CIDS report No. 1/2017

LIMITS TO THE RIGHT OF FREE ACCESS TO INFORMATION IN THE SECURITY SECTOR

THE CASE OF MONTENEGRO

By

Aleksandra Rabrenović, PhD[1]

Rajko Radević, M.A.[2]

[1] Research Fellow, Institute of Comparative Law, Belgrade.

[2] Doctoral candidate at the University of Ljubljana, International Security Programme; expert on integrity in the security sector and coordinator of the Norwegian Project *Strengthening Integrity in the Defence and Security Sector* in Montenegro.

Limits to the right of free access to information in the security sector – the case of Montenegro

Summary

This paper explores the limits to the right of free access to information in the security sector in Montenegro. The first section of the paper contains an analysis of international standards in the area, with a special emphasis on the method of conducting the *harm test* and the *public interest test* when deciding on requests for free access to information. Particular attention is paid to the analysis of *Global Principles on National Security and the Right to Information*, developed by international experts in Tshwane in 2013 and based on the best arrangements from national legal frameworks and practices. In the second section, the current legal framework governing free access to information in the Montenegrin security sector is analysed along with some problems in its implementation. The last section of the paper includes recommendations for improving the current legal framework governing free access to information in the security sector in Montenegro and its implementation, formulated along the lines of the best relevant international standards.

Key words: free access to information, protection of national security, Tshwane principles, data secrecy, Montenegro.

1. Introduction

The right of free access to public information is one of the key founding principles of all democratic societies. Although it was only recently recognised as a fundamental human right,[3] the adoption and consistent practical implementation of this right significantly contributes to reducing the risk of corruption and other unethical conduct in the public sector. In addition to respecting human rights and freedoms, this principle reinforces the accountability of state authorities and promotes public transparency.

[3] OECD, "The Right to Open Public Administration in Europe: Emerging Legal Standards", *SIGMA Paper* No. 46, 2010, SIGMA publishing.

The right of access to information is, however, subject to certain limitations involving the protection of national security. The option of restricting access to data to protect national security is completely legitimate, but it must be accompanied by defined justification, determined in the national legislation. Nonetheless, the concept of national security most often remains undefined in national legislations,[4] and the concept is differently interpreted across countries. Apart from the term *national security*, other terms are also in use, such as *state security*[5], *public security*[6], *defence*[7], *national interests*[8], *state secret*[9], which makes it even more complicated to establish uniform standards in this field.

In societies in transition, and even in mature democracies, striking a balance between free access to information and protection of national security – the latter most often ensured by classifying data – is frequently a controversial and problematic area.[10] There is an apparent tendency on the part of many state authorities across the world to classify a considerable amount of information due to new or emerging but vague challenges, risks and threats to security, as reflected in the fight against terrorism.[11] Certainly, that objective may be justified, but if used too frequently, in the long term it may undermine the democratic functioning of a society. In fact, historical evidence unambiguously indicates that national interests and security are best protected by the implementation (to the extent possible) of the principle of transparency, i.e. when the public is aware of state activities, including those relative to national security.[12]

---

[4] According to 2013 research on free access to information and protection of national security covering 20 European countries, legal systems in more than half of them contain no definition of national security, *Cf.* A. Jacobsen, *National Security and the Right to Information in Europe*, 2013, University of Copenhagen, Centre for Advance Security Theory, 7.
[5] See the legislation of the Czech Republic, the Netherlands and Russia, *ibid*.
[6] Belgium and Slovenia, *ibid*.
[7] France, Romania and Spain, *ibid*.
[8] Poland and Romania, *ibid*.
[9] Albania and Turkey, *ibid.*
[10] F. Cardona, *Guide to Good Governance No 4: Access to Information and Limits to Public Transparency*, Centre for Integrity in the Defence Sector, 2016, Norwegian Ministry of Defence, http://cids.no/wp-content/uploads/pdf/7933-DSS-Access-to-information-GGG-4-skjerm.pdf, 7 August 2016.
[11] L. Friedman, V. Hansen, "Secrecy, Transparency and National Security", *William Mitchell Law Review*, Vol. 38:5, 2012, 1610-1628.
[12] The Global Principles on National Security and the Right to Information (Tshwane Principles), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf , 7 August 2016.

