Organization for Security and Co-operation in Europe
Office of the Representative on Freedom of the Media

Comments on Draft Law on State Secret of the Republic of Moldova

Commissioned by the Office of the OSCE Representative on Freedom of the Media from Mr. David Banisar, Director, FOI Project, Privacy International

2008

Contents

Overview

The protection of state secrets needs to be balanced against access to information, freedom of expression and other society rights. Across the region, many nations have taken the opportunity in the past few years when revising their old secrets laws to limit excessive secrecy.

Currently, the Law on State Secret of the Republic of Moldova is excessively broad when compared to international and regional standards. The bill shows little improvement over the existing Law. In many areas, it expands secrecy including in the definition of state secrets; the types of information that can be classified; it also includes a new undefined category of "restricted" secrets which does not require harm to be shown; the extension of classification; and the reductions in parliamentary oversight. It does introduce some modest improvements including better defining the categories of secrets and the inclusion of the public interest test. But overall, the adoption of the bill would represent a step backwards rather than making the system of secrets more open, efficient and accountable.

National Security and Its Costs

Every country has highly sensitive information relating to national security that needs protection and rules governing its protection. A significant number of OSCE participating States have adopted laws that set out detailed procedures for the classification, protection and declassification of information that could affect national security.[1] These laws regulate the types of information that can be classified, limitations, the duration of the classification and procedures for vetting employees.

There is often a conflict between these procedures and the public and journalists attempting to obtain and publish information of interest to the public. Broad exemptions to access imposed by security protections frequently raise serious concerns about national security being used to undermine basic rights, a situation that occurs even in some long-standing democracies.

The protection of classified information should not be used as a trump card that can be issued to stop discussion of important issues. It must be balanced against other important societal interests, including the free flow of information, democratic accountability, fair trials and fighting against corruption.

It has long been recognized that excessive secrecy by government bodies is ultimately counterproductive. The most important consequence is that it undermines public trust, especially when used in abusive ways, such as to support political agendas or hide abuses, corruption and mismanagement. If, because of excessive secrecy, the public believes that the government is only doing something for its own benefit, the credibility and legitimacy of that government is seriously undermined and it will have grave difficulties in gaining public support for any of its activities.

As US Supreme Court Justice Potter Stewart noted in the *Pentagon Papers* case in 1971, "For when everything is classified, then nothing is classified, and the system becomes one to be

[1] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.

disregarded by the cynical or the careless, and to be manipulated by those intent on self protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained." [2]

Some of the other harms of excessive secrecy are:

- *A weakening of the protections for important information*. Even the most secret of files can be leaked when the classification system is not carefully organized. In April 2003, many of the security files of the UDBA, the former Yugoslavian secret police, were published on a web site in Thailand.[3]

- *Preventing government agencies and those outside from learning important information and lessons*. The September 11 Commission in the United States found many examples of excessive classification preventing information sharing between government bodies which might have prevented the attacks from occurring. [4]

- *Direct monetary costs.* The creation and protection of classified information imposes significant burdens on public authorities. These include personnel security, physical security, information security, training, management and planning. In the US, the estimated cost of creating and protecting classified information was over $9.9 billion in 2007.[5]

In recent years, many countries in the region have revised their national laws to better reflect the modern views that excessive secrecy is harmful to a nation's overall interest. The 2007 OSCE review found that many had changed their laws in the past five years to allow for greater openness while adopting freedom of information laws. [6]

Defining State Secrets

Of primary importance for all laws on state secrets is to ensure that they are not overly broad and only protect information that is necessary for ensuring the national security of the nation. This concept is widely recognised by a variety of international and regional organisations including the UN, OSCE and CoE.

The OSCE Representative on Freedom of Media has recommended that participating States limit their secrets laws to only national security related measures:

[2] NY Times v. US, 403 US 713 (1971). For more details, see National Security Archive, The Pentagon Papers Case. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB48/
[3] REF/RL Balkan Report, 25 April 2003.
[4] National Commission on Terrorist Attacks Upon the United States, Final Report. http://www.9-11commission.gov/report/index.htm
[5] Informational Security Oversight Office, Report to the President for Fiscal Year 2007, 30 May 2008. http://www.archives.gov/isoo/reports/2007-annual-report.pdf
[6] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007; Access to information by the media in the OSCE region: Country Reports, 21 June 2007.

