Funded by
the European Union

SOCIAL
JUSTICE
CENTER

National Security, State Secret and Freedom of Information

National Security, State Secret and Freedom of Information

Social Justice Center

2024

This research has been produced with the assistance of the European Union, within the project "Supporting Accountable and Human Rights-oriented Security Sector through Research, Advocacy and Inclusive Dialogue". Its contents are the sole responsibility of Social Justice Center and they do not necessarily reflect the views of the European Union.

Responsible Person for the Publication: Guram Imnadze

Researcher: Mariam Gobronidze

Translator: Mariam Begadze

Cover Design: Roland Raiki

The rule of citation: *Social Justice Center, Mariam Gobronidze, National Security, State Secret and Freedom of Information, 2024.*

Address: Abashidze 12 b, Tbilisi, Georgia
Phone: +995 032 2 23 37 06

www.socialjustice.org.ge
info@socialjustice.org.ge
https://www.facebook.com/socialjustice.org.ge

Contents

"For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, [...] the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained." [1]

US Supreme Court Justice Potter Stewart

The Pentagon Papers Case, 1971

Introduction

Ensuring democratic governance and fundamental human rights is profoundly influenced by the decisions made by the state regarding war, peace, and national security protection. However, an inherent conflict exists between national security concerns and freedom of information standards. On the one hand, public access and transparency of government decisions are vital for upholding democracy and human rights. Access to information not only shields individuals from illegal or improper actions by governments, officials, and private entities but also empowers the public to actively participate in shaping government policy. On the other hand, effective conduct of international relations, military operations, and intelligence activities necessitates a certain degree of secrecy.[2]

National security is not a value in itself but a condition that enables a nation to preserve its core values. In contrast, open government is both a fundamental value and a condition essential to democratic societies. Access to government information is a crucial foundation for freedom of expression, which, in turn, is particularly important for ensuring government accountability.[3] Thus, equating national security with open government overemphasizes the former and undermines the critical scrutiny that must accompany any efforts to restrict free access to information on national security grounds.[4]

As each nation evolves into a technologically complex information society, it becomes increasingly vulnerable to a multitude of unidentifiable sources of hostile actions. Consequently, it is becoming increasingly challenging to distinguish information of genuine national security importance from other types of information, often obscured under the guise of national security. The need for a specialized regime of access to classified information, justified by the protection of national security, is increasingly

---

[1] NY Times v. US, 403 US 713 (1971). For more details, see National Security Archive, The Pentagon Papers Case. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB48/.

[2] See background and rationale in: Global Principles on National Security and The Right to Information ("The Tshwane Principles"), finalized in Tshwane, South Africa, issued on 12 June 2013.

[3] Hitoshi Nasu, State Secrets Law and National Security, The International and Comparative Law Quarterly, Vol. 64, No. 2 (APRIL 2015), p. 369, Cambridge University Press, available at: https://www.jstor.org/stable/24760684, accessed: 15.09.2022.

[4] Thomas S. Blanton, National Security and Open Government In The United States: Beyond The Balancing Test, In "National Security And Open Government: Striking The Right Balance", Campbell Public Affairs Institute - The Maxwell School of Syracuse University, 2003, p. 33.

acknowledged by the majority of states, regardless of differences in their legal systems or socio-economic conditions. Despite the efforts of human rights defenders and civil society organizations to prevent the expansion of exceptions to best practice standards for the protection of freedom of information on the grounds of national security, this approach is perceived as a necessary evil for safeguarding state secrets in the rapidly developing digital age. However, this trend poses the risk of diminishing the quality of access to and use of information in a democratic society.[5] Moreover, the government's unqualified invocation of the national security argument can undermine fundamental institutional safeguards against governmental abuse of public trust, such as the rule of law, judicial independence, legislative oversight, media freedom, and open government.[6]

However, in contemporary reality, where governments possess extensive information about their citizens, (especially those who regularly use public services)[7], the practice of excessive secrecy correlates directly with a decline of public trust in government. In this context, there is a noticeable shift in public opinion: people now expect much greater transparency and accountability from their government than in the past.[8] Therefore, it is imperative to develop new paradigms beyond existing balancing tests. Without such advancements, current security issues will continue to undermine fundamental values and exacerbate the crisis of trust between the public and the executive.[9]

Finding the appropriate balance is further complicated by the fact that, in most countries, courts generally side with the government on security matters (deference - where courts refuse to scrutinize cases in detail due to their perceived lack of institutional competence or legitimacy, results in an unconditional acceptance of executive decisions). Such a deferential stance is reinforced by the legislation of many countries, which establishes exceptions not only to freedom of information but also to the standard evidential rules and the rights of the accused, even if there is the slightest suspicion of risks on the grounds of national security protection.[10]

The purpose of this document is to analyze the conflict between the expanded scope of state secret protection under the national security argument and access to information/public accountability. To ensure that the state security approach does not threaten the development of a democratic society, it is crucial to examine what constitutes secret information, who determines its secrecy, the procedures

[5] Hitoshi Nasu, op. cit., p. 403-404.

