Strasbourg, 7 March 2008

CDL(2008)030*

Opinion no. 458 / 2007

Engl.Only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

COMMENTS

ON THE LAW ON STATE SECRETS (1994)

OF THE REPUBLIC OF MOLDOVA

by

Mr Iain CAMERON (Substitute 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.*

Introductory observations

1. I have taken as basis for this assessment the English translation of the law, which may not accurately reflect the original version on all points. Some of the issues raised in this opinion may therefore find their cause in the quality of the translation rather than the substance of the provisions concerned.

2. Although the present opinion is limited to the 1994 law, it should be noted that the subject of state secrecy is difficult to keep separate from other relevant legislation. This includes first, the Criminal Code, which criminalizes both the revealing of secret information, and offences relating to misuse of secrecy.[1] Second, legislation setting out rights of access to official information[2], third, legislation dealing with the protection of personal data[3] and fourth legislation on security and intelligence agencies.[4]

3. 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.

4. 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.[5] 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

[1] See in particular Articles 344 and 345 of the Criminal Code of the Republic of Moldova, adopted by Law nr. 985-V on April 18, 2002

http://www.legislationline.org/upload/legislations/e3/eb/0e3bf0290e9b404cb57debe4ebc4.htm.

[2] See, in this respect, Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents, Adopted by the Committee of Ministers on 21 February 2002. Which lists the following exemptions that member states shouldapply: i. national security, defence and international relations; ii. public safety; iii. the prevention, investigation and prosecution of criminal activities; iv. privacy and other legitimate private interests; v. commercial and other economic interests, be they private or public; vi. the equality of parties concerning court proceedings; vii. nature; viii. inspection, control and supervision by public authorities; ix. the economic, monetary and exchange rate policies of the state; x. the confidentiality of deliberations within or between public authorities during the internal preparation of a matter.

[3] The law on Information Processing and State Information Resources (N 467-XV of 21.11.2003) was dealt with in a separate opinion issued on 20 February 2006 by an independent expert commissioned by the Directorate General of Legal Affairs of the Council of Europe (PCRED/DGI/EXP(2006)1)

[4] Law On the Information and Security Service of the Republic Of Moldova CDL(2006)001. See Opinion no. 367/2006 On the Law on the Information and Security Service of the Republic Of Moldova CDL-AD(2006)011

[5] As the Inter-American Court of Human Rights put it in Claude Reyes and others v. Chile "access to public information is an essential requisite for the exercise of democracy, greater transparency and responsible public administration and that, in a representative and participative democratic system, the citizenry exercises its constitutional rights through a broad freedom of expression and free access to information. ...In this regard, the State's actions should be governed by the principles of disclosure and transparency in public administration that enable all persons subject to its jurisdiction to exercise the democratic control of those actions, and so that they can question, investigate and consider whether public functions are being performed adequately," 19 September 2006, Series C no. 151, paras 84 and 86.

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.). During the Soviet era, there was a tendency among states in Eastern and Central Europe to regard almost all official information as secret.[6] In transitional states, and even well-established democratic states, as there can still be strong bureaucratic interests in preserving secrecy, it must be recognised that changing a culture of secrecy is a long-term process.[7]

5. 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.[8] It is for this reason that the European Court of Human Rights (EctHR) has allowed states a certain margin of appreciation in this sphere.[9]

6. Bearing these points in mind, the Law of State Secrets can now be studied. As well as the Act itself, I have also had access to an earlier OSCE analysis of it.[10] The Act has seven chapters, and these will be looked at in turn.

Chapter I - General provisions

7. Chapter I sets out the different institutional responsibilities in the field of secrecy. Here it can be noted that the statute provides that the parliament is inter alia to "regulate the legal basis of the relations in the field of state secret protection" (Article 3(1)). The specification of exactly what classes of information is to be kept secret is left to the government, or the responsible administrative bodies. The advantage of this is that it avoids having what may be a very lengthy and clumsy statute, which moreover may have to be continually amended (taking up parliamentary time which could be better used for discussing issues of principle). The disadvantage with delegating classification authority is first at the level of legal security: the precise classes of information covered by secrecy may not be easily accessible in practice. Second, this method risks not simply the details of the contents being delegated to - largely - unaccountable bureaucrats, but the formulation of secrecy policy itself.

