MEMORANDUM

on

Moldova's Draft Law on State Secrets

London
November 2008

ARTICLE 19 · 6-8 Amwell Street · London EC1R 1UQ · United Kingdom
Tel +44 20 7278 9292 · Fax +44 20 7278 7660 · law@article19.org · http://www.article19.org

TABLE OF CONTENTS

About the ARTICLE 19 Law Programme

The ARTICLE 19 Law Programme advocates for the development of progressive standards on freedom of expression and access to information at the international level, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation. These publications are available on the ARTICLE 19 website: http://www.article19.org/publications/law/standard-setting.html.

On the basis of these publications and ARTICLE 19's overall legal expertise, the Law Programme operates the Media Law Analysis Unit which publishes a number of legal analyses each year, commenting on legislative proposals as well as existing laws that affect the right to freedom of expression. The Unit was established in 1998 as a means of supporting positive law reform efforts worldwide, and our legal analyses frequently lead to substantial improvements in proposed or existing domestic legislation. All of our analyses are available online at http://www.article19.org/publications/law/legal-analyses.html.

If you would like to discuss this Memorandum further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at law@article19.org.

SUMMARY OF RECOMMENDATIONS

Key Recommendations:

- In case of inconsistency between secrecy provisions, including in the State Secrets Law, and access provisions, particularly the Law on Access to Information, the latter should prevail. Language should be added to either the State Secrets Law or the Law on Access to Information to this effect.
- Private parties should not be required to classify the information they create and hold, outside of cases where they are bound to do this under a contractual relationship with the public sector.
- The types of information that are subject to classification, as provided for in Article 7, should be defined more precisely and should exclude broadly defined terms.
- The harm test used for classification should be made more stringent. Only information the disclosure of which can seriously undermine national security should be subject to classification.
- The Law should include a public interest override, allowing for the disclosure of information when the public interest in disclosure outweighs the potential harm from disclosure.
- The duration of classification should be shortened from the current maximum of 25 years.
- The Law should provide for regular review of classified materials within a shorter period of time than the current five years.
- The Law should provide protection to whistleblowers who act in good faith and with a reasonable belief that the information was substantially true and disclosed
- Pubic authorities, their staff and persons specially authorised to have access to information should bear sole responsibility for protecting State secrets.

INTRODUCTION

This Memorandum analyses the draft Law of Republic of Moldova on State Secrets (the draft Law), which has been passed at the first reading by Parliament.[1] The aim of this Memorandum is to assess the draft Law against international standards on freedom of expression and information, with a view to promoting a law which is as far as possible in line with those standards. Our comments make particular reference to Moldova's treaty obligations under the *International Covenant on Civil and Political Rights* (ICCPR) and the *European Convention on Human Rights* (ECHR), both of which have been ratified by Moldova. A summary of international standards relevant to the draft Law is provided in Section Two of this Memorandum.

The draw Law raises concerns in regard to the overly broad definition of State secret, which includes information created and held by private parties. The classification regime is exceedingly broad and makes possible for information which has no a direct connection with national security, such as economic, scientific or pubic administration-related information, to be classified as State secret. Moreover, the harm test used for classification level is very weak and the duration for classification is quite long. The draft Law does not include a public interest override and fails to provide protection to whistleblowers. These shortfalls pose a very substantial threat to the right to information and expression.

1. ANALYSIS OF THE LAW

1.1. Overview

The draft Law consists of 40 articles divided into 8 Chapters. Chapter I contains a number of general provisions, including the definitions found in Article 1 and the list of responsibilities of State bodies regarding secrets found in Article 5. Chapter II delineates the categories of information which may be subject to classification, while Chapter III defines the secrecy levels and the procedure for classifying information as a State secret. Chapter IV regulates the manner in which State secrets should be held, while the protection of State secrets is addressed in Chapter V. Chapter VI deals with controls over the protection of State secrets and Chapter VII provides for liability for violating the State secrets law. Lastly, Chapter VIII contains final provisions relating to the coming into force of the law.

1.2. Relationship with the Access to Information Law

The draft Law defines "state secrets" and different categories of State secrets in unduly broad terms, with the effect that a wide variety of types of information may be classified as State secrets (described in more detail below). This would appear to be in conflict with

[1] The analysis is based on an unofficial English translation of the Law. ARTICLE 19 accepts no responsibility for errors based on inaccurate or mistaken translation.

the right to information recognised by both the Constitution of Moldova[2] and the Moldovan Law on Access to Information 2000. It is a matter of some concern that the draft Law has no provisions to address the inevitable conflicts with the law on access to information.