[6] See background and rationale in: Global Principles on National Security And The Right To Information ("The Tshwane Principles"), finalized in Tshwane, South Africa, issued on 12 June 2013.

[7] John Wadham, National Security And Open Government In The United Kingdom, In "National Security And Open Government: Striking The Right Balance", Campbell Public Affairs Institute - The Maxwell School of Syracuse University, 2003, p. 76.

[8] Introduction to the White Paper on Freedom of Information, December 11, 1997.

[9] Thomas S. Blanton, National Security And Open Government In The United States: Beyond The Balancing Test, In "National Security And Open Government: Striking The Right Balance", Campbell Public Affairs Institute - The Maxwell School of Syracuse University, 2003, p. 33.

[10] See background and rationale in: Global Principles On National Security And The Right To Information ("The Tshwane Principles"), finalized in Tshwane, South Africa, issued on 12 June 2013.

involved, and the duration of such secrecy. To this end, the document analyzes relevant national legislation and compares it with the international best practices.

Key Findings

- In the contemporary world, states possess vast amounts of information about their citizens and tend to "overclassify" information under the pretext of national security protection.
- The national security argument is often used to restrict access to information that is inherently public but politically damaging to the government.
- According to Georgian legislation, there is no independent body responsible for overseeing classification of information and judicial oversight is insufficient due to the lack of appropriate expertise and a deferential approach.
- The list of individuals with authority to classify information is quite extensive. According to the legislation, the lowest-ranking official with such authority is a unit head, potentially encompassing thousands of public officials, which is particularly problematic in the absence of an effective oversight mechanism.
- Although Georgian legislation requires substantiation of harm when restricting access to information, the degrees of harm defined by the law are vague and inconsistent. Additionally, the legislation does not incorporate an essential component of the harm test—balancing the restriction against other public interests.
- Excessive secrecy poses a risk to the effective protection of important information. Specifically, when there is an abundance of classified information, it becomes challenging to manage and control the necessary protective measures effectively.

1. Freedom of Information and International Standards

"Information is the oxygen of democracy."[11] Thus, the primary purpose of access to information is to promote democratic governance. The right to access state-held information aims to improve governmental operations and enhance its accountability.[12]

One of the principal basis for recognizing this right is internationally articulated in Article 19 of the Universal Declaration of Human Rights, adopted in 1948, which states, that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[13]

The right of access to information, as an element of freedom of expression, is also enshrined in Article 19 of the International Covenant on Civil and Political Rights (ICCPR). In its General Comment 34, adopted in 2011, the UN Human Rights Committee elucidated that Article 19 of the ICCPR encompasses the right to access information held by public authorities. It mandates states to proactively disseminate information in the public interest and to ensure that access is „easy, prompt, effective and practical". The Comment further stipulates that countries should implement "necessary procedures" and adopt appropriate legal norms to realize the freedom of information. Additionally, it clarifies that responses to requests must be timely, authorities must provide reasons for withholding information, and states must establish appeals mechanisms in cases of refusal to disclose information.[14]

Today, freedom of information is recognized as a component of the right to freedom of expression by both official UN bodies and all three major regional human rights systems.[15] Consequently, the essence of freedom of expression encompasses the public's right to unrestricted access to information regarding

[11] The Public's Right to Know: Principles on Freedom of Information Legislation updated (London: 2015), Preface. Available at: https://cutt.ly/kexkC51u.

[12] Hitoshi Nasu, op. cit., p. 388-389.

[13] However, freedom of information legislation has its origins in Sweden, where the world's first Freedom of Information Act was passed in 1766. - see Freedom of Information: Legislation and Practice Georgia, United States of America, United Kingdom/Scotland, Estonia - Comparative Analysis, e. Chabrava, 2012, Available at: https://bit.ly/45n8XbN; One of the most important first steps to strengthen freedom of information at the international level was taken at the first session of the United Nations General Assembly in 1946, when, in the resolution 59 (I) adopted at the session, freedom of information was recognised as a fundamental human right. - Standards of freedom of expression, Tbilisi, 2004, p. 9, Available at: https://cutt.ly/lexkBloL.

[14] International standards: Right to information, Available at: https://www.article19.org/resources/international-standards-right-information/.

