Human Rights Council, however, two key activities are reflected below.

Country visits and follow-up visits

5. From 3 to 7 December 2007, as a follow-up to the official visit to the United States of America in May 2007, the Special Rapporteur visited Guantánamo Bay for the purpose of observing hearings under the 2006 Military Commissions Act. The visit supported concerns previously reflected in the report of the Special Rapporteur[4] regarding the incompatibility of the Military Commissions Act with relevant international standards. The hearing illustrated numerous challenges faced by the military judge to ensure fair trial principles.

6. From 7 to 14 May 2008 the Special Rapporteur conducted an official visit to Spain. The mission report will be submitted to a future session of the Human Rights Council. The preliminary findings of the Special Rapporteur were reflected in a

[1] A/62/263.
[2] A/HRC/6/17.
[3] A/HRC/6/17/Add.1-4.
[4] A/HRC/6/17/Add.3.

press statement[5] issued during a press conference held on 14 May, where he acknowledged the tragic incidents of domestic and international terrorism in Spain, highlighted the international role of Spain in countering terrorism while respecting human rights and identified elements of best practice regarding the use of the criminal justice system to combat terrorism. The Special Rapporteur examined a number of key issues including concerns regarding the definition of terrorist crimes in Spanish statutory law and judicial practice and the practice of incommunicado detention. He highlighted positive aspects regarding the trial of the 11 March 2004 bombings but did note concerns regarding the pretrial phase and the right to review by a higher court. He acknowledged the Government's efforts to address issues concerning victims of terrorism by legislative and administrative measures.

III. Right to a fair trial in the fight against terrorism

7. The right to a fair trial is one of the fundamental guarantees of human rights and the rule of law. It comprises various interrelated attributes and is often linked to the enjoyment of other rights, such as the right to life. The Human Rights Committee adopted in 2007 general comment No. 32, which stands as a substantial commentary of the right to a fair trial under article 14 of the International Covenant on Civil and Political Rights and reflects upon a considerable body of jurisprudence.[6] In the course of his mandate, the Special Rapporteur has noted several times with concern that in the fight against terrorism fair trial rights have not always been respected. This report reflects therefore upon various aspects of article 14, of the Covenant as well as the case law, legislation and practice of a number of Member States in order to identify a set of best practices in respect of the right to fair trial in the context of counter-terrorism.[7]

A. The framework of applicable law

8. Article 14 (1) of the International Covenant on Civil and Political Rights guarantees that all persons are to be treated equally before courts and tribunals. It provides for everyone to be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law in the determination of any criminal charge, or of the rights and obligations of a person in a "suit at law". Broadly speaking, the latter expression refers to various civil (private law) or administrative proceedings before a judicial body.[8] Although article 14 (1) as a whole does not operate in the context of certain types of proceedings, such as extradition, expulsion or deportation procedures, the first sentence of article 14 is applicable whenever domestic law entrusts a judicial body with a judicial task and requires that any such proceedings conform to basic principles of fair trial.[9] In certain issues article 13 of the Covenant incorporates the notions of due process

[5] The press statement is available at http://www.unhchr.ch/huricane/huricane.nsf/view01/57DBD56D289BCDCEC1257440004402FB?opendocument.

[6] CCPR/C/GC/32 (2007), General Comment No. 32.

[7] The Special Rapporteur is grateful for the assistance and cooperation of Dr. Alex Conte, consultant on security and human rights, Mathias Vermeulen, LLM and the International Commission of Jurists in the preparation of the present report.

[8] Human Rights Committee, General Comment No. 32, para. 16.

[9] Ibid., para. 7.

reflected in article 14.[10] In the context of extradition and deportation proceedings the prohibition against *refoulement* may apply not only where there is a risk of torture or other cruel, inhuman or degrading treatment,[11] and in many situations where the death penalty is sought, but also to cases involving a risk of exposure to a manifestly unfair trial.[12] The remaining provisions of article 14 (paras. 2 to 7) set out certain rights and guarantees applicable to the determination of criminal charges, including the right to a defence, the presumption of innocence, and the right to have one's conviction or sentence reviewed by a higher tribunal.

9. Various elements of the right to a fair trial, as codified in article 14 of the Covenant, are also to be found within customary law norms and other international treaties, including treaties pertaining to international humanitarian law or to countering terrorism. In similar terms to article 14, the right to a fair trial is guaranteed by article 6 of the European Convention on Human Rights, article 8 of the American Convention on Human Rights and, in somewhat lesser detail, article 7 of the African Charter on Human and Peoples' Rights and article 13 of the Revised Arab Charter on Human Rights. The Rome Statute of the International Criminal Court also includes the basic requirements for a fair trial in the context of international criminal law.[13] Equally, common article 3(1)(d) of the Geneva Conventions of 1949 on international humanitarian law prohibits the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples. Similar minimal guarantees that are considered to reflect customary international law[14] are to be found in article 75(4) of Additional Protocol I (relating to international armed conflicts) and article 6(2) of Additional Protocol II (relating to non-international armed conflicts). Fair trial guarantees under human rights treaties continue to apply during armed conflict, subject to the rare instances where a State permissibly derogates from the fair trial clauses in the human rights treaties in question.[15]

10. Furthermore, provisions within many universal terrorism-related conventions also require compliance with the right to a fair trial and the rule of law. In the context of the International Convention for the Suppression of the Financing of

[10] Ibid., para. 62; *Ahani v. Canada*, Communication No. 1051/2002, CCPR/C/80/D/1051/2002 (2004), para. 10.9.

[11] *C v. Australia*, Communication No. 832/1998, CCPR/C/72/D/832/1998 (2001), and *Ahani v. Canada*, Communication No. 1051/2002, CCPR/C/80/D/1051/2002 (2004).

[12] *A R J v. Australia*, Communication No. 692/1996, CCPR/C/60/D/692/1996 (1997), para. 6.15; see OHCHR, *Fact Sheet 32. Human Rights, Terrorism, and Counter-Terrorism*, p. 34; International Commission of Jurists, Legal Commentary to the ICJ Berlin Declaration. Geneva, 2008, p. 97.

[13] Article 67(1) of the Rome Statute identifies as basic requirements: the presumption of innocence; privilege against self-incrimination; the right to communicate with legal representatives freely and in confidence; the right to remain silent without such silence being a consideration in the determination of innocence or guilt; the right not to make an unsworn oral or written statement in one's own defence; and the right not to have imposed upon the accused any reversal of the burden of proof or onus of rebuttal.

[14] Inter-American Commission on Human Rights, Report on Terrorism and Human Rights, OEA/Ser.L/V/II.116 (Doc. 5 rev. 1 corr) 22 October 2002, paras. 257-259.

[15] See *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories, Advisory Opinion* (2004), ICJ Reports 2004, p. 178, 136, para. 106, as to the continued application of international human rights law, including under international conventions, during armed conflict.

Terrorism, for example, article 17 requires the fair treatment of any person taken into custody, including enjoyment of all rights and guarantees under applicable international human rights law, and article 21 sets out a "catch-all" provision making it clear that the Convention does not affect the enjoyment of other rights, obligations and responsibilities of States parties.

11. Because the right to a fair trial is recognized not only in human rights treaties but also within international humanitarian law, international criminal law, counter-terrorism conventions and customary international law, a fair trial cannot be denied through the excuse that human rights treaties or some of them would represent a special category of territorial treaties, not applicable when a State acts outside its own borders.

B. The non-derogable and fundamental nature of fair trial rights

12. Despite its absence from the list of non-derogable rights in article 4(2) of the International Covenant on Civil and Political Rights, the Human Rights Committee has treated the right to a fair trial as one which may not be subject to derogation where this would circumvent the protection of non-derogable rights.[16] Even in situations when derogation from article 14 is permissible, the principles of legality and the rule of law require that the fundamental requirements of fair trial must be respected. This means that: only a court of law may try and convict a person for a criminal offence; the presumption of innocence must always be respected; and the right to take proceedings before a court to decide without delay on the lawfulness of detention must not be diminished by any derogation from the Covenant.[17] In the context of fair trial rights under international humanitarian law, it should be remembered that there can be no derogation from the relevant provisions of the Geneva Conventions or their Additional Protocols. Indeed, denial of the right to a fair trial can amount to a war crime in certain circumstances.

IV. The judiciary

A. Effective access to court

13. The Special Rapporteur has noted a growing number of complaints that legislation introduced to combat terrorism, or legislation on national security or asylum,[18] restricts rights by precluding or limiting recourse to an independent judiciary and accords broad powers to the executive.[19] Typically, such laws suspend *habeas corpus* or *amparo*, and establish an internal review or appeal mechanism devoid of any judicial involvement. In this regard, the Special Rapporteur is equally

[16] See Human Rights Committee, General Comment No. 32, paras. 6 and 59. See General Comment No. 29, *States of Emergency (Article 4)*, CCPR/C/21/Rev.1/Add.11 (2001), paras. 7 and 15. The Revised Arab Charter of Human Rights, in force since March 15, 2008, even treats the right to fair trial (art. 16) as a non-derogable right in times of emergency (article 4.2).

[17] See Human Rights Committee, General Comment No. 29, para. 16.

[18] On detention of terrorism suspects under States' immigration legislation and the need for judicial review, see A/62/263, chap. III. para. 81.B.

[19] See, also, report of the Special Rapporteur on the independence of judges and lawyers, A/HRC/4/25, para. 32.

concerned about the frequent abuse of immunity[20] or indemnity clauses[21] in counter-terrorism laws and in the broad invoking of national security concerns as a blanket bar to access to justice.

14. Article 14 of the International Covenant on Civil and Political Rights encompasses the right of access to court in the determination of both criminal charges and rights and obligations in a suit at law, for the purpose of ensuring that no individual is deprived of his or her right to claim justice. The right of access to courts and tribunals is not limited to citizens of the State, but must be available to all individuals, regardless of nationality or statelessness, or whatever their status (whether asylum seekers, refugees, or other persons who may find themselves in the territory or subject to the jurisdiction of a State).[22] The right under article 14(3)(c) of the Covenant to be tried without undue delay in the determination of any criminal charge means, in practical terms, that a person must be brought before the courts without delay and that criminal proceedings, including any appeal arising from them, must be disposed of promptly. What constitutes "reasonable time" is a matter of assessment in each particular case, taking into account factors such as the complexity of the case, the conduct of the accused, and the manner in which the matter was dealt with by the administrative and judicial authorities.

15. It should be remembered that article 14(5) of the Covenant guarantees the right to one's conviction and sentence to be reviewed by a higher tribunal without delay, which is not limited to matters of law but also a review of facts.[23] Effective access to appeal rights includes the need to provide reasoned decisions, which is particularly important since it is often through access to independent review and appeal mechanisms that the right to an effective remedy is facilitated.[24] Equally, when a trial *in absentia* has taken place, there must be an opportunity for a fresh determination of the merits of the case in the presence of the accused once the accused has found out about the proceedings.[25]

16. A specific issue of concern for the Special Rapporteur regarding access to justice is the practice of listing and de-listing individuals and groups as terrorist or associated entities, whether by the Security Council through its Al-Qaida and Taliban Sanctions Committee, by the European Union, or by national procedures. This practice has had a serious impact on due process related rights for individuals suspected of terrorism, as well as their families.[26] Because the indefinite freezing of the assets of those listed currently operates without a right to be de-listed, this amounts to a criminal punishment due to the severity of the sanction. As long as

---

[20] See, for example, India, Armed Forces Special Powers Act, 1958, para. 6; Sri Lanka, Prevention of Terrorism Act, para. 15, Russian Federation, Federal Law n.35-Z, article 22.

[21] See Sri Lanka, Indemnity (Amendment) Act 1988, para. 2; Pakistan, Anti-Terrorism Act 1997, para. 39.

[22] See Human Rights Committee, General Comment No. 32, para. 9.

[23] See the repeated jurisprudence of the Human Rights Committee on this point including, in *Fernández v. Czech Republic*, Communication No. 1104/2002, CCPR/C/83/D/1104/2002 (2005), para. 7.

[24] See *Singh v. Canada*, Communication No. 761/1997, CCPR/C/60/D/761/1997 (1997), para. 4.2. See also *Amnesty International and Others v. Sudan*, African Commission on Human and Peoples' Rights, Communication No. 48/90, 50/91, 52/91, 89/93 (1999), eighth annual activity report 1994/1995, para. 37.

[25] See *Colozza v. Italy*, (1985) 7 EHRR 516, para. 29.

