MEMORANDUM

on

The Bulgarian Law on the Protection of Classified Information

by

ARTICLE 19
Global Campaign for Free Expression
London
October, 2001

Introduction

The Bulgarian authorities have prepared a draft Law on the Protection of Classified Information largely as a result of their desire for Bulgaria to join the NATO defence alliance. A programme to promote membership in NATO was put in place after Decision of the Council of Ministers No. 192 of 17 February 1997 on Full Membership of NATO, and progress on preparation of a classification law started in 1999. The law, originally prepared during the previous government, has now been adopted by the Council of Ministers and is expected to go before Parliament shortly.

This follows on closely, and indeed partly overlaps with, the preparation and passage of a Freedom of Information Law, adopted in the summer of 2000. One of our concerns is that this as yet fledgling law could be largely undermined by an excessively broad classification law, particularly given the climate of secrecy that still pervades in Bulgaria. Indeed, we question why a secrecy law has been developed separately from the freedom of information law when it would have been more logical and more open to develop these systems together, as has been done in other democratic countries, such as South Africa and the United States. In these countries, secrecy is established as part of the regime of exceptions to the right to obtain information, rather than as an independent system.

This Memorandum sets out our main concerns with the draft Classification Law, in particular as they affect freedom of expression and information, and official openness. We have not commented on various aspects of the draft law that may affect other

human rights. Our comments are based on the draft received by ARTICLE 19 in October 2001. This Memorandum also sets out in brief various international standards relating to freedom of information. For more detail on these standards and their implications for legislation, please refer to our website.[1]

Our specific concerns fall into two main categories. First, the scope of classification under the draft law is potentially extremely broad, far beyond what is necessary to protect legitimate secrecy interests. Second, the procedures under the law, for example to ensure that documents are properly classified, could be substantially improved.

International and Constitutional Standards

International Guarantees of Freedom of Expression

There can be little doubt about the importance of freedom of information. During its first session in 1946, the United Nations General Assembly adopted Resolution 59(1) which stated:

> Freedom of information is a fundamental human right and… the touchstone of all the freedoms to which the UN is consecrated.

In ensuing international human rights instruments, freedom of information was not set out separately but as part of the fundamental right of freedom of expression, which includes the right to seek, receive and impart information. The Universal Declaration of Human Rights (UDHR) is generally considered to be the flagship statement of international human rights, binding on all states as a matter of customary international law. Article 19 of the UDHR guarantees the right to freedom of expression and information in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The International Covenant on Civil and Political Rights (ICCPR), a legally binding treaty which Bulgaria ratified in 1970, guarantees the right to freedom of opinion and expression in very similar terms to the UDHR, also in Article 19. The European Convention on Human Rights, which is also binding on Bulgaria, protects the right to freedom of expression and information at Article 10. These guarantees allow for some restrictions on freedom of expression and information but only where these are prescribed by law, pursue a legitimate aim and are necessary in a democratic society to protect that aim.

Standards Relating to Freedom of Information

[1] At www.article19.org.

Numerous official statements have been made to the effect that the right to freedom of expression includes a right to access information held by public authorities. The right to information has also been proposed as an independent human right. Some of the key standard setting statements on this issue follow.

The UN Special Rapporteur on Freedom of Opinion and Expression has frequently noted that the right to freedom of expression includes the right to access information held by public authorities. He first broached this topic in 1995 and has included commentary on it in all of his annual reports since 1997. For example, in his 1998 Annual Report, the UN Special Rapporteur stated:

> [T]he right to seek, receive and impart information imposes a positive obligation on States to ensure access to information, particularly with regard to information held by Government in all types of storage and retrieval systems….[2]

In November 1999, the three special mandates on freedom of expression – the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression – came together for the first time under the auspices of ARTICLE 19. They adopted a Joint Declaration which included the following statement:

> Implicit in freedom of expression is the public's right to open access to information and to know what governments are doing on their behalf, without which truth would languish and people's participation in government would remain fragmented.[3]

Similarly, in October 2000, the Inter-American Commission on Human Rights approved the Inter-American Declaration of Principles on Freedom of Expression,[4] the most comprehensive official document to date on freedom of expression in the Inter-American system. The Principles unequivocally recognise freedom of information, including the right to access information held by the State, as both an aspect of freedom of expression and a fundamental right on its own:

> 4. Access to information held by the state is a fundamental right of every individual. States have obligations to guarantee the full exercise of this right. This principle allows only exceptional limitations that must be previously established by law in case of a real and imminent danger that threatens national security in democratic societies.

