



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

## **Comments on the Croatian Draft Bill on Data Secrecy<sup>1</sup>**

**David Banisar  
Director, Freedom of Information Project of Privacy International<sup>2</sup>**

April 2007

### **Overview**

National security and freedom need to be balanced. The replacement of the existing 1996 law is welcome but the current Draft is flawed and represents a lost opportunity to adopt a law that is consistent with modern western standards on protection of state secrets. As it currently stands, the Draft raises serious concerns about its effects on public access to government information and should be significantly amended before it is considered by the Parliament.

### **Secrecy and its Costs**

The protection of national security-related information is an important function in every nation. However, the protection must be limited in scope, reasonable, and balanced with the need for public access to information to ensure a free and democratic society. A properly functioning security of information system recognizes that a limited amount of sensitive information needs to be protected and then only for the duration that it is sensitive. Less sensitive information is given lesser protections or none at all.

It has been long 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 disregarded by the cynical or the careless, and to be manipulated by those intent on self

---

<sup>1</sup> This analysis is based on translations of the Draft Bill on Data Secrecy provided to the author in March 2007.

<sup>2</sup> Homepage: <http://www.privacyinternational.org/foi>

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.”<sup>3</sup>

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.<sup>4</sup>
- *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.<sup>5</sup>
- *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, and management and planning. In the US, the estimated cost of creating and protecting classified information was over \$8 billion in 2005.

## Overbroad Coverage

The most significant problem with the Draft is its overbroad coverage. It applies to many areas of information which are not traditionally state secrets and does not adequately set distinct boundaries between state secrets and non-state secrets.

### *Broad Areas of Classification*

The types of information that can be included as classified information are far too broad and violate international norms. Article 5 defines possible state secrets to include areas such as criminal investigations and the fields of science, research, technology, economy and finance. Article 6 includes areas such as protecting “international reputation”, and the economic and financial systems.

These wide areas of public policy are inappropriate to include in a law on state secrets. They are not required by NATO or the European Union and are likely to seriously undermine access to information.

They also violate international norms. The use of broad classification categories such as these in state secrets acts is considered by the UN Human Rights Committee to be a violation of

---

<sup>3</sup> 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/>

<sup>4</sup> REF/RL Balkan Report, 25 April 2003.

<sup>5</sup> National Commission on Terrorist Attacks Upon the United States, Final Report. <http://www.9-11commission.gov/report/index.htm>

Article 19 of the International Covenant of Civil and Political Rights. The Committee review of the Uzbek Law on Protection of State Secrets stated:

The Committee is particularly concerned about the definition of "State secrets and other secrets" as defined in the Law on the Protection of State Secrets. It observes that the definition includes issues relating, inter alia, to science, banking and the commercial sector and is concerned that these restrictions on the freedom to receive and impart information are too wide to be consistent with article 19 of the Covenant [...] The State party should amend the Law on the Protection of State Secrets to define and considerably reduce the types of issues that are defined as "State secrets and other secrets", thereby, bringing this law into compliance with article 19 of the Covenant.<sup>6</sup>

### *The Restricted Category*

Of particular concern is the creation of a new catch-all category of "Restricted" information which allows for the classification of information when it would "harm the activities and performance of tasks of state bodies, bodies of local and regional self-government units and legal persons with public powers." The Article is problematic because of both its broad scope and its lack of limits. The adoption of this standard would seriously undermine the public's right of access to information under the Act on the Right of Access to Information, Article 38 of the Constitution and international obligations.

Unlike Articles 6, 7 and 8, Article 9 does not specifically define the types of information which are covered by the Article. Therefore, presumably, it applies to all of the categories listed in Article 5.

Article 9 gives public bodies nearly unlimited authority to apply it. The very low threshold that the information disclosure would "harm the activities and performance" could be applied by state or local officials in nearly every decision where they perceive that a controversy could upset their plans. It is unnecessary to include this provision in a law on protection of much more sensitive information and is likely to lead to a significant reduction in public access to information.

A better approach is already found in Croatian law for access to non-national security related information. Article 8 of the Act on the Right of Access to Information sets a clear list of both the types of information and the specific harms that are required before information access can be restricted:

- (2) Bodies of public authority may deny the right of access to information if there is any well-founded suspicion that its publication would:
  - 1) make it impossible to take measures or carry out action to prevent and uncover criminal offenses or for the prosecution of perpetrators of criminal offenses;
  - 2) make it impossible effectively, independently or without prejudice to conduct court, administrative or other legally established proceedings, to execute court decisions or penalties;

---

<sup>6</sup> Concluding observations of the Human Rights Committee: Uzbekistan. 26/04/2001. CCPR/CO/71/UZB

- 3) make impossible the work of bodies who carry out administrative supervision, or supervision of legality;
- 4) cause serious damage to the life, health and safety of people or the environment;
- 5) make it impossible to implement economic or monetary policies;
- 6) endanger the right of intellectual property, except in cases of the express written consent of the author or owner.