8. It is certainly not impossible for the parliament to set out in advance and in reasonable detail all the categories of information which should be kept secret. This is the case in e.g. Sweden, (Secrecy Act, 1980). The provisions have to be set out with a sufficient degree of specificity that they can be applied directly by concerned officials, even non-lawyers. By contrast, opting for a delegation-model provides for greater flexibility, but makes it necessary to have strong and objective oversight of how the different administrative authorities apply their powers in practice.

---

[6] And not simply these states. The UK had the same approach in its Official Secrets Act 1911, which was in force until 1989.

[7] See, e.g. D. Vincent, The culture of secrecy: Britain, 1832-1998, Oxford, Oxford University Press, 1998.

[8] See the brief comparative study by C. Pourgourides, Fair trial issues in criminal cases concerning espionage or divulging state secrets PA Doc. 11031, 25 December 2006.

[9] Stoll v. Switzerland, 12 December 2007, para. 107.

[10] D. Banisar, Comments on the Moldovan Draft Law on State and Official Secrets 26 September 2005 http://www.osce.org/documents/rfm/2005/09/16421_en.pdf.

Chapter II - Information covered by state secrecy

9. Chapter II consists of a single article, Article 5, which sets out four broad categories of information that can be classified as state secrets: military; economy, science and technology; foreign policy; and state (intelligence) security. Under each category, there are a number of sub-categories, most of which in turn apply to multiple areas. In total, there are over one hundred different categories of information.[11] Having said this, the wording of most of the categories at first sight do not seem to give too much cause for concern. Some of the categories in Article 5(2), in particular scientific research and economic information seem relatively wide, but this may be the translation. If they are limited to military-scientific information and military-economic (armaments industry, civil defence) then even Article 5(2) does not diverge significantly from the practice of other Council of Europe.

10. Nonetheless, there are indications that this first impression regarding Article 5 may be incorrect. Everything depends on how wide an interpretation the implementing administrative bodies give to the categories of information set out in Article 5. Here it should be noted that Article 12, dealing with information which should not be classified refers to inter alia (b) emergencies, catastrophes that threaten the security and health of people and their consequences, as well as the natural disasters, their forecasts and consequences; (c) real situation in the sphere of education, health protection, ecology, agriculture, trade, as well as the legal order". On an objective interpretation, the "real situation" regarding e.g. education should not be capable of falling under the wording of *any* of the categories of information in Article 5, which is supposed to be *the* precondition for classification. Several parts of Article 12 would not be necessary at all if Article 5 was being followed strictly. This gives rise to concern that classifying authorities in practice are not following the relatively narrow categories set out in Article 5. If this is the case, then the problem cannot simply be dealt with by tightening the categories in Article 5. Steps must be taken to change the structural causes of such a culture of secrecy.[12]

11. Another point which can be noted here is the divergence between Article 5(3) foreign policy and economy, and the other subsections. Foreign policy and foreign-related economic information is only covered by secrecy where this "can put under [at] risk the interests of the country". No such requirement is made in the other subsections. The question is whether this is an additional requirement to be satisfied before such information can be classified, raising the classification threshold or whether it in fact lowers the classification threshold. And is it simply assumed that the dissemination of any information falling within the other subcategories will "put under risk the interests of the country"? The classification threshold, and the relationship between classification and the criminal offence of revealing secret information, are dealt with further below.

12. Although security is one of the categories, there is no mention of police/law enforcement information, some of which must obviously be kept secret (e.g. ongoing investigations, surveillance technology or capabilities or intelligence on suspected organized crime). This is presumably covered by other legislation. The same can be said for information relating to e.g. internal fiscal policy, taxation, on regulatory inspections. Some of this information must be protected by criminal penalties because of the risk that it otherwise be used or leaked by unscrupulous civil servants for personal gain, e.g. regarding an impending decision to raise interest rates, or an impending investigation of a company under safety at work legislation.

[11] Ibid.

[12] See in particular comments to Articles 8, 14, 26 and 29.

