Strasbourg, 2 March 2012

CDL(2012)020 *

Opinion no. 669/2012

Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

COMMENTS

ON THE DRAFT LAW

ON AMENDMENTS TO THE

LAW ON CLASSIFIED INFORMATION

OF MONTENEGRO

by

Mr I. CAMERON (Member, Sweden)

**This document has been classified restricted on the date of issue. Unless the Venice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe documents.*

1. The present opinion is limited to the amendments. However, it is not possible to comment on these without also commenting to some degree upon the Law itself. The subject of state secrecy is difficult to keep separate from other relevant legislation. This includes: the Criminal Code, which criminalizes both the revealing of secret information, and offences relating to misuse of secrecy; legislation setting out rights of access to official information; legislation dealing with the protection of personal data and legislation on security and intelligence agencies. I should note that, at a late stage I received the analysis of the draft law made by OSCE expert Alexander Kashumov and I have been able to take some of the points he has made into account.

2. A state must be able to keep certain information secret, and to protect this secrecy with both administrative mechanisms and the criminal law. Secrecy can however also hide incompetence, ulterior motives and corruption. Secrecy moreover makes life easier for state authorities, in that it shields them, and their policy-making, from scrutiny from citizens and the media. State authorities are thus continually tempted to keep information secret and to over-classify information.

3. Transparency is necessary for democracy to function properly. Tightly drawn legislation on secrecy is an important precondition for the exercise of freedom of information, which in turn is a vital aspect of constitutional control in a Rechtsstaat. State secrecy should be kept to a minimum. It should at all times be justified by pressing social needs. Excessive secrecy carries with it considerable costs, most seriously in terms of undermining public trust and so the legitimacy of government, but also in terms of inefficiencies in government when information is not flowing properly and the extra financial costs involved in keeping secret matters which do not need to be secret (classification costs, expensive information security and personnel screening procedures etc.). In transitional states, and even well-established democratic states, there can still be strong bureaucratic interests in preserving secrecy, so it should be recognised that changing a culture of secrecy is a long-term process.

4. As there are different systems of public administration in operation in Council of Europe member states, states can obviously differ to some extent as to how they go about protecting administrative secrecy. There are variations among Council of Europe states not just in terms of how secrecy is defined and how the sensitive areas to which the rules relate are managed, but also in terms of the practical arrangements and conditions for prosecuting persons who disclose information illegally. [1] It is for this reason that the European Court of Human Rights (ECHR) has allowed states a certain margin of appreciation in this sphere. [2]

5. The applicable European norms can be found in a variety of sources, some binding, some "soft law" standards (guidelines, best practices etc.).[3] For Montenegro, some standards are to be found in the European Convention on Human Rights and the case law of the European Court of Human Rights (ECtHR). Other important Council of Europe treaties binding on Montenegro are the Convention on Access to Official Documents, 2009 (not yet in force, hereinafter the 2009 Convention) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 and its Additional Protocol regarding

[1] See the brief comparative study by C. Pourgourides, Fair trial issues in criminal cases concerning espionage or divulging state secrets, PACE Doc. 11031, 25 December 2006.
[2] ECtHR, *Stoll v. Switzerland* judgment of 12 December 2007, para. 107.
[3] See CDL-AD(2007)016, Report on Democratic Oversight of the Security Forces, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007). See also Recommendation 1792 (2007) of the Parliamentary Assembly of the Council of Europe (CoE) called on the CoE member States to "[e]xamine existing legislation on official secrecy and amend it in such a way as to replace vague and overly broad provisions with specific and clear provisions, thus eliminating any Parliamentary Assembly of the Council of Europe, Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets, risks of abuse or unwarranted prosecutions.

Supervisory Authorities and Transborder Dataflows (2001).[4] Other relevant instruments are the Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (UNECE) – the Århus Convention. As Montenegro has applied for EU membership, the EU acquis is also relevant, in particular, Directive 2003/4/EC of the European Parliament and of the Council on public access to environmental information and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The NATO requirements as to classification are also important for Montenegro.

