Strasbourg, 20 March 2008

Opinion no. 458 / 2007

CDL-AD(2008)008
Or.Eng.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

OPINION

ON THE LAW ON STATE SECRET

OF THE REPUBLIC OF MOLDOVA

Adopted by the Venice Commission
at its last 74th Plenary Session,
(Venice, 14-15 March 2008)

on the basis of comments by

Mr IAIN CAMERON (substitute Member, Sweden)
Mr Olivier DUTHEILLET DE LAMOTHE (substitute Member, France)

I. Introduction

1. By a letter dated 5 November 2007, Mr Esanu, Deputy Minister of Justice of Moldova, requested the Venice Commission's assessment of the 1994 Law on State Secret of the Republic of Moldova (CDL(2008)008).

2. Messrs Iain Cameron and Olivier Dutheillet de Lamothe were appointed as rapporteurs. The present opinion, which is based on their comments (CDL(2008) 30 and 31 respectively), was adopted by the Venice Commission at its 74th Plenary Session (Venice, 14-15 March 2008).

II. General observations

3. The Commission has taken as its basis 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.

4. 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: the Criminal Code, which criminalizes both the revealing of secret information, and offences relating to misuse of secrecy[1]; legislation setting out rights of access to official information[2]; legislation dealing with the protection of personal data[3] and legislation on security and intelligence agencies.[4]

5. 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.

6. 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

[1] See in particular Articles 344 and 345 of the Criminal Code of the Republic of Moldova, adopted by Law nr. 985-XV 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. It lists the following exemptions that member states should apply: 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 Venice Commission's Opinion no. 367/2006 On the Law on the Information and Security Service of the Republic Of Moldova, CDL-AD(2006)011.

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 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]

7. 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]

III. Chapter I - General provisions

8. Chapter I sets out the different institutional responsibilities in the field of secrecy.

9. Article 4 provides that the parliament is *inter alia* to "regulate the legal basis of the relations in the field of state secret protection" (Article 4(1)). The specification of exactly what classes of information are to be kept secret is left to the government, or the responsible administrative bodies.

10. The advantage of delegating classification authority 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 is first at the level of legal security: the precise classes of information covered by secrecy may not be easily accessible in practice. There is also a risk that not simply the details of the contents but the formulation of secrecy policy itself be delegated to - largely - unaccountable bureaucrats.

---

[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.

[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, PACE Doc. 11031, 25 December 2006.

[9] ECtHR, *Stoll v. Switzerland* judgment of 12 December 2007, para. 107.

11. 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.

IV. Chapter II – The definition of state secrecy

12. Article 5 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.[10]

13. This *material* definition of state secret supplements the *formal* definition of state secret contained in Article 2 of the Law, providing that the notion of state secret covers "the information protected by the state in the field of its military, economic, technical, scientific, external policy activity, counterintelligence and operative investigation, the dissemination, disclosure, loss, defalcation or destruction of which may infringe the security of the Republic of Moldova."

14. Many States (the United States, the United Kingdom, the Netherlands, France for example) and international treaties (NATO, UEO, EU) have opted for a merely formal definition of state secret[11]. Other states, e.g. Sweden (Secrecy Act, 1980), have attempted to list material definitions[12]. If such an approach is taken, 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. Even with the Swedish Secrecy Act, however, some categories are of necessity broadly formulated (including those dealing with the secrecy of particularly sensitive foreign relations and military secrecy). The risk with this approach is that the objective difficulty to cover all the information which needs to be protected may lead to protecting too much information by providing too broad a definition.

15. This risk appears to be realised with the Moldovan legislation. The wording of some of the categories in Article 5(2), in particular scientific research and economic information, seem relatively wide (although this may depend on inaccurate translation); only if they are limited to military-scientific and military-economic (armaments industry, civil defence) information, would they not diverge significantly from the practice of other Council of Europe states.

16. More importantly, the categories of information set out in Article 5 are open to a very wide interpretation by the implementing administrative bodies. This seems to have been somewhat anticipated in the law. Indeed, if Article 5 were to be interpreted strictly, Article 12, which deals

---

[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.