We note that the in better systems, a request for information may be denied only if it falls within the scope of an exception specifically listed in the access to information law. The regime of exceptions in the access to information law should be comprehensive and not be permitted to be extended by classification laws. In accordance with this, in a number of countries, access to information laws supersede secrecy laws, so that in case of conflict the access law prevails. This is the case, for example, in countries like India,[3] Pakistan[4] and South Africa[5].

Even where this is not the case, classification itself is often regarded simply as an internal information management system. In this case, when a request for information is made, the mere fact of classification does not mean that the request will be denied. Rather, the question will be whether or not the classification is correct, in accordance with the rules in the access and secrecy laws.

Recommendations:

- In case of inconsistency between the secrecy law and the access to information law, the latter should dominate. Language should be added to this effect to either the draft Law or the Law on Access to Information Law.
- Mere classification of information should not be regarded as sufficient to deny a request for information. Rather, the issue should be whether the information has been appropriately classified.

1.3. Scope of the Draft Law

Overview

Article 2 of the draft Law provides that the legal framework for State secret protection applies to both national and foreign citizens and stateless persons, as well as to information that is considered secret by a foreign State or international organisation. Article 10(2) obliges legal entities that carry out activities by using information defined as State secrets, together with the beneficiary of those activities, to develop a list of information that is to be classified, setting the level and terms of its classification as secret.

[2] Article 34.
[3] Freedom of Information Act, 2002,
[4] Freedom of Information Ordinance, 2002, Ordinance No. XCVI of 2002, 27 October 2002.
[5] Promotion of Access to Information Act, Act No. 2, 2000.

According to the procedure for classifying information as secret set out in Article 12, officials within public authorities and 'other legal entities' are required to undertake preliminary classification of information as secret in case this cannot be determined though the detailed lists of information that is to be classified, as provided for in Article 10.

Article 16 entitles the heads of public authorities that are authorised to hold information defined as a State secret to decide on classification of information that is the property of legal entities and citizens, if this information falls within the definition of a State secret. Material damage caused to the owner of the information due to such classification is to be compensated by the State.

Analysis

We note with concern that the draft Law applies to information created and held by private persons and entities which have no contractual relationship with the public sector regarding this information. For example, scientific works or scientific research by private individuals or organisations that can serve as a basis for the creation of advanced technologies or new types of production may be subject to classification.[6] We refer to the guidelines of State secret legislation set out by Privacy International, which call on State authorities to distinguish between private and public authors of information and not to classify information created by private parties.[7]

Furthermore, private parties should not be obliged to ensure the preliminary classification of the information created and held by them. This entails enormous administrative resources and imposes a huge burden on them, which may entail criminal liability if not discharged.

Finally, we are concerned about the restriction on the ownership by legal entities and citizens of information classified as secret. The power of the authorities to gain ownership of information created and held by private parties will enable the latter to monitor and control private parties. This is not only a violation of international guarantees of freedom of expression but is also contrary to good business practices and principles of fairness.

Recommendation:

- Information created and held by private parties should not be classified as secret except in cases where this is required by a contractual relationship between the party and the public sector.

[6] See Article 7(2)(f).

[7] Privacy International, *Legal Protections and Barriers on the Right to Information, State Secrets and Protection of Sources in OSCE Participating States*, London, May 2007. Available at: www.privacyinternational.org/foi/OSCE-access-analysis.pdf.

1.4. Restrictions on Access – Classification of Information

Outline
Article 1 of the draft Law defines the term 'state secret' to include "information protected by the state in the areas of its national defence, economy, science and technology, external relations, state security, protection of legal order and activities of public authorities whose unauthorized disclosure or loss can harm the interests and/or the security of the Republic of Moldova." Article 6 provides that defining information as a State secret should be done in compliance with principles of legality, reason and suitability. Article 7 describes the six categories of information that are eligible to be classified: national defence, economy, science and technology, foreign relations, protection of legal order, and activities of public authorities, as well as the particular types of information in these fields that may be classified. Article 9 gives the government the power to approve the list of information defined as State secrets. This list is to be published in the Official Gazette and can be reviewed "within the possibilities".