6. Article 3 of the draft law, dealing with protected interests, is reformulated so as to better correspond with Article 3 of the 2009 Convention. The threshold is "has or might have harmful consequences". The draft law does not attempt to further specify categories of information, unlike Article 15 of the draft law on free access to information. There is a risk of tension between the two draft laws where one specifies only protected interests and the other lays down in considerably more detail the specific protected categories. While some states provide for a general protection of "defence" and "security" interests, other states have showed that it is possible to break down defence and security interests into tighter, and so more useful, categories.[5] More specification (and thus narrowing down of secret information) is thus desirable, also because classification of information involves costs. According to the amended Article 11, the power to specify in more detail the categories within "top secret" "secret" and "confidential" is delegated to the government.

7. Article 4 is amended to extend the reasons for not classifying. This is an improvement. However, it is unclear how this fits in with the duties under Article 7 not to disclose classified information. While the requirements of Article 4 should "trump" the duty not to disclose, it would be preferable to state clearly that, where the conditions for Article 4 are fulfilled, it is permissible for people with a duty of confidentiality to break that duty. Montenegro may intend to put this in other legislation. Certainly, the Parliamentary Assembly has recommended improved protection for whistleblowers.[6]

8. Article 10 is amended to allow, exceptionally, an official to classify a category of documents, rather than a specific document "where the same type of classified information is being produced and repeatedly used in continuity". This is practicable, although it should be pointed out that this may increase routine (over)classification. It would be appropriate for the Agency (below paragraph 12) to devote special attention to the use of such powers.

9. Article 19 is amended. The fourth, "restricted", category of information still retained. In some states, the restricted category tends to be used for "working documents". It is questionable if this is still necessary, bearing in mind the fact that the draft Access to Information Law allows the non-disclosure of working documents. Normal disciplinary procedures for civil servants are probably sufficient to deter publication of working documents which are not classified as top secret, secret or confidential.

Another point in relation to Article 19 concerns the power of the authorized person to prolong the term of protection. I agree here with Mr. Kashumov's concerns that this seems disproportionate and problematic.

11. The amendments to Article 26 allowing the disclosure of classified information to prosecutors and judges are to be welcomed. Indeed, they are absolutely necessary. However, in a criminal trial, disclosure to the prosecutor raises the issue of equality of arms under Article

[4] ETS no. 108. The OECD has also adopted guidelines on protection of personal integrity regarding transborder data flows. To a large extent these are equivalent to the 1981 Data Protection Convention.
[5] See eg Estonia, State Secrets Act 26 January 1999 or Poland, Classified Information Protection Act, 22 January 1999.
[6] Parliamentary Assembly Recommendation 1916 (2010).

6 of the European Convention on Human Rights. I agree with Mr. Kashumov that the defence lawyer should also have access to relevant classified information collected as evidence in a court case. The defence lawyer can be subject to a duty of confidentiality. If this is not allowed, then as pointed out in earlier opinions by the Venice Commission,[7] and stressed by the ECtHR,[8] there are alternative mechanisms for reconciling the requirements of fair trial with security (eg security screened advocates) which must then be provided and which must work adequately in practice.[9]

12. Article 26 also provides for access to the Council of the personal data protection agency.[10] This calls for a short discussion of the need for oversight of classification procedures.

As I have noted in my comments on the draft law on free access to information, in a system providing for a principle of free access to information, classification is an administrative measure, indicating the level of internal access which should apply to the document in question, and the care (safeguards etc.) which should be taken with it. In other words, classification does not mean that the document *is* confidential, secret etc., and that the public should not have access to it, but simply that the classifying body considers this to be so. However, for the bureaucracy, keeping documents from the public gaze can make their lives much easier (at least in the short term). Thus, in many states, including states with a long tradition of free access to information, there is a practice of over-classification and access to classified documents may be routinely denied (especially where time limits are short).