[15] Various declarations and recommendations issued by the Committee of Ministers of the Council of Europe, the African Commission on Human and Peoples' Rights, and the Inter-American Commission on Human Rights have also confirmed the right of individuals to access information held in public institutions. These official documents have been accompanied by a noticeable global trend towards the introduction of freedom of information laws over the past decade. See Toby Mendel, National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles, In "National Security And Open Government: Striking The Right Balance", Campbell Public Affairs Institute - The Maxwell School of Syracuse University, 2003, p. 17.

governmental actions taken on their behalf. Without such access, „truth would languish and people's participation in government would remain fragmented".[16]

Despite the international recognition of the right of access to information held by the government, its legal status was not well established until the adoption of the Johannesburg Principles[17] in 1995. Principle 11 of the document, like other international instruments, sees this right as part of the right to freedom of expression. This principle states that access to information may be limited only in accordance with the general three-part test used to limit freedom of expression.[18]

Today, the right to access information is recognized globally, as demonstrated by the rapid increase in the number of countries adopting freedom of information laws. As of 2021, 124 countries have enacted such laws, and additional eight countries have had national ordinances or regulations granting individuals the general right to access information held by public agencies. These laws also obligate public authorities to provide this information in a timely and proactive manner.[19] However, the extent to which these laws adhere to the established standards for restrictions varies significantly from country to country.[20]

In Georgia, the right to access public information is enshrined in the Constitution. Specifically, Article 18 states that everyone has the right to access any information or official document available in a public institution, in accordance with the law.[21] However, similar to international standards, there are exceptions to this provision, whereby certain information may be withheld from individuals or the public.

[16] 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, International Mechanisms for Promoting Freedom of Expression, London, under the auspices of Article 19, 26 November 1999, Available at: https://www.ohchr.org/en/statements/2009/10/default-title-402; In November 1999, 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 met for the first time at the invitation of ARTICLE 19 and adopted a joint declaration. ... Various declarations or recommendations issued by the Committee of Ministers of the Council of Europe, the African Commission on Human and Peoples' Rights and the Inter-American Commission on Human Rights have also confirmed the right of individuals to receive information from public officials. These official announcements have been accompanied by a notable global trend toward the implementation of freedom of information laws over the past decade. For more information, see Toby Mendel, named paper, p. 17.

[17] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1 October 1995, Available at: https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf.

[18] Toby Mendel, op. cit., p. 16.

[19] International standards: Right to information, Available at: https://www.article19.org/resources/international-standards-right-information/

[20] Toby Mendel, op. cit., p. 16.

[21] By adopting the General Administrative Code in 1999, Georgia took an important step towards freedom of information and transparency of public institutions. In particular, the provisions regulating the accessibility of information have expanded even more, because the third chapter of the Code is dedicated to the issue of freedom of information.

2. Exemptions to Freedom of Information

Article 19 of ICCPR, which protects the freedom of information along with the freedom of expression, recognizes that the exercise of the rights carries with it special duties and responsibilities and may therefore be subject to certain restrictions. These restrictions must:

- be provided by law;
- serve for the protection of national security, public order, or public health or morals.[22]

Article 10 of the European Convention on Human Rights contains a similar provision, but it regulates the second criterion somewhat differently while maintaining the requirement of being prescribed by law. According to this provision, restrictions must be necessary in a democratic society for interests such as national security, territorial integrity, public safety, the prevention of disorder or crime, the protection of health and morals, the protection of the reputation or rights of others, the prevention of information disclosure, the preservation of confidential information, or the maintenance of the authority and impartiality of the judiciary.[23]

According to Article 18 of the Constitution of Georgia, a person's access to public information can be restricted if there is at least one of the reasons below:

- Information contains commercial secrets;
- Information contains professional secrets;
- Information is acknowledged as a state secret by law or in accordance with the procedures established by law as necessary in a democratic society to ensure national security or public safety or to protect the interests of legal proceedings.

This document examines the limitations on access to public information, specifically those related to its designation as a state secret, whether by law or through legally established procedures.

2.1. The Standard of Prescribed by Law and the Concept of State Secrets

Under the framework of the ICCPR, restrictions on access to information must satisfy both procedural and substantive criteria. According to the established standards, the procedural aspect involves the imposition of restrictions by law, providing a legal basis for countries to enact state secrets legislation. However, as per the practice of the European Court of Human Rights, the mere existence of such legislation is insufficient to meet this criterion. The legislation must also fulfill qualitative

[22] Hitoshi Nasu, op. cit., p. 389.
[23] See Article 10, Convention is available at: https://cutt.ly/VexkCujN.

requirements. Specifically, the court asserts that laws restricting access to information should be based on the principle of foreseeability and must eliminate any potential for arbitrariness or abuse of power.[24]

The second and more essential criterion is the necessity to restrict access to information. Such an interference with the right must serve a specific purpose; it should be essential for protecting state or public security, as well as the interests of ongoing litigation.

Even in a democratic country, the government must be able to control the flow of information in a manner that is transparent and perceptible to the public. States are empowered, and even obliged, to implement measures ensuring a safe environment for their citizens. Consequently, it is natural for states to classify certain documents and information as "official secrets," as their disclosure could threaten public order and state security. To achieve this objective, states employ specific measures to prevent the disclosure of classified information (preventive measures) and, in the event of a breach, to punish the perpetrators (punitive measures). By safeguarding information critical to national security, states ensure a secure environment for individuals and society.