[26] See A/HRC/17/6/Add.2, paras. 33-36.

there is no independent review of listings at the United Nations level, there must be access to domestic judicial review of any implementing measure.[27] Even where listing does not result in the indefinite freezing of assets, but holds other consequences which might fall short of a criminal punishment, it should be noted that access to courts and a fair trial may also arise from the general provisions of article 14(1), as applicable to a suit at law. At a minimum, the standards required to ensure a fair hearing must include the right of an individual to be informed of the measures taken and to know the case against him or her as soon as possible, and to the extent possible, without thwarting the purpose of the sanctions regimes; the right to be heard within a reasonable time by the relevant decision-making body; the right to effective review by a competent and independent review mechanism; the right to counsel with respect to all proceedings; and the right to an effective remedy.[28] The Special Rapporteur has raised similar concerns pertaining to Turkey's classification of organizations linked to terrorist crimes and the need, in that regard, to ensure that procedures for designation are transparent and objective, and accompanied by a right to appeal to an independent judicial body.[29]

1. Access to court by those in detention

17. The provisions of article 14(3) interact with the obligation under article 9(3) of the Covenant to promptly bring a detainee before a competent authority. In cases involving serious charges such as homicide or murder (or terrorism as properly defined),[30] and where an accused is denied bail by the court, an accused must be tried in as expeditious a manner as possible,[31] even in bona fide emergency situations where there is a serious terrorist threat.[32] Developments in counter-terrorism law and practice have seen the emergence of regimes under which a person may be detained outside the context of initiated criminal proceedings, including in administrative or preventive detention for security reasons,[33] or investigative detention (detention for the purpose of questioning and investigation prior to the laying of charges). The Special Rapporteur emphasizes the importance of speedy and regular court review of any form of detention, entailing a real possibility of release.

18. Extended periods of police detention (*détention en garde à vue*), without bringing a suspect before a judge, has been a long-standing practice of concern in

[27] See A/61/267, chap. III; A/HRC/4/26/Add.3, para. 20; and A/HRC/6/17/Add.2, para. 72.

[28] See A/HRC/4/88, paras. 17-22.

[29] See A/HRC/4/26/Add.2, para. 90(e).

[30] See E/CN.4/2006/98, chap. III.

[31] See *del Cid Gómez v. Panama*, Communication No. 473/1991, CCPR/C/54/D/473/1991 (1995), para. 8.5; and *Glenrry Francis et al. v. Trinidad and Tobago*, Communication No. 899/1999, CCPR/C/75/D/899/1999 (2002), para. 5.4.

[32] *Brogan v. UK* (1998) ECHR, Series A, No. 145-B, para. 61.

[33] As permitted, for example, in Sri Lanka, where the Prevention of Terrorism Act allows arrest without a warrant and permits detention for an initial period of 72 hours without the person being produced before the court (sect. 7), and thereafter for up to 18 months on the basis of an administrative order issued by the Minister of Defence (sect. 9). See also CCPR/CO/79/LKA (2003), para. 13.

several countries, for instance in France,[34] Russia,[35] Northern Africa[36] and South-East Asia.[37] The Special Rapporteur is concerned that the absence of an express provision in the law to the maximum period of such detention, could lead to instances of indefinite detention.[38] Equally, the Special Rapporteur is concerned about strict bail provisions, for instance in Australia.[39]

19. Of special concern to the Special Rapporteur is the use of "administrative detention" as a counter-terrorism tool against persons on the sole basis of a broadly formulated element of suspicion that a person forms a 'threat to national security' or similar expressions that lack the level of precision required by the principle of legality. Much of the information concerning the reasons for such detention is often classified, so that the detainee and his or her lawyer have no access to this information and thereby no effective means of contesting the grounds of the detention.[40] This form of administrative detention appears to be at odds with numerous aspects of the right to a fair hearing under article 14 of the Covenant, and of access to an independent and impartial court, especially when there is no possibility for a review of the detention on the basis of substantive grounds.[41]

20. The Special Rapporteur emphasizes that a court must always be empowered to review the merits of the decision to detain and to decide, by reference to legal criteria, whether detention is justified, and, if not, to order release. It is therefore of

[34] In its concluding observations of July 2008 the Human Rights Committee expressed concern that Act No. 2006/64 of 23 January 2006 permits the initial detention of persons suspected of terrorism for four days, with extensions up to six days, in police custody (*garde à vue*), before they are brought before a judge to be placed under judicial investigation or released without charge, and that terrorism suspects in police custody are guaranteed access to a lawyer only after 72 hours, and access to counsel can be further delayed till the fifth day when custody is extended by a judge. See, CCPR/C/FRA/CO/4 (2008), para. 14.

[35] In the Russian Federation, the Law on Operative-Search Activity, as well as the federal Law No. 18-FZ of 22 April 2004, amending article 99 of the Code of Criminal Procedure, allows the detainment of suspects of "terrorism" for up to 30 days without being charged. See also CAT/C/RUS/CO/4 (2007).

[36] See International Commission of Jurists, Eminent Jurists Conclude Subregional Hearing on Terrorism and Human Rights in the Maghreb, press release dated 7 July 2006.

[37] International Commission of Jurists, International Panel Ends Hearing In South-East Asia, press release dated 6 December 2006.

[38] For instance, in the Philippines, the 2007 Human Security Act allows, in sect. 19, "in the event of an 'actual or imminent terrorist attack', the detention of a terrorist suspect for 'more than three days' if the police obtain the written approval of a court or a 'municipal, city, provincial or regional official'."

[39] A/HRC/4/26/Add.3, para. 34.

[40] In Malaysia, for instance, section 73.1.b of the Internal Security Act allows any police officer to arrest without a warrant and detain for up to 60 days any person in respect of whom he has reason to believe that "he has acted or is about to act or is likely to act in any manner prejudicial to the security of Malaysia or any part thereof or to maintenance of essential services therein or to the economic life thereof". After 60 days, sect. 8 of the Internal Security Act allows the Minister of Internal Security to extend the detention without trial for two years, without submitting any evidence for review by the courts. There is no possibility for a legal remedy on substantive grounds for detainees held under section 8 of the ISA. Written submission of Suara Rakyat Malaysia (SUARAM) to the Eminent Jurist Panel on Terrorism, Counter-Terrorism and Human Rights, July 2006.

[41] The same concerns pertain to the detention of persons under Military Order 1229 and the Incarceration of Unlawful Combatants Law 2002 in Israel. See A/HRC/6/17/Add.4, paras. 23-26.

crucial importance that the court has the power to review the evidence on which the individual is held.[42]

2. Detention and access to court by persons participating in hostilities

21. In the case of privileged combatants apprehended during the course of an international armed conflict, such persons may be detained as prisoners of war until the end of hostilities. Prisoners of war must be released at the end of hostilities, unless suspected, convicted or sentenced of war crimes, in which case the right to a fair trial continues to apply. Furthermore, persons directly participating in hostilities during the course of a non-international armed conflict may arguably be detained for the duration of the hostilities, but can alternatively be treated as criminal suspects for their use of violence. While acknowledging the need to ensure that there is no impunity for those that commit war crimes, the Special Rapporteur emphasizes that the chance of ensuring a fair trial diminishes over time. For this reason, States should determine, without awaiting for the end of hostilities, whether a person will be tried or not and, in the affirmative cases, proceed with the criminal trial.

22. The Special Rapporteur further emphasizes the need for clarity as to the status of any person detained in relation to an international or non-international armed conflict. The persons detained at the US military facility at Guantánamo Bay have, for example, been categorized by the United States of America as "alien unlawful enemy combatants", regardless of the circumstances of their capture. Not only is this term one of convenience without legal consequences, but the Special Rapporteur has noted serious concerns about the overall length of detention of detainees at Guantánamo Bay (for a period of several years without charge), which fundamentally undermines the right of fair trial.[43] He has also expressed serious concerns about the ability of detainees at Guantánamo Bay to seek a judicial determination of their status, and of their continuing detention.[44] Determination of whether a detainee is an "alien unlawful enemy combatant" is undertaken by the Combatant Status Review Tribunal (CSRT) and the Administrative Review Board (ARB), which are both described by the Department of Defense as administrative, rather than judicial, processes. Detainees are not provided with a lawyer during the course of hearings. Even more problematic is the fact that decisions of the Combatant Status Review Tribunal and the Administrative Review Board are subject to limited judicial review only. These restrictions result in non-compliance with

---

[42] Under the 2006 Terrorism Act in the United Kingdom, a person may be detained for a period of up to 28 days, or potentially 42 days if the Counter-Terrorism Bill 2008 (UK) is enacted in its current form. A detainee must, under the Act, be brought before a court within 48 hours and may only be subject to periods of detention of seven days at a time. See sects. 23-25 and schedule 8 of the Terrorism Act 2006 (UK). The review by a district judge to examine further detention concerns only whether continued detention is necessary to obtain, preserve or examine relevant evidence, and whether the case is being pursued diligently and expeditiously by the police. The judge does not examine the merits of the case against the suspect. In its concluding observations of July 2008, the Human Rights Committee expressed its concern over both the current and the proposed law, emphasizing that any terrorist suspect arrested should be promptly informed of any charge against him or her and tried within a reasonable time or released. See CCPR/C/GBR/CO/6, para. 15.

[43] A/HRC/6/17/Add.3, para. 12.

[44] As was confirmed by the United States Supreme Court in June 2008 in *Boumediene v. Bush* 553 US (2008), the denial of the right of *habeas corpus* to Guantánamo detainees through the Military Commissions Act of 2006 was unconstitutional.

various provisions of the Covenant.[45] The Special Rapporteur has similarly reminded the United States and other States responsible for the detention of persons in Afghanistan and Iraq that these detainees also have the right to court review of the lawfulness of their detention without delay and, if suspected of a crime, to a fair trial within a reasonable time.[46]

B. Competence, independence and impartiality

23. The right to a fair trial before a competent, independent and impartial court or tribunal involve elements which are in nature both objective (independence) and subjective (competence and impartiality). The requirements of independence and impartiality must be treated as absolute requirements, which are not capable of limitation.[47] Independence calls for the protection of judicial officers from any form of political influence in their decision-making, including any influence which might be affected against their term of office, security, remuneration, or conditions of service.[48] A situation where the functions and competencies of the judiciary and the executive are not clearly distinguishable, or where the latter is able to control or direct the former, is incompatible with the notion of an independent tribunal.[49] The requirement of competence calls for the appointment of suitably qualified and experienced persons to act as judicial officers in any hearing.[50]

24. While the Covenant does not prohibit the establishment or use of military or special courts and tribunals, nor the centralization of judicial investigation, prosecution and trial (whereby terrorist cases are exclusively dealt with by one ordinary court),[51] the Special Rapporteur calls for caution in allocating terrorism cases to military, special or specialized courts, as this potentially raises issues under article 14[52] or article 26 of the Covenant. An additional factor speaking against such solutions is that rulings of special or specialized courts may often not be subject to full review of the conviction and sentence, in respect of issues of law and fact, as required by the Covenant in article 14(5).[53]

1. Military courts or tribunals or other special courts

25. In many countries, the cumulative effect of simplified provisions for dismissal of judges sitting in military or special courts, the lack of security of tenure of

[45] A/HRC/6/17/Add.3, paras. 13 and 14.

[46] A/HRC/6/17/Add.3, para. 18.

[47] See Human Rights Committee, General Comment No. 32, para. 19. See also *Gonzalez del Rio v. Peru*, Human Rights Committee Communication No. 263/1987, CCPR/C/46/D/263/1987 (1992), para. 5.2

[48] See Human Rights Committee, General Comment No. 32, para. 19.

[49] Ibid. On the issue of the control or direction of a tribunal by the judiciary, see also *Oló Bahamonde v. Equatorial Guinea*, Communication No. 468/1991, CCPR/C/49/D/468/1991 (1993), para. 9.4.

[50] See *Findlay v. United Kingdom* (1997) ECHR 8, para. 75.

[51] The Special Rapporteur will address the jurisdiction of the Spanish Audiencia Nacional in a forthcoming report to the Human Rights Council. Meanwhile, see the Special Rapporteur's press statement of 14 May 2008, highlighting his preliminary findings, http://www.unhchr.ch/huricane/huricane.nsf/view01/57DBD56D289BCDCEC1257440004402FB?opendocument.

[52] See Human Rights Committee, General Comment No. 32, para. 22.

[53] See *Gómez Vázquez v. Spain*, Human Rights Committee Communication No. 701/1996, CCPR/C/69/D/701/1996 (2000).

judges, the fact that often judges are serving (military) officers appointed by the executive, and the broad discretional power of the executive to refer cases to such courts, lead to serious questions concerning the independence and impartiality of such courts, even where instructions are given to members of a court that they are to act independently.