This approach should be adopted and harmonized between the two laws to ensure the principle of maximum access to information.

Information that is received from international organisations and is required to be protected under NATO and EU obligations should be treated separately and exempted only as required by those international agreements. A similar category of restricted information was considered in Albania in 2006 based on the same perceived demands of NATO and the EU harmonization. Ultimately, the Parliament rejected the broad proposal and limited it to national security-related information.

#### *Application to Non-government Parties*

An underlying concern about these new categories is how they will apply to the media and those outside the government who received unauthorized information. The Draft is silent on the application of the current provisions of the Criminal Code on disclosure of state and official secrets which applies to those outside of the officials who handle information. Will the new restrictions on the release of Classified or “Restricted” information be a criminal offense to the members of the media and NGOs?

Article 21(2) appears to require that outside parties inform the data owner if they receive unauthorized information and require that the data owner take measures for the “elimination of possible damaging consequences.” This would have severe effects on the media which would be required to ensure that all of the information that it receives from its sources is an authorized release. This application would be a clear violation of Article 10 of the European Convention on Human Rights.

#### *Recommendations*

- *The designation of classified information should not apply to criminal investigations, science, research, technology, economy or finance unless it directly affects the national security of the nation.*
- *The restricted information category should only apply to specifically designated NATO, EU national security or related received information and should not apply to domestic purely national information.*

- *The Criminal Code should be amended to ensure that it only applies to those who have a direct legal obligation not to disclose information due to their position or employment.*

## **Unlimited Duration of Secrets**

The Draft does not provide for effective limits on the duration that information, including the lowest category of Restricted information, can be classified. It only allows for infrequent reviews and sets no time-frames for how long information should be classified. These omissions are likely to result in the excessive classification of information for extended periods.

Article 14 of the Draft bill requires that there are periodic reviews of information. Top Secret information is reviewed at least every five years, Secret and Confidential information is reviewed every 4 years and restricted information is reviewed every 2 years. Most modern legislation on protecting state secrets includes this function but the Draft time-frames are much longer than the best practices of other democratic nations. The Georgian and Estonian State Secrets Act require that each possessor of secrets review the classification yearly and note when it has been declassified. In Sweden, the classification is re-evaluated each time the document is accessed. In Moldova, the reviews must happen "regularly".

Another significant omission is the lack of a limit on how long the information can be classified. This is inconsistent with nearly every state secrets law in the democratic world. Most secrets laws recognize that a maximum time frame should be set for each category of classification since otherwise the information will likely never be declassified. Even under the current national law there are limits. The Act on the Right of Access to Information says that exempted information such as is found in the Restricted category should not be withheld for more than 20 years or when the reasons that cause it to be withheld are completed.

The current international trend is to set limits on the maximum duration of classified information to between ten and twenty years. 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 and the US, 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. In the US, fifty percent of all information is set for declassification in 10 years or less.<sup>7</sup>

### *Recommendations*

- *Information should be reviewed yearly to ensure that it is still necessary to be classified. When it is no longer necessary, the information should be sent to the National Archive for public release.*
- *The duration of the categories should be set accordingly to their sensitivity.*

---

<sup>7</sup> Information Security Oversight Office, Annual Report 2003.

- *Top Secret – 10 years*
  - *Secret – 5 years*
  - *Confidential – 2 years*
  - *Restricted – No time*
- *The maximum number of extensions of classification should be limited in law. Additional justifications should be required for any extensions.*
  - *Any remaining files from pre-democratic governments should be declassified and released.*

## Categories of Information Prohibited from being Designated as State Secrets

The Draft also has only limited exemptions for what can be classified which does not meet international obligations and the best practices of democratic countries. Article 3 of the Draft prohibits the classification of information “for the purpose of concealing a criminal act, overstepping or misuse of authority or any other type of illegal activity.” While it is an important recognition that classification systems can be abused, the categories of information are far too narrow. There are other obligations on public authorities such as the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters on disclosure of possible hazards to public health or the environment which would not be allowed under this article.

The following are some other examples of information which cannot be classified in other countries:

- *Inefficiency and errors.* The Moldovan Secrets Act law prohibits the classification of information about the inactivity of public authorities and officials.<sup>8</sup> Under the Romanian Law on Protection of Information, information cannot be made a state secret to hide “administrative errors, limitation of access to information of public interest, illegal restriction of exercising the rights of any person or harming other legitimate interests.”<sup>9</sup>
- *Benefits and compensation.* The Georgian Law on State Secrets prohibits classification of information about state privileges, compensations and benefits to individuals, officials, enterprises, institutions, and organizations.<sup>10</sup>
- *Human Rights.* The CIS Interparliamentary Assembly Model Law on State Secrets recommends that information on “mass repressions for political, social and other reasons” not be subject to classification as a state secret.<sup>11</sup>

<sup>8</sup> Law on State Secrets no. 106-XIII of 17 May 1994. <http://www.ijnet.org/Director.aspx?P=MediaLaws&ID=25362&LID=1>

<sup>9</sup> Law no. 182 of April 12th, 2002 on the protection of classified information. Published in the Official Gazette, Part I no. 248 of 12 April 2002.