Within Europe, the Steering Committee for Human Rights of the Council of Europe has set up a Group of Specialists on access to official information, which is expected to finalise a draft recommendation on access to information shortly. The draft will then be forwarded via the Steering Committee to the Committee of Ministers for adoption.[5] The European Union has also recently taken steps to give practical legal effect to the right to information. The European Parliament and the Council adopted a

---

[2] Report of the Special Rapporteur, *Promotion and protection of the right to freedom of opinion and expression*, UN Doc. E/CN.4/1998/40, 28 January 1998, para. 14. These views were welcomed by the Commission. See Resolution 1998/42, 17 April 1998, para. 2.

[3] 26 November 1999.

[4] 108th Regular Session, 19 October 2000.

[5] Draft Recommendation No R (…)… of the Committee of Ministers to member States on access to official information, elaborated by the DH-S-AC at its 7th meeting, 28-30 March 2001.

regulation on access to European Parliament, Council and Commission documents in May 2001.[6] The preamble, which provides the rationale for the Regulation, states in part:

> Openness enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and accountable to the citizen in a democratic system. Openness contributes to strengthening the principles of democracy and respect for fundamental rights….

The purpose of the Regulation is "to ensure the widest possible access to documents".[7]

These international developments find their parallel in the passage or preparation of freedom of information legislation in countries in every region of the world. Most States in Europe now have freedom of information legislation on the books with the passage by the United Kingdom, in November 2000, of the Freedom of Information Act, 2000. In Asia, a Freedom of Information Bill is currently before the Indian Parliament and draft legislation has been or is being prepared in Pakistan and Nepal. Freedom of Information laws or codes have been passed in Hong Kong, Japan, the Philippines, South Korea and Thailand and bills are being presented in Taiwan and Indonesia. Similar developments are taking place in Africa and South America.

National Security and Secrecy

An authoritative statement of the principles relating to national security restrictions for reasons of secrecy are set out in the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, adopted in October of 1995 by a group of experts in international law and human rights convened by ARTICLE 19 and the Centre for Applied Legal Studies of the University of the Witwatersrand. The *Johannesburg Principles*, which are based on international law, evolving State practice, and the general principles of law recognised by the community of nations, outline the prevailing standards for withholding information in the name of national security. The standards set out in these principles have in some cases been directly confirmed by cases at the European Court of Human Rights.[8]

The *Johannesburg Principles* recognise that the right to seek, receive and impart information may, at times, be restricted on specific grounds, including the protection of national security. However, national security cannot be a catchall for limiting access to information. A number of the *Johannesburg Principles* are relevant to the issue of classification laws, including the following:

> **Principle 2: Legitimate National Security Interest**

---

[6] Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.
[7] *Ibid*., Article 1(a).
[8] See, for example, *The Observer and Guardian v. United Kingdom*, (*Spycatcher* case), 26 November 1991, 14 EHRR 153 and *Incal v. Turkey*, 9 June 1998, Application No. 22678/93.

(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

(b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Principle 15: General Rule on Disclosure of Secret Information

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Principle 16: Information Obtained Through Public Service

No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Constitutional Guarantees

The right to freedom of expression is also protected by Article 39 of the Bulgarian Constitution, which states:

(1) Everyone shall be entitled to express an opinion or to publicise it through words, written and oral, sound or image, or in any other way.
(2) This right shall not be used to the detriment of the rights and reputation of others, or for the incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of enmity or violence against anyone.

Article 40 of the Constitution provides special protection for freedom of the media while the right to freedom of information is explicitly protected by Article 41, stating:

(1) Everyone shall be entitled to seek, obtain and disseminate information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality.
(2) Citizens shall be entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or official secret and does not affect the rights of others.

Scope of Secrecy

The Categories Set out in the Law

Section 31 of the draft Classification Law sets out four categories of secret information, the first three of which are State secrets and the last of which is official secrets. These categories are as follows:

- top secret (State secret)
    - where unauthorised access would extremely seriously jeopardise sovereignty, independence, territorial integrity or foreign policy and international relations, or could entail the threat or fact of irreparable or extremely serious harm to national security, defence, foreign policy or the protection of the constitutional order;
- secret (State secret)
    - where unauthorised access would seriously jeopardise sovereignty, independence, territorial integrity or foreign policy and international relations, or could entail the threat or fact of hardly reparable or serious harm to national security, defence, foreign policy or the protection of the constitutional order;
- confidential (State secret)
    - where unauthorised access would jeopardise sovereignty, independence, territorial integrity or foreign policy and international relations, or could entail the threat or fact of harm to national security, defence, foreign policy or the protection of the constitutional order; and
- restricted (official secret)
    - where information is classified as such by State authorities or local self-government.