Article 11 creates four levels of secrecy: a) "top secret" – a secrecy level assigned to information the unauthorised disclosure of which may produce exceptionally serious damage to the interests and security of the Republic of Moldova; b) "secret" – for information the unauthorised disclosure of which may seriously harm the interests and the security of the Republic of Moldova; c) "confidential" – for information the unauthorised disclosure of which may harm the interests and/or the security of the Republic of Moldova; and d) "restricted" – for information the unauthorised disclosure of which cannot be in favour of the interests and/or the security of the Republic of Moldova, or which may lead to the disclosure of information classified as "top secret", "secret", or "confidential".

Analysis
We welcome the requirement that the list of State secrets must be published in the Official Gazette and be subject to review. This is an important safeguard against arbitrary decisions by officials to create new categories of secret information.

At the same time, there are a number of problems with this classification regime. We are concerned that the list of types of information that can be protected contains broad terms, which makes it possible to restrict access to more information than is necessary. For example, Article 7(1) defines as State secrets in the sphere of national defence "data and geodesic, gravimetric, cartographic and hydrometeorologic characteristics that are important for national defence". The standard should not be whether something is important for defence but whether disclosure of the information would harm national security (or some other legitimate interest). Moreover, Article 7 contains definitions of types of information which are virtually unlimited such as "other methods, forms and means of state secrets protection." A well written law should clearly delineate the types of information that may be protected so that the system cannot be used to restrict information arbitrarily in the name of national security.

Furthermore, the harm test for classification is very weak. International standards do not allow every national security interest to underpin secrecy. We refer to Principle 2 of the Johannesburg Principles, set out in Section II of this Memorandum, which provides that "a restriction should 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 of threat of force, or its capacity to respond to the use or threat of force…." [emphasis added]. A higher threshold should be established to classify information as State secret, even in such important areas as national security. Adequately stringent harm tests are absolutely critical to an appropriate regime of State secrecy. To mandate the withholding of information where disclosure would do no harm makes no sense and is contrary to international standards.

Recommendations:

- The types of information which may be classified, set out in Article 7, should be defined more precisely and should exclude broadly defined terms.
- The harm test used for classification levels should be made more stringent. Only information whose disclosure can seriously undermine a legitimate national security interest should be subject to classification.

1.5. Overriding Public Interest in Disclosure

The Law fails to provide for disclosure when the public interest in disclosure outweighs the State's need for protection. As recognised by the Johannesburg Principles, no person shall be punished for the disclosure of information if "the public interest in knowing the information outweighs the harm from disclosure."[8] This position has been endorsed by the Special Rapporteurs in a Joint Declaration on Freedom of Information and Secrecy Legislation.[9] It is integral to the proper functioning of government that the broader public interest in disclosing the information always be considered. There is often a significant public interest in the disclosure of the information for a wide range of legitimate reasons. For example, public disclosure of information may be necessary in order to bring about reform in State organisations, or to identify wrongdoing or harm. These interests must be accommodated rather than adopting a closed-door attitude to all information which may touch upon confidentiality interests.

We also consider that the public interest override should apply to information about the collaboration of certain public figures with the intelligence services during the communist period. This is significant for making decisions related to voting in democratic elections. In Bulgaria, for example, special legislation ensures that the public

[8] Principle 15.
[9] Joint Declaration by 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 adopted on 6 December 2004 (2004 Joint Declaration). Available at: http://www.cidh.org/Relatoria/showarticle.asp?artID=319&lID=1.

can access information about public figures' collaboration with the former totalitarian secret services.

Recommendation:

- The Law should include a public interest override, allowing for the disclosure of information when the public interest in disclosure outweighs the potential harm from disclosure.
- The public interest in having information about public figures' collaboration with the former communist secret services should override the protection of State secrets.

1.6. Duration

Outline

Article 13 provides that 'top secret' information is classified for up to 25 years, 'secret' information for up to 15 years, 'confidential information for up to 10 years, 'restricted' information for up to 5 years. Information about persons who secretly collaborate or have previously collaborated with bodies which carry out intelligence, counter-intelligence and operative investigation operations may be classified for up to 75 years, regardless of the secrecy level. In exceptional situations, the Inter-departmental Commission for State Secret Protection can prolong the term of classification. Article 18 allows for declassification of information when the factual circumstances mean that further protection of the information as State secret is unreasonable.