> The definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences. [7]

This has also been recommended by the CoE Parliamentary Assembly which in 2007 called on 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 risks of abuse or unwarranted prosecutions[8]

Unfortunately, the bill at hand takes the opposite approach and expands the definition of what type of information is intended to be protected. These changes substantially extend the rationale of the law to cover a wide variety of other issues that are not related to national security that should be dealt with in other specific civil laws.

Under the current 1994 Law on State Secret, Article 2 limits classification to only information which "may infringe the security of the Republic of Moldova". Under Article 1 of the bill, the harm to be prevented is no longer only related to the security of the Republic but the broader and undefined "harm [to] the interests and/or the security of the Republic". In addition, the section extends application of state secrets to all public authorities rather than just those involved in counterintelligence and operative investigation.
Under Article 6(3) of the current law, the rationale for classification is for "preventing the gross infringement of the security of Moldova". Again, the revised Article 6(3) of the bill no longer limits the application of the law to serious infringements on the security of the state, but now extends it to protect the "eventual economic consequence, as well as of other nature, on the basis of the interests of the state, society and person."

Recommendations

- *Reduce the application of the law to only information the release of which would harm national security.*

Expanded Categories of Classified Information

Article 5 of the current Law of State Secret sets out four broad categories of information that can be classified as state secrets: military; economy, science and technology; foreign policy; and state security. Under each category, there are a number of sub-categories and most of the sub-categories themselves apply to multiple areas. In total, over one hundred different categories of information are covered. The government has developed a detailed list of information to be kept secret. This list is published. The heads of public bodies create detailed lists of information in their possession which are not published.

[7] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.
[8] Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets, §1.1.1

As noted before, the extensive list of information to be classified is overly sweeping. [9] The list of information should be shortened and simplified to only apply to information t hat is directly relating to national security. For instance, the US Executive Order on Classified National Security Information sets out eight areas that are eligible for classification:

> (a) military plans, weapons systems, or operations;
> (b) foreign government information;
> (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
> (d) foreign relations or foreign activities of the United States, including confidential sources;
> (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
> (f) United States Government programs for safeguarding nuclear materials or facilities;
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
> (h) weapons of mass destruction. [10]

Other countries have taken an even more specific method to ensure oversight. In Estonia, the State Secrets Act sets out specifically each of the types of information that can be classified, under which category they can be classified, and for how long they can be classified. [11] In Sweden, all exemptions to the Freedom of the Press Act are specifically adopted by Parliament as amendments to the Act on Secrecy. [12]

In comparison, the bill extends the categories of secrecy. Article 7 of the bill sets out the categories of information that can be classified. This section now includes over a dozen new categories of information that can be classified compared with Article 5 of the existing law. These include information relating to civil protection measures (1(c)), border guards 4(c), geographic data (1(e)), telecommunications networks of public authorities 4(e), and scientific or research that would affect external economic activities (2)(f).

Many of these new categories are overly broad and are not limited to the national security area and may lead to substantial restrictions on information. Of particular concern is the catch-all sections under Article 7(5) on anything that may lead to the disclosure of state secrets. This seems unnecessary since the actual disclosure of particular state secrets should be covered by the specific categories that are already set out and would give broad authority for officials to limit access to unclassified information under the vague justification that it may at some future point be combined with some other unknown information to cause the release of classified information.

[9] See 2004 OSCE review; CoE Venice Commission, Opinion on the Law on State Secret of the Republic of Moldova CDL-AD(2008)008, 20 March 2008.
[10] Executive Order 13,292 on Classified National Security Information, March 28, 2003.
[11] State Secrets Act. RT I 1999, 16, 271 §§ 4-8.
[12] Act on Secrecy of March 20, 1980 as amended.

Recommendations

- *Reduce the categories of information to only information that would directly and negatively affect national security.*
- *Eliminate catch-all category under 7(5).*

Levels of State Secrets Expanded

Under Article 7 of the 1994 law, three levels of classification are authorised: Special Compartment, Top Secret and Secret. Article 11 of the bill replaces this with four categories, Top Secret, Secret, Confidential and Restricted.

For the first three categories, the bill requires showing that a harm will occur if the information is released. The inclusion of levels of harm – "exceptionally grave" for Top Secret, "seriously harm" for Secret and "harm" for Confidential – is an improvement over the existing law which sets out no standards.

