Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13315
01 October 2013

National security and access to information

Committee Opinion[1]
Committee on Culture, Science, Education and Media
Rapporteur: Mr Hans FRANKEN, Netherlands, Group of the European People's Party

A. Conclusions of the committee

Supporting the Tshwane Principles, the Committee on Culture, Science, Education and Media welcomes the report by the Committee on Legal Affairs and Human Rights. However, the committee wishes to propose a few amendments to the draft resolution. Those amendments aim to strengthen the protection of human rights and clarify the balance of freedom of information with the protection of national security as well as other human rights in accordance with the jurisprudence of the European Court of Human Rights.

B. Proposed amendments

Amendment A (to the draft resolution)

After paragraph 3, insert the following paragraph:

> *"Recalling the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, the Assembly strongly confirms that the systematic violation of human rights undermines true national security and may jeopardise international peace and security. A State responsible for such violation shall not invoke national security as a justification."*

Explanatory note: Like Article 10 of the European Convention on Human Rights (ETS No. 5, "the Convention"), Article 19 of the International Covenant on Civil and Political Rights specifies national security as a legitimate ground for restricting freedom of information. The right to the protection of private life and correspondence under Article 8 of the European Convention on Human Rights also contains national security as a legitimate ground for restricting this right. The 1984 Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights include the above paragraph on States systematically violating human rights, which are hence barred from using national security concerns as an excuse to fight democratic opposition. As seen in the recent Manning and Snowden cases, large-scale intrusions of privacy in the name of national security are technically feasible and frequent today, and it can be assumed that other countries with a weaker democratic practice are using the same technologies for privacy intrusions, in particular against political opponents. Therefore, it is important to recall this principle here.

1. Reference to committee: Doc. 12548, Reference 3762 of 15 April 2011. Reporting committee: Committee on Legal Affairs and Human Rights. See Doc. 13293. Opinion approved by the committee on 1 October 2013.

Amendment B (to the draft resolution)

After paragraph 5, insert the following paragraph:

> *"Public authorities may access private information and communications or personal data on grounds of national security only, where this has been prescribed by law, an overriding requirement of the need for such access is established and the concrete measure is necessary in a democratic society in order to protect the existence of the nation or its territorial integrity or political independence against force or threat of force. Public authorities must not delegate this power to private persons or companies contracted to work for the protection of national security. Measures applied in this context must be open to administrative or judicial review."*

Explanatory note: Article 8 of the European Convention on Human Rights protects the right to the protection of private life and correspondence. It also contains the requirements for any intrusions into private life and correspondence and lists national security as a possible ground for such an intrusion. As national security services do not always seem to be aware of this provision, it is useful to recall the requirements under the Convention. In addition, the definition established by the Siracusa Principles is certainly helpful in order to avoid an overbroad definition of national security.

The recent case of Edward Snowden has not only shed light on the protection of whistle-blowers, but also on the fact that private companies and persons have been contracted by public authorities to access through Internet and mobile communication a vast amount of secret information which is potentially relevant for national security. This out-sourcing inevitably lowers the protection of private life and correspondence of surveyed individuals and increases the risk of abuse of such delegated powers. Therefore, the power of investigation and surveillance must remain with competent public authorities and must not be delegated to private persons or companies.

Amendment C (to the draft resolution)

In paragraph 8.1, at the end of the first sentence, insert the following sentence:

> *"by the public, where such information is of public concern, or by an individual who has the right to receive information such as personal data."*

Explanatory note: Article 10 of the European Convention on Human Rights establishes the right of the public to be informed of matters of public concern, which may include the right to have access to such information held by public authorities. However, public authorities hold also a lot of information concerning the private life of citizens, which is protected by Article 8 of the Convention, such as personal health information or personal financial data. Obviously, the latter must not be freely accessible to the public. Individuals concerned may have the right to access such personal data under Article 8 of the Convention. In addition, judicial authorities hold information, the disclosure of which could compromise the right to a fair trial under Article 6 of the Convention. Therefore, any and all information held by public authorities must not be accessible freely or publicly.

Amendment D (to the draft resolution)

In paragraph 8.2, delete the following words: "such as the protection of international relations, health and safety or the environment, or on privacy interests".

Explanatory note: Article 10 of the European Convention on Human Rights defines exhaustively the exceptions to the right to freedom of information. These are not matched by those listed in paragraph 8.2, whose present text departs from, and hence might seem to undermine, Article 10 of the Convention. National security is not as equally important as "the protection of international relations, health and safety or the environment". The text should only refer to the subject matter of this report, which is national security; there is no need to mention other exceptions such as "the protection of international relations" which is not a legitimate aim under the European Convention on Human Rights, or "privacy interests", which incorrectly refer to the right to the protection of private life under the Convention.

Amendment E (to the draft resolution)

At the end of paragraph 8.3, add the following sentence:

> *"The neutrality of the Internet requires that public authorities, internet providers and others abstain from using invasive wiretapping technologies, such as deep packet inspection, or from otherwise interfering with the data traffic of Internet users."*

Explanatory note: Network neutrality is a principle recommended for the Internet by the Council of Europe and the European Union; this principle shall ensure that Internet users are not discriminated against by giving higher speed for the transmission of data to particular, typically commercial content providers. In addition, Internet neutrality can be compromised by invasive inspections or interferences with data traffic on the Internet. The brief reference in paragraph 8.3 should therefore be explained in an additional sentence at end of the paragraph.

Amendment F (to the draft resolution)

At the end of paragraph 8.4, add the following sentence:

> *"Public archives containing secret information should periodically review whether the legitimacy of secrecy still exists on national security grounds."*

Explanatory note: Countries have set up quite different rules for the access of individuals to public archives in the field of national security, such as military archives or archives established by security services. It may be necessary, however, to have access to such archives in order to establish historic facts, investigate wrongdoings by public authorities or receive secret information about one's own or a close relative's life.