Analysis

We commend the draft Law for accommodating the need for the level of protection to change over time and to allow for declassification where appropriate. However, we consider that the proposed duration of classification is too long and note that in many countries the duration of classification is much shorter. For example, the Macedonian Law on Classified Information limits 'state secrets' to 10 years, 'highly confidential' information to five years, 'confidential information' to three years and 'internal' information to two years. In Albania, secrets are limited to ten years under the Law on Classified Information. Privacy International recommends that no information be classified for more than 15 years unless compelling reasons can be shown for withholding it.[10]

Recommendation:

- The maximum period of classification should be shortened, for example to 15 years.

[10] Note 7.

1.7. Bodies Responsible for Classifying Information

Overview
The draft Law grants a number of State bodies powers in relation to the protection of State secrets, including Parliament, the President, the government, central and local public authorities, the Information and Security Service, and the Inter-departmental Commission for State Secret Protection.

Analysis
We note with concern that the draft Law fails clearly to delineate the powers of various State officials and bodies regarding State secrets. For example, Article 5(2)(c) provides that the President "within the scope of his/her competences, exercise *other duties* related to settling problems appeared as a result of classifying, declassifying and protection of information". [emphasis added] Similarly, the government, "within the scope of its competence, fulfils *other duties* in the field of state secrets". [emphasis added] The lack of clarity and overlapping powers with respect to the competence of public bodies risks obstructing the operation of the law and may lead to undue restrictions on the right to information. 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 have stated in a Joint Declaration that secrecy laws should set out clearly the competence of public bodies relating to classification of information.[11]

Recommendation:
- All public bodies with powers and responsibilities in relation to State secrets should have those powers and responsibilities clearly and precisely defined.

1.8. Review of Classification

Article 37 provides that the Information and Security Service shall carry out control over the protection of State secrets by public authorities (inter-departmental control) and legal entities. It is bound to inform Parliament of the findings and conclusions it draws from these activities. The decision to deny access to State secrets is taken by the head of the public authority or other legal entity and should be communicated in written form, and can be appealed in the hierarchically higher institution or court.[12]

While we commend the draft Law for providing for a right of appeal to court against denials of the right of access to information, we are concerned that control over the protection of State secrets is assigned to the security services, which might use their control powers to gather information which they would otherwise need court permission to obtain. Our concern is further heightened by the weak accountability safeguards for the Information and Security Service. For example, the draft Law does not specify the

[11] 2004 Joint Declaration, note 9.
[12] Article 25(2).

regularity of its reporting to Parliament and fails to ensure that the reports will be publicly available.

Article 37 assigns control responsibilities for the protection of State secrets to the heads of public authorities, the information and security service, and heads of the offices of the Parliament and President. Article 10(5) imposes an obligation on the heads of public authorities to review on a periodic basis, at least once every 5 years, the detailed list of information that is to be classified as State secrets to assess the underlying reasons for classifying the information and the secrecy levels assigned.

While a 5-year period for periodic review is not unreasonable, our view is that the time limit should ideally be shorter. We note that in Georgia and Estonia, such reviews are carried out every year,[13] while the Hungarian classification law provides for review every three years and the Bulgarian law every two years. In Sweden, the classification is re-evaluated each time the document is accessed. We note that this does not mean that the information will necessarily be re- or declassified, but merely that the need for classification is assessed more regularly.

Recommendations:

- The system for overseeing protection of State secrets should not be overseen by the security services.
- The Law should provide for a regular review of classified materials within a shorter period of time than every 5 years.

1.9. Whistleblowers

The Law fails to provide protection for whistleblowers, individuals who release classified information in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrongdoing. Protection for disclosure in the public interest should extend to employees who come across protected material that discloses wrongdoing, if they release the information in good faith.

Wrongdoing for this purpose should be defined broadly to 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 granted to those who disclose information relating to a serious threat to health, safety or the environment, regardless of whether the information is linked to individual wrongdoing.