13. A modern state engaged in the provision of, or regulation of, a wide range of public services obviously comes into possession of a great deal of personal data on citizens and residents apart from tax returns. The media can be interested in prominent citizens' personal information, and exert influence on civil servants possessing this information. Revealing of, e.g. information on individuals' health can only very indirectly be seen as damaging the interests of the state, but here are nonetheless very strong reasons for protecting the secrecy of this information. Some European states, including, presumably, Moldova, choose to regulate the confidentiality of such official information in another statute or statutes. Some European states, such as Sweden, put all the categories of official information which are to be kept secret, in the interests of both the state and individuals, in the same statute, but provide for different criteria for classification. There is much to be said for the second method, however either method is acceptable, as long as all important information is properly covered, and the legislation itself is clear and accessible ("in accordance with the law" within the meaning of the case law of the European Court of Human Rights), there are differential criteria for classification and that revealing less or more secret information is subject to differently formulated crimes and disciplinary measures.

Chapter III - Classification of information

14. Article 6 sets out the principles for classifying information. In any system, generally speaking, the main functions of classification are to enable the leadership of administrative agencies easily to limit the group of civil servants who should have access to the information in question, and to give warning to these officials coming in contact with the information in question as to the level of care they should take in handling the information.[13] In the Moldovan law, information is to be classified in accordance with the principles of legality, reasoning [reasonableness] and suitability. As regards reasonableness in particular, the "harm" criterion for classification is preventing the "gross infringement of the security of the Republic of Moldova." This article seems to be intended as an additional requirement to be satisfied. As such, as already mentioned, the relationship between this requirement and the requirement set out in Article 5(3) for foreign and foreign economic policy is not clear. More generally, one can say that setting such a classification threshold is obviously sensible and that "gross infringement" is not lower a threshold than that set in other Council of Europe states. However, again, everything depends upon how "gross infringement" is interpreted in practice.

15. The "gross infringement" threshold should be read in conjunction with Article 7. Article 7(1) provides that the "level of classification of information that constitutes state secret should correspond to the level of damages that can be caused to the security of the Republic of Moldova in cases of dissemination of such information." Article 7(2) provides for three levels of secrecy classification: special compartment [special importance], top secret and secret. It would nonetheless appear that the unlawful dissemination of information from *any* of these three categories is regarded as causing a "gross infringement" of Moldovan security. Although there are three categories of secret, there is no guidance in the statute as to what level of harm is necessary for each to apply. Bearing this in mind, would be advisable to have three different criteria of harm, e.g. "damaging to Moldovan national security", "highly damaging to Moldovan national security" and "extremely damaging to particularly vital Moldovan national security interests".

16. Article 8 is a key provision in the statute, as it provides that authority to classify is delegated by the heads of the relevant state administration bodies to persons working in these bodies (hereinafter a "designated official"). The designated official must take a motivated decision in

[13] See also below, comments on Article 26.

each case (Article 8(2)). An inter-departmental Commission is established.[14] This also drafts a list which is approved by the President of Moldova and published "if necessary" (Article 8(3)). However, a document can be also be classified by virtue of being placed on the departmental list. This is a secret list (Article 8(4)). This secret list is thus not simply an elaboration in greater detail of the inter-departmental Commission list, itself a specification of the categories set out in Article 5, but an alternative method for classification – something which is confirmed by Article 9. There are obvious dangers here as regards legal security (accessibility of the law). Moreover, it provides a potent weapon to the heads of relevant state administration bodies to shield the body from criticism. In practice, notwithstanding the wording of Article 5, it opens the way for classifying information which is embarrassing for some reason. It even appears to make it possible to classify, quietly, after the information has come into being, e.g. when its embarrassment potential becomes apparent.

17. It is difficult from the statute alone, to determine whether these possible problems exist in practice. If they do, then these provisions should be changed. It is understandable that the initial competence to classify should lie with the designated official in the administrative body involved in the production of the information concerned. In that sense, it is logical to let each administrative body classify its own documents. However, these classifications should be further specifications of (and so, in full accordance with) the published inter-departmental list, not alternative methods of classification. Moreover, departmental classifications must be capable of being annulled by higher authority acting either proprio motu or on appeal by an interested citizen. This higher authority must genuinely take into account countervailing interests and not simply security concerns.[15]

18. Article 10 provides that information in the hands of private bodies or individuals can also be classified as state secrets. With privatization of even central state functions, such a provision is not unusual in Council of Europe states. For example, a telecommunications company may receive requests from a security agency, authorized by a judge or other body, to provide phone records. Another area of application of such a provision is in relation to defence/security contracting. A corporation may develop a weapon, or technology, the technical details of which should be kept secret. In most cases, the device or technology concerned will have been developed pursuant to an express contract with the state. Even without such a contract, such a provision does not seem to be objectionable, provided that the application of it is exceptional, the official's decision to classify can be appealed to the courts (as is the case, Article 10(3)) and compensation is payable (as is also the case, Article 10(2)).[16] But outside of the area of defence or security contracting (including the provision of services which can have a security-related nature, such as telecommunications) it is difficult to see any legitimate application for this provision. The provision as it is at present formulated seems to provide significant scope for abuse, e.g. against journalists or researchers who are gathering and systematizing non-secret information which the government of the day or an administrative agency deems to be critical of it.[17] The provision seems thus to be much too widely formulated and it should be rewritten.