Section 31(4) also provides for a fourth category for information classified as an official secret to the extent required by a corresponding interest protected by law.

Section 28 sets two conditions on State secrets. First, they must relate to matters found in the list contained in Schedule 1. Second, access must "jeopardise or harm" the interests of the Republic of Bulgaria relating to national security, defence, foreign policy or the protection of the constitutional order.

The provisions on official secrets are supplemented by Section 29 which provides that official secrets are classified information where unauthorised access would "affect adversely" the interests of the State or would prejudice another interest protected by law. Subsequent sub-paragraphs of Section 29 provide that categories of official secrets shall be established by the Council of Ministers for the State government sphere and by the Head for the respective "organizational entity" (including departments, local governments and various other public entities).

Under this scheme, a classification of top secret, secret or confidential requires the showing of a reasonable degree of harm, as required under international guarantees of freedom of expression. This requirement is also found in the law and practice of many democratic States, including members of NATO. In the US, for example, information may only be withheld for reasons of national security where the information "reasonably could be expected to result in damage to the national security and the

original classification authority is able to identify and describe the damage."[9] Furthermore, for State secrets, only information relating to matters listed in Schedule 1 may be classified, although there are serious problems with this list (see below).

The standards relating to a classification of restricted or otherwise as an official secret are far less stringent. It may be noted that this level of classification does not exist in many other countries, including the United States. Sweden permits only one level of classification, namely secret. For an official secret, the body only needs to consider that unauthorised access would lead to an "adverse effect", hardly a stringent standard. Furthermore, the categories of legitimate interests are not set out in law and, for organisational entities, it is the body which holds the information which is to set out these categories. In practice, this effectively allows these bodies to classify at will. It is true that classification at this level only lasts for 2 years but this is sufficiently long to undermine the right to freedom of information and presumably "sensitive" documents, for example revealing corruption or incompetence, could simply be reclassified.

Schedule 1: The List of State Secrets

Concerns about the extent of classification under the draft law are considerably heightened by the scope of the List of Information Classified as State Secret in Schedule 1. It is no exaggeration to say that the 107 items listed in this document are sufficiently broad to cover practically any document a public body might hold. The approach taken here may again be contrasted with that of the United States, where there is a very short list of categories (only seven items). There are a number of specific problems with the items on this list.

Excessive Breadth

Many of the items in Schedule 1 are absurdly broad. Restrictions on freedom of expression must be necessary, which implies that they do not go beyond what is required to achieve the legitimate aim. Excessively broad restrictions fail to meet this standard. A few items serve to illustrate this problem (the list here is by no means comprehensive).

> **No. 10** Summarised data on the imports and exports of weaponry, combat material and munitions for the needs of the armed forces.

At least some information concerning the procurement and/or sale of arms, munitions and other military hardware should be made available to the public and the media. Otherwise, military spending and sales would provide fertile grounds for corruption.

> **No. 72** Data concerning staff issues at the security services and public order services, except for the data contained in the Law on the Budget.

[9] Executive Order #12958, at §1.2.

The public is entitled to know how the security services and public order services, which include the police, are organised and staffed. This provision would, for example, allow the authorities to withhold information about the overall number of police officers employed.

> **No. 96** Research particularly essential to the interests of the national economy and assigned by ministries and other State authorities.

Again, this is a matter of public spending where in many, if not most, cases there will be no warrant at all for withholding this information from the public. Often, such research must be made public if it is to have any positive impact on the economy. This provision would include, for example, research on better farming methods, which obviously needs to be widely disseminated.

Void for Vagueness

A number of items on the Schedule 1 list are extremely vague. Vague provisions fail to meet the standard that restrictions on freedom of expression must be prescribed by law. In particular, vague provisions are not sufficiently clear that individuals know what is prohibited. Again, the following list is illustrative rather than comprehensive.

> **No. 33** Information on the budget funds and State-owned property allocated and made available for special purposes.

It is quite unclear what "special purposes" means.

> **No. 38** State, provincial and municipal economic mobilisation programmes.

It is difficult to interpret the term "economic mobilisation programme" clearly. Would this, for example, include any programme for rejuvenating the economy, which could include training programmes, back to work programmes and so on (where secrecy is totally unwarranted) or does it refer only to macro-economic policy?