As I understand it, there is a three-fold system of oversight (as well as the control which the courts exercise, if and when a person is prosecuted for disclosure of classified information) corresponding to the three different laws in the field. The first is the "internal" supervision provided by the Directorate under Article 73 *et seq*. of the Law on Classified Information. This is largely focused on effectiveness, but may have some restraining effect on over-classification bearing in mind the fact that classification involves expenditure and resources. This is, however, likely to prove insufficient.

The second mechanism of oversight is the Agency provided for under the draft Law on Free Access to Information. Where, as a result of complaints from the public about denial of access of information, or its general supervisory powers, the Agency sees a pattern of over-classification I consider that it should have the power to make recommendations to this effect, and recommendations on training and other measures necessary to encourage openness. As I note in my comments to this draft law, it is unclear whether it does have such a power.

The third mechanism of oversight is indirect and relates to a specific category of classified information, namely information involving personal data. The Council of the personal data protection agency receives complaints from subjects of data retention. The Council can then investigate and determine whether this data is being held in accordance with the requirements of the law on data protection. The Council has access even to classified data.

---

[7] Report On The Democratic Oversight Of The Security Services, CDL-AD(2007)016, para. 216.

[8] A. and others v. UK, No. 3455/05, 19 February 2009, at para. 205 "The Court has held nonetheless that, even in proceedings under Article 6 for the determination of guilt on criminal charges, there may be restrictions on the right to a fully adversarial procedure where strictly necessary in the light of a strong countervailing public interest, such as national security, the need to keep secret certain police methods of investigation or the protection of the fundamental rights of another person. There will not be a fair trial, however, unless any difficulties caused to the defendant by a limitation on his rights are sufficiently counterbalanced by the procedures followed by the judicial authorities".

[9] In A and others, ibid. the Court found violations of the Convention for this reason.

[10] http://azlp.me/

It is important that these two external oversight bodies develop sufficient competence to provide a genuine check on, in the Agency's case, wrongful denial of access (which indirectly provides protection against over-classification) and in the case of the Council of the personal data protection agency, the retention of personal data in police and security files.

There are a number of points which should be made here. Essentially, all that an independent oversight body can offer is a second subjective opinion on whether the laws (on, respectively, free access and data protection) are being complied with. But a second opinion is valuable. The oversight bodies are "one step removed" from the bureaucracy. The balancing of, respectively, privacy and freedom of information rights on the one hand and effectiveness in security and administration on the other is not the main concern of the bureaucracy. Hence, the privacy/freedom of information contra effectiveness balancing task mainly falls to the oversight bodies.

In order to do this job credibly, the oversight bodies must have knowledge of "good practice" in classification of data and in handling of personal data. This in turn requires considerable experience. Normally, top secret and secret data should be compartmentalised, that is, available only on a need to know basis, in order to minimize risk of abuse. However, the oversight bodies, if they are to be a credible safeguard against abuse, must have access on demand to all the secret and top secret filed in the system. This in turn involves an element of vulnerability: if, for example, the oversight bodies are penetrated by organized crime figures, then these figures can get access to whole data banks. The composition of the oversight bodies, and the selection of their members is thus extremely important. Moreover, the oversight bodies must themselves operate with a considerable degree of secrecy. To be perceived as legitimate safeguards by the public, some form of parliamentary involvement in the selection of the chair and the other members of the body is usually seen as necessary. The Montenegro laws appear to provide for adequate powers, safeguards of independence and parliamentary involvement in the selection process of both external oversight bodies. However, this is an area which should be kept under proper supervision and control, to ensure that oversight, and remedies, are effective both on paper and in practice.[11]

[11] See in particular the ECtHR judgment in Segerstedt-Wiberg v. Sweden, No. 62332/00, 6 June 2006.