Protection for whistleblowers encourages accountability in the public sector and is fundamental to open and accountable government. The Special Rapporteurs' 2004 Joint Declaration on Freedom of Information and Secrecy Legislation stresses the need for

[13] Note 7.

information 'safety valves' such as whistleblowers and calls for the protection of those who disclose information in good faith.[14] Whistleblower protection is found in access to of information legislation in some countries and is the subject of a special law in others. For example, in Slovenia, the Criminal Code allows for the publication of official secrets when "the intention of publicly disclosing irregularities in the organisation, operations and administration of the office … provided that publication has no harmful effects on the state". In Austria, State secrets are not violated when there is a justified public or private interest.[15]

Recommendation:

- The law should provide protection to whistleblowers who act in good faith and with a reasonable belief that the information was substantially true and disclosed evidence of wrongdoing.

1.10. Criminal, Civil and Administrative Responsibility

Article 38 provides that officials and citizens bear criminal, administrative and disciplinary liability according to the legislation for the infringement of the law.

We observe that the draft Law renders everybody responsible for violations of its provisions. This is not in compliance with the position taken by the Special Rapporteurs on freedom of expression, who declared: "Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately secret information under their control. Other individuals, including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information. Criminal law provisions that don't restrict liability for the dissemination of State secrets to those who are officially entitled to handle those secrets should be repealed or amended."[16] Accordingly, liability in a number of countries is limited to those who have a duty to protect secrets because they are officials or have authorised access. For example, in Georgia, the Law on Freedom of Speech and Expression says that the prohibition on publishing secrets only applies to officials and government employees.[17]

Recommendation:

- Pubic authorities, their staff and persons authorised to have access to information should bear sole responsibility for protecting State secrets.

[14] Note 9.
[15] Note 7.
[16] 2004 Joint Declaration, note 9.
[17] Note 7.

2. INTERNATIONAL STANDARDS

2.1. Freedom of Expression and the Right to Information

Secrecy laws impact both on the right of individuals to express themselves – for example, by placing restrictions on what may be published in the media – and on the right of everyone to access information held by public bodies.

Both the right to freedom of expression and the right to information are well-established in international law. Freedom of expression is guaranteed in Article 19 of the *Universal Declaration on Human Rights* (UDHR)[18], Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR)[19], and Article 10 of the *European Convention on Human Rights* (ECHR).[20] Moldova has ratified both the ICCPR and ECHR.

The right to access information held by public bodies is a fundamental human right recognised in international law as part of Article 19 of the UDHR and ICCPR, which guarantee a right to *seek and receive* information. It is crucial as a right in its own regard as well as central to the functioning of democracy and the enforcement of other rights. Without the right to information, State authorities can control the flow of information, 'hiding' material that is damaging to the government and selectively releasing 'good news'. In such a climate, abuse of power thrives and human rights violations can remain unchecked. Certain types of information whose disclosure would harm legitimate interests may be withheld, but only if a number of safeguards, outlined in the next section, are met.

The Charter for European Security of the Organisation of Security and Cooperation in Europe, of which Moldova is a Member State, declared that the public's right to access information and a free media was "an essential component of any democratic, free and open society."[21] In 2001, the Parliamentary Assembly urged participating States to "strengthen their efforts to promote transparency and accountability".

2.2. Restrictions on Freedom of Expression

One of the key issues regarding freedom of expression and information is defining when a public body can refuse to disclose information, or when the exercise of freedom of expression may be restricted. Under international law, freedom of expression may be subject to restrictions in accordance with the requirements stipulated in Article 19(3) of the ICCPR:

[18] *UN General Assembly Resolution 217A (III*), adopted 10 December 1948.
[19] *UN General Assembly Resolution 2200A (XXI),* adopted 16 December 1966, in force 23 March 1976. Moldova ratified the ICCPR in 1993.
[20] *Convention for the Protection of Human Rights and Fundamental Freedoms*, 213 U.N.T.S. 222, in force 3 September 1953. Moldova ratified the ECHR in 1997.
[21] OSCE, Charter for Economic Security, 1999.

> The exercise of the rights [to freedom of expression and information] may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Any restriction on freedom of expression and information must meet a strict three-part test, as recognised by the UN Human Rights Committee. This test requires that any restriction must a) be provided by law; b) be for the purpose of safeguarding one of the legitimate interests listed; and c) be necessary to safeguard that interest.

The first condition is not satisfied merely by setting out the restriction in domestic law. Legislation must itself be in accordance with human rights principles set out in the ICCPR.[22] The European Court of Human Rights, in its jurisprudence on the similarly worded ECHR provisions on freedom of expression, has developed two fundamental requirements. The law must be adequately accessible; individuals must be able to know what the applicable law is. The law should also be formulated with sufficient precision to enable individuals to be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[23] Vague or broadly defined restrictions consequently do not satisfy the "provided by law" criterion.