Repetitive, Inappropriate or Circular

Several of the items listed in Schedule 1 are repetitive, inappropriate or circular. For example Items **Nos. 25, 26** and **32** all refer to classification of information on the "operational" and/or "organisational" activities of the Security Service. Items **Nos. 36** and **107** both classify information exchanged between Bulgaria and international organisations or States, the only difference between them being that the first addresses information marked as "Top Secret" and the second with information marked as "Secret".

> **No. 80** Detailed information on the activities planned, carried out or completed in the context of pre-trial proceedings, where its disclosure might impede the proper progress of criminal prosecution.

Information concerning everyday criminal proceedings is not normally considered a State Secret (a category reserved for data harmful to national security or foreign policy), and rules relating to criminal procedure are usually found in the criminal code.

Several items include a reference to material already classified, for example as Secret or Top Secret. This is clearly a circular way of defining a State secret. Examples include items **Nos. 23, 24, 36, 48, 49** and **82**.

The Lack of a Public Interest Override

The draft Classification Law does not include a provision allowing for classification to be overcome in the public interest. This is a crucial element in any freedom of information system since it is almost impossible to frame exceptions in sufficient detail to cover all possible situations. The public interest override plays a key role in ensuring that information of importance reaches the public. As the ARTICLE 19 Principles note:

> Even if it can be shown that disclosure of the information would cause substantial harm to a legitimate aim, the information should still be disclosed if the benefits of disclosure outweigh the harm.[10]

Recommendations:

- the classification category of official secret, or restricted, as provided for in Sections 31(3) and (4), as well as in Section 29(2), (3) and (4), should be abolished; alternately, the test of harm for official secrets should be strengthened and a list of relevant categories should be provided in a schedule to the law;
- Schedule 1 should be completely reworked to incorporate the following:
  - the number of items on the list should be significantly reduced;
  - all excessively broad and/or vague items should either be removed or amended; and
  - all repetitive, inappropriate and circular items should be removed; and
- the draft Classification Law should incorporate a public interest override.

Procedural Protections

Pursuant to Section 34(1) of the draft Classification Law, documents are assigned a classification by the individual entitled to sign off on the document. This classification cannot be downgraded or removed without that person's consent, or the consent of his or her supervisor (Section 34(6)). Pursuant to Section 38, the individual who assigned the original classification must review it regularly, at least once every two years, but in the absence of reclassification documents are, pursuant to Section 37, presumed to remain confidential for the following periods:

- top secret: 50 years;

[10] *The Right to Know: Principles on Freedom of Expression Legislation* (ARTICLE 19: London, 1999).

- secret: 25 years;
- confidential: 5 years; and
- restricted: 2 years.

Each "organizational entity" is required to appoint an authorised information security officer, who is responsible for ensuring that the level of classification is correct (Article 24(1)(10). Furthermore, the National Information Security Authority (NISA) is required to provide "methodological guidance" to these information officers (Article 22(5)).

These provisions do provide some procedural means to ensure that documents are properly classified but these protections do not go far enough, given the importance of this matter. In particular, leaving classification up to the discretion of individuals, and then effectively giving those same individuals a veto over reclassification fails to provide safeguards against mistaken, or even abusive, classification. This may be contrasted with the approach in other countries, including the United States, where those who classify are required to get it right and their decisions are subject to full judicial review. The system in Sweden is even more open. There, documents may be marked secret, but this has no formal bearing on an information request; the regular freedom of information process must be followed.

Furthermore, while regular review of classification is to be welcomed, the secrecy periods are excessively long. It would be better if documents were subject to presumptive declassification, for example every 10 years as is the case in the United States, subject to the classifying authority showing a need for further classification.

To combat the prevailing culture of secrecy and to help expose wrongdoing, secrecy laws should provide protection to whistleblowers, individuals who release information on wrongdoing, as long as they acted in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrongdoing. Wrongdoing for these purposes should include the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body. Protection should also be afforded to those who release information disclosing a serious threat to health, safety or the environment, whether linked to individual wrongdoing or not.

Recommendations:

- the authorised information security officer should be able to amend classifications originally assigned to ensure appropriate and consistent classification;
- classification should be subject to full judicial review, in camera if necessary;
- there should be a presumption that even secret and top secret material is subject to declassification within a relatively short time period, say 10 years, although this may be overridden where necessary; and
- the law should provide protection for whistleblowers.