As examples, one can refer to the public agency established after the fall of the Berlin Wall to provide access to the archives of the former East German Ministry for State Security ("Stasi") as well as the cases of individual access granted by Russian authorities to researchers regarding the archives of the KGB of the former USSR.

Amendment G (to the draft resolution)

Delete sub-paragraphs 8.5.1 and 8.5.2.

Explanatory note: The second sentence of paragraph 8.5 goes far beyond the corresponding Principles 9 and 10 of the Tshwane Principles. In fact, the latter principles identify legitimate grounds for withholding information as well as categories of information with a "high presumption" of an overriding interest in the disclosure. They do not claim that "an important contribution to an ongoing public debate" (paragraph 8.5.1) or the promotion of "public participation in political debate" (paragraph 8.5.2) should per se have priority over national security. National security concerns are frequently the focus of public or political debates. If such debates were per se considered "an overriding public interest", national security interests would become an empty phrase. Besides being highly imprecise and abstract, such postulations would not be covered by Article 10 of the European Convention on Human Rights.

Amendment H (to the draft resolution)

After paragraph 8.7, insert the following paragraph:

> *"Recalling Recommendation No. R (2000) 7 of the Committee of Ministers, the Assembly reiterates that the following measures should not be applied if their purpose is to circumvent the right of journalists not to disclose information identifying a source: i) interception orders or actions concerning communication or correspondence of journalists or their employers; ii) surveillance orders or actions concerning journalists, their contacts or their employers; or iii) search or seizure orders or actions concerning the private or business premises, belongings or correspondence of journalists or their employers or personal data related to their professional work."*

Explanatory note: Interception, search and surveillance measures applied on grounds of national security might compromise the right of journalists not to disclose their sources of information under Article 10 of the European Convention on Human Rights. This issue has been raised in the recent search of the premises of the newspaper *The Guardian* in London. It is therefore useful to recall the relevant Committee of Ministers Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information.

Amendment I (to the draft resolution)

At the end of paragraph 8.8, second sentence, replace the words “an independent body” with the words “a national authority”.

Explanatory note: The expression “independent body” does not specify whether such body should be a public authority or a private body. As the right to have access to information of public concern is based on Article 10 of the European Convention on Human Rights, the denial and possible violation of such right requires an effective remedy before a “national authority” under Article 13 of this Convention. The “national authority” referred to in Article 13 does not necessarily have to be a judicial authority, but if it is not, its powers and the guarantees which it affords are relevant in determining whether the remedy before it is effective (see the judgment of the European Court of Human Rights in *Kudla v. Poland,* Application No. 30210/96, paragraph 157).

C. Explanatory memorandum by Mr Franken, rapporteur for opinion

1. While Article 10 of the European Convention on Human Rights protects the right to freedom of information and its Article 8 protects the rights to private life, these rights may be restricted on grounds of national security under the Convention. The balance to be struck between those rights and national security is the focus of the report by the Committee on Legal Affairs and Human Rights.

2. The Committee on Culture, Science, Education and Media recalls the exchange of views on this subject with Ms Agnes Callamard, Executive Director of ARTICLE 19 (London) and Ms Dunja Mijatovic, OSCE Representative on Freedom of the Media, which was organised by its Sub-Committee on the Media and hosted by the Swedish Parliament in Stockholm on 12 September 2011.

3. Significant work has been pursued by ARTICLE 19 and other non-governmental organisations in defining common principles on freedom of expression and information in the context of national security. Particular reference has to be made to the Johannesburg Principles of 1 October 1995[2] as well as the Tshwane Principles of 12 June 2013.[3] The latter have largely guided the report by Mr Arcadio Díaz Tejera (Spain, SOC) on behalf of the Committee on Legal Affairs and Human Rights.

4. The recent disclosures of secret information by two American citizens, Bradley Manning and Edward Snowden, have focused wide international attention on the limitations of freedom of information on national security grounds in accordance with Articles 8 and 10 of the Convention. Therefore, the Parliamentary Assembly held a current affairs debate on 27 June 2013 on State interference with privacy on the Internet. The report of the Committee on Legal Affairs and Human Rights is hence very timely and important.

5. The European Court of Human Rights has had the opportunity to clarify the scope of protection of private life and correspondence afforded under Article 8 of the European Convention on Human Rights with regard to secret surveillance on grounds of national security. The Court had found already in *Klass and others v. Germany* (Application No. 5029/71):[4] “Powers of secret surveillance of citizens, characterising as they do the police State, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. … [T]he Court, in its appreciation of the scope of the protection offered by Article 8, cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic

2. See www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.
3. See www.opensocietyfoundations.org/sites/default/files/Global%20Principles%20on%20National%20Security%20and%20the%20Right%20to%20Information%20%28Tshwane%20Principles%29%20-%20June%202013.pdf.
4. See http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510.

legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."

6. The United Nations Commission on Human Rights considered in 1984 the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights,[5] which include the following recommendations regarding national security:

– National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.

– National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.

– National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.

– The systematic violation of human rights undermines true national security and may jeopardise international peace and security. A State responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population.

7. In his latest report to the United Nations General Assembly, Mr Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, specifically addressed the human rights concerns regarding communications surveillance, including on grounds of national security. He concluded *inter alia* that State surveillance of communications must be under the supervision of an independent judicial authority, States should criminalise illegal surveillance by public or private actors, and mutual legal assistance treaties should regulate access to communications data held by foreign corporate actors.[6]

5. See www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=4672bc122.
6. See www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.