<sup>10</sup> Model Law On State Secrets. Adopted at the twenty-first plenary session of the CIS Interparliamentary Assembly (decision № 21-10 of 16 June 2003).

<sup>11</sup> Id.

- *Basic scientific information.* The Romanian Law on Protection of Information and the US Executive Order on Classified National Security Information prohibit the classification of basic scientific information with no connection to national security.<sup>12</sup>
- *Basic statistics and information.* The Lithuanian Law on State Secrets prohibits the classification of “statistical data concerning the state of economy and finances [...] as well as the state of health care, education, ecology, social and demographic situation, [and] results of social studies.”<sup>13</sup> Georgia prohibits the classification of international agreements and treaties, most normative acts, and non-military maps. The Georgian, CIS and Russian laws all prohibit classification of information on currency and gold reserves.
- *Embarrassment.* The US Executive Order prohibits the classification of information to “prevent embarrassment to a person, organization or agency, or retain competition.”

#### *Recommendation*

- *The categories of information that cannot be classified should be expanded.*

## **Lack of Public Interest Reviews**

Another weakness in the Draft is the failure to recognize that there are instances where information should be released because there is a strong public interest, even if it is properly classified and may cause harm if it is released. This is also a weakness of the existing 2003 Act on the Right of Access to Information.

Article 19(2) allows for the relaxation of the obligation of secrecy but it appears to only allow the removal of restrictions if Articles 6-9 do not apply. This reverses the typical recognition of the public interest having a higher need.

In comparison, other nations have adopted public interest tests in their laws of information which also apply to classified information. For example, in Slovenia, the Access to Public Information Act public interest test applies to classified information below the level of Secret.<sup>14</sup> In New Zealand and the UK, a mere designation of something as classified does not prevent its review and possible release under the access to information laws.

#### *Recommendation*

- *A test should be incorporated to ensure that information is released when there is a public interest even if it is properly classified.*

---

<sup>12</sup> Executive Order 12958-Classified National Security Information, as Amended. <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>

<sup>13</sup> Law on State Secrets and their Protection. No. I – 1074. 25 October 1995.

<sup>14</sup> Access to Public Interest Act, §6(2)

## Whistleblowing Procedures

Similarly, there are no protections for officials and others (whistleblowers) who reveal information about possible public harms which are not covered in Article 3 such as environmental hazards, mismanagement or dubious practices. This is inconsistent with both European and international laws.

There are strong recognitions in international law on the protection of whistleblowers. The Council of Europe Civil Law Convention on Corruption (CETS No 174) recognizes that employees who disclose information about possible corruption should not be subject to sanctions.<sup>15</sup> It is also recognized in the UN Convention against Corruption and other international instruments and in the Stability Pact Declaration on “10 joint measures to curb corruption in South Eastern Europe” agreed to in May 2005.<sup>16</sup>

The lack of protection of whistleblowers also violates international human rights law. The UN Human Rights Committee has been critical of states that use State Secrets Acts to repress the release of important information. In 2001, it criticized the United Kingdom government for using the Official Secrets Act against whistleblowers and journalists:

The Committee is concerned that powers under the Official Secrets Act 1989 have been exercised to frustrate former employees of the Crown from bringing into the public domain issues of genuine public concern, and to prevent journalists from publishing such matters.

The State Party should ensure that its powers to protect information genuinely related to matters of national security are narrowly utilised, and limited to instances where it has been shown to be necessary to suppress release of the information.<sup>17</sup>

Other countries in Europe expressly include this provision in their national laws. For instance, in Denmark, the Criminal Code allows for the disclosure of classified information if the person “acted in order to lawfully safeguard obvious public interest or the interest of himself or other persons.”<sup>18</sup> In Moldova, the Law on Access to Information protects the unauthorized release of even national security information when there is a public interest:

7(5) No one can be punished for the fact that he or she made public information with limited access, if releasing this information does not damage or cannot damage legitimate interests related to national security, or if the public interest for knowing the information is larger than the damage that can result from its dissemination.

Similar provisions also exist in the freedom of information laws in Montenegro and the former Yugoslav Republic of Macedonia.