26. The Special Rapporteur is especially concerned about cases where the executive has broad discretionary powers either to refer terrorist suspects to military or special courts,[54] or to review or confirm the decisions of these courts, which gives the executive the ultimate control over the accused and the outcome of the trial.[55] Individuals accused of the same or similar offences should not be treated with different standards of justice at the whim of the executive. In *Kavanagh v. Ireland*, the Human Rights Committee found a violation of article 26 of the Covenant (non-discrimination) because of the discretionary nature of the prosecutor's power to prosecute a case of organized crime before a special criminal court, rather than in a normal trial before a jury.[56]

27. The Special Rapporteur is equally concerned about lower fair trial guarantees that often characterize military and special courts in practice due to prolonged periods of pre-charge and pretrial detention, with inadequate access to counsel, intrusion into the attorney-client confidentiality and strict limitations on the right to appeal and bail.[57] Moreover, the Special Rapporteur is concerned that lower procedural and evidential standards in these courts often encourage systematic resort to extralegal practices such as torture to extract confessions of alleged terrorist suspects. The Special Rapporteur welcomes the fact that several countries, such as Algeria and India, have abolished the practice of trying terrorist suspects at special courts and have transferred jurisdiction over terrorism cases back to ordinary courts.

28. The use of military tribunals should be limited to trials of military personnel for acts committed in the course of military actions,[58] and the trying of any civilians by military should take place only in limited exceptional situations where resort to such trials is necessary and justified by objective and serious reasons such as military occupation of foreign territory where regular civilian courts are unable to

[54] See sect. 12.2 of Pakistan's Anti-Terrorism Act (1997) and article 179 of the constitution of the Arab Republic of Egypt (2007), article 179. The Special Rapporteur has also made extensive critical comments about the jurisdiction and operation of United States military commissions under the 2006 Military Commissions Act, see A/HRC/6/17/Add.3, chap. III.

[55] In Egypt, military verdicts are subject to review by other military judges and confirmation by the President. Under the Military Commissions Act in the United States, the "Convening Authority", appointed by the Secretary of Defense, reviews and approves charges against persons determined to be alien unlawful enemy combatants, appoints military commission members, and reviews military commissions' verdicts and sentences.

[56] *Kavanagh v. Ireland*, Human Rights Committee Communication No. 819/1998, CCPR/C/71/D/819/1998 (2001).

[57] International Commission of Jurists, Military Jurisdiction and International Law: *Military Courts and gross human rights violations* (vol. 1) Geneva, 2004.

[58] A/HRC/Sub.1/58/30 (2006), para. 46; E/CN.4/2006/58, para. 29.

undertake the trials.[59] The Special Rapporteur reiterates his concern that the possibility exists for civilians to be tried by a military commission at Guantánamo Bay, in the case of persons who might be categorized by the United States as unlawful enemy combatants but who in fact were not directly involved in the conduct of hostilities in an armed conflict.[60]

2. Compensation to victims of terrorism

29. During his mission to Turkey, the Special Rapporteur was encouraged by the creation by Turkey of one of the few models of systematically addressing the issue of compensation to victims of terrorism. While he recommended as an element of best practice the underlying principles of the Act on the Compensation of Losses Resulting from Terrorist Acts and Measures Taken to Fight Against Terror (Compensation Act), he was troubled by some aspects of its implementation. Despite the judicial nature of the tasks performed by the loss assessment commissions established under the Compensation Act, the commissions are composed primarily of government officials. This, combined with inconsistencies in the award of compensation, and in the admissibility of claims, led the Special Rapporteur to conclude that the compensation mechanisms lacked judicial independence and objectivity.[61] Rights of review and appeal to judicial courts are frustrated by delays and thereby discourage recourse to them.[62]

C. Open administration of justice

30. One of the central pillars of a fair trial under article 14 of the International Covenant on Civil and Political Rights is the open administration of justice, important to ensure the transparency of proceedings and thus providing an important safeguard for the interest of the individual and of society at large.[63] While paragraph 1 permits exclusion of the press and public for reasons of national security, this must occur only to the extent strictly necessary and should be accompanied by adequate mechanisms for observation or review to guarantee the fairness of the hearing.[64] The Special Rapporteur has therefore been troubled by reports of prosecution applications for the entirety of certain criminal proceedings to be held in camera.[65] He further recalls that article 14(1) requires that any judgement must be made public, unless the interest of juvenile persons otherwise requires, or the proceedings concern matrimonial disputes or the guardianship of children.

---

[59] See Human Rights Committee, General Comment No. 32, para. 22. See also *Madani v. Algeria*, Human Rights Committee Communication No. 1172/2003, CCPR/C/89/D/1172/2003 (2007), para. 8.7; *Bee v. Equatorial Guinea*, Human Rights Committee Communications Nos. 1152/2003 and 1190/2003, CCPR/C/85/D/1152 and 1190/2003 (2005), para. 6.3; and *Benhadj v. Algeria*, Human Rights Committee Communication No. 1173/2003, CCPR/C/90/D/1173/2003 (2007), para. 8.8. For jurisprudence of the European Court of Human Rights on this point see *Ocalan v. Turkey* [2005] ECHR 282 (para. 115); and *Incal v. Turkey* [1998] European Court of Human Rights 48, para. 75.

[60] A/HRC/6/17/Add.3, para 30.

[61] A/HRC/4/26/Add.2, paras. 40-54 and 80.

[62] Ibid., para 43.

[63] See Human Rights Committee, General Comment No. 32, para. 67.

[64] A/HRC/Sub.1/58/30 (2006), para. 45.

[65] See, for example, his comments in A/HRC/6/17/Add.2, para. 32.

V. Aspects of a fair hearing

A. Privilege against self-incrimination

31. The privilege against self-incrimination is of relevance to the right to a fair hearing in two contexts. It may be a matter that invokes article 14(3)(g) of the International Covenant on Civil and Political Rights through the conduct of an investigative hearing where a person is compelled to attend and answer questions.[66] The issue also arises where methods violating the provisions of article 7 (torture and any other inhumane treatment) are used in order to compel a person to confess or testify. On the latter point, it has been observed that such methods are often used, with a growing tendency to resort to them in the investigation of terrorist incidents or during counter-terrorism intelligence operations more generally.[67] Where such allegations are made out, the Human Rights Committee has not hesitated to find a violation of article 14(3)(g), *juncto* articles 7 or 10.[68]

32. The Special Rapporteur stresses that the practical implementation of article 14 (3)(g) of the Covenant is dependent on safeguards and procedural rules that ban in law and practice statements made involuntarily. The Special Rapporteur is therefore concerned about the deviation of ordinary criminal procedures that appear to create a coercive framework that facilitates confessions, for instance in Sri Lanka and Pakistan, where confessions of "terrorist suspects" made to senior police officers are allowed as evidence in court.[69] Experiences from the past, for instance in Northern Ireland,[70] have taught that such deviations, especially in combination with prolonged periods of pre-charge detention, have encouraged the use of methods violating the provisions of article 7 (torture and any other inhumane treatment). No statements or confessions or other evidence obtained in violation of article 7 may be invoked as evidence in any proceedings covered by article 14, including during a state of emergency, except when a statement or confession is used as evidence that torture or other treatment prohibited by the provision has occurred.[71] It is therefore of concern to the Special Rapporteur that, for instance in Algeria, legislation does not explicitly exclude as evidence confessions obtained under torture,[72] and that in trials before military commissions at Guantánamo Bay, testimony obtained through abusive interrogation techniques that were used prior to the Detainee Treatment Act

[66] See the Australian Security Intelligence Organization Act 1979, referred to in A/HRC/4/26/Add.3, paras. 31-32. See also sect. 83.28 of the Canadian Criminal Code. The provision was subject to a sunset clause and expired after the Canadian House of Commons voted against extending its application in February 2007.

[67] See Human Rights Committee, General Comment No. 32, para. 41; and A/HRC/6/17/Add.3, chap. IV.

[68] See *Burgos v. Uruguay*, Human Rights Committee Communication No. 52/1979, CCPR/C/OP/1, para. 13.

[69] Sri Lanka, Prevention of Terrorism Act No. 14 (1979), para. 16 (c). Pakistan, Anti-Terrorism Act (1997), article 21H.

[70] Written submission of the Committee on the Administration of Justice to the Eminent Jurist Panel on Terrorism, Counter-Terrorism and Human Rights, entitled "War on Terror: Lessons from Northern Ireland", 31 January 2008.

[71] See Human Rights Committee, General Comment No. 32, para. 6, and General Comment No. 29, paras. 7 and 15. Again, numerous violations of article 14, *juncto* article 7, have been found by the Committee, including in *Khudayberganov v. Uzbekistan*, Human Rights Committee Communication No. 1140/2002, CCPR/C/90/D/1140/2002 (2007), para. 8.4.

[72] CCPR/C/DZA/CO/3 (2007), para. 19.

of 2005 may be used as evidence if found to be "reliable" and its use "in the interests of justice"[73] and that even though evidence obtained by torture is now categorically inadmissible, evidence obtained by other forms of coercion may, by determination of a military judge, be admitted into evidence.[73]

33. The Special Rapporteur points out that the broader context in which the accused or a witness makes a statement, such as the existence of secret or prolonged arbitrary detention, irrespective of the coerciveness of the actual interrogation, is also of crucial importance to assess the conformity of a statement with article 14 (3)(g).[74]

B. Evidence obtained in breach of human rights or domestic law

34. Some countries maintain a strict distinction between admissible and inadmissible evidence, often related to trial before a jury that determines issues of fact on the basis of the trial judge's instructions on issues of law. In such systems, testimonies or other types of evidence may be excluded from the case by the judge as inadmissible. Other legal systems, typically those based on the civil law tradition, may rely on the theory of free evaluation of evidence, albeit with the exclusion of evidence obtained by torture as the exception. Due to the important role of intelligence in detecting terrorist crimes and the secrecy accompanying methods of intelligence gathering, States may feel tempted to modify their rules concerning the admissibility of evidence presented in terrorism cases. For instance, evidence obtained by warrantless surveillance, possibly in direct contravention of domestic law, may be used in terrorism cases, either on its own or through indirect hearsay testimony. The Special Rapporteur takes the view that, also in respect of evidentiary issues, terrorism must be combated within the framework of the law and that States, and in particular their judicial organs, need to remain vigilant in upholding the position that the use of evidence obtained in breach of human rights or of domestic law renders the trial unfair.[75]

C. Equal treatment and equality of arms

35. The principle of the equality of arms requires the enjoyment of the same procedural rights by all parties unless distinctions are based on law and can be justified on objective and reasonable grounds, and so long as such distinctions do not entail actual disadvantage or other unfairness to one of the parties.[76] The principle is fundamental to safeguarding a fair trial and may engage various particular aspects of article 14, such as access to evidence, participation in the

[73] A/HRC/6/17/Add.3, para. 27.

[74] See *R v. Joseph Terrence Thomas*, VSCA 165 (18 August 2006).

[75] The European Court of Human Rights, however, has in some cases taken the approach that a violation of the right to privacy (article 8 of the European Convention on Human Rights) through unlawful methods of obtaining evidence can be established separately, without necessarily rendering the trial as a whole as unfair (*Khan v. United Kingdom*, [2000] ECHR 195), whereas the reliance by a court upon evidence obtained in violation of the prohibition against inhuman treatment (article 3 of the European Convention on Human Rights) did render the trial unfair and constituted a violation also of article 6 of the Convention on fair trial (*Jalloh v. Germany*, [2006] ECHR 721).

[76] See Human Rights Committee, General Comment No. 32, para. 13.

hearing, or representation (these matters are discussed further in this report). It should be noted, in this regard, that the right to a fair trial is broader than the sum of the individual guarantees within article 14, and depends on the entire conduct of the trial.[77] Disproportionate aggregation of resources between the prosecution and the defence in terrorism cases is a matter that strikes at the heart of the principle of the equality of arms required in the safeguarding of a fair trial.

D. Disclosure of information

36. Article 14(3)(b) of the International Covenant on Civil and Political Rights provides that an accused must have adequate time and facilities for the preparation of his or her defence, and to communicate with counsel of choosing. Determination of what constitutes adequate time and facilities requires an assessment of each individual case, but this must at least include access to documents and other evidence that an accused requires to prepare the defence case.[78] All materials that the prosecution plans to offer in court against the accused, or that are exculpatory, must be disclosed to the defence.[79] This obligation exists even in the case of classified information which is not provided to prosecution counsel.[80] Exculpatory material should be understood as including not only material establishing innocence but also other evidence that could assist the defence, such as indications that a confession was not voluntary. In cases of a claim that evidence was obtained in violation of article 7 of the Covenant, information about the circumstances in which such evidence was obtained must be made available to allow an assessment of such a claim.[81] It is therefore important that an accused be provided with information about the circumstances by which all evidence adduced at trial has been obtained so that he or she may know whether to challenge such evidence.[82]

E. Representation

37. The right to representation involves the right to be represented by legal counsel of choice and the right to self-representation. The right to represent oneself is not absolute and the interests of justice may, in the case of a specific trial, require the assignment of a lawyer against the wishes of the accused. Any restriction of the wish of accused persons to defend themselves must, however, have an objective and

[77] See *Official Records of the General Assembly, Forty-fourth Session, Supplement No. 44* (A/44/40) annex X, sect. E: Communication No. 207/1986, *Yves Morael v. France*, para. 9.3.