2. International standards relative to the processing of requests for free access to information – including the *harm test* and the *protection of public interest* test

The right of free access to information is proclaimed in a number of international instruments, which are, however, not yet systematic. Apart from documents of the United Nations[13] and other relevant international legal sources,[14] the Council of Europe has set the most relevant European standards in this area. The European Convention on Human Rights[15] emphasises the right to freedom of expression, and to receive and share information. A particularly important international instrument is the Recommendation of the Council of Ministers to member states on access to official documents of the Council of Europe,[16] as this document lists the best European standards in the area of free access of information.[17] The European Union, too, has dedicated considerable attention to establishing the right of free access to information, by guaranteeing such a right in the Treaty of Lisbon and the Charter on Fundamental Rights.[18]

In spite of the fact that the area of free access to information has developed substantially during the past decades, the international standards in this policy field have yet to be established as a legitimate legal source and have not been generally accepted even by the majority of western countries. After centuries of obscure and opaque practices where concealing information was considered as a source of political power – as is still the case

[13] United Nations, *Universal Declaration of Human Rights, General Assembly Resolution 217 A (III)*, 1948; International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI) of 16 December 1966.
[14] *Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters*, Aarhus, Denmark, 1998; V. A. Knezevic Bojovic, "Free access to informatio of public importance" in A. Rabrenović (ed.), *Legal corruption prevention mechanisms in South East Europe – with a special emphasis on the sector of defence*, Institute of Comparative Law, 2013, 124-127.
[15] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, http://www.refworld.org/docid/3ae6b3b04.html, 30 August 2016.
[16] Council of Europe: Committee of Ministers, *Recommendation Rec(2000)2 of the Committee of Ministers to member states on access to official documents*, adopted by the Committee of Ministers on 21 February 2002,http://www.legislationline.org/documents/action/popup/id/6652, 30 August 2016, hereinafter - CoE Recommendation.
[17] It is also important to mention the Council of Europe Convention on Access to Official Documents, adopted on 18 June 2009, which is yet to enter into force. At the time of writing, (August 2016), the Convention had been ratified by eight countries; ten ratifications are required for its entry into force.
[18] A. Knezevic Bojovic, *op. cit*, 126-127.

in a number of developed and developing countries – it will take time to make a fundamental change in this field and to create a culture of openness and transparency.

The Council of Europe Recommendation on access to its official documents recognises national security as a legitimate reason to limit free access to information.[19] However, it requires that all such limitations – national security reasons included – should be defined in law and be proportionate to the estimated consequences of public access.[20] According to the Recommendation, access to a document may be refused if the disclosure of the information contained in it would harm national security and if there is no overriding public interest in disclosing that information.[21]

Carefully interpreted, the sections of the Council of Europe Recommendation referred to indicate that there are no absolute exceptions to the right of free access to information in any area, including national security and classified information. In any given case it is necessary to assess the risk of harm to a defined interest if the information is disclosed. This means that access to a document may not be limited *a priori* on the grounds of its classification – there must be a specific assessment of whether the information it contains would harm or might harm the interest of national security, or whether there is an overriding public interest in making the information publically available.[22] This is also the reasoning of the European Court of Justice when it interprets exceptions to free access to information, including those related to the protection of national security.[23]

Quite often, relevant practice poses a challenge regarding how to provide guarantees that public authorities will conduct a risk assessment in each individual case in order to determine exceptions to the right of free access to information, particularly in the security sector.[24] There are two types of risk assessment democratic states may apply and which

[19] Part IV of the CoE Recommendation.
[20] Part IV item 1 of the CoE Recommendation.
[21] Part IV item 2 of the CoE Recommendation.
[22] Part IV of the CoE Recommendation on limitation to free access to information, item 2.
[23] Opinion of Advocate General Maduro in Joined Cases C-39/05 P and C-52/05 P, Sweden and Turco v Council (2007), Section 32.
[24] OECD, "The Right to Open Public Administration in Europe: Emerging Legal Standards", *SIGMA Paper* No. 46, 2010, SIGMA publishing.

would ensure additional guarantees for the protection of transparency and the general public interest. The purpose of such assessment is to reduce the opportunity for an authority to abuse the right to refuse access to information, without a valid reason for such refusal. The two risk assessments in question are the *harm* and *public interest* tests.