[14] It is unclear whether this body is the same as the inter-governmental Commission referred to in Article 14(2). See further, comments on Article 29.

[15] See also the comments as regards Articles 14 and 29 below.

[16] Although having said this, from the wording it is not apparent if the appeal can concern the size of the compensation awarded (which should also be possible), or only the decision to classify.

[17] See in this respect PA Recommendation 1792 (2007), Fair trial issues in criminal cases concerning espionage or divulging state secrets.

19. Article 11 deals with the length of time of classification, namely twenty-five years for "special compartment" and top secret information and ten years for secret information. These are relatively long periods, but not exceptional in international comparison (although see the final comment made to Article 14, below). The government can, by means of notification to the inter-departmental commission decide on a longer period of classification for "special compartment" information. However, it must be stressed that, where there is no proper supervision of officials' classification of documents, there is an inbuilt bureaucratic tendency to over-classify documents.[18] This holds true even though the act sensibly provides for a duty on designated officials to review periodically the content of the departmental list (at least every five years – Article 11(3)).

20. Article 12 as already mentioned, provides for a prohibition on the classification of certain information, namely,

> "(a) the violations of human and citizens rights and freedoms;
>
> (b) emergencies, catastrophes that threaten the security and health of people and their consequences, as well as the natural disasters, their forecasts and consequences;
>
> (c) real situation in the sphere of education, health protection, ecology, agriculture, trade, as well as the legal order; (d) cases of infringement of legality, inactivity and illegal actions of the state authorities and officials, if disclosure of this information will not endanger the security of the Republic of Moldova."

21. In addition, under Article 12(2) "Classification is not allowed if it negatively affects the implementation of the governmental and sartorial programmes for social - economic and cultural development, or if it restricts competition of economic agencies." This presumably entails inter alia that where classification of information would have the effect of distorting competition between private companies this is not permissible.

22. To begin with, as previously noted, this provision indicates that the categories in Article 5 are not interpreted strictly. Secondly, subsection (d) allows for information on wrongdoing by officials to be classified where disclosure would damage security. However, as no such qualification is made in subsections (a)-(c) it would seem reasonable to assume that wrongdoing affecting citizens' rights etc. may not be classified, even if revealing it would damage security. However, this interpretation may not be correct in practice.

23. Although the Act does not explicitly provide a justification or excuse for the revealing of secret information, Article 12 provides some support for this. The issues of "whistleblowing", the right of the press to publish even secret information (when this is in the public interest) and the protection of journalists sources, has been the subject of considerable discussion in the Parliamentary Assembly, recommendations by the Council of Ministers and cases before the ECtHR.[19] I consider that there can be extreme situations for example, when this indicates major wrongdoing by a security agency, in which officials should be able to disclose to the media

[18] Cf. Banisar, p. 8.

[19] Observer and Guardian v. the United Kingdom, judgment of 26 November 1991, Series A no. 216, Hadjianastassiou v. Greece, 16 December 1992, A/252, Verenigning Weekblad Bluf v. Netherlands, 9 February 1995, A/306-A, Fressoz and Roire v. France. 21 January 1999, Editions Plon, v. France, No. 58148/00, ECHR 2004-IV Tourancheau and July v. France, No. 53886/00, 24 November 2005, Dammann v. Switzerland, No. 77551/01, 25 April 2006, Leempoel & S.A. ED. Ciné Revue v. Belgium, No. 64772/01, November 2006, Dupuis and others v. France No 1914/02, 7 June 200, Voskuil v. Netherlands**,** No. 64752/01, 22 November 2007, Tillack v. Belgium**,** No 20477/05, 27 November 2007, Stoll v. Switzerland, op. cit.