The term "state secret" is widely used across all countries, yet it remains quite vague, lacking a universally accepted definition. This ambiguity arises from the fact that the concept of state secrets cannot be uniform, as the specific time and context must be considered. Consequently, it must be interpreted in light of contemporary understandings. To this end, the existence of a law on state secrets is essential.[25] In countries where the freedom of information is legally upheld, state secret laws limit this freedom in exceptional circumstances. The legal framework should delineate the elements of state secrets and specify the documents and information that can be classified as such. This ensures the balance between the fundamental rights and freedoms of individuals and state security, thereby providing a basis for the legality and legitimacy of these restrictions.[26]

In Georgia, the law "On State Secrets" regulates the legal relations related to the recognition, classification and protection of information as state secrets. According to the normative act, the definition of state secret has several aspects. Information is a state secret if:

- It concerns the state defense, economy, foreign relations, intelligence, state security, law and order and public safety;
- According to law and/or the procedure established by the international treaty/agreement/, it is subject to advance classification or recognition as a state secret;
- It is subject to state protection;
- Its disclosure or loss may harm Georgia or a party to the international treaty or agreement concluded by Georgia in the contexts of:

[24] Indeed, the fact that there was no legislation in Chile to regulate the issue of limiting access to official information was crucial to the finding of a violation of the obligation of freedom of information by the Inter-American Court of Human Rights in Claude-Reyes et al v. Chile. See at Hitoshi Nasu, op. cit., p. 390.

[25] In countries where freedom of information is constitutionally guaranteed without specific legislation implementing it, the scope of state secrets can be defined by executive orders and court practice. See ar Hitoshi Nasu, op. cit., p. 370.

[26] State Secret As An Instrument To Maintain State Security, Associate Professor Dr. Cemil KAYA, pp. 52-53.

- sovereignty;
- constitutional order;
- political and economic interests. [27]

The concepts of state secrets and national security are interpreted in a problematic manner not only by authoritarian governments, which tend to abuse their powers egregiously and in bad faith. Authorities generally exhibit a tendency to interpret these concepts expansively. At the root of this problem is that national security, unlike other justifications for restricting freedom of information, is inherently political and necessitates threat assessments, frequently from external sources.[28]

The fact that the use of national security arguments by authorities often serves illegitimate purposes, with information being used to conceal illegal behavior or crimes, is a persistent fundamental problem associated with the development of the modern "national security state." As Arnold Wolfers notes, "higher security aspirations make the nation suspicious of hiding more aggressive goals." Paul Chevigny extends this argument, noting that "... the problem with the 'national security state' is that ... it can lead to a repetition of irrational decisions." The executive's broad discretionary powers to control the disclosure of information related to national security can distort public debate on foreign policy and national security issues. The traditional view that the information related to national security is not and should not be a matter of public concern is increasingly untenable. Given that the concept of national security has begun to invade the everyday lives of individuals due to the expanding range of security risks and the evolving nature of security,[29] it is necessary to reconsider this approach.

The UN Special Rapporteur has expressed concern that the widespread practice of classifying information justified on the grounds of national security is particularly problematic in the context of investigating human rights violations. This secrecy can serve as a significant obstacle to establishing facts and ensuring accountability, thereby impeding justice and provision of remedies.[30]

According to the 12th Johannesburg Principle, states should define by law only those specific and narrow categories of information, withholding of which is necessary to protect legitimate national security interests.[31] However, many laws invoke "national security", as a basis for restricting access to information, without clearly defining it and specifying the detailed list of exceptions.[32]

Georgian legislation establishes five broad types of information, which can be categorized as state secrets. These are information concerning:

(1) National Defense;

[27] Law of Georgia "On State Secrets", Article 1, Paragraph 1.
[28] Toby Mendel, op. cit., p. 6.
[29] Hitoshi Nasu, op. cit., p. 398.
[30] F La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc A/HRC/14/23 (20 April 2010) (n 153) para 57.
[31] Toby Mendel, op. cit., p. 16.
[32] Ibid, p. 18

(2) Economics;
(3) Foreign relations;
(4) Intelligence; State security and protection of law and order;
(5) Public safety.

Although the law regulates only general types of classifiable information, the Government of Georgia defines the specific categories of secret information for particular areas through by-laws, more specifically, resolutions.[33] According to the detailed list developed by the government, more than two hundred different categories of information are classified as state secrets.

2.2. The Harm and Balancing Tests

Broad exceptions to access to information imposed by security arguments often raise serious concerns due to the risk of undermining fundamental human rights. This issue is also prevalent in countries with a long history of democracy. The argument of protecting classified information should not be used as a weapon to stifle discussion on important issues. It must be balanced with other significant public interests, such as the free exchange of information, democratic accountability, fair administration of justice, and anti-corruption action.

Excessive secrecy by government agencies has long been recognized as ultimately counterproductive. This approach undermines public trust, particularly when it is employed to support a specific political agenda or to conceal corruption and misgovernance. When the public perceives that the government acts solely in its own interest, its credibility and legitimacy are significantly diminished. Consequently, the government faces substantial challenges in gaining public support for its activities. [34] Therefore, it is crucial to adopt the harm test and the approach of balancing interests to ensure transparency and accountability.