The *harm test* means that public authorities are obliged to assess whether disclosure of any requested information would harm a certain (previously clearly stated) protected interest, in our case the protection of national security. Most frequently, limitations to the general principle of transparency are explicitly stated in the law, for example, that "free access to information shall be refused if the disclosure of such information would endanger the interest of national security (…)".[25] If a public authority determines that disclosure of information would directly endanger national security, the principle of secrecy will outweigh that of free access. At the same time, however, public authorities frequently have no obligation to assess whether the public's right to know should be considered more important; they simply judge whether access to certain information would damage the protected interest. That is insufficient. If public authorities conclude that disclosure would endanger what is determined to be "national interest", they have to do more than merely state a conclusion. They should be required to provide a justification which clearly argues that under the given circumstances *actual* damage might occur, i.e., that their conclusion is not simply based on hypothetical assumptions. Furthermore, it must be demonstrated that there is *a high level of certainty* that such damage would occur.[26] The harm test is stipulated by the legislation in Germany, Finland and Sweden.[27]

In terms of its content, the *public interest test* differs from the harm test, because it provides an opportunity for a public authority to give access to classified or protected (secret) information even if it assesses that the public access might cause damage. The justification for such access would be that there is overriding public interest in disclosure of the information in question. Such a legal provision balances the protection of secret data and the public's right to obtain access to information held by state authorities.

[25] *Ibid,* 24.
[26] *Ibid,* 24-25.
[27] *Ibid,* 26.

Unlike the harm test, the public interest test provides discretionary power to a public authority to make an assessment of, and to balance what is more important in each given case: the principle of transparency, or keeping certain information secret. Ideally, the public interest test should be preceded by the harm test. Public interest tests are carried out in the countries belonging to the so-called Westminster system, such as the United Kingdom,[28] Ireland, Australia, Canada and New Zealand,[29] but also largely in France, Spain[30] and Slovenia.[31] Interestingly, legal systems in certain countries clearly give priority to the public interest (there is a presumption that disclosure is in the interest of the public),[32] while others are somewhat more in favour of withholding information, unless it is evident that the public interest prevails.[33]

3. Global Principles on National Security and the Right to Information – the Tshwane Principles

An important question arising from how to practice the *harm* test and the *public interest* test may be formulated as: how do you assess risks? How may a person processing requests for free access to information, or a person tasked with classifying information, properly assess whether disclosure would harm the interest of national security or whether there is a prevailing public interest in the disclosure of some specific information? Even if such assessments may seem relatively simple on the surface, they are far from being easy in practice.[34] Striving to overcome this predicament, numerous

[28] Information Commissioner's Office, *The Public Interest Test, Freedom of Information Act*, https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf, 15 August 2016.
[29] M. Cook, *Balancing the Public Interest: Applying the Public Interest Test to Exemptions in the UK Freedom of Information Act*, 2003, The Constitution Unit, https://www.ucl.ac.uk/spp/publications/unit-publications/97.pdf, 15 August 2016.
[30] *Ibid*, 29.
[31] N.P. Musar, "Weighting Test with Emphasis on Public Interest Test in Accessing Information of Public Character", *Slovenian Law Review Podjetje in delo*, Ljubljana, Gospodarski vestnik 2005, Vol. 31; No. 6/7, 1694-1706.
[32] Such as the legislation of the United Kingdom and Australia. See M. McDonagh, "The Public Interest Test in FOI Legislation", 9-10, http://www.right2info.org/resources/publications/eu-mcdonagh-maeve-the-public-interest-test-in-foi-legislation, 10 August 2016.
[33] Such as the legislation of Ireland, Canada and New Zeland. *Ibid*.
[34] J. Vasiljević, "Implementation of the Law on Free Access to Information of Public Importance, the Law on Personal Data Protection and the Information Secrecy Law", in S. Gajin, G. Matić (ed.) *Implementation of the Information Secrecy Law – the ten most significant obstacles*, OSCE, CUPS, 2014, 79-91.

international organisations have contributed to better regulations in this area, in order to reduce the scope for misjudgement or a very strict interpretation.

An important instrument aimed at providing more detailed guidelines is the document *Global Principles on National Security and the Right to Information*, also known as the Tshwane Principles.[35] This document focuses on national security as a reason to deny the right of free access to information, but it also suggests that all reasons for such denial should be in accordance with the conditions the document specifies.[36] The Tshwane principles are based on international, regional and national recommendations and regulations, as well as best relevant practices.