even very secret information without fear of criminal or disciplinary punishment. In such cases there should be not either be a threat of prosecution of the media. Article 7(5) of the Moldovan Law on Access to Information it is a defence for anyone in a criminal trial for unauthorized release of information that this was in the public interest. I agree with the OSCE expert opinion that this defence should be incorporated in an amended Law on State Secrets to make completely clear that even national security information can be released when it is in the public interest to do this.[20]

Chapter IV - Declassification of information

24. Article 13 provides for declassification of information inter alia by reason of changed circumstances. It is not clear whether information is automatically declassified after the expiry of the time limits in Article 11. Instead, Article 13(3) seems to provide that declassification occurs in the National Archives if the administrative body providing for secrecy has delegated such a power of declassification to the national Archives. Automatic declassification should be stated clearly in the statute. Article 14 allows citizens, enterprises etc. to address requests for review of classified documents to the classifying body, or the interdepartmental Commission. Within three months, the body in question is obliged to examine the request and give a motivated answer. If the request is not within the competence of the body which has received it, it is to be forwarded within one month to the body which is so entitled to hear the review or the interdepartmental Commission (Article 14(2)). Officials who fail to perform their tasks in this respect are subject to disciplinary penalties (Article 14(3)). These penalties are not specified but are presumably set out in other applicable legislation. It can also be noted that the Criminal Code provides for criminal responsibility for officials who are grossly negligent or who misuse their office. An appeal lies to the courts for wrongful classification.

25. As regards the value of a review by the interdepartmental Commission, see the comments to Article 29. It may seem valuable that an appeal lies to the courts, but six points should be made here. The first is that it is not clear whether an appeal is an ultimate remedy, and that an unsuccessful request for review must precede the resort to this remedy. It would seem sensible to make it clear that this is an ultimate remedy. Secondly, the value of an appeal obviously depends upon an individual or enterprise knowing that a given document or other information exists, that it is in the hands of a given administrative agency and that it is classified. Admittedly, the statute permits an individual or enterprise to address a request for review to the interdepartmental Commission, which would presumably occur where it is unclear which agency (if any) has the information in question. Still, where there is no official duty to register/log *all* documents, or where this duty is not taken seriously, or where the official register is not available on demand to the public, then a right of appeal is more apparent than real. This may be a matter dealt with in other legislation, but if it is not, then the right of appeal does not exist in practice. Thirdly, Article 14 makes no mention of standing requirements, i.e. the need for an individual or an enterprise to show an interest in the information in question. The administrative advantages in limiting rights of appeal (cost, overuse of court time) should be weighed against the damage such a requirement will pose to the system of constitutional control. Obviously a standing requirement, if set too high, has the potential to undermine totally the value of an appeal, so if such a requirement is introduced it should be set very low, and exceptions should be considered for the mass media. Fourthly, the value of an appeal depends upon the capacity and competence of the courts to make a genuinely objective assessment of the need for classification in the particular case. Lest this is seen as being unduly critical of the Moldovan courts, it should be stressed that this problem can exist in any state, where for any reason adequate judicial competence or capacity is lacking in practice. It may be especially

[20] Banisar, p. 6 who also notes that Council of Europe Civil Law Convention on Corruption, ETS no. 174 binding on Moldova, provides that employees who disclose information about corruption should not be subject to sanctions

pertinent to Moldova, bearing in mind the lack of guidance in statute as to what is a gross infringement of Moldovan security. In any event, where the courts do not in practice have a genuinely independent and critical approach to the issue, then a formal right of appeal is arguably worse than not having an appeal at all, as it gives the appearance of fairness without there being any fairness in practice.

26. Fifthly, the relationship is unclear between this article and whatever rights of access exist under Moldovan law to secret files containing personal information. As the ECtHR stressed in Rotaru v. Romania[21] and Segerstedt-Wiberg v. Sweden[22] it must always be possible for an individual to challenge before a competent and objective body (judicial or quasi-judicial) the holding, by agents of the State, of information on his or her private life or the truth of such information, and, moreover, to obtain damages and correction/deletion of the file where it contains incorrect information or the holding of the information is adjudged unnecessary or disproportionate.

27. Sixthly and finally, the Moldovan parliament should give serious consideration, to the question of access to personal files from the Soviet era. Admittedly, there are important interests to be balanced here. On the one hand, there are the legitimate interests of the victims of police state oppression, and the interests of historians. On the other, there is still information which should be kept secret in these files, for e.g. foreign policy reasons, and there is also the risk that peoples' careers and personal lives can be damaged or destroyed by leaking or revealing unconfirmed or speculative information from the files, e.g. that a person might have been a police informer. Different solutions have been reached in different Council of Europe states. [23] However, some means of reconciling these different interests must be achieved.