The UN Human Rights Committee, in its interpretation of Article 19 of ICCPR, emphasized that limiting access to information on the grounds of national security requires more than merely asserting a connection to national security. There must also be demonstrable harm resulting from the disclosure of such information. Consequently, the non-disclosure of information—such as "the enactment of laws that restrict the dissemination of public information for other legitimate public interests that do not threaten national security, or the prosecution of journalists, researchers, environmental activists, human rights defenders, or others for disseminating such information"—is inconsistent with the objectives of the Convention.[35]

This approach is reflected in Georgian legislation, which stipulates that the disclosure or loss of classified information must pose a threat to the sovereignty, constitutional order, or political and

[33] Appendix No. 2 of the Resolution No. 507 of the Government of Georgia „On the approval of normative acts related to the implementation of the Law of Georgia „On State Secrets" – „List of information classified as state secrets".
[34] Comments on Draft Law on State Secret of the Republic of Moldova, Commissioned by the Office of the OSCE Representative on Freedom of the Media from Mr. David Banisar, Director, FOI Project, Privacy International 2008, p. 3.
[35] Hitoshi Nasu, op. cit., p. 391.

economic interests of Georgia or a party to the international treaty or agreement concluded by Georgia.[36] Ideally, the harm test involves an assessment of potential harm; however, in practice, this harm is often not specific and therefore, difficult to evaluate.[37] This issue is also evident in Georgian legislation, where concepts such as national sovereignty, constitutional order, and political-economic interests are challenging to define. Consequently, this provision is rather broad, allowing for an extensive and potentially unjust application.

Applying the harm test in practice presents a significant challenge. As noted by the US Public Interest Declassification Board (PIDB)[38] in its report, "[e]stimating the level of harm that could result from an unauthorized release or disclosure of information is often an exercise in speculation and is more of an art than a science, especially when prediction harm is impossible". [39]

The Johannesburg Principle 4 establishes a three-part test for determining exceptions to the right of access to information. According to this test, in addition to the requirement that the information must relate to a legitimate purpose specified by law (such as the protection of national security) and that its disclosure must substantially harm that purpose, it is crucial that the harm caused by disclosure outweighs the public interest in accessing the information. Certain circumstances, such as the presence of corruption, will override the interest in secrecy and necessitate the disclosure of information. Johannesburg Principle 13 further elucidates that the public interest "shall be a primary consideration" when deciding whether to disclose information.[40] This implies that even if disclosure is determined to cause harm, this does not automatically preclude the access to the requested information. There may be instances where the non-disclosure of sensitive information held by public bodies would result in greater harm than its disclosure, such as in cases of environmental disasters or food safety risks.[41] Therefore, even when the disclosure of information may harm legitimate interests under the law, it should still be disclosed if the harm does not outweigh the public interest in accessing the information.

The existence of such a public interest test is essential because it is impossible to narrowly define exceptional cases extending to only the information that should always be considered secret.[42] Therefore, the balancing of interests prevents the automatic classification of such information as secret, which is low-risk information despite being related to one of the basis of classification. This is also confirmed by the practice in Georgia, where merely exceptional grounds and a damage test do not ensure the protection of public interest—specifically, access to public information. Consequently, the absence of a legal obligation to balance interests allows the executive to overuse the practice of information classification.

---

[36] Law of Georgia "On State Secrets", Article 1, Paragraph 1.
[37] Classified Information, A review of current legislation across 15 countries & the EU, Transparency international, p. 24.
[38] For more information about the Council, see: https://www.archives.gov/declassification/pidb
[39] Classified Information, A review of current legislation across 15 countries & the EU, Transparency international, p. 25.
[40] Ibid, p. 18.
[41] Classified Information, A review of current legislation across 15 countries & the EU, Transparency international, p. 26.
[42] Toby Mendel, op. cit., p. 18.

The OSCE Representative on Freedom of the Media (hereinafter referred to as the OSCE Representative) recommended that information of a wide range of public interest should not be classified. In particular, information concerning:[43]

- violation of law or human rights;
- improper administration practices or administrative errors;
- threats to public health or the environment;
- health condition information of the elected high officials;
- statistical, socio-economic or cultural issues;
- core scientific issues;
- issues with important, sensitive content for individuals or organizations;

Georgian legislation shares the OSCE recommendations and regulates this issue in a similar way. It lists in detail the categories of information that cannot be classified as state secrets:[44]

- Information that may violate or limit the fundamental rights and freedoms of a person, his legal interests, as well as harm the health and safety of the population;
- Normative acts, including international treaties and agreements of Georgia, except for the normative acts of relevant agencies related to state interests in the fields of national defense, state security, and law and order, which regulate respective state defense, intelligence, state security, law and order protection, and operational search activities;
- Maps, except for military and special purpose maps, on which information and data related to national defense and state security included in the list of classifiable information are presented;
- Information about natural disasters, catastrophes and other specific events that have occurred or may occur and threaten the safety of the population;
- Information regarding the state of the environment, of the population health, standard of living (including medical services and social security), as well as socio-demographic indicators, education and culture of the population;
- Information about corruption, illegal actions of officials and criminogenic situation;
- Information about the privileges, compensation, monetary rewards and benefits granted by the state to a citizen, official, enterprise, institution or organization;
- Information about the State Monetary Fund and the national gold reserve;
- Information about health status of public and political officials.[45]

[43] OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.
[44] OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.
[45] Law of Georgia "On State Secrets", Article 7.