The Tshwane Principles repeatedly highlight the need for a narrow interpretation of protection of national security. First of all, only those public authorities with exclusive power to protect national security should use this reason as a ground to reject disclosure of the requested information.[37] In addition, no item of information should be withheld on account of national security if the public authority is unable to prove the following: that limitation to public access is (1) prescribed by law and (a) the need of a democratic society (b) the necessity to protect legitimate national security interests, and (c) the law provides adequate guarantees against misuse. Furthermore (2), there should be an effective supervision of the validity of such limitations by an independent body along with full judicial protection.[38]

One of the key principles in the Tshwane document is the ninth principle since it provides a more detailed definition of the type of information that public authorities are entitled to withhold in order to protect national security. This definition facilitates the application of

[35] The Global Principles on National Security and the Right to Information (Tshwane Principles),https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf , 7 August 2016, hereinafter: Tshwane Principles.
[36]The document is a direct outcome of work of numerous organisations and academic institutions, over 500 experts from more than 70 countries and 14 meetings held across the world. The process reached its culmination at the final assembly in Tshwane in South Africa, held in June 2013, which is how the document was named.
[37] Principle 1, item d) of Tshwane Principles: Right to information.
[38] Principle 3 of Tshwane Principles: Requirements for restricting the right to information on national security grounds.

the harm test and covers the following types of information: a) information about current plans, operations and capabilities at a time when such information is used operationally; b) information about the production, capabilities or the use of weapons systems or other military systems, including communications systems; c) information about specific measures to safeguard the state territory, critical infrastructure or national institutions against threats, use of force or sabotage, the effectiveness of which depends on secrecy; d) information pertaining to, or derived from the operations, sources and methods of intelligence services, insofar as they concern national security matters; and e) information about national security matters supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; other diplomatic communications insofar as they concern national security matters.[39] In addition to the above-mentioned requirements, the Tshwane Principles also specify that good practice involves establishing an exclusive list of categories of information in the national legislation that are narrowly defined. As a minimum, they should be described at the same detailed level as listed above.[40]

The Tshwane Principles also specify the categories of information in which there is a high probability that the public interest will prevail over the protection of national interest.[41] These categories facilitate the application of the *public interest test* and include the following information: a) violations of international human rights and humanitarian law; b) safeguards regarding the right to liberty and security of persons, the prevention of torture and other ill-treatment, and the right to life; c) government structures and the power of government, including, among other things, information about the existence of all defence and security authorities, their legal regulations, and information needed for the assessment of and control over the expenditure of their budget funds; d) decisions to

[39] Principle 9 item a) of Tshwane Principles: Information that legitimately may be withheld.
[40] Principle 9 item b) of Tshwane Principles: Information that legitimately may be withheld. Under this document, states have the liberty of adding categories of information to those listed above, but only when these categories are clearly and narrowly defined in the law and as such necessary for the protection of legitimate national security interests. When proposing additional categories, states should explain how the disclosure of information in such categories would harm the national security. See Principle 9 item c) of Tshwane Principles: Information that legitimately may be withheld.
[41] Principle 10 of Tshwane Principles: Categories of information with a high presumption or overriding interest in favour of disclosure.
[41] *Ibid.*

use military force or acquire weapons of mass destruction; e) information about the security sector's financial management, including any information that might enable the public to understand the manner in which security sector funds are spent, such as the planned budget and end-of-year financial statements on the execution of the budget, financial management and public procurement rules, etc.; g) public health, safety and the environment.[42]

Finally, the third section of the Tshwane Principles (principles 11-17) thoroughly addresses the rules for classification and declassification of documents. These principles particularly emphasise the obligation of public authorities to state clearly and unambiguously the reasons for classification. Such reasons should belong to the category of information previously mentioned in the ninth principle; apart from that, there should be a description of the harm that might occur if such information is made public, including the level of seriousness and degree of likelihood of negative consequences. Classification levels should correspond with the likelihood and level of harm identified in the explanation, that is, the decision made by public authorities to retain secrecy. Classified information should be marked appropriately and the duration of classification should also be indicated.[43]

Principle 13 deals with the classification procedure, which is only to be carried out by authorised persons. According to that principle, persons empowered by law to classify information should delegate their powers to a limited number of their immediate subordinates only in order to make the classification procedure efficient.