[78] See Human Rights Committee, General Comment No. 32, para. 34. See also *van Marcke v. Belgium*, Human Rights Committee Communication No. 904/2000, CCPR/C/81/D/904/2000 (2004), para. 8.3.

[79] See the ruling of the Federal Supreme Court of Germany in the case of Motassadeq, whose trial got remanded because the United States had refused to share with the German courts potentially exculpatory evidence. Decision of the Federal Supreme Court of Germany, 3 March 2004, Strafverteitiger (BGH), StV 4/2004.

[80] A/HRC/6/17/Add.3, para. 26.

[81] See Human Rights Committee, General Comment No. 32, paras. 6 and 33; General Comment No. 29, paras. 7 and 15; and *Convention against Torture*, article 15.

[82] A/HRC/6/17/Add.3, para. 28.

sufficiently serious purpose and not go beyond what is necessary to uphold the interests of justice.[83]

38. In the context of the fight against terrorism, limitations upon representation by counsel of choice are sometimes being imposed out of fear that legal counsel may be used as a vehicle for the flow of improper information between counsel's client and a terrorist organization. This fear is being addressed by States either excluding or delaying the availability of counsel;[84] requiring consultations between counsel and client to be electronically monitored, or to take place within the sight and hearing of a police officer,[85] or appointing special (chosen by State) counsel in place of the person's counsel of choice.[86] The appointment of such a special legal counsel may also arise where the disclosure of information redacted for security reasons would be insufficient to guarantee a fair trial and allow the person concerned to answer the case.

39. Equally, the Special Rapporteur notes with concern that a number of terrorism laws do not explicitly exempt the lawyer-client relationship from the scope of various criminal offences such as material support to terrorism. Where measures are taken to monitor the conduct of consultations between legal counsel and client, strict procedures must be established to ensure that there can be no deliberate or inadvertent use of information subject to legal professional privilege. Due to the importance of the role of counsel in a fair hearing, and of the chilling effect upon the solicitor-client relationship that could follow the monitoring of conversations, such monitoring should be used rarely and only when exceptional circumstances justify this in a specific case.[87] The decision to prosecute someone for a terrorist crime should never on its own have the consequence of excluding or limiting confidential communication with counsel. If restrictions are justified in a specific case, communication between lawyer and client should be in sight but not in hearing of the authorities.[88]

40. Generally speaking, there must be a reasonable and objective basis for any alterations from the right to choose one's counsel, capable of being challenged by judicial review. Any delay or exclusion of counsel must not be permanent; must not prejudice the ability of the person to answer the case; and, in the case of a person held in custody, must not create a situation where the detained person is effectively held incommunicado or interrogated without the presence of counsel.[89] The Special Rapporteur was concerned, in this regard, by the Criminal Procedures (Non-Resident Detainee Suspected of Security Offence) (Temporary Provision) Law 2006 of Israel which, in combination with accompanying regulations, permits a

[83] See Human Rights Committee, General Comment No. 32, para. 37, and its corresponding views in *Correia de Matos v. Portugal*, Communication No. 1123/2002, CCPR/C/86/D/1123/2002 (2006), paras. 7.4-7.5.

[84] As permitted under the Terrorism Act 2000 (UK), para. 8 to schedule 8.

[85] Ibid., para. 9.

[86] As permitted in the context of the control orders regime under the Prevention of Terrorism Act 2005 (UK), and provided for under para. 7 of the Schedule thereto.

[87] See *Erdem v. Germany* [2001] ECHR 434, para. 65.

[88] See also, Human Rights Committee, General Comment No. 32, para. 34.

[89] See *Official Records of the General Assembly, Forty-third Session, Supplement No. 40* (A/43/40), annex VII, sect. C, Communication No. 176/1984, *Penarrieta et al. v. Bolivia*, para. 16; and *Dimitry Gridin v. Russian Federation*, Communication No. 770/1997, CCPR/C/69/D/770/1997 (2000), para. 8.5.

security suspect to be detained for up to 21 days without access to a lawyer or family visits such that a detainee may be held without contact with the outside world for periods that could amount to weeks at a time.[90]

41. According to the wording of article 14(3)(d) of the Covenant, every person has the right to "defend himself in person or through legal assistance of his own choosing". In situations where counsel is assigned under legal aid, however, the Human Rights Committee has accepted that limitations may be imposed on the right to choice of counsel.[91] The question of special advocates has been addressed by British courts and the European Court of Human Rights on more than one occasion. In *R (Roberts) v. Parole Board*, the House of Lords considered the ability of the Parole Board to appoint special advocates, Lord Carswell taking the view that the compatibility of special advocates with the right to a fair trial is a matter to be assessed in the particular circumstances of each case and that there may be cases where it would not be fair and justifiable to rely on special advocates.[92] In a later case concerning the validity of control orders under the Prevention of Terrorism Act 2005 (UK), Lord Bingham of the House of Lords emphasized that, while the assistance that special advocates can give has been acknowledged,[93] their use must never undermine the ability of an accused or respondent to effectively challenge or rebut the case against him or her.[94] There are real dangers that procedures accompanying the appointment of special advocates (such as the inability to communicate with the client after classified information is provided to the special advocate) frustrate and undermine the ability of a person to instruct counsel for the purpose of answering the case.[95]

F. Standard of proof

42. As an almost universally recognized principle, the standard of proof applicable to criminal proceedings is that of proof beyond a reasonable doubt, and of the balance of probabilities in civil proceedings. Given the nature of certain terrorism-related proceedings which fall short of criminal prosecutions, and despite the serious consequences that may follow such proceedings, the Special Rapporteur urges States to carefully consider the applicable standards of proof and whether a hybrid of the two should be applicable. He expresses concern, for example, over the fact that control orders, under the regimes in the United Kingdom and Australia,

[90] A/HRC/6/17/Add.4, para. 24.

[91] *Teesdale v. Trinidad and Tobago*, Human Rights Committee Communication No. 677/1996, CCPR/C/74/D/677/1996 (2002), para. 9.6.

[92] *R (Roberts) v. Parole Board* [2005] UKHL 45, para. 144.

[93] As in *Chahal v. United Kingdom* (1996) 23 EH RR 413; *Al-Nashif v. Bulgaria* (2002) 36 EHRR 655, para. 97; and *M v. Secretary of State for the Home Department* [2004] 2 All ER 863, para. 34.

[94] *Secretary of State for the Home Department v. MB and AF*, see note 93 above.

[95] As observed by Lord Bingham, ibid., para. 35; and Lord Woolf in *Roberts*, see note 92 above, para. 83 (vii).

may be imposed on a simple balance of probabilities but may nevertheless put significant burdens upon a controlled person, including a deprivation of liberty.[96]

VI. Death penalty cases

43. Article 6 of the International Covenant on Civil and Political Rights prohibits the reintroduction of capital punishment in countries that have abolished it, either generally or in respect of specific crimes such as terrorist crimes.[97] As article 6 of the Covenant is non-derogable in its entirety, any other State which seeks to retain the death penalty for terrorist crimes is obliged to ensure that fair trial rights under article 14 of the Covenant are rigorously guaranteed. Given the measures already noted in this report concerning the trial of terrorism offences and related proceedings, the Special Rapporteur therefore emphasizes that any trial for terrorism offences which could lead to the imposition of the death penalty, as well as all stages before the trial,[98] and the consideration of appeals on matters of fact and law after the trial,[99] must rigorously comply with all aspects of a fair trial. The Special Rapporteur has expressed concern, in this regard, at the ability of military commissions at Guantánamo Bay to determine charges in respect of which the death penalty may be imposed. Given that any appeal rights subsequent to conviction are limited to matters of law, coupled with the various concerns noted by him pertaining to the lack of fair trial guarantees in proceedings before military commissions, the Special Rapporteur has concluded that any imposition of the death penalty as a result of a conviction by a military commission under the Military Commissions Act 2006 is likely to be in violation of article 6 of the Covenant.[100]

VII. Conclusions and elements of best practice

44. The right to a fair trial is a fundamental guarantee in both criminal and civil proceedings. Its principles, contained within international human rights treaties and customary law, are applicable to judicial guarantees under international humanitarian law and to procedural guarantees pertaining to extradition, expulsion or deportation proceedings. The right to a fair trial may not be subject to derogation where this would circumvent the protection of non-derogable rights and, even when derogation is permissible, certain fundamental safeguards may not be abrogated by

---

[96] See the Prevention of Terrorism Act 2005 (UK), section 4(7), and the Anti-Terrorism Act (No. 2) 2005 (Australia), section 104.4. On the latter see A/HRC/4/26/Add.3, para. 37. On the question of control orders amounting to a deprivation of liberty, see the House of Lords judgments in *Secretary of State v. JJ and Others* [2007] UKHL 45; *Secretary of State v. MB and AF* [2007] UKHL 46; and *Secretary of State v. E and Another* [2007] UKHL 47.

[97] Removal, by a State which has abolished capital punishment, of a person to a jurisdiction where the death penalty is sought against that person amounts to a violation of article 6 of the International Covenant on Civil and Political Rights: see *Judge v. Canada*, Human Rights Committee Communication No. 829/1998, CCPR/C/78/D/829/1998 (2002).

[98] See *Makhmadim Karimov et al. v. Tajikistan*, Human Rights Committee Communication Nos. 1108 and 1121/2002, CCPR/C/89/D/1108 and 1121/2002 , para. 7.5.

[99] See Human Rights Committee, General Comment No. 32, para. 51. See also *Robinson LaVende v. Trinidad and Tobago*, Human Rights Committee Communication No. 554/1993, CCPR/C/61/D/554/1993 (1997), para 5.8; and *Bondlal Sooklal v. Trinidad and Tobago*, Communication No. 928/2000, CCPR/C/73/D/928/2000 (2001), para. 4.10.

[100] A/HRC/6/17/Add.3, para. 31.

way of derogation. Judicial guarantees under international humanitarian law cannot be subject to derogation.

45. All aspects of counter-terrorism law and practice must be in compliance with international human rights law, including the right to a fair trial. Having regard to emerging practices in the fight against terrorism, the Special Rapporteur emphasizes the following basic principles as elements of best practice in securing the right to a fair trial in terrorism cases:

(a) All persons, regardless of nationality or statelessness, must have access to court in the determination of criminal charges or their obligations in a suit at law. Such access must be without delay and include full review by a higher tribunal of any criminal conviction and sentence. In the case of persons detained in relation to an international or non-international armed conflict, there is a special need for clarity as to the status of any such person, accompanied by the ability to seek a meaningful judicial review of their status and the lawfulness of their deprivation of liberty, entailing the possibility of release. Concerning the listing of terrorist or associated entities, and so long as there is no independent review of listings at the United Nations level, there must be access to domestic judicial review of any implementing measure. A person subject to such measures must be informed of the measures taken and to know the case against him or her, and be able to be heard within a reasonable time by the relevant decision-making body. Those held in detention, including in immigration detention facilities, must have access to a judicial hearing as to the legality of their detention within no longer than 48 hours of being detained. In the case of any period of extended detention occurring outside the context of actual criminal proceedings (such as investigative or preventive detention) the need for continued detention of the person must be regularly reviewed by a judicial authority, which should occur at least every seven days;

(b) The requirements of independence and impartiality of judges or other persons acting in a judicial capacity may not be limited in any context. Judicial officers must be free from any form of political influence in their decision-making. The use of military courts should be resorted to only in respect of military persons for offences of a military nature, and any hearing before such courts must be in full conformity with article 14(1) of the International Covenant on Civil and Political Rights. The use of special or specialized courts in terrorism cases should be avoided. While the involvement of judicial officers in investigative hearings is not in violation of article 14 per se, the judiciary must retain procedural powers to ensure that such hearings are conducted in accordance with the rule of law and without endangering the independence of the judiciary;

(c) The right to a fair hearing includes the open administration of justice. Any exclusion of the press or public on national security grounds must occur only to the extent strictly necessary on a case-by-case basis and should be accompanied by adequate mechanisms for observation or review;

(d) Where any person is compelled to provide information at investigative or intelligence hearings, the privilege against self-incrimination requires that the information obtained at such hearings, or derived solely as a result of leads disclosed, at those hearings must not be used against the person. Law enforcement representatives should not be present during intelligence-gathering hearings and a clear demarcation should exist and be maintained between intelligence gathering and criminal investigations. There may be no circumstances in which the use of

evidence obtained by torture or cruel, inhuman or degrading treatment may be used for the purpose of trying and punishing a person. If there are doubts about the voluntariness of statements by the accused or witnesses, for example, when no information about the circumstances is provided or if the person is arbitrarily or secretly detained, a statement should be excluded irrespective of direct evidence or knowledge of physical abuse. The use of evidence obtained otherwise in breach of human rights or domestic law generally renders the trial as unfair;

(e) As criminal offences, the prosecution of acts of terrorism should be undertaken with the same degree of respect for the established rigours of criminal law applicable to ordinary offences. The principle of the equality of arms furthermore requires the enjoyment of the same procedural rights by all parties unless distinctions are based on law and can be justified on objective and reasonable grounds, and so long as such distinctions do not entail actual disadvantage or other unfairness to one of the parties;

(f) All materials that the prosecution plans to offer in court against the accused, or that are exculpatory, must be subject to disclosure. The protection of national security may justify the redaction of information, so long as compensatory mechanisms are adopted to ensure that this does not prejudice the overall right to a fair hearing and to be aware of, and able to respond to, the case;

(g) Any delay or exclusion of legal representation on security grounds must not be permanent, must not prejudice the ability of the person to answer the case, and, in the case of a person held in custody, must not create a situation where the detained person is effectively held incommunicado. Measures taken to monitor the conduct of consultations between legal counsel and client must be accompanied by strict procedures to ensure that there can be no deliberate or inadvertent passing on of information subject to legal professional privilege;

(h) States should take care in prescribing standards of proof applicable to terrorism-related proceedings which fall short of criminal prosecutions and take into account, in that regard, the nature of consequences flowing from such proceedings;

(i) In countries where terrorist crimes remain subject to the death penalty, the State is obliged to ensure that fair trial rights under article 14 of the Covenant are rigorously guaranteed.