Chapter V - Transfer of secret information

28. Article 15 provides for transferral of secret information between state bodies and to enterprises or individuals. Obviously transfer between state bodies must be possible. To the extent that this involves merging of data bases containing personal information, this raises issues of data protection but these issues are presumably dealt with in other legislation. Article 15, at least in translation, is a particularly long and clumsily drafted provision. Generally speaking with transferral it is necessary to provide that the original level of classification applies for the agency to which it is transferred and that this agency undertakes to protect the information with the same level of care. As regards transferral of secret information to private bodies, the circumstances in which this can occur are more, or much more circumscribed. It also gives rise to a number of difficult problems, inter alia data protection of personal information, patent protection and issues of commercial advantage/distortion of fair competition (see also Article 12(2)). It is not possible, from the translation, to understand the meaning of, let alone the implications of, this article. Whatever redraft may be made of this article, it is necessary to take full account of these concerns.

29. Article 16 deals with transmission of information to other states. International organisations are not mentioned in Article 16, but are so mentioned in Articles 24 and 25. This discrepancy should be corrected. Articles 24 and 25 deal with transfer of information to Moldova, and thus the three articles should be grouped together, most suitably in chapter V.

---

[21] judgment of 4 May 2000.

[22] ECtHR, *Segerstedt-Wiberg v. Sweden* judgment of 6 June 2006.

[23] See, e.g. the Polish Consitutional Court decision of May 2007, commented by M. Safjan, Transitional Justice: The Polish Example, the Case of Lustration

1 EJLS (2007).

30. Treaties on transfer are to be signed by the government and concluded by the parliament (Article 4(3)(d) and (h)) Article 24 states however that such treaties are concluded in accordance with the procedure adopted by the government. Obviously, the normal rule is that parliament should conclude all these treaties. Where, for some special security reason, the government considers that the details of a treaty should not be given to parliament as a whole, some other means must be used of guaranteeing adequate parliamentary insight. Transferral of secret information is on occasion necessary in security matters, not least in combating international terrorism. However, it is not explicitly stated that no information may be transferred without such a pre-existing treaty, and this should be made clear.

31. Information may only be transferred in an individual case after an expert's opinion from the inter-departmental Commission. This seems sensible, however, no standards are set out for this expert to follow. There can be considerable dangers involved for individual rights when personal data information is transferred to international bodies and states. Accordingly, I wisch to stress that the standards and guidelines set out in its earlier opinion democratic oversight of internal security services[24] should be written into the legislation, and applied by the expert when making his/her decision. Such decisions should be capable of being monitored by applicable parliamentary and other oversight bodies. The same requirement of an adequate degree of insight applies mutatis mutandis to information transferred to Moldova. Article 24 states merely that limits set by the transferring power are to be respected.

Chapter VI - Protection of state secrets

32. Article 17, setting out the institutions involved in protection of state secrets would seem better placed in chapter I. Articles 18-22 deal with requirements and modalities of access by officials and citizens. These articles largely concern the issue of security screening of personnel. It is obviously necessary to have rules regarding security screening. What is important here is that officials applying for posts subject to security clearance are always made aware that screening will occur and that there is a real right of appeal before a competent and objective judicial decision against a decision to refuse, modify, or annul a security clearance. The risk of remedies only existing on paper in this area is clear.[25] It is also necessary for officials to accept certain restrictions on their right of privacy, as a result of the need to make investigations (and periodic reinvestigations) into their security backgrounds. Finally, the technical details dealing with physical protection of secret information must largely be left to government ordinances and administrative rules, and so the statute must provide for appropriate delegation powers. The points made above on Article 14 as regards court appeal apply mutatis mutandis here. Otherwise the provisions appear to be satisfactory.[26]

33. Finally, Article 26 refers to responsibility for violation of the legislation "in accordance with the legislation". The "legislation" is presumably the Criminal Code, but administrative (disciplinary) legislation may also be meant. This will presumably only be applicable to officials, not individuals who have been granted access to secret information for some reason, and to whom only the criminal law applies (and so criminal penalties for violation of a condition of access). It is particularly important here to separate the issue of criminal responsibility from the issue of administrative classification. As pointed out in the general comments section, information can obviously be wrongly classified, either in ignorance, or as a result of illicit

[24] Study no. 388 / 2006, CDL-AD(2007)016.