Finally, Principle 15 highlights the obligation of each public authority to establish and make public a periodic review and a detailed and accurate list of the classified information it holds.[44] Principle 17 defines the procedure for declassification of information, which should be regulated in the national legislation. In that regard, particular attention should be given to the process of declassifying information of public

[42] *Ibid*.
[43] Part III.A of Tshwane Principles: Rules regarding classification and declassification of documents.
[44] Principle 15 of Tshwane Principles: Duty to preserve and manage information.

importance.[45] Declassified documents should also be proactively disclosed and made publicly accessible.[46]

4. Free access to information of public importance in the security sector in Montenegro – the current situation

In Montenegro, the right of free access to information is guaranteed in the Constitution and through separate legislation. Article 51 of the Constitution states the right of free access to information of public importance with regard to information held by public authorities and institutions that exercise public powers; it also defines the exceptions to this right and lists the protection of national security and defence as one justification for such exceptions.[47] The right of free access to information is further elaborated in the Law on Free Access to Information, adopted in 2012.[48] This law is a revised version of the first Montenegrin Law on Free Access to Information from 2005.[49]

The 2012 Law on Free Access to Information has significantly improved the general legal framework governing this area.[50] Even if it lists several categories of information with limited public access (security protection included),[51] it also provides reinforced guarantees for the review of exceptions to the right of free access to information. In February 2013, the Personal Data Protection Agency was granted the power to decide in the second instance on requests for free access to information, except in cases of classified information – that category remains exclusively in the hands of the Administrative Court.

---

[45] Principle 17 of Tshwane Principles: Declassification procedures.
[46] *Ibid.*
[47] Article 51, Section 1 and Section 2 of the Constitution of Montenegro, *Official Gazette of Montenegro,* 1/2007, 38/2013.
[48] The Law on Free Access to Information, *Official Gazette of Montenegro*, 44/12, came into force on 17 February 2013.
[49] Law on Free Access to Information, *Official Gazette of Montenegro* 68/05.
[50] The Law on Free Access to Information is aligned with relevant international standards in the following aspects: it requires no justification for a request for free access to information, the time limit within which institutions are to provide the requested information is 15 days and access is free of charge (obligation to cover certain costs of the applicants). The new law has also improved the system for the protection of the right of free access to information by imposing an obligation on the Personal Data Protection Agency – body independent from the executive power – to oversee and protect free access to information; this power was previously given to the Ministry of Culture.
[51] Article 14 of the Law on Free Access to Information, *Official Gazette of Montenegro* 44/12, dated 9 August 2012.

When deciding whether information – classified or not – should be made public under the Law on Free Access to Information, it is mandatory to conduct the harm test in all cases involving protection of security.[52] The harm test is to be conducted by persons deciding whether to grant or deny access to information, and they can deny access only when disclosure of such information would substantially endanger national security. This procedure complies with Recommendation R (2002)2 of the Council of Europe Committee of Ministers and the Tshwane Principles, as it implies that initial classification of data should not be considered an automatic reason for denying disclosure. Instead, the risk and "balance of interests" should be assessed on a case-by-case basis.

Despite the fact that the Law on Free Access to Information clearly provides for an obligation to conduct harm tests and to balance the different interests concerned in a decision to disclose or not to disclose information in the field of national security,[53] the other critical item of legislation regulating this area, the Information Secrecy Law,[54] fails to define such an obligation. The Information Secrecy Law makes no reference to the free access to information principle as regulated by law, which could also be interpreted as exempting classified information from the scope of those regulations. Nevertheless, according to the Administrative Court case law, public authorities are obliged to conduct harm tests whenever classified information is involved,[55] which is a step in the right direction.

Once a harm test is completed, employees processing requests for access to information are obliged to assess whether disclosure of such information would cause damage that is more important than public access to the particular information concerned – the *public interest test*. The Law on Free Access to Information defines a list of cases in which there is an overriding interest of public access – corruption, suspicion of criminal offence,

[52] The single exception to the mandatory harm test is the field of personal data protection, Article 16, Section 1 and 2 of the Law on Free Access to Information.
[53] Article 16 of the Law on Free Access to Information.
[54] Information Secrecy Law, *Official Gazette of Montenegro*, 14/08, 76/09, 41/10, 40/11, 38/12, 44/12.
[55] See the Ruling of the Administrative Court no. U 307/2016 of 8 February 2016.

illegal receiving or spending of public funds, endangerment of public safety, life, public health, and the environment.[56] In these cases, public officials are to supply the applicant with the requested information without delay.