United Nations A/HRC/13/37

General Assembly

Distr.: General
28 December 2009

Original: English

Human Rights Council
Thirteenth 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

Summary

The Special Rapporteur, in chapter I of the present report, lists his key activities from 1 August to 15 December 2009. The main report, contained in chapter II, highlights several concerns of the Special Rapporteur regarding the protection of the right to privacy in the fight against terrorism. The importance of the right to privacy and data protection is highlighted in section A.

Article 17 of the International Covenant on Civil and Political Rights is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy. The Special Rapporteur argues, in section B, that article 17 should be interpreted as containing elements of a permissible limitations test. In this context, he calls upon States to justify why a particular aim is legitimate justification for restrictions upon article 17, and upon the Human Rights Committee to adopt a new general comment on article 17.

The Special Rapporteur highlights the erosion of the right to privacy in the fight against terrorism in section C. This erosion takes place through the use of surveillance powers and new technologies, which are used without adequate legal safeguards. States have endangered the protection of the right to privacy by not extending pre-existing safeguards in their cooperation with third countries and private actors. These measures have not only led to violations of the right to privacy, but also have an impact on due process rights and the freedom of movement — especially at borders — and can have a chilling effect on the freedom of association and the freedom of expression.

Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality and reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified, in section D, some of the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews and good practice from around the world.

The concluding section makes recommendations to various key actors (domestic legislative assemblies, domestic executive powers and the United Nations) in order to improve the protection of the right to privacy in the fight against terrorism.

Contents

I. Introduction

1. This report is submitted to the Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to General Assembly resolution 63/185 and Human Rights Council resolution 10/15. The main report lists the activities of the Special Rapporteur from 1 August to 15 December 2009 and focuses thematically on the right to privacy as a human right in the counter-terrorism context. The addenda contain a communications report (A/HRC/13/37/Add.1) and a report on the fact-finding mission to Egypt from 17 to 21 April 2009 (A/HRC/13/37/Add.2).

2. Regarding upcoming country visits, the Special Rapporteur hopes to conduct a mission to Tunisia prior to presenting this report. The Special Rapporteur has suggested dates in late January and early February 2010 and is awaiting a response from the Government. The Special Rapporteur also hopes to conduct official visits to Chile and Peru in 2010. There are outstanding visit requests for Algeria, Malaysia, Pakistan, the Philippines and Thailand.

II. Activities of the Special Rapporteur

3. On 18 and 19 September 2009, the Special Rapporteur convened an expert group meeting at the European University Institute in Florence to discuss thematic issues related to his mandate.[1] The meeting partly coincided with a public event on the "Fight against Terrorism: Challenges for the Judiciary", jointly organized with the Venice Commission and the Sub-Committee on Crime Problems of the Council of Europe. The event was co-funded by the Åbo Akademi University Institute for Human Rights, through its project to support the mandate of the Special Rapporteur.

4. On 29 and 30 September 2009, the Special Rapporteur, along with the other mandate holders involved, participated in informal consultations in Geneva regarding a global joint study on secret detention (A/HRC/13/42). He also met with representatives of the Permanent Missions of Egypt and Tunisia in regard to country visits conducted or planned.

5. On 2 and 3 October 2009, the Special Rapporteur participated in a Wilton Park Conference on "Terrorism, security and human rights: opportunities for policy change" and was a panellist for the discussion on the role of international organizations in response to terrorism and the protection of human rights.

6. On 4 October 2009, the Special Rapporteur delivered a keynote address on the occasion of the inauguration of the academic year at the Faculty of Law at the University of the Basque Country (Universidad del País Vasco) in Bilbao, Spain.

7. From 12 to 14 October 2009, the Special Rapporteur participated in two events in Vienna: the International Workshop of National Counter-Terrorism Focal Points and the Counter-Terrorism Implementation Task Force (CTITF) Retreat. The workshop was jointly organized by a number of member States and the United Nations Office on Drugs and Crime, in close cooperation with the CTITF Office and the Counter-Terrorism Executive Directorate (CTED). It provided a forum to exchange views on how to better link global and national counter-terrorism efforts by fostering greater networking among national

[1] The Special Rapporteur is grateful for the assistance of the members of the expert panel, Dr. Gus Hosein and his research assistant, Mathias Vermeulen, and the participants of his PhD candidate seminar at the European University Institute, in producing this report.

counter-terrorism focal points and facilitating their role as interface between national, regional and global counter-terrorism efforts. The CTITF retreat focused on ways forward to expand and strengthen partnerships between member States, the United Nations system, regional and other organizations and civil society in implementing the United Nations Global Counter-Terrorism Strategy.[2]

8. On 20 October 2009, the Special Rapporteur was represented at a seminar in Brussels on "Strengthening the UN Targeted Sanctions through Fair and Clear Procedures", organized by the Belgian Federal Public Service for Foreign Affairs, Foreign Trade and Development Cooperation.

9. From 26 to 28 October 2009, the Special Rapporteur was in New York to present to the Third Committee of the General Assembly his report,[3] which focused on the gender impact of counter-terrorism measures. The Special Rapporteur had a formal meeting with the Al-Qaida and Taliban Sanctions Committee of the Security Council and met with the Director of the Counter-Terrorism Executive Directorate (CTED). The Special Rapporteur was a panellist at a side event "Engendering Counter-Terrorism and National Security" hosted by the Centre for Human Rights and Global Justice of the New York University School of Law. He also met with a number of non-governmental organizations and gave a press conference.

10. On 29 October 2009, the Special Rapporteur met with the Assistant Secretary for Democracy, Human Rights and Labor and other officials of the United States State Department in Washington D.C., to discuss current and future legal developments with the new Administration, in follow-up to his visit to the United States of America in 2007,[4] and more general issues concerning international humanitarian and human rights law in the counter-terrorism context.

III. The right to privacy

A. The right to privacy as enshrined in constitutions and international human rights treaties

11. Privacy is a fundamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals.[5] The right to privacy has evolved along two different paths. Universal human rights instruments have focused on the negative dimension of the right to privacy, prohibiting any arbitrary interference with a person's privacy, family, home or correspondence,[6] while some regional and domestic instruments have also included a positive dimension: everyone has the right to

[2] See General Assembly resolution 60/288.
[3] A/64/211.
[4] See A/HRC/6/17/Add.3.
[5] Lord Lester and D. Pannick (eds.), *Human Rights Law and Practice* (London, Butterworth, 2004), para. 4.82.
[6] See the Universal Declaration on Human Rights (art. 12); the International Covenant on Civil and Political Rights (ICCPR, art. 17); the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14); and the Convention on the Rights of the Child (art. 16).

respect for his/her private and family life, his/her home and correspondence,[7] or the right to have his/her dignity, personal integrity or good reputation recognized and respected.[8] While privacy is not always directly mentioned as a separate right in constitutions, nearly all States recognize its value as a matter of constitutional significance. In some countries, the right to privacy emerges by extension of the common law of breach of confidence, the right to liberty, freedom of expression or due process. In other countries, the right to privacy emerges as a religious value. The right to privacy is therefore not only a fundamental human right, but also a human right that supports other human rights and forms the basis of any democratic society.

12. The State's ability to develop record-keeping facilities was enhanced with the development of information technology. Enhanced computing power enabled previously unimaginable forms of collecting, storing and sharing of personal data. International core data protection principles were developed, including the obligation to: obtain personal information fairly and lawfully; limit the scope of its use to the originally specified purpose; ensure that the processing is adequate, relevant and not excessive; ensure its accuracy; keep it secure; delete it when it is no longer required; and grant individuals the right to access their information and request corrections.[9] The Human Rights Committee provided clear indications in its general comment No. 16 that these principles were encapsulated by the right to privacy,[10] but data protection is also emerging as a distinct human or fundamental right. Some countries have recognized data protection even as a constitutional right, thereby highlighting its importance as an element of democratic societies. The detailed article 35 of the 1976 Constitution of Portugal can be seen as an example of best practice here.

13. The right to privacy is not an absolute right. Once an individual is being formally investigated or screened by a security agency, personal information is shared among security agencies for reasons of countering terrorism and the right to privacy is almost automatically affected. These are situations where States have a legitimate power to limit the right to privacy under international human rights law. However, countering terrorism is not a trump card which automatically legitimates any interference with the right to privacy. Every instance of interference needs to be subject to critical assessment.

B. Permissible limitations to the right to privacy

14. Article 17 of the International Covenant on Civil and Political Rights is the most important legally binding treaty provision on the human right to privacy at the universal level. The Covenant has been ratified by 165 States and signed by another 6 States.[11]

[7] See the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8) and the Cairo Declaration on Human Rights in Islam (A/45/421-S/21797, art. 18), 5 August 1990.

[8] African Charter on Human and People's Rights (art. 11). See also the African Union's Declaration of Principles on Freedom of Expression in Africa (art. 4.3) and the American Declaration of the Rights and Duties of Man (art. 5).

[9] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

[10] Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[11] As of 16 November 2009. The six countries whose signature has not yet been followed by ratification are China, Cuba, Guinea-Bissau, Nauru, Panama and San Marino.

Article 4 of the Covenant allows States parties to derogate from some provisions of the Covenant, including article 17. Derogations can be made only during a state of emergency threatening the life of the nation and they are subject to several conditions.[12] During the more than 30 years since the entry into force of the Covenant in 1976, fewer than 10 States parties have introduced a state of emergency with reference to acts, or the threat of, terrorism.[13] Four of them have in that context sought to derogate also from article 17 of the Covenant.[14] Another eight States have announced derogation from article 17 without an explicit reference to terrorism as the cause for a state of emergency.[15] However, the notifications in question have remained rather generic, instead of specifying, in line with the requirements under article 4, what concrete measures derogating from article 17 are necessary within the exigencies of the situation.[16] Overall, there is not a single case of a State seeking to derogate from article 17 with reference to terrorism that would demonstrate compliance with all requirements of article 4. Further, only one State has announced derogation from the Covenant with reference to the current (related to the events of 11 September 2001) threat of international terrorism.[17] The situation is similar in respect of reservations to article 17. Although international law generally allows for reservations by States to human rights treaties, provided such reservations are not incompatible with the object and purpose of the treaty,[18] only one State party has submitted a reservation to article 17.[19]

15. Consequently, it appears that States have only rarely resorted to the acknowledged mechanisms available under international law in general, and the Covenant in particular, for unilateral exceptions to the right to privacy. Even when notifications of derogation from article 17 have been submitted, those notifications have remained generic, instead of referring to practical measures and specific forms of derogation. To the Special Rapporteur, the State practice reported above demonstrates that, generally, States appear to be content that the framework of article 17 is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations, including when responding to terrorism. The Special Rapporteur supports this view. Article 17 is written in a manner that allows States parties the possibility to introduce restrictions or limitations in respect of the rights enshrined in that provision, including the right to privacy. Such restrictions and limitations will therefore be subject to the monitoring functions of the Human Rights Committee as the treaty body entrusted with the task of interpreting the provisions of the Covenant and addressing the conduct of States parties in respect of their treaty obligations. The main mechanisms for the exercise of those functions are the mandatory reporting procedure under article 40 of the Covenant and, for those 113 States

[12] For the position of the pertinent treaty monitoring body in respect of the scope and effect of derogations, see Human Rights Committee, general comment No. 29 (2001).

[13] Azerbaijan, Chile, Colombia, El Salvador, Israel, Nepal, Peru, the Russian Federation and the United Kingdom.