[11] In France, for example, a Law decree of 29 July 1939 provided a material definition of state secret, setting out four categories of first class secret information (military, diplomatic, economic or industrial) which by their nature could only be known by qualified persons and ought not to be disclosed to anyone else. This definition proved unsatisfactory. Indeed, these four categories did not cover all information which needed to be protected. This law decree was abrogated by an ordinance of 4 June 1960. The 1994 criminal code now provides a purely formal definition: "Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion. Peuvent faire l'objet de telles mesures, les renseignements, procédés, objets, documents, données informatisées ou fichiers, dont la divulgation est de nature à nuire à la Défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale."

[12] Although these deal with the issue of classification, and do not prejudge the issue of whether revealing such classified information constitutes a crime, see below para. 56.

with information which should not be classified and 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", would be largely superfluous. On an objective interpretation, in fact, 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.

17. 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.[13]

18. Article 5(3) relating to foreign policy and economy diverges from 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.

19. 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.

20. 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.

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

V. Chapter III - Classification of information

21. 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.[14] 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.

22. 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, it 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". This kind of three-level definition is used, for example, by UEO and by NATO.

23. 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 each case (Article 8(2)). An inter-departmental Commission is established.[15] This also drafts a list which is approved by the President of Moldova and published "if necessary" (Article 8(3)). However, a document can 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.

24. This raises 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

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

[15] 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.

embarrassment potential becomes apparent. In addition, civil servants may have a pecuniary interest in increasing the amount of classified information.[16]

25. 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.

26. Further, the Ministry for National Security, in order to exercise in a meaningful, effective and consistent manner its supervisory responsibilities, needs to be given the full picture; all the classified information, therefore, need to be duly registered and listed by the inter-departmental Commission. This is also crucial to the effectiveness of individual applications under Article 14 of the law.[17]

27. 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.[18]

28. 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)).[19]

29. 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 instead 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.[20] The provision seems thus to be much too widely formulated and it should be rewritten.

---

[16] See the comments as regards Article 18 (4) and (5).

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

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

[19] 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.

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

30. 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.[21] 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)).

31. 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." In addition, pursuant to 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 classification of information is impermissible when it would have the effect of distorting competition between private companies.

32. As previously noted, Article 12 indicates that the categories in Article 5 are not interpreted strictly. Secondly, subsection (d) of this provision is ambiguous. It 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.

33. Although the law under consideration does not explicitly provide a justification or excuse for the revealing of secret information, Article 12 provides some support for this. The issues of "whistle blowing", 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.[22]

34. The Venice Commission considers that there can be extreme situations, for example in cases of major wrongdoing by a security agency, in which officials should be able to disclose to the media even very secret information without fear of criminal or disciplinary punishment. In such cases, there should not be a threat of prosecution of the media either.

---

[21] See Banisar, p. 8.

[22] ECtHR, *Observer and Guardian v. the United Kingdom* judgment of 26 November 1991, Series A no. 216; *Hadjianastassiou v. Greece* judgment of 16 December 1992, Series A no. 252*; Verenigning Weekblad Bluf v. Netherlands* judgment of 9 February 1995, Series A no. 306-A; *Fressoz and Roire v. France* judgment of 21 January 1999; *Editions Plon, v. France* judgment of 18 May 2004, ECHR 2004-IV; *Tourancheau and July v. France* judgment of 24 November 2005; *Dammann v. Switzerland* judgment of 25 April 2006; *Leempoel & S.A. ED. Ciné Revue v. Belgium* judgment of 9 November 2006; *Dupuis and others v. France* judgment of 7 June 2007; *Voskuil v. Netherlands* judgment of 22 November 2007; *Tillack v. Belgium* judgment of 27 November 2007; *Stoll v. Switzerland*, op. cit.

35. Article 7(5) of the Moldovan Law on Access to Information provides as a defence for anyone in a criminal trial for unauthorized release of information that this was "in the public interest". The Venice Commission agrees 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.[23]

VI. Chapter IV - Declassification of information

36. 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.