The existing legal framework in Montenegro contains no detailed instructions on how to conduct harm tests and public interest tests when information concerning national security is involved. There is neither a methodology nor examples of situations in which a public authority is entitled to withhold information. The Tshwane Principles, on the other hand, address both the methodology and provide examples. More detailed instructions in this area would be helpful for the authorised Montenegrin officials when assessing whether disclosure of requested information would imply damaging consequences. If the answer is affirmative, regulations should include instructions on how to assess whether the consequences should be considered more relevant than the interest of public access to the information in question. Without thoroughly developed instructions, authorised officials are faced with the very complex task of explaining the rationale behind their decision and in justfying the existence of a defined interest that gives good reason for withholding the information.

According to the Information Secrecy Law, only persons authorised to classify data may declassify them before the expiry of the set classification period, which is in line with the Tshwane Principles. It is, however, problematic that such declassification depends on the approval of the head of the public authority concerned. [57] This statutory provision means that the declassification procedure is centralised at the highest organisational level and consequently, bottlenecks in decision-making are created. This problem is particularly visible in Montenegro's current environment where public authorities tend to classify a large number of documents as *Restricted.*[58] Even if this is the lowest level of classification, it involves an equally complicated declassification procedure as for documents with much higher classification.

[56] Article 17 of the Law on Free Access to Information.
[57] Article 18, Section 2 of the Information Secrecy Law, "Official Gazette of Montenegro" 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14.
[58] Interview with representatives of the Agency for Personal Data Protection and Free Access to Information, 24 May 2016.

Amendments to the Information Secrecy Law of 2012 have introduced a new overall system for the classification of information that is fully in compliance with international standards. In addition, they ensure an automatic equivalence between the old and the new classification system.[59] Under Article 85, information originally classified as *state secret* becomes *top secret*; *official secret* or *military secret-highly confidential become secret*; *official secret* or *military secret-confidential* become *confidential*, while *official secret* or *military secret-internal* are equivalent to *restricted*. Article 85, Section 2, however, further specifies that in the case of use of data inherited from the previous system of classification, each item of information is to be reclassified under the new rules with new and equivalent categorisation (for example, a separate classification for each paragraph in the text). This means that the entire document must be assessed in accordance with the new system of classification.

Compulsory periodic reviews of classification levels have also been introduced; such a provision is in line with the Tshwane Principles. The reviews are to be managed by a commission established within each separate authority, and authorised officials receive proposals for changes in the classification level or for declassification of information from their commission. According to the Law, a decree should have been adopted by the Government to regulate in more detail the criteria for categorisation of data as *top secret*, *secret* or *confidential*. Such a decree was drafted; however, the idea was abandoned since it would include some new detailed criteria in addition to those already specified by the Information Secrecy Law.

The Ministry of the Interior (MoI) has set up a commission for periodic review of classified information; its duty is to examine information classified as *top secret*, *secret*, *confidential* and *restricted* in accordance with the new classification criteria specified by the Information Secrecy Law.[60] The commission was established in September 2015 and

[59]Information Secrecy Law, "Official Gazette of Montenegro" 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14.
[60] The Information Secrecy Law sets out the following criteria for classification of information: *a top secret* classification shall be applied to classified information the disclosure of which would do irreparable

since then, classification levels of some 600 classified items of information have been examined in the light of the new legal requirements. However, the work is still ongoing. This activity is in line with the *Action Plan for the Implementation of the Strategy against Corruption and Organised Crime*, which provides for mandatory compiling, publishing and updating of a list of declassified information with a view to strengthening transparency, and to promote a culture of openness in public affairs.[61] The MoI's procedures are consistent with the Tshwane Principles.

Contrary to the Action Plan for the Implementation of the Strategy against Corruption and Organised Crime, however, the MoI's list of declassified information remains unavailable to the public.