[14] Colombia, El Salvador, Nepal and the Russian Federation.

[15] Algeria, Armenia, Ecuador, Nicaragua, Panama, Serbia and Montenegro, Sri Lanka and the Bolivarian Republic of Venezuela. In some of these cases, there may have been a factual link to terrorism, although this was not mentioned in the notification concerning a state of emergency.

[16] For instance, when seeking to derogate from ICCPR, many Latin American States have plainly notified that some named provisions of the Covenant will be "suspended". This is not in line with the requirements of article 4 as explained in general comment No. 29.

[17] The United Kingdom on 18 December 2001. The derogations did not include article 17 and were withdrawn on 15 March 2005.

[18] For the position of the pertinent treaty monitoring body in respect of reservations to the ICCPR and its optional protocols, see Human Rights Committee, general comment No. 24 (2004).

[19] Liechtenstein maintains a reservation concerning the scope of the right to respect for family life with regard to foreigners.

that have ratified the First Optional Protocol to the Covenant, the procedure for individual complaints.

16. The wording of article 17 of the Covenant prohibits "arbitrary or unlawful" interference with privacy, family or correspondence, as well as "unlawful attacks" on a person's honour and reputation. This can be contrasted with the formulation of such provisions as article 12, paragraph 3; article 18, paragraph 3; article 19, paragraph 3; article 21 and article 22, paragraph 2, which all spell out the elements of a test for permissible limitations. In its most elaborate form, this test is expressed in article 21 and article 22, paragraph 3, as consisting of the following three elements: (a) restrictions must be prescribed by national law; (b) they must be necessary in a democratic society; and (c) they must serve one of the legitimate aims enumerated in each of the provisions that contain a limitations clause.

17. The Special Rapporteur takes the view that, despite the differences in wording, article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17. Consequently, limitations to the right to privacy or other dimensions of article 17 are subject to a permissible limitations test, as set forth by the Human Rights Committee in its general comment No. 27 (1999). That general comment addresses freedom of movement (art. 12), one of the provisions that contains a limitations clause. At the same time, it codifies the position of the Human Rights Committee in the matter of permissible limitations to the rights provided under the Covenant. The permissible limitations test, as expressed in the general comment, includes, inter alia, the following elements:

(a) Any restrictions must be provided by the law (paras. 11–12);

(b) The essence of a human right is not subject to restrictions (para. 13);

(c) Restrictions must be necessary in a democratic society (para. 11);

(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);

(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);

(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).[20]

18. The Special Rapporteur takes the view that these considerations apply also in respect of article 17 of the Covenant, as elaborations of the notions of "unlawful" and "arbitrary". Where the textual difference between article 17 and the Covenant provisions that explicitly introduce a limitations test nevertheless matters is in the absence of an exhaustive list of legitimate aims in article 17. Here, the Special Rapporteur calls upon States to justify why a particular aim is legitimate as justification for restrictions upon article 17, and upon the Human Rights Committee to continue monitoring measures undertaken by States parties, including through the consideration of periodic reports and of individual complaints.

[20] See Human Rights Committee, general comment No. 27 (1999).

19. In the view of the Special Rapporteur, the Human Rights Committee should draw up and adopt a new general comment on article 17, replacing current general comment No. 16 (1988). The existing general comment is very brief and does not reflect the bulk of the Committee's practice that has emerged during the more than 20 years since its adoption. Nevertheless, many of the elements for a proper limitations clause, presented above in the light of the subsequent general comment No. 27, were already present in 1988.[21] In its subsequent case law under the Optional Protocol, the Committee has emphasized that interference with the rights guaranteed in article 17 must cumulatively meet several conditions, i.e., it must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant, and be reasonable in the particular circumstances of the case.[22] Further, in finding violations of article 17, the Committee has applied the requirements of legitimate aim, necessity and proportionality.[23]

C. Erosion of the right to privacy by counter-terrorism policies

20. When considering current counter-terrorism policies, States often contend that there are two new dynamics that must be considered alongside privacy protection. First, States claim that their ability to prevent and investigate terrorist acts is linked intimately with increased surveillance powers. The majority of counter-terrorism legislation activities since the events of 11 September 2001 have therefore focused on expanding Governments' powers to conduct surveillance. Second, States claim that since terrorism is a global activity, the search for terrorists must also take place beyond national borders, with the help of third parties which potentially hold extensive amounts of information on individuals, generating a rich resource for identifying and monitoring terrorist suspects. States that previously lacked constitutional or statutory safeguards have been able to radically transform their surveillance powers with few restrictions. In countries that have constitutional and legal safeguards, Governments have endangered the protection of the right to privacy by not extending these safeguards to their cooperation with third countries and private actors, or by placing surveillance systems beyond the jurisdiction of their constitutions.

1. Increasing surveillance measures

21. The range of surveillance operations runs from the specific to the general. At the specific level, legal systems are capable of authorizing and overseeing: undercover operations and covert surveillance to identify illegal conduct; the accumulation of intelligence on specific individuals to identify breaches of law; and targeted surveillance of individuals to build a legal case. The Special Rapporteur had earlier specified that States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[24] Worldwide, there has been a rise in communications surveillance through the interception of communications by intelligence and law enforcement agencies. There is a remarkable convergence in the types of policies pursued to enhance surveillance powers

[21] See Human Rights Committee, general comment No. 16 (1988). See, in particular, paragraphs 3 and 4 that elaborate upon the notions of arbitrary and unlawful interference in ICCPR, art. 17.

[22] See *Van Hulst v. The Netherlands*, communication No. 903/1999, 2004.

[23] See *Madafferi v. Australia*, communication No. 1011/2001, 2004, and *M.G. v. Germany*, communication No. 1482/2006, 2008.

[24] A/HRC/10/3, para. 30.

to respond to terrorism threats. Most of these policies rely upon existing or new technologies, such as "bugs" and tracing technologies that can access the geographical position of mobile phones, technology that reports to Governments the contents of private text conversations of users of voice over Internet protocol,[25] or that installs spyware on suspects' computers in order to enable remote computer access.[26] In some countries, security services have even proposed banning communication technologies that are more difficult to intercept, such as smartphones.[27] The Special Rapporteur is also concerned about the tracking of cross-border communications without judicial authorization.[28]

22. In the name of countering terrorism, States have expanded initiatives to identify, scan and tag the general public through the use of multiple techniques which might violate an individual person's right to privacy. When surveillance occurs of places and larger groups of people, the surveillance is typically subject to weaker regimes for authorization and oversight. Human rights standards have been tested, stretched and breached through the use of stop-and-searches; the compilation of lists and databases; the increased surveillance of financial, communications and travel data; the use of profiling to identify potential suspects; and the accumulation of ever larger databases to calculate the probability of suspicious activities and identify individuals seen as worthy of further scrutiny. More advanced techniques are applied as well, such as the collection of biometrics or the use of body scanners that can see through clothing.[29] Some intrusions into people's lives can be permanent as people's physical and biographical details are frequently centralized in databases.

(a) Stop and search powers

23. States have expanded their powers to stop, question, search and identify individuals, and have reduced their controls to prevent abuse of these powers. These powers have given rise to concerns regarding racial profiling and discrimination in Europe[30] and the Russian Federation[31] and concerns that these powers antagonize the relationship between citizens and the State. Equally, the proportionality requirement in the limitations test to the right to privacy raises questions whether blanket stop and search powers in designated security zones, such as in the Russian Federation[32] or the United Kingdom,[33] are really necessary in a democratic society.

(b) The use of biometrics and dangers of centralized identity systems

24. A key component to new identity policies is the use of biometric techniques, such as facial recognition, fingerprinting and iris-scanning. While these techniques can, in some circumstances, be a legitimate tool for the identification of terrorist suspects, the Special

---

[25] D. O'Brien, "Chinese Skype client hands confidential communications to eavesdroppers", Electronic Frontier Foundation, 2 October 2008.

[26] See the article at the following address: http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html.

[27] S. Das Gupta and L. D'Monte, "BlackBerry security issue makes e-com insecure", *Business Standard*, 12 March 2008.

[28] See, for instance, the Swedish Government's bill on adjusted defence intelligence operations, adopted in June 2008, p. 83.

[29] See the European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection.

[30] Open Society Justice Initiative, *Ethnic Profiling by Police in Europe*, June 2005.

[31] Open Society Justice Initiative and JURIX, *Ethnic Profiling in the Moscow Metro*, June 2006.

[32] 2006 Federal Act No. 35 on Counteraction of Terrorism.

[33] See, e.g., United Kingdom Appeal Court, *R. v. Commissioner of Police for the Metropolis and another*, 2006.

Rapporteur is particularly concerned about cases where biometrics are not stored in an identity document, but in a central database, thereby increasing the information security risks and leaving individuals vulnerable. As the collection of biometric information increases, error rates may rise significantly.[34] This may result in the wrongful criminalization of individuals or social exclusion. Meanwhile, unlike other identifiers, biometrics cannot be revoked: once copied and/or fraudulently used by a malicious party, it is not possible to issue an individual with a new biometric signature.[35] In this context, it has to be noted that, contrary to its scientific objectivity, DNA evidence can also be falsified.[36]

25. Centralized collection of biometrics creates a risk of causing miscarriages of justice, which is illustrated by the following example. Following the Madrid bombings of 11 March 2004, the Spanish police managed to lift a fingerprint from an unexploded bomb. Fingerprint experts from the United States Federal Bureau of Investigation (FBI) declared that a lawyer's fingerprint was a match to the crime-scene sample. The person's fingerprint was on the national fingerprint system because he was a former soldier of the United States. The individual was detained for two weeks in solitary confinement, even though the fingerprint was not his. Examiners failed to sufficiently reconsider the match, a situation that was made worse for him when it was discovered that he, as a lawyer, had defended a convicted terrorist, was married to an Egyptian immigrant, and had himself converted to Islam.[37]

(c) The circulation of secret watch lists

26. Another available technique is watch-list monitoring. The most common type of watch-list monitoring is the "no-fly/selectee" list. Such lists are circulated to airlines and security officials with instructions to detain and question any passenger with a certain name. Little is known of the extent to which these lists are being used, but where these systems are publicly overseen, a number of errors and privacy concerns have arisen, particularly in the United States[38] and Canada.[39] Data integrity issues remain, as the lists have to be continually checked for errors and the identification processes must be performed with great care. These lists are frequently kept secret as they could tip off suspected terrorists, but at the same time this secrecy gives rise to problems of individuals being continually subject to scrutiny without knowing that they are on some form of list, and without effective independent oversight. Such secret surveillance could constitute a violation of the right to privacy under article 17 of the International Covenant on Civil and Political Rights.

27. Where terrorist lists have been made public, article 17 of the Covenant is triggered in another form. The Human Rights Committee has concluded that the unjustified inclusion of a person on the United Nations 1267 Committee's Consolidated List constituted a violation of article 17. It considered that the dissemination of personal information

[34] See, for example, M. Cherry and E. Imwinkelried, "A cautionary note about fingerprint analysis and reliance on digital technology", *Judicature*, vol. 89, No. 6 (2006).

[35] See E. Kosta et al., "An analysis of security and privacy issues relating to RFID enabled ePassports", International Federation for Information Processing, No. 232 (2007), pp. 467–472.

[36] See, for example, D. Frumkin et al., "Authentification of forensic DNA samples" *Forensic Science International: Genetics* (17 July 2009).

[37] See the United States Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case*, January 2006.

[38] See the United States Department of Justice, *Audit of the FBI Terrorist Watchlist Nomination Practices*, May 2009.

[39] See the Office of the Privacy Commissioner Canada, *Audit of the Passenger Protect Program of Transport Canada*, November 2009.

constituted an attack on the honour and reputation of the listed persons, in view of the negative association that would be made between the names and the title of the sanctions list.[40]

28. Public and secret watch lists often also breach fundamental principles of data protection. Information generated for one purpose is reused for secondary purposes, and sometimes shared with other institutions, without the knowledge or consent of the individuals concerned. Erroneous information is used to make decisions about people, which result in restrictions on travel. These individuals may be refused a visa, turned away at a border or prevented from boarding a plane, without having been presented with evidence of any wrongdoing.

(d) Checkpoints and borders

29. Through the use of new technologies and in response to rising concerns regarding terrorism, States are increasing the monitoring, regulation, interference and control of the movement of people at borders. Now, with the use of more advanced technologies and data-sharing agreements, States are creating comprehensive profiles on foreign travellers to identify terrorists and criminals even in advance of their arrival at borders, by accessing passenger manifests and passenger reservation records from carriers. States analyse this information to identify patterns that correspond to those of terrorists or criminals. At the border, individuals are subjected to further — potentially invasive — information collection practices.