---

<sup>15</sup> Council of Europe, Civil Law Convention on Corruption, ETS No 174.  
<http://conventions.coe.int/treaty/en/Treaties/Html/174.htm>

<sup>16</sup> Ministerial Conference on Joint Measures to Curb Corruption in South Eastern Europe, Declaration on 10 joint measures to curb corruption in South Eastern Europe, 12 May 2005.

<sup>17</sup> Concluding Observations of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland. 05/11/2001. CCPR/CO/73/UK,CCPR/CO/73/UKOT.

<sup>18</sup> Criminal Code §152e(2).

## *Recommendation*

- *A provision allowing for public interest whistleblower protection should be incorporated.*

## **Lack of Adequate Oversight**

The Draft authorizes the Office of the Council of National Security to supervise classification and declassification of the data while most of the tasks are decentralized and much of the specific tasks are given to the state and local bodies.

A particular area of concern is the decentralization of the rules for classification. In Article 16, each state, regional and local body adopts their own “Rule Book on Criteria for Determining Security Levels”. The bodies have only 60 days to create these Rule Books following adoption of the law which then must be approved by the Office. This is likely to lead to very inconsistent development of rules. Many will be overly restrictive unless central rules are developed which receive input from experts and also the public.

A better approach is to ensure that independent bodies outside the intelligence and defense services also have oversight of the system. There is a growing recognition that these bodies provide the most effective means to ensure a balanced classification policy. Of particular importance is the ability of the bodies to order declassification.

- In the United States, the Information Security Oversight Office, a division of the National Archives, has extensive powers including implementing directives, instructions and regulations; inspections and general oversight; security education and training; receiving and taking action on complaints, appeals, and suggestions from persons inside or outside the executive branch; statistical collection, analysis and reporting; acting as a spokesperson for government security policy; conducting special studies and projects; recommending policy changes to the President; and convening and chairing interagency meetings to discuss matters.<sup>19</sup> The Public Interest Disclosure Board can recommend the declassification of any information based on a request from a Member of Congress.
- In other places, the information commissioners have been given power to declassify information. In Slovenia, the Access to Public Information Act was amended in 2005 to give the Information Commissioner the power to review information to see if it has been improperly classified. 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 secrets.

Another missing area is any public accountability of secrecy. In the United States, the Information Security Oversight Office collects statistics on the classification and declassification of information each year and presents a public document on the amount of classification and its estimated costs. The document provides an important role in the public debate over the system.

---

<sup>19</sup> ISOO Homepage: <http://www.archives.gov/isoo/>

### *Recommendations*

- *The role of the Office of the Council for National Security should be strengthened to ensure adequate oversight and consistency in rules.*
- *All rules and regulations on classified information should be published and subject to review and comment by experts and the public before adoption.*
- *Statistics on the amount of information classified and declassified and costs should be published annually.*
- *An independent information commission should be created to oversee access to information and review decisions on declassification.*

## **Conclusion and Recommendations**

The current Draft fails to meet its stated goals of adopting “the modern standards of data secrecy in the EU and NATO countries and in other developed democratic countries”. It provides for overbroad protections for information, creates unnecessary new categories, fails to effectively limit the time information can be classified, does not recognize public interest or whistleblowers, and provides for little oversight. Instead of giving effective protection to classified information, it tips the balance towards excessive secrecy. The Draft should be revised in consultation to ensure that access to information is not unnecessarily restricted.

### *Recommendations*

- *The designation of classified information should not apply to criminal investigations, science, research, technology, economy or finance unless it directly affects the national security of the nation.*
- *The restricted information category should only apply to specifically designated NATO, EU national security or related received information and should not apply to domestic purely national information.*
- *The Criminal Code should be amended to ensure that it only applies to those who have a direct legal obligation not to disclose information due to their position or employment.*
- *Information should be reviewed yearly to ensure that it is still necessary to be classified. When it is no longer necessary, the information should be sent to the National Archive for public release.*
- *The duration of the categories should be set accordingly to their sensitivity.*
  - *Top Secret – 10 years*
  - *Secret – 5 years*
  - *Confidential – 2 years*

- *Restricted – No Time*
- *The maximum number of extensions of classification should be limited in law. Additional justifications should be required for any extensions.*
- *Any remaining files from pre-democratic governments should be declassified and released.*
- *The categories of information that cannot be classified should be expanded.*
- *A test should be incorporated to ensure that information is released when there is a public interest even if it is properly classified.*
- *A provision allowing for public interest whistleblower protection should be incorporated.*
- *The role of the Office of the Council for National Security should be strengthened to ensure adequate oversight and consistency in rules.*
- *All rules and regulations on classified information should be published and subject to review and comment by experts and the public before adoption.*
- *Statistics on the amount of information classified and declassified and costs should be published annually.*
- *An independent information commission should be created to oversee access to information and review decisions on declassification.*