The final category, Restricted, however, is overly broad and unnecessary. It allows for the classification of information when an official determines that its disclosure "cannot be in the favour of the interests and/or security" of the country or if it may lead to the disclosure of information in the above categories. The article is problematic because of both its broad scope and its lack of limits in what is "cannot be in the favour of the interests" which could include exposure of corruption, mis-dealings, politically embarrassing materials and other non-national security related information. The adoption of this standard would seriously undermine the public's right of access to information. It is also unnecessary because information that may disclose classified information should already be protected under the other regimes, and should not be solved by creating a new one.

The new category is also inconsistent with recommendations of the OSCE Representative on Freedom of the Media:

> Information designated as "Official" or "work secrets" should not be considered for classification as state secrets. Limits on their disclosure should be found in the access to information law. [13]

In comparison, other laws in the CEE region that include a fourth category better define what is to be covered. In the Czech Republic, the Act on the Protection of Classified Information adopted in 2005 sets out strict definitions for harm and different levels of "disadvantageous". The lowest category, "disadvantageous to the interests of the Czech Republic" is defined as "the divulgence of classified information to any authorized person or misuse of classified information, which can result in a breach of activities of the Armed Forces of the Czech Republic; obstructing impeding or endangering the vetting or investigation of offenses; damage to important economic interests of the Republic, EU or other member states; breach of important commercial or political negotiations of the Czech Republic with a foreign power; or a breach of security or intelligence operations." [14]

[13] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.
[14] Act N. 412 of 21 September 2005 on the Protection of Classified Information., § 3 (5) .

Recommendations

- *Greater detail about harms should be included in the definitions.*
- *The category of "Restricted" should be eliminated from the bill.*

Duration of State Secrets

Nearly all state secrets acts set limits on the length of time that information should be classified. Classified information is best thought of as having a "lifecycle". [15] At different times, the need for protection will change. The older the information, the less likely that the harm envisaged will be realized, and the higher the public interest in releasing this information.

The OSCE Representative has recommended that information should only be classified for a limited duration:

> Information should only be classified as a state secret for a limited period of time where the release of the information would cause a serious harm to the interests of the nation. Information that is classified should be regularly reviewed and have a date after which it will be declassified and released. It should be presumed that no information should be classified for more than 15 years, unless compelling reasons can be show for withholding it. [16]

The current Law on State Secret sets a maximum classification period for the "Of Special Importance" and "Strictly Confidential" categories at twenty-five years and ten years for Secret information. These time frames are too long. Typically, government officials in most countries apply the maximum length as a default under the perception that it is better to be overly careful. The end result is the over-classification of information, and the monetary and social costs of unnecessary protection are significant.

The bill does not substantially improve the situation. It requires that information that is Top Secret to be classified for 25 years, Secret for 15 years, Confidential for 10 years and the controversial category Restricted for 5 years.

Many other countries in the region that have recently enacted laws that adopt shorter durations because of the recognition of the problems of excessive secrecy. For instance, in the former Yugoslav Republic of Macedonia, the Law on Classified Information sets the duration for "State Secret" at ten years, "Highly Confidential" at five years, "Confidential" at three years and "Internal" at two years. In Albania, the default for information to be classified is set at ten years unless the person who issues the classification can identify an earlier date or event that would cause it to be available earlier or makes a specific determination that it is sensitive to near a later date.

[15] See Background on the Principles and Process of "Life Cycle Risk Assessment", http://www.opsec.org/opsnews/Sep97/protected/Secrecy.html

[16] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.

Also lacking is a provision to allow for the automatic declassification and release of formerly secret information of public interest. In Poland, the Classified Information Protection Act required that all pre-1990 records be reviewed and those found to be not necessary to continue to keep secret were automatically released within 36 months. In Hungary, the Act on State and Official Secrets required the review and declassification of all records from before 1980 within one year of its enactment.

The OSCE Representative has also recommended that information should be reviewed and declassified:

> Governments should institute a review of all secret information over 15 years old and automatically declassify and release it. All information that was designated as secret by a previous non-democratic government should be declassified and presumptively released unless it is shown that its release would endanger the national security or be an unwarranted invasion of privacy.[17]

In addition, nearly all of countries in the CEE have now adopted laws on the disclosure of secret police files and other records.[18] This allows for citizens who were victimized by intelligence services to better understand what was done and who was responsible.

In contrast, Article 13(2) of the bill allows for many of these records to be protected from disclosure for up to 75 years "regardless of secrecy level".