30. Many States now require carriers to submit passenger manifests prior to departure. States are also seeking access to passenger name records, which include identification information (name, telephone number), transactional information (dates of reservations, travel agent, itineraries), flight and seat information, financial data (credit card number, invoice address), choice of meals and information regarding place of residence, medical data, prior travel information, and frequent-flyer information. This information is used for profiling and risk-assessing passengers, usually by submitting queries to various multi-agency law enforcement and terrorist databases and watch lists. As a result, foreign carriers may be restricted from issuing an individual with a boarding pass solely on the basis of the results of a database query in the destination country, without due process.

31. The increased monitoring of immigrants and travellers for various purposes gives rise to a number of privacy challenges. States are gaining information on travellers from third parties who are compelled to comply lest they be refused landing rights or given punitive fines, even though privacy guarantees may not meet the requirements of domestic privacy laws. Moreover, foreigners might not be granted equal access to judicial remedies in these countries and rights at borders are usually significantly restricted. The United States Government policy on access to travellers' laptops is a useful example. Despite the need to meet constitutional due process requirements for searching a laptop within the United States, the Department of Homeland Security has approved the accessing of travellers' computers without judicial authorization.[41]

32. Lastly, States are establishing additional information requirements. Individuals can be prevented from entering States for refusing to disclose information, and States may insist upon disclosure without ensuring that there is lawful authority to require this information. Additionally, information collected for one purpose is now being used for additional purposes; for example, the European Union's European Dactyloscopie system

[40] See Human Rights Committee, communication No. 1472/2006, paras. 10.12–10.13.

[41] See the Department of Homeland Security, *Privacy impact assessment for the border searches of electronic devices*, 25 August, 2009.

(EURODAC) for managing applications of asylum-seekers and illegal immigrants through the use of fingerprints is now proposed to be extended to aid the prevention, detection, and investigation of terrorist offences and other serious offences. The European Data Protection Supervisor has expressed doubts as to whether these proposals are legitimate under the right to privacy.[42]

2. How surveillance has affected other rights

33. Surveillance regimes adopted as anti-terrorism measures have had a profound, chilling effect on other fundamental human rights. In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed. Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively. Surveillance has also resulted in miscarriages of justice, leading to failures of due process and wrongful arrest.

34. In many nations around the world, users are being monitored to review what sites they are visiting and with whom they are communicating. In Germany, the Federal Intelligence Service was found in 2006 to have been illegally spying on journalists using communications surveillance and placing spies in newsrooms.[43] In Colombia, the Administrative Department of Security was found, in 2009, to have been conducting illegal surveillance of members of the media, human rights workers, Government officials and judges, and their families for seven years.[44] In numerous countries across the world, internet users must show identification and their sessions are recorded for future use by authorities. For instance, in Internet service providers in Bangladesh were required in 2007 to turn over records of their users' identities, passwords and usage to the authorities. Some users were then visited by the authorities, who searched though their computers and contact lists.[45] In the United States, the FBI counter-terrorism unit monitored the activities of peace activists at the time of the 2004 political conventions.[46] These surveillance measures have a chilling effect on users, who are afraid to visit websites, express their opinions or communicate with other persons for fear that they will face sanctions.[47] This is especially relevant for individuals wishing to dissent and might deter some of these persons from exercising their democratic right to protest against Government policy.

35. In addition to surveillance powers, many anti-terrorism laws require individuals to proactively disclose information and provide broad powers for officials to demand information for investigations. In this context, the Special Rapporteur has earlier expressed his concerns about the use of national security letters in the United States.[48] Some countries have expanded this power to require the disclosure of information originally collected for journalistic purposes. In Uganda, the 2002 Anti-Terrorism Act allows for wiretapping and

---

[42] See the statement by the European Data Protection Supervisor on law enforcement access to EURODAC, 8 October 2009.

[43] Deutsche Welle World, "Germany stops journalist spying in wake of scandal", 15 May 2006.

[44] See *Semana*, 21 February 2009.

[45] See *E-Bangladeshi*, "Crackdown on internet users in Bangladesh", 3 October 2007 (translating BBC reports).

[46] See the American Civil Liberties Union, "ACLU uncovers FBI Surveillance of main peace activists", 25 October 2006.

[47] See D.S. Sidhu, "The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, vol. 7 (2007), p. 375.

[48] A/HRC/6/17/Add.3, para. 51.

searches of the media if there are "special reasonable grounds" that the information has "substantial value" in an anti-terrorism investigation.[49] The Special Rapporteur stresses that the legitimate interest in the disclosure of confidential materials of journalists outweighs the public interest in the non-disclosure only where an overriding need for disclosure is proved, the circumstances are of a sufficiently vital and serious nature and the necessity of the disclosure is identified as responding to a pressing social need.[50]

36. The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a "function creep", when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism. In the United States, environmental and other peaceful protestors were placed on terrorist watch lists by the Maryland State Police before political conventions in New York and Denver.[51] In the United Kingdom, surveillance cameras are commonly used for political protests and images kept in a database.[52] A recent poll in the United Kingdom found that one third of individuals were disinclined to participate in protests because of concern about their privacy.[53]

37. Freedom of movement can also be substantially affected by surveillance. The creation of secret watch lists, excessive data collection and sharing and imposition of intrusive scanning devices or biometrics, all create extra barriers to mobility. As described in previous sections, there has been a substantial increase in the collection of information about people travelling both nationally and internationally. Information is routinely shared and used to develop watch lists that have led to new barriers to travel. When profiles and watch lists are developed using information from a variety of sources with varying reliability, individuals may have no knowledge of the source of the information, may not question the veracity of this information, and have no right to contest any conclusions drawn by foreign authorities. A mosaic of data assembled from multiple databases may cause data-mining algorithms to identify innocent people as threats.[54] If persons are prohibited from leaving a country, the State must provide information on the reasons requiring the restriction on freedom of movement. Otherwise, the State is likely to violate article 12 of the International Covenant on Civil and Political Rights.[55]

38. One of the most serious effects of surveillance measures is that they may lead to miscarriages of justice and violate due process guarantees. The challenge of gaining access to judicial review is that some legal regimes may prevent access to the courts unless individuals can show that interference has taken place, which is precluded by the secretive

[49] Anti-terrorism Act, third schedule, para. 8.

[50] See also recommendation No. R (2000) 7, of the Council of Europe Committee of Ministers to member States on the right of journalists not to disclose their sources of information and Ontario Superior Court of Justice, *O'Neill v. Canada (Attorney General)*, 2006, para. 163.

[51] See L. Rein and J. White, "More groups than thought monitored in police spying", *The Washington Post*, 4 January 2009.

[52] See P. Lewis and M. Vallée, "Revealed: police databank on thousands of protesters", *The Guardian*, 6 March 2009.

[53] See A. Jha and J. Randerson, "Poll shows public disquiet about policing at environmental protests", *The Guardian*, 25 August 2009.

[54] See United States National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*, October 2008.

[55] See, similarly, Human Rights Committee, *B. Zoolfia v. Uzbekistan*, communication No. 1585/2007, 2009, para. 8.3.

nature of the surveillance programmes. Individuals may not be able to prove or demonstrate that they are actually under surveillance. As a result, individuals may not be able to appeal to courts for remedy. In relevant cases, courts have ruled that individuals lack standing because they cannot demonstrate that they were under surveillance and any injuries have been considered speculative.[56] In other cases, where interference can be proven, States have sometimes applied the "State secrets" privilege to avoid scrutiny of illegal surveillance projects.[57] The Special Rapporteur commends the approach of the European Court of Human Rights (ECHR) where individuals do not need to prove that such measures necessarily had applied to them.[58]

3. Extending legal boundaries

39. Mutual legal assistance treaties are established to permit countries to cooperate in investigations and to share information in specific cases.[59] Agreements have also been established to permit the sharing of information on individuals engaged in activities, e.g., all passengers travelling to another country or all individuals conducting interbank financial transactions. More opaque are the agreements between intelligence agencies to share databases and intelligence data. These databases are often subject to wide-ranging exemptions from the domestic legal system. Even if domestic legislation applies, the data may refer to foreign nationals who may not be permitted to exercise any rights in domestic courts. Individuals may not be aware of the fact that they are subject to surveillance — e.g., that they are on a list of suspected terrorists — because intelligence-driven lists are not publicly available and therefore they may not appeal for review. When that list is shared internationally individuals may not be able to identify why they were first placed on it, or otherwise be able to remove themselves from the multiplicity of lists that have emerged since then.

40. States have increased not only their cooperation with each other in the fight against terrorism, but also with private third parties that have personal information of individuals in order to identify and monitor terrorist suspects. Some Governments have subsequently endangered the protection of the right to privacy by not extending domestic privacy safeguards to their cooperation with third countries and private actors.

41. Third parties, such as banks, telephone companies or even cybercafes, now hold extensive personal information about individuals. Access to this information therefore provides significant details about the private lives of individuals. At the same time, government agencies may gain access to this information with fewer restrictions than if the information was held by individuals themselves, in the home, or even by other government agencies. In the United States, for instance the Supreme Court has ruled that, as data provided to third parties such as banks or telephone companies is shared "freely" with these parties, individuals may not reasonably expect privacy.[60] Where there is a lack of constitutional protections that require a legal basis for the interference in the private lives of individuals, the burden then falls on the private organization to decide how to respond to a request from a government agency. Generally, the private sector prefers that Governments

---

[56] This was most recently concluded in *Amnesty International et al. v. John McConnell et al.*, United States District Court for the Southern District of New York, 20 August 2009.

[57] See United States District Court for the Northern District of California, *Al-Haramain Islamic Foundation et al. v. Bush et al.*, 1 May 2009.

[58] See ECHR, *Klass v. Germany*, 6 September 1978, para. 38.

[59] See G. Hosein, *International Co-operation as a Promise and a Threat, in Cybercrime and Jurisdiction: A Global Survey* (T.M.C. Asser Press), 2006.

[60] See United States Supreme Court, *Smith v. Maryland*, 1979, in the case of communications data, and *United States v. Miller*, 1976, in the case of financial information.

establish a legal basis for obliging organizations to produce personal information upon request, as it removes their obligation to consider the nature of the case.

42. Third parties are also increasingly being called upon to collect more information than is necessary, and to retain this information for extended periods of time. The United Kingdom, for instance, has proposed that telecommunications companies actively monitor and retain information on individuals' online activities including social-networking activities – information that these companies have no justified interest in collecting.[61] Similarly, the European Union's data retention directive[62] has generated considerable criticism. When, in 2008, the German Federal Constitutional Court temporarily suspended the German law implementing that directive, it noted that "the retention of sensitive data, comprehensive and without occasion, on virtually everyone, for Government purposes that at the time of the storage of the data cannot be foreseen in detail, may have a considerable intimidating effect".[63] Also in Germany, research showed a chilling effect of data retention policies: 52 per cent of persons interviewed said they probably would not use telecommunication for contact with drug counsellors, psychotherapists or marriage counsellors because of data retention laws.[64]

43. In this context, the Special Rapporteur is concerned that, in many countries, data retention laws have been adopted without any legal safeguards over the access to this information being established or without the fact that new technological developments are blurring the difference between content and communications data being considered. While constitutional provisions tend to require safeguards on access to communications content, the protection of transaction logs is more limited. While this information may be integral to investigations, it may also be just as privacy-sensitive as the content of communications transactions.

44. With the goal of combating terrorism financing and money laundering, States have obliged the financial industry to analyse financial transactions in order to automatically distinguish those "normal" from those "suspicious". For instance, the European Union established a directive in 2005 on "the prevention of the use of the financial system for the purpose of money laundering and terrorist financing"[65] requiring that financial institutions follow due diligence by reporting suspicious and "threshold" activities to financial intelligence units (FIUs). The additional processing of this information by the FIUs remains opaque, but States like Australia[66] and Canada[67] are processing millions of transactions each year through advanced data-mining tools.

45. Third parties may also be subject to foreign laws requiring disclosure. The United States Government, for instance, issued administrative subpoenas to the Society for

---

[61] See British All Party Parliamentary Group on Privacy, *Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme*, June 2009.

[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal*, L 105 (2006), pp. 54–63.

[63] Constitutional Court decision No. 256/08, 11 March 2008.

[64] German Forsa Institute, *Meinungen der Bunderburger zur Vorratsdatanspeicherung*, 28 May 2008.

[65] See Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal*, L 309 (2005), pp. 15–36.

[66] See Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2008–09*, October 2009.

[67] See Financial Transaction and Reports Analysis Centre of Canada, *FINTRAC Annual Report 2008*, 11 September 2008.