[25] See for example, I. Cameron, National Security and the ECHR, Kluwer 2000, pp. 225-252 regarding the ECtHR, *Leander v. Sweden* judgment of 26 March 1987.

[26] Article 23 seems to be related to Article 16 and it is again not possible, from the translation of Article 23, to understand the meaning of this article.

motives or as part of structural tendency of over-classification. More minor administrative (disciplinary) penalties (e.g. reprimand, modification of security clearance) may well be justified for negligent handling of, or the wrongful revealing of, classified information without taking account of the content of the information in question, to see if it really should have been classified. This is much more doubtful as regards more serious disciplinary measures such as demotion or refusal of promotion and dismissal. It is not acceptable at all as regards criminal penalties.[27] Here it is absolutely necessary that the criminal court which tries a person for a criminal offence has the capacity, competence and objectivity to make a genuinely objective determination of whether objectively speaking, a "state secret" has been unauthorizedly revealed. However, Article 344 of the Moldovan Criminal Code does not appear to set a harm requirement. Instead, the offence appears to be constituted simply by the revealing of a "state secret". This reading of the relevant provisions may not be correct. If it is however, I must emphasize that it is definitely not permissible that the court simply accepts the classification as proof, or even prima facie proof, that the information in question is objectively a state secret, and so finds that the unauthorized revealing of it constitutes an offence under Article 344.

Chapters VII and VIII - Financial support, control and supervision of state secrets

34. Article 27 provides that concerned administrative agencies must finance security measures from their respective budgets. The Ministry of Finance has the power of audit of the costs of security measures and so it, and the heads of the administrative bodies in question, must have access to the financial information necessary to perform this task. Article 28 provides that "the parliamentary control over observance of the legislation regarding state secret and related expenditures is performed by permanent parliamentary commissions. State administration bodies, protecting state secret are obliged to provide all necessary information to the mentioned commissions." This is a sensible provision, in line with the recommendations of the Venice Commission on oversight of internal security agencies but again, its value depends upon how it is interpreted in practice. I suggest that when changes are made in these provisions full account is taken of the problems identified, and standards set out, for parliamentary and budgetary control of the security sector in its study on democratic oversight of internal security services.

35. Article 29 provides for interdepartmental control, which is the responsibility of the Ministry for National Security. The "ownership" of the issue is thus situated in the Ministry which can reasonably be regarded as having a vested interest in keeping as much information secret as possible. Even though the membership of the inter-departmental Commission is confirmed by the President, it is advisable to ensure that the Commission is a not composed purely, or even mainly, of people from the Ministry of National Security. It would seem advisable to create a body with a degree of genuine institutional independence from the administration in general, and the Ministry of National Security in particular, Different methods can be used for establishing a body which has both a degree of independence from the administration, but not to the point where the administration is antagonistic to the body, withdrawing cooperation in practice. Second it is necessary that the experts on the Commission do not simply have a security mandate. As indicated in the general comments, other important considerations are administrative efficiency and good governance. Good governance requires keeping the level of state secrecy to the minimum necessary to maintain national security. Third, it is necessary that

[27] In line with the case law of the ECtHR, disciplinary penalties may be so serious as to qualify as "criminal charges" within the meaning of Article 6.

the body has the powers and resources it needs to provide effective supervision over the security information sector. All these goals can be achieved. There are many best practices to draw upon. Other states have created independent oversight bodies or information commissioners with a mandate to scrutinize all official information, and specially-security screened procedures for monitoring secret information.[28]

Concluding remarks

36. The law has a number of satisfactory provisions, but falls short in an important number of respects from what can be regarded as good practices in the field of state secrecy.

[28] See e.g. the French Commission consultative du secret de la défense nationale (CCSDN) consolidated report for 1998-2004 at http://lesrapports.ladocumentationfrancaise.fr/BRP/054000109/0000.pdf and the Hungarian Data Protection and Freedom of Information commissioner,

http://abiweb.obh.hu/dpc/index.php?menu=reports/2004/III/4&dok=reports/2004/229 See also the mechanisms for independent review of security information in Study no. 388 / 2006, CDL-AD(2007)016 op. cit.