A legal obligation to provide these files has been found in Article 8 of the European Convention of Human Rights by the European Court of Human Rights in a number of cases.[19] As noted by the Court:

> [U]nless the contrary is shown on the facts of a specific case, it cannot be assumed that there remains a continuing and actual public interest in imposing limitations on access to materials classified as confidential under former regimes... [T]here may be a situation in which there is a compelling State interest in maintaining the secrecy of some documents, even those produced under the former regime. Nevertheless, such a situation will only arise exceptionally given the considerable time which has elapsed

[17] OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.

[18] See e.g. Act for Access and Disclosure of Documents and for Revealing Affiliation of Bulgarian Citizens with the State Security and Intelligence Services of the Bulgarian Army (Bulgaria); Act N. 140/1996 Coll. of 26 April 1996 on Disclosure of Files Established by Activities of the Former State Security Force (Czech Rep.) Act Regarding the Records of the State Security Service of the Former German Democratic Republic (Stasi Records Act) of 20 December 1991 (Germany); Act III of 2003 on the Disclosure of the Secret Service Activities of the Past Regime and the Historic Archive of the National Security Services, 14 January 2003 (Hungary); Law on preserving and application of the documents of former KGB and establishment of the fact of cooperation with former KGB, 17 November 2003.(Latvia); ACT of 18 December 1998 on the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation (Poland); Law No. 189 of 7 December 1999 on the access to the personal file and the disclosure of the Securitate as a political police (Romania).

[19] Leander v. Sweden judgment of 26 March 1987, Series A no. 116; Rotaru v. Romania, Application no. 28341/95, 4 May 2000; Segerstedt-Wiberg and Others v. Sweden, Application no. 62332/00; Turek v. Slovakia, Appliation 57986/00, [2006] ECHR 138 (14 February 2006); Bobek v. Poland, Application no. 68761/01, 17 July 2007.

since the documents were created. It is for the Government to prove the existence of such an interest in the particular case, because what is accepted as an exception must not become the norm.[20]

This has also been recommended by the CoE Parliamentary Assembly as far back as 1996 which recommended:

> The Assembly welcomes the opening of secret service files for public examination in some former communist totalitarian countries. It advises all countries concerned to enable the persons affected to examine, upon their request, the files kept on them by the former secret services.[21]

Recommendations

- *The durations of classifications should be sharply reduced in line with other laws in the regions to ensure that information is not classified beyond the time that is necessary to protect national security. The durations should be 10 years for Top Secret, 5 years for Secret and 2 years for Confidential, with the possibility of renewing that period if it is shown that harm will result from declassification.*
- *A system should be put in place to ensure the effective review of classified information and its declassification when it is no longer sensitive.*
- *Information relating to the intelligence services of Moldova prior to 1991 should be automatically declassified and a process to allow access to those files, especially to those who were the victims of the intelligence services, should be implemented.*

Prohibitions on Classification for Public Interest Reasons

Most secrets acts typically provide that certain categories of information cannot be classified. These usually include human rights violations, violations of other laws and information relating to environmental hazards.

Some of these requirements are based on international law. Information relating to human rights violations cannot be classified as a state secret under the International Covenant on Civil and Political Rights.[22] The UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters requires the disclosure of possible hazards to public health or the environment.[23]

The OSCE Representative on Freedom of the Media has recommended that a wide variety of information of public interest should not be classified:

> Information relating to violations of the law or human rights, maladministration or administrative errors, threats to public health or the environment, the health of senior elected officials, statistical, social-economic or cultural information, basic scientific

[20] Bobek v. Poland, Application no. 68761/01, 17 July 2007.
[21] Resolution 1096 (1996) on measures to dismantle the heritage of former communist totalitarian systems
[22] The UN Working Group on Arbitrary Detention, Recommendation: Human Rights and State Secrets, E/CN.4/2001/14, 20 December 2000.
[23] See e.g. §5(1)(c).

> information, or that which is merely embarrassing to individuals or organisations should not be classified as a state or official secret. [24]

Article 8 of the bill on "information that is not defined as a state secret" offers some small improvements on the existing law. It now includes a number of additional categories of information that cannot be classified including the quality of food products and a ppliances and the health status of persons who hold a public function.