In addition to assessing harm, the difficulty lies in balancing the harm against the public interest in disclosing state secrets. While the disclosure of information may cause some damage to national security, the severity of this damage must be weighed against the public interest in revealing information about government misconduct or illegal actions.[46] Consequently, exercising the right to access public information necessarily involves value judgments that can sometimes be quite arbitrary. In weighing competing interests, it is crucial to assess what is necessary and proportionate. This arbitrariness is further exacerbated by the vagueness of the concept of "public interest." Furthermore, in many states, the concept of national security encompasses the maintenance of public order and stability. As a result, national security, particularly internal national security, which refers to the protection of public law and order, is often considered the overriding public interest and is interpreted in such a way that it cannot be outweighed by other public interests that necessitate the disclosure of state secrets.[47] This approach is also prevalent in Georgia, contributing to excessive secrecy and undermining the protection of fundamental human rights and freedoms.

3. The Current Policy Regarding State Secrets and the Procedure for Classifying Information as State Secrets

The country's policy on state secrets, integral to Georgia's sovereignty, defense, and national security, is formulated by the Parliament of Georgia. Its implementation is ensured by the state government and municipal bodies of Georgia within the competence granted to them by the legislation of Georgia. The State Security Service is responsible for the organizational and security measures for protecting state secrets and overseeing their control. An exception exists for information under the jurisdiction of the Georgian Intelligence Service, which independently ensures its protection.[48]

The classification of information as state secrets is predicated on its alignment with a designated list of such information. The rationale for designating information as state secrets, considering its significance, is the duty of the state entity, enterprise, institution, or organization (regardless of its legal form) that developed or received the information for review or storage. The authority to classify information as state secrets lies with officials designated by the Parliament, the President, or the government, who are also responsible for maintaining its confidentiality.[49]

The competence of whistleblowers is another fundamental issue. Specifically, it is crucial to determine who should assess the potential harm to national security that the disclosure of information might cause and weigh it against the public interest. As noted, the ambiguity regarding the extent of certain individuals' competence to balance these interests raises concerns. Given that a representative of the executive branch evaluates the potential harm or threat to the national security or public interest from

[46] Hitoshi Nasu, op. cit., p. 392.
[47] Ibid, p. 395.
[48] Law of Georgia "On State Secrets", Article 3.
[49] Law of Georgia "On State Secrets", Article 11.

disclosing information, there is an inherent risk of misusing the law on state secrets. Such a framework provides the opportunity to discourage political activists and civil society who act as observers of wrongful and/or illegal actions of the government.[50]

Given that the list of authorized individuals is extensive, the issue is also pertinent in Georgia. According to the law, the lowest-ranking official with the authority to classify information as confidential is a unit head. This means there could be thousands of civil servants whose competence remains unverifiable, especially in the absence of effective and proactive control mechanisms. This is especially problematic considering the lack of effective and proactive oversight.

4. The Degree of Secrecy of Information Containing State Secrets and the Level of Secrecy

Information deemed a state secret is classified by assigning it a corresponding secrecy stamp. This stamp is a requisite for information containing state secrets and must indicate the degree of confidentiality. Additionally, it must specify the duration of the confidentiality period and identify the authorized individual who issued the classification.

In Georgia, the following classifications of state secrets are established:

- "Of special importance" (equated with TOP SECRET): This classification pertains to information whose dissemination or loss may result in particularly serious consequences the state interests of Georgia in areas such as defense, economy, state security, civil safety, law and order, and politics. It can also cause particularly severe consequences for Georgia's international agreements or for the country or organization participating in such agreements.
- "Completely secret" (equated with SECRET): This category includes information whose dissemination or loss may result in serious consequences for Georgia's defense, state security, civil safety, maintenance of law and order, political and economic interests, as well as the interests of persons defined by law. Additionally, the disclosure of such information may lead to serious consequences for the country or organization involved in an international treaty or agreement with Georgia.
- "Secret" (equated with CONFIDENTIAL): Information under this classification, if disseminated, may harm Georgia's defense, state security, civil safety, law and order, political and economic interests, and the interests of persons defined by law. Furthermore, its disclosure may negatively affect Georgia's international agreements or the interests of countries or organizations participating in those agreements.
- "For restricted use" (equated with RESTRICTED): This designation applies to information whose dissemination may adversely impact Georgia's defense, state security, civil safety,

[50] Hitoshi Nasu, op. cit., p. 397-398.

law and order, political and economic interests, as well as the interests and activities of countries or organizations involved in international treaties or agreements with Georgia.