Worldwide Interbank Financial Telecommunication (SWIFT), the Belgian cooperative responsible for enabling messaging between more than 7,800 financial institutions in over 200 countries. By gaining access to the SWIFT data centre in the United States, the country's Treasury was then able to monitor foreign financial transactions across the SWIFT network, to find and identify terrorist suspects.[68] Human rights groups filed legal complaints in over 20 courts arguing that, by handing this information over to United States authorities, SWIFT was in breach of local privacy laws.[69]

46. The Special Rapporteur is also concerned that surveillance is being embedded in technological infrastructures, and that these will create risks for individuals and organizations. For example, the development of standards for lawful interception of communications requires telecommunications companies to design vulnerabilities into their technologies to ensure that States may intercept communications. These capabilities were abused in Greece where unknown third parties were able to listen to the communications of the Prime Minister of Greece, and dozens of other high-ranking dignitaries.[70] More recently, these same capabilities were reported to have been used by the Government of the Islamic Republic of Iran to monitor protestors.[71] To avoid abuse, surveillance technologies should log who accesses data, thereby leaving a trail that can itself be monitored for abuse.[72]

47. In some States, constitutional safeguards continue to apply, however. In Canada, for example, the Charter of Rights and Freedoms protects privacy of information held by third parties when it reveals "intimate details of the lifestyle and personal choices of the individual".[73] This requires balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.[74] The jurisprudence of the European Convention of Human Rights has similarly extended the right to privacy to information held by third parties. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data requires both the public and private sectors to protect the information that they hold and regulates the sharing of information with government agencies. Exceptions apply when protecting State security, public safety or the monetary interests of the State, suppressing criminal offences or protecting individuals or the rights and freedoms of others.[75]

D. Best practices

48. The Special Rapporteur is concerned that there is a trend towards extending such State surveillance powers beyond terrorism. Following the events of 11 September 2001, a number of legislatures introduced sunset clauses into and reviews of anti-terrorism legislation, as it was assumed that extraordinary powers may be required for a short period of time to respond to the then danger. These sunset clauses and reviews were not included

[68] See also the statement of United States Under Secretary Stuart Levey on the Terrorist Finance Tracking Program, 23 June 2006.

[69] See, for example, Privacy International, "Pulling a Swift one? Bank transfer information sent to U.S. authorities", 27 July 2006.

[70] See, for background, V. Prevelakis and D. Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007.

[71] See, for reference, Nokia Siemens Networks, "Provision of lawful intercept capability in Iran", 22 June 2009.

[72] See footnote 54.

[73] See Supreme Court of Canada, *R. v. Plant*, 1993, and *R. v. Tessling*, 2004.

[74] *R. v. Plant.*

[75] Article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

in some areas of policymaking and, in later policies, were not considered at all. Many of the investigative powers given to law enforcement agencies under anti-terror laws are granted to these agencies to conduct investigations unrelated to terrorism. Meanwhile, States are following each other's lead on policy without considering the human rights implications. Many of the policies outlined above were introduced first as extraordinary, but then soon became regional and international standards. Collectively, such interference is having significant negative impacts on the protection of the right to privacy, as there is limited access to legal safeguards. Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality, or reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews and good practice from around the world.

1. The principle of minimal intrusiveness

49. Some interference with the private lives of individuals is more intrusive than others. Constitutional protection of property and people has been extended over the past 50 years to include communications,[76] information that is related to a biographical core[77] and a right to the confidentiality and integrity of information-technological systems.[78] These protections require States to have exhausted less-intrusive techniques before resorting to others. The United Kingdom Parliament's Home Affairs Committee reviewed and adapted these ideas for modern data-centred surveillance systems into the principle of data-minimization, which is closely linked to purpose-specification.[79] In its review, the Parliamentary committee recommended that Governments "resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or to implement proposals for increased surveillance, should be based on a proven need". The Special Rapporteur contends that States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate.

2. The principle of purpose specification restricting secondary use

50. Whereas data protection law should protect information collected for one purpose being used for another, national security and law enforcement policies are generally exempted from these restrictions. This is done through secrecy provisions in lawful access notices, broad subpoenas and exemption certificates such as national security certificates, which exempt a specific database from adhering to privacy laws. The Special Rapporteur is concerned that this limits the effectiveness of necessary safeguards against abuse. States must be obliged to provide a legal basis for the reuse of information, in accordance with constitutional and human rights principles. This must be done within the human rights framework, rather than resorting to derogations and exemptions. This is particularly important when information is shared across borders; furthermore, when information is shared between States, protections and safeguards must continue to apply.[80]

---

[76] See United States Supreme Court, *Katz v. United States*, 1967.

[77] See footnote 74.

[78] See German Constitutional Court decision No. 370/07, 27 February 2008.

[79] See the United Kingdom Parliament's Home Affairs Committee, *A Surveillance Society? Fifth report of the session 2007–2008*, 8 June 2008.

[80] See, for instance, with regard to passenger name records, the article 29 Data Protection Working Party's opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, 30 September 2004.

3. The principle of oversight and regulated authorization of lawful access

51. Surveillance systems require effective oversight to minimize harm and abuses. Where safeguards exist, this has traditionally taken the form of an independent authorization through a judicial warrant and/or a subpoena process with the opportunity of independent review. Many policies have attempted to restrict oversight and lower authorization levels, however: communications interception laws have minimized authorization requirements for some communications; secret subpoenas are issued to gain access to information held by third parties and have restricted the ability to seek judicial protections; and States are increasingly allowing intelligence and law enforcement agencies to self-authorize access to personal information where previously some form of independent authorization and effective reporting was necessary.

52. Some States have taken measures to address the erosion of safeguards. In the United States, after a number of court cases and because of the reauthorization requirements under the USA Patriot Act, more opportunities for judicial review have been reintroduced. Changes to the communications surveillance practices in Sweden and the United States have reintroduced some limited safeguards in the form of judicial warrants. Similarly, the European Court of Justice ruled that courts had to review the domestic lawfulness of international watch lists.[81]

53. The Special Rapporteur is concerned that the lack of effective and independent scrutiny of surveillance practices and techniques calls into question whether interferences are lawful (and thus accountable) and necessary (and thus applied proportionately). He commends the hard work of oversight bodies within government agencies, including internal privacy offices, audit departments and inspectorate-generals, as they too play a key role in identifying abuses. The Special Rapporteur therefore calls for increased internal oversight to complement the processes for independent authorization and external oversight. This internal and external accountability system will ensure that there are effective remedies for individuals, with meaningful access to redress mechanisms.

4. The principle of transparency and integrity

54. The application of secrecy privileges for surveillance systems inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers. Individuals may be subject to inappropriate surveillance, where profiles are developed through data mining, and erroneous judgements, without any prior notification of the practice. Furthermore, the lack of clear and appropriate limitations to surveillance policies makes it difficult to prove that these powers are not used in arbitrary and indiscriminate manners.

55. The principle of transparency and integrity requires openness and communication about surveillance practices. In some States, individuals must be notified when and how they are under surveillance, or as soon as possible after the fact. Under *habeas data* constitutional regimes in Latin America[82] and European data protection laws, individuals must be able to gain access to and correct their personal information held within data stores and surveillance systems. These rights must be ensured across borders by ensuring that legal regimes protect citizens and non-citizens alike.

56. Open debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of

[81] *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council and Commission*, September 2008.

[82] See, e.g., Constitution of Brazil, art. 5 (LXXI); Constitution of Paraguay, art. 135; Constitution of Argentina, art. 43.

the necessity and lawfulness of surveillance. In many States, parliaments and independent bodies have been charged with conducting reviews of surveillance policies and procedures, and on occasion have been offered the opportunity for pre-legislative review. This has been aided by the use of sunset and review clauses in legislation.

5. The principle of effective modernization

57. Even as more invasive information is available with greater ease, States have not developed commensurate protection. In fact, in the name of modernizing their surveillance powers, States sometimes have intentionally sought to apply older and weaker safeguard regimes to ever more sensitive information.[83] Conscious of the need to consider how technology and policy change may have a negative impact on individuals, some States have introduced privacy impact assessments that articulate privacy considerations in the design of new surveillance techniques, including how policymakers considered many of the principles listed above, including data minimization and rights to redress. The Special Rapporteur believes that the use of such tools as privacy impact assessments may help inform the public about surveillance practices, while instilling a culture of privacy within government agencies as they develop new surveillance systems to combat terrorism. International standards must also be adopted to require States to enhance their safeguards to reflect technological change.

IV. Conclusions and recommendations

A. Conclusions

58. **The Special Rapporteur is concerned that what was once exceptional is now customary. First, States no longer limit exceptional surveillance schemes to combating terrorism and instead make these surveillance powers available for all purposes. Second, surveillance is now engrained in policymaking. Critics of unwarranted surveillance proposals must now argue why additional information must not be collected, rather than the burden of proof residing with the State to argue why the interference is necessary. Third, the quality and effectiveness of nearly all legal protections and safeguards are reduced. This is occurring even as technological change allows for greater and more pervasive surveillance powers. Most worrying, however, is that these technologies and policies are being exported to other countries and often lose even the most basic protections in the process.**

59. **International legal standards must be developed to ensure against these forms of abuse. This would be aided by adherence to principles outlined in this report, including ensuring that surveillance is as unintrusive as possible and that new powers are developed with appropriate safeguards and limitations, effective oversight and authorization and regular reporting and review and are accompanied by comprehensive statements regarding the impact on privacy. The general public and legislatures have rarely had the opportunity to debate whether anti-terrorism powers are necessary, proportionate or reasonable. The Special Rapporteur believes that following emergent good practices may prove beneficial to all.**

[83] See the Policy Engagement Network, *Briefing on the UK Government's Interception Modernisation Programme*, June 2009.

B. Recommendations

For legislative assemblies

60. **The Special Rapporteur recommends again that any interference with the right to privacy, family, home or correspondence should be authorized by provisions of law that are publicly accessible, particularly precise and proportionate to the security threat, and offer effective guarantees against abuse. States should ensure that the competent authorities apply less intrusive investigation methods if such methods enable a terrorist offence to be detected, prevented or prosecuted with adequate effectiveness. Decision-making authority should be structured so that the greater the invasion of privacy, the higher the level of authorization needed.**

61. **Adherence to international standards for privacy and human rights protection must be a tenet national law. Accordingly, a comprehensive data protection and privacy law is necessary to ensure that there are clear legal protections for individuals to prevent the excessive collection of personal information, that ensures measures are in place to ensure the accuracy of information, that creates limits on the use, storage, and sharing of the information, and which mandates that individuals are notified of how their information is used and that they have a right to access and redress, regardless of nationality and jurisdiction.**

62. **Strong independent oversight mandates must be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information. Therefore, there must be no secret surveillance system that is not under the review of an effective oversight body and all interferences must be authorized through an independent body.**

63. **All current and proposed counter-terrorism policies must include privacy impact assessments to review and communicate how the policy and technologies ensure that privacy risks are mitigated and privacy is considered at the earliest stages of policymaking.**

64. **The Special Rapporteur recommends that stronger safeguards be developed to ensure that the sharing of information between governments continues to protect the privacy of individuals.**

65. **The Special Rapporteur also recommends that stronger regulations are developed to limit Government access to information held by third parties, including reporting schemes, and to minimize the burden placed on third parties to collect additional information, and that constitutional and legal safeguards apply when third parties are acting on behalf of the State.**

66. **The Special Rapporteur warns that legislative language should be reconsidered to prevent the use of anti-terrorism powers for other purposes. New systems must be designed with a limitation of scope in the specifications.**

For Governments

67. **The Special Rapporteur urges Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to ensure against abuse.**

68. **The Special Rapporteur recommends open discussion and regular reporting on information-based surveillance programmes. Reports to legislative and oversight**

bodies, as well as independent reviews of practices will help inform future policymaking and deliberation on anti-terrorism policy.

69. Any watch list- or profile-based surveillance programme must include due process safeguards for all individuals, including rights to redress. The principle of transparency must be upheld so that individuals can be informed as to why and how they were added to watch lists or how their profile was developed, and of the mechanisms for appeal without undue burdens.

70. Given the inherent dangers of data mining, the Special Rapporteur recommends that any information-based counter-terrorism programme should be subjected to robust and independent oversight. The Special Rapporteur also recommends against the development and use of data-mining techniques for counter-terrorism purposes.

71. In light of the risk of abuse of surveillance technologies, the Special Rapporteur recommends that equal amounts of research and development resources be devoted to privacy-enhancing technologies.

For the Human Rights Council

72. The Special Rapporteur recommends the development of a programme for global capacity-building on privacy protection. The international replication of anti-terrorism laws and the global standards on surveillance must be counterbalanced with greater awareness of the necessary safeguards for the protection of individuals' dignity.

73. The Special Rapporteur urges the Human Rights Council to establish a process that builds on existing principles of data protection to recommend measures for the creation of a global declaration on data protection and data privacy.

For the Human Rights Committee

74. The Special Rapporteur recommends that the Human Rights Committee begins drafting a new general comment on article 17 of the International Covenant on Civil and Political Rights, with the goal of elaborating a proper limitation test, thereby providing guidance to States on appropriate safeguards. The general comment should also give due attention to data protection as an attribute of the right to privacy, as enshrined in article 17 of the Covenant.

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.

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.