The second condition requires that legislative measures restricting free expression must truly pursue one of the aims listed in Article 19(3) of the ICCPR, namely the protection of the rights or reputations of others, national security, public order (*ordre public*), or public health or morals.

The third condition means that even measures which seek to protect a legitimate interest must meet the requisite standard established by the term "necessary." This is a very strict test:

> [The adjective 'necessary'] is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable". [It] implies the existence of a "pressing social need."[24]

2.3. Restrictions on Access to Information

International law provides further guidance as to when public bodies may legitimately refuse to disclose information they hold. In accordance with Article 19(3) of the ICCPR, a public body must disclose any information which it holds and is asked for, unless:

---

[22] *Faurisson v. France*, 8 November 1996, Communication No. 550/1993 (UN Human Rights Committee).
[23] *Sunday Times v. the United Kingdom*, 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights).
[24] *Ibid*., para. 59.

1. The information concerns a legitimate protected interest listed in the law;
2. Disclosure threatens substantial harm to that interest; and
3. The harm to the protected interest is greater than the public interest in having the information.[25]

1. Legitimate Protected Interest

Right to information laws should contain an *exhaustive* list of all legitimate interests which may justify a refusal to disclose information. This list should be limited to matters such as law enforcement, the protection of personal information, national security, commercial and other confidentiality, public or individual safety, and protecting the effectiveness and integrity of government decision-making processes.[26]

Exceptions should be narrowly drawn to avoid capturing information the disclosure of which would not harm the legitimate interest. Furthermore, they should be based on the content, rather than the type of document sought. To meet this standard, exceptions should, where relevant, be time-limited. For example, the justification for classifying information on the basis of national security may well disappear after a specific national security threat subsides.

2. Substantial Harm

Once it has been established that the information falls within the scope of a legitimate aim listed in the legislation, it must be established that disclosure of the information would cause substantial harm to that legitimate aim. In some cases, disclosure may benefit as well as harm that aim.

3. Harm outweighs public interest benefit in disclosure

The third part of the test requires the public body to consider whether, even if disclosure of information causes serious harm to a protected interest, there is nevertheless a wider public interest in disclosure. For instance, in relation to national security, disclosure of information exposing instances of bribery may concurrently undermine defence interests and expose corrupt buying practices. The latter, however, may lead to eradicating corruption and therefore strengthen national security in the longer term. In such cases, information should be disclosed notwithstanding that it may cause harm in the short term.

Cumulatively, the three-part test is designed to guarantee that information is only withheld when it is in the overall public interest. If applied properly, this test would rule out all blanket exclusions and class exceptions as well as any provisions whose real aim is to protect the government from harassment, to prevent the exposure of wrongdoing, to conceal information from the public or to entrench a particular ideology.

[25] See ARTICLE 19, *The Public's Right to Know*, Principle 4. Available at: http://www.article19.org/pdfs/standards/righttoknow.pdf.
[26] *Ibid.*

2.4. National Security

The *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* (Johannesburg Principles)[27] were adopted in October 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.[28] They contain a specific set of minimum principles related to restrictions on freedom of expression and the right to information on national security grounds. The Johannesburg Principles have been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and are used as a reference tool by the UN Commission on Human Rights.[29] They 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. The following principles are of particular relevance:

> **Principle 2: Legitimate National Security Interest**
> (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.
>
> **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.
>
> **Principle 12: Narrow Designation of Security Exemption**
> A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.
>
> **Principle 13: Public Interest in Disclosure**
> In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.
>
> **Principle 14: Right to Independent Review of Denial of Information**
> The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for

[27] Available at: http://www.article19.org/pdfs/standards/joburgprinciples.pdf.
[28] For more on the Johannesburg Principles see Toby Mendel, *Johannesburg Principles: Overview and Implementation*. Available at: http://www.article19.org/pdfs/publications/jo-burg-principles-overview.pdf.
[29] See UN Doc. Nos. E/CN.4/RES/2003/42, E/CN.4/RES/2002/48, /CN.4/RES/2001/47, E/CN.4/RES/2000/38, E/CN.4/RES/1999/36, E/CN.4/RES/1998/42, E/CN.4/RES/1997/27 and E/CN.4/RES/1996/53.

information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.