The composition of severity and probability of harm elements in different countries' state secret laws varies, but each establishes a system in which, the level of protection for classified information aligns with the severity and probability of harm.[51] The Georgian legislation, as detailed in the aforementioned list, primarily bases its assessment rules on the severity of harm. However, international standards necessitate evaluating the second component—the probability of harm—and balancing this potential harm with other public interests, a consideration currently absent in Georgian law.

Another problematic aspect is the vagueness of the terms and definitions used, making it difficult to draw a clear line between the types of secrecy. The legislation employs terms such as "particularly serious consequences," "serious consequences," "harm," and "adversely impact" to determine the degree of harm. These ambiguous definitions complicate the accurate assessment of the degree of harm attributable to the listed categories. For example, when defining the harm for the purposes of criminal law, legislation always uniformly defines the degree of harm (for example, in the case of the crime of damaging health, the categories of particularly serious, serious or less serious harm are defined), or in the presence of other types of harm, the legislation specifies what is considered harm (for example, in the case of significant harm, the legislation specifically defines what constitutes "significant" damage).

For the categories of "special importance," "top secret," and "secret," the law requires the presence of harm to a protected interest in the event of disseminating information. However, the definition for the "for restricted use" category is excessively broad, referring to only a potential negative impact as a criterion for harm. When evaluating a similar provision in Moldovan legislation, the Venice Commission highlighted the norm's vagueness.[52] Furthermore, the existence of the "restricted use" category does not align with the recommendations of the OSCE representative, which suggest that only information of "official importance" or "occupational secrets" should not be classified as state secrets. In turn, the limitations on their disclosure should be governed by access to information legislation.[53]

5. Term of Confidentiality and Periodic Revision and Disclosure

The OSCE representative recommends that information be classified only for a limited period of time: information should be labelled as a state secret only when its disclosure would significantly harm national interests. Such classified information must undergo regular review and include a date after which it will be declassified and made public. [54]

[51] Classified Information, A review of current legislation across 15 countries & the EU, Transparency international, p. 24.
[52] OSCE-Moldova opinion, p. 7.
[53] See OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.
[54] Ibid.

In Georgia, the term of classified status for state secret information depends on its degree of secrecy: 20 years for information of "special importance," 10 years for "top secret" information, 5 years for "secret" information, and 3 years for "restricted use" information. The period of secrecy is calculated from the date the secrecy stamp is assigned.

In matters related to intelligence, counter-intelligence, and/or operational-search activities, the head of the service carrying out these activities has the authority to extend the confidentiality period if the disclosure of information would harm the state interests of Georgia. The extension, modification of classification level, or declassification of secrecy recognized by international treaties and agreements involving Georgia is conducted in accordance with the requirements of these treaties and agreements. After the confidentiality period of other information expires, the Prime Minister or the President of Georgia, within their respective competencies, have the authority to extend this period. This authority grants significant discretion to these officials, as there are no upper limits for the extension of the secrecy term, posing a threat to the freedom of information, particularly in the absence of effective independent oversight mechanisms.

6. Control of Activities Related to Classified Information

An effective system of oversight is particularly crucial in the realm of security, as the services responsible for its protection conduct much of their work in secrecy and, therefore, cannot be readily monitored by the public. The best practice model includes oversight of security services by internal departmental/executive bodies, parliamentary and judicial bodies, as well as independent specialized oversight institutions whose mandates and powers are established by publicly accessible law. An effective security oversight system encompasses at least one civilian institution independent of both the security and intelligence services and the executive branch in general. The functions of these oversight bodies may include all aspects of the security services' activities, including legal compliance, efficiency of activities, financial management, and general administrative practices.[55]

Article 14 of the Johannesburg Principles mandates that states provide appropriate measures for realizing the freedom of information, including the right to review by an independent body and ultimately by a court. The experiences of many countries with constitutional guarantees of access to public information affirm this necessity. Implementing freedom of information requires specific legislation that includes appeal mechanisms.[56]

[55] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight.
[56] Toby Mendel, op. cit., p. 18-19.

According to Georgian legislation, the authorized person or administrative body, or their superior, has the right, both on their own initiative and upon the motivated instruction of the State Security Service of Georgia, to:

- repeal the illegal decision to consider information as a state secret;
- change the degree of secrecy of information containing state secrets.

The court also has the authority to annul illegal and/or unsubstantiated decisions to classify information as a state secret.