However 8(f) represents a weakening from the current law in that it only applies to "cases of law infringement" of authorities and high officials rather than the previous application t o "cases of infringement, inactivity, and illegal actions of officials". In comparison, the Romanian Law on Protection of Information prohibits the classification of information " for the purpose of hiding law infringements, administrative errors, limitatio n of access to information of public interest, illegal restriction of exercising the rights of any person or harming other legitimate interests." [25] The US Executive Order on Classified National Security Information prohibits the classification of informatio n to "conceal violations of law, inefficiency, or administrative error, prevent embarrassment to a person, organization or agency, retain competition, or prevent or delay the release of information that does not require protection in the interest of nation al security information."

To made the section more effective, additional categories should be included. This should include basic scientific information, maps and the state of gold and foreign currency reserves.

Recommendations

- *The categories of inform ation that cannot be classified as a State Secret should be expanded. This should specifically include information on all violations of law, administrative practice and ethics.*

Whistleblower Protections

It is a welcome addition in Article 8(2) that cla ssification is prohibited in cases of access to information of a public interest. However, this should also be extended to allow for the protection of whistleblowers who release information that has been already classified but is of a significant public in terest. This would make it more consistent with Article 7(5) the Law on Access to Information which protects the unauthorized release of even national security information when there is a public interest and the recent European Court of Human Rights case of *Guja v. Moldova* which recognized a fundamental right of whistle -blowing for public officials:

> [T]he Court notes that a civil servant, in the course of his work, may become aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest. The Court thus considers that the signaling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in

[24] OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary o f preliminary results of the survey, 30 April 2007 .
[25] Law no. 182 of April 12th, 2002 on the protection of classified information. Published in the Official Gazette, Part I no. 248 of April 12th 2002.

> the workplace should, in certain circumstances, enjoy protection… T he interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence… [26]

The OSCE Representative on Freedom of the Media has recommended that whistleblowers of all forms should not be prosecuted:

> Whistleblowers who disclose secret information of public interest to the media should not be subject to legal, administrative or employment -related sanctions.

The CoE Parliamentary Assembly has also recommended that secrets laws ensure that whistleblowers are protected. The 2007 PA Resolution states that member states should:

> [L]ook into ways and means of enhancing the protection of whistle -blowers and journalists, who expose corruption, human rights violations, environmental destruction or other abuses of public authority, in all Council of Europe member states; [27]

More generally, a comprehensive system to protect whistleblowers based on the requirements of the *Guja* decision should be implemented. [28]

Recommendations

- *Whistle-blowing protections should be included to ensure the release of information of strong public interest to the public.*
- *A free-standing whistleblower protection law as set out by the European Court of Human Rights should be adopted.*

Classifying Privately Held Informati on

Article 16 of the bill retains provisions in the 1994 law that allow public authorities at their own initiative to classify as state secrets information in the possession of companies and citizens. Under the bill, the information can be appropriated by the state if the private party refuses to sign a contract placing limits on its use.

Given the broad definitions under Article 6 (3) of information that can be classified, this provision is of grave concern for freedom of expression and should be strict ly limited or dropped. As it standards, it gives authorities the power to restrict and punish journalists and civil society from gathering and publishing information of a public interest.

Recommendation

[26] Guja v Moldova, App 14277/04, 12 February 2008.
[27] Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espion age or divulging state secrets, §1.2
[28] See e.g. Legea nr. 571/2004 privind protectia personalului din autoritatile publice, institutiile publice si din alte unitati care semnaleaz a incalcari ale legii (Romania Law 571/2004 Act on the Protection of Whistleblowers). Available at http://legislatie.resurse-pentru-democratie.org/571_2004.php

- *Information created and held by private parties should not be classified as secret except in cases where there is a prior legal relationship between the party and the government relating to the information.*

Use of Secrets in Court Cases

Article 34 of the bill allows for closed hearings for using state secrets in criminal, civil and administrative cases. This provision raises serious concerns for fair trials and other proceedings as required under Article 6 of the European Convention on Human Rights. The COE Parliamentary Assembly has expressed concern over these types of cases and made the following recommendations:

> 10.5. courts should be vigilant in ensuring a fair trial, with particular attention to the principle of equality of arms between the prosecution and the defence, in particular:
> 10.5.1. the defence should be adequately represented in the selection of experts advising the court on the secret nature of relevant information;
> 10.5.2. experts should have a high level of professional competence and should be independent from the secret services;
> 10.5.3. the defence should be allowed to question the experts before the jury and challenge their testimony through experts named by the defence, including experts from other jurisdictions;
> 10.6. proceedings should be as open and transparent as possible, in order to boost public confidence in their fairness; at the very least, the judgments must be made public.[29]