There has been a slight increase in the number of requests for free access to information submitted to MoI; the vast majority of these requests have been granted while the remaining requests relate to classified information for which access have been rejected. In 2014, the number of requests for free access to information amounted to 404, of which 388 (or 96%) were granted. As few as five requests (1%) were rejected, on the grounds that the information requested was classified. In 2015, MoI received 579 information requests, 516 (89%) were granted, 40 (2%) were forwarded to the competent authority, and four requests (1%) were rejected due to classification.[62] Contrary to popular belief, requests for free access to information largely come from citizens wishing to learn more about issues in which they are involved. So far, few requests have been submitted by civil society organisations.[63]

---

damage to the security and interests of Montenegro; *a secret* classification shall be applied to classified information the disclosure of which could seriously harm the security or interests of Montenegro; *a confidential* classification shall be applied to classified information the disclosure of which could harm the security or interests of Montenegro; *a restricted* classification shall be applied to classified information the disclosure of which could harm the performance of tasks of a public agency. *Cf.* Article 12 of the Information Secrecy Law.

[61] Directorate for Anti-Corruption Initiative of the Ministry of Justice of Montenegro, Report on implementation level for partly completed and uncompleted measures and activities from the Strategy against Corruption and Organised Crime (2010-2014), Podgorica, December 2015.

[62] MoI, May 2016.

[63] Interview with the MoI officer in charge of free access to information, May 2016.

5. Conclusion

Due to the traditional tendency to shield information related to operational secrecy, the security sector often represents a closed system and, therefore, is vulnerable to unethical conduct. Free access to information promotes democratic transparency and accountability by allowing the public to be informed about public affairs. This strengthens the control of citizens over public institutions, including the security sector. For that reason, the promotion of the principle of transparency in the public sector deserves particular attention.

Rejection of requests for access to information on national security grounds must be based on a strict and narrow interpretation of the legal limitations in order to reduce the risk of potential wrongdoing on the part of the public authorities that the information concerned relates to. In that field, public authorities in any country may significantly benefit from the *Global Principles on National Security and the Right to Information*, also known as the Tshwane principles, as they contain detailed guidelines for the process of decision-making on free access to information in the field of national security.

In Montenegro, the principle of transparency in the security sector has been strongly reinforced by the new legal framework governing free access to information; however, the principle has yet to be internalised. In practice, the implementation still remains inconsistent with relevant international standards, notably because the Ministry of Interior and other public authorities tend to classify most data and are reluctant to declassify documents after having received requests for free access to information.

In order to promote transparency in the security sector in Montenegro, consideration should be given to introducing several steps that may help to remedy the remaining deficiencies:

1) A special methodology should be developed in order to elaborate in more detail how to carry out the harm test and the balance test; such methodology could be used by all public authorities, particularly in cases involving classified information;

2) The obligation of authorised officials to obtain approval from the head of authority when declassifying "restricted" documents should be abolished; the same option should be considered for information classified as "secret" in order to avoid bottlenecks in the decision-making process. The proposed simplification would help foster an organisational culture in which the principle of free access to information is reinforced and has become an integral part;

3) It is necessary to strengthen the competence of officials who are entitled to decide on requests for free access to information and officials authorised to determine the classification level for information that is deemed to be classified. Training on how to conduct the harm test and the public interest test should be part of that;

4) A special methodology should be developed to determine more detailed criteria and to give examples of different levels of data classification. This would facilitate the work of the earlier mentioned commissions that have been established in order to review classification levels, as well as the work of officials who are empowered to classify information;

5) It will be important to establish procedures in order for reports on declassified information to be published on the web pages of the government institution concerned, including the Ministry of Interior.

In summary, the implementation of the above proposals would be a significant step towards increasing public transparency in Montenegro and would strengthen the accountability of Montenegro's public authorities.

The CIDS reports are papers produced by the centre's core staff or associated subject matter experts. The purpose is to make public research, knowledge and in-depth analysis produced in-house that otherwise may go unnoticed. Generally, the reports are posted to www.cids.no (English language versions) or www.sifs.no (Norwegian language versions) and promoted through postings on social media.

The reports in this series are based on studies carried out by the named author, and have been dubject to quality control according to the integrity standards of the Centre for Integrity in the Defence Sector - CIDS.

Any comments should be submitted to us by the address below or by contact details found on the homepages.

CENTRE FOR INTEGRITY
IN THE DEFENCE SECTOR
KONGENS GATE 4
P.O. BOX 890 SENTRUM
0104 OSLO, NORWAY

CIDS