Furthermore, state bodies, individuals, and legal entities have the right to appeal the decision on secrecy or declassification of information in accordance with the procedure established by Georgian legislation. They also have the right to submit a reasoned proposal to the authorized person for the declassification of this information. The authorized person is required to consider the proposal and inform the initiator of the decision within one month. These individuals must provide the aforementioned information to the authorized person or institution in a manner that does not harm state secrets or state and public security interests.[57]

6.1. Mosaic Theory and Judicial Oversight

The judiciary serves as the arbiter and assessor of the reasonableness of restricting access to information in a democratic society. In this process, the most important question lies in the following: what are the standards of protection of civil rights and liberties to be applied by courts to evaluate compliance with laws governing the non-disclosure of information?[58]

Critics of judicial review argue that judges often lack the expertise and experience necessary to understand the broader, more complex threats to national security.[59] A practical manifestation of this argument is the "mosaic theory", developed and widely applied in the United States. This theory describes the basic principle of gathering information related to intelligence or other security measures: different elements of information that are of meagre relevance individually and not useful to their owner, when combined with other elements of information can be found to be of additional value and acquire the value for national security. The value of the mosaic thus created surpasses the sum of its individual parts.[60]

---

[57] Law of Georgia "On State Secrets", Article 15.

[58] David E. Pozen, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 YALE L. J., (2005), p. 630-631, Available at: https://scholarship.law.columbia.edu/faculty_scholarship/573

[59] The judiciary is generally considered ill-equipped to evaluate or 'second-guess' the national security significance of certain information. See: Centre for International Environmental Law v Office of the US Trade Representative, 718 F3d 899 (DC Cir, 2013); Meredith Larson v Department of State (n 23) 865; Leghaei v Director General of Security (2007) 241 ALR 141, 147 (Brennan CJ); A v Secretary of State for the Home Department [2005] 2 AC 68 (House of Lords).

[60] See also Michael P. Goodwin, A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts, 32 Hastings Comm. & Ent. L.J. 179 (2010). Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol32/iss2/1

For several decades, government agencies have invoked the mosaic theory to justify classifying the documents, thereby avoiding detailed consideration and justification of their decisions. Following the terrorist attacks of September 11, 2001, the relevance of the mosaic theory increased alongside heightened terrorism threats, leading courts to adopt a more deferential approach. This effectively placed executive decisions to classify information beyond effective judicial oversight.[61] The widespread and almost unchecked use of the theory in the U.S. led to the declassification of more than 14 million new documents in 2003 alone, nearly a 75% increase since 2001.[62]

In the post-9/11 era, amid pervasive fear of terrorism, courts became more accommodating of highly speculative and generalized mosaic arguments from executive agencies, often requiring a lower standard of proof regarding the reasoning, detail, and persuasiveness of these decisions.[63] In the more than 30 years, between the theory's inception and 2005, U.S. courts have rejected a government agency's mosaic arguments only once.[64] The mosaic theory's speculative nature made it effectively unassailable in practice, giving the executive branch greater control over information and compromising government transparency in favor of security. Such an approach is only justifiable in emergency situations.[65]

It is difficult to challenge the highly speculative nature of the mosaic theory argumentatively. The extreme form of the mosaic theory can be described the following way: an unidentified adversary could, at an unspecified time, use this information in conjunction with other unknown information to construct a mosaic that threatens national security in unpredictable ways. Professor Jane Kirtley aptly notes that this theory "is impossible to disprove... because who can say with certainty that it is not true?".[66] Assessing what kind of "reasonably foreseeable" harm might result from disclosure—the legal standard applied by judges when reviewing the classification decisions—becomes particularly problematic within such an ambiguous theoretical construct.[67]

As noted, the theory assumes that it is risky for judges to assess the sensitivity of individual facts because they lack the comprehensive "big picture." While enforcement agencies possess unique knowledge and expertise regarding the negative consequences of disclosure, the courts' deferential approach should not serve as a means to evade responsibility. Courts should fulfill their role as arbiters by assessing the justification of the executive's arguments.[68] However, as the arguments underpinned by the mosaic theory have become increasingly speculative post-9/11, the expertise gap between the government and the courts has widened, complicating judicial consideration of these issues.[69]

---

[61] Ibid, p. 630-631.
[62] Ibid, p. 648.
[63] Ibid, p. 667.
[64] Ibid, p. 679.
[65] Ibid, p. 667.
[66] Ibid, p. 672.
[67] Ibid, p. 672.
[68] Ibid, p. 639.
[69] Ibid, p. 666.

The widespread use of the deferential approach by courts, based on weak arguments, fosters executive opportunism, ignores the issue of burden of proof distribution, disregards legislative intent, and lacks theoretical boundaries and limits. Ultimately, it encourages excessive secrecy practices. Moreover, there is no solid analytical justification for such a narrowing of judicial review based on the mosaic theory.[70] Some believe that agencies invoke the mosaic theory precisely when they recognize the weakness of their case for classifying the document as secret.[71]

Therefore, rather than courts considering mosaic theory arguments with excessive deference, the increased potential for misuse necessitates additional scrutiny and skepticism. The argument that judges lack the "big picture view" to contextualize information and, therefore, cannot perceive the mosaic, oversimplifies and masks the uniquely problematic nature of the issue.[72]

Judges also fear the responsibility for putting the country's security