Recommendations

- *Limits on access to secret information should be proportional and should not limit access by elected officials, judges and others who have a need to access information to provide oversight or handle cases.*
- *Litigants and/or their legal representatives should be guaranteed access to all information that is relevant or used in a court or administrative hearings that affects a person's civil, political or socio-economic rights.*
- *Proceedings should be open and transparent to the media and public to ensure public confidence.*

Reduced Oversight

Elected representatives play an important role in ensuring that the secrecy system is balanced and fair. Access is also necessary for parliamentary functions. Without full access to information, adequate oversight of important military and intelligence services cannot be conducted. Investigations into important areas, such as possible abuses and corruption are limited. More fundamentally, the bodies are less accountable to the elected representatives of the people.

[29] See Resolution 1551 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets; Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets.

The important role of the Parliament in overseeing the effective and non-abusing conduct of the secrecy system is limited in the bill. Article 28 of the 1994 law gives the Parliament control over the legislation and expenditures and obliges state bodies to provide information.

Under the bill, this has been eliminated by Article 5 which removes specific obligations for officials to provide information. In addition, control of the budget and approval of the budget relating to secrets has been removed from Article 4.

Currently, there is no general oversight body for freedom of information such as is found in many other nations in the region including Hungary, Serbia and Slovenia. This body can play an important role in ensuring that there is no excessive secrecy. In Hungary, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information is entitled to change the classification of state and official secrets. [30] In Slovenia, the Information Commissioner can check the accuracy of the classification. In the US, the Information Security Oversight Office (ISOO), a part of the national archives, is given independent authority to review classification.

The OSCE Representative has recommended that an independent body that is familiar with openness should have oversight power including the right to oversee and order disclosure:

> An independent body that is not part of the intelligence, military or security services should have oversight over classified information and ensure that the system is operating properly, receive complaints about improperly classified information and review and order the declassification of information.

Recommendations

- *The role of the Parliament in overseeing secrecy policy should be expanded rather than reduced.*
- *An independent body should be created to enforce freedom of information legislation with the power to review state secrets decisions to ensure access to information.*

Conclusions and Recommendations

The bill differs little from the current Law on State Secret. In many areas the bill is more restrictive than the existing law and violates significant obligations under international and regional agreements.

Recommendations

- *Reduce the application of the law to only information the release of which would harm national security.*
- *Reduce the categories of information to only information that would directly and negatively affect national security.*
- *Eliminate catch-all category under 7(5).*

[30] Hungary, Act LXV of 1995 on State Secrets and Official Secrets.

- *Greater detail about harms should be included in the definitions.*
- *The category of "Restricted" should be eliminated from the bill.*
- *The durations of classifications should be sharply reduced in line with other laws in the regions to ensure that information is not classified beyond the time that is necessary to protect national security. The durations should be 10 years for Top Secret, 5 years for Secret and 2 years for Confidential, with the possibility of renewing that period if it is shown that harm will result from declassification.*
- *A system should be put in place to ensure the effective review of classified information and its declassification when it is no longer sensitive.*
- *Information relating to the intelligence services of Moldova prior to 1991 should be automatically declassified and a process to allow access to those files, especially to those who were the victims of the intelligence services, should be implemented.*
- *The categories of information that cannot be classified as a State Secret should be expanded. This should specifically include information on all violations of law, administrative practice and ethics.*
- *Whistle-blowing protections should be included to ensure the release of information of strong public interest to the public.*
- *A free-standing whistleblower protection law as set out by the European Court of Human Rights should be adopted.*
- *Information created and held by private parties should not be classified as secret except in cases where there is a prior legal relationship between the party and the government relating to the information.*
- *Limits on access to secret information should be proportional and should not limit access by elected officials, judges and others who have a need to access information to provide oversight or handle cases.*
- *Litigants and/or their legal representatives should be guaranteed access to all information that is relevant or used in a court or administrative hearings that affects a person's civil, political or socio-economic rights.*
- *Proceedings should be open and transparent to the media and public to ensure public confidence.*
- *The role of the Parliament in overseeing secrecy policy should be expanded rather than reduced.*
- *An independent body should be created to enforce freedom of information legislation with the power to review state secrets decisions to ensure access to information.*