37. As regards the value of a review by the inter-departmental Commission, see the comments to Article 29. As regards the possibility of appealing to courts, this appears valuable, although several considerations are necessary in this respect. In the first place, it should be made clear that an appeal is an ultimate remedy, and must be preceded by an unsuccessful request for review by the inter-departmental Commission.

38. 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 inter-departmental Commission, which would presumably occur where it is unclear which agency (if any) has the information in question. However, as noted above (para. 26) the decentralized system of classification means that even the Inter-departmental Commission may not know all the documents which exist and have been classified. 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.

39. 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.

[23] See 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.

40. 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 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.

41. 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[24] and Segerstedt-Wiberg v. Sweden[25], 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.

42. 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 hand, 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.[26] However, some means of reconciling these different interests must be achieved.

VII. Chapter V – Disposing of information that represents state secret

43. 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, the transferral 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.

44. 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 corruption, 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.

---

[24] ECtHR, *Rotaru v. Romania* judgment of 4 May 2000.

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

[26] See, e.g., the Polish Constitutional Court decision of May 2007, commented by M. Safjan, Transitional Justice: The Polish Example, the Case of Lustration, 1 EJLS (2007).

45. 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.

46. 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. In principle, 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.

47. 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. Transferring personal data information to international bodies and states may entail considerable dangers for individual rights: the Venice Commission therefore stresses that the standards and guidelines set out in its earlier opinion on democratic oversight of internal security services[27] 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.

48. Article 24 states merely that limits set by the transferring power are to be respected.

VIII. Chapter VI - Protection of state secrets

49. Article 17 sets out the institutions involved in protection of state secrets; it would seem better placed in chapter I.

50. 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. It is important to underline in this context that officials applying for posts subject to security clearance should always be made aware that screening will occur and that there must be 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.[28]

51. The law establishes the principle that officials who have permanent access to secret information and acquire working experience in this connection are entitled to wage raises. This principle seems problematic, in a situation like the Moldovan one where classification is largely decentralised and left to the discretion of certain officials.

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

[28] 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.

52. Certain restrictions imposed on officials who have or have had access to state secret, such as on the right to temporarily leave the country or on the right to privacy as a result of the need to make investigations (and periodic reinvestigations) into their security backgrounds, may be justified but must not be excessive. An effective court appeal must be provided (see mutatis mutandis the comments relating to Article 14).

53. 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.

54. Article 23 seems to be related to Article 16 and but the meaning of this provision, at least in translation, is unclear.

55. 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 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.[29]

56. It is absolutely necessary that the criminal court which tries a person for a criminal offence must have the capacity, competence and objectivity to make a genuinely objective determination of whether a real "state secret" has been revealed without authorisation. 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 document classified as a "state secret". This reading of the relevant provisions may not be correct. If it is however, the Venice Commission 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.

IX. Chapters VII and VIII - Financial support to state secret protection measures

57. 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.

58. 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

[29] 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.

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. However, its value depends upon how it is interpreted in practice. The Venice Commission suggests 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.

59. Article 29 provides for inter-departmental 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.

60. 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 a degree of independence from the administration, but not to the point where the administration is antagonistic to the body, withdrawing cooperation in practice. 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. It is further necessary that the body has the powers and resources it needs to provide effective supervision over the security information sector.

61. 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.[30]

X. Concluding remarks

62. Protection of secrecy is a vital concern of every state. It is a complex and sensitive matter, and legislation in this field must be carefully drafted. The Venice Commission has earlier identified a number of good practices in this field, and considers that Council of Europe member States should draw inspiration from them in order to improve their legislation in this field so as to allow for a satisfactory balance between the security interests of the state and the fundamental rights and freedoms which any democratic state has to ensure to everyone, as well as to avoid abuse and corruption.

63. The law on state secret of Moldova falls short in an important number of respects from what can be regarded as good practices in the field of state secrecy. Several provisions would therefore need amendments or clarification.

64. The Venice Commission stands ready to assist the Moldovan authorities, should they decide to amend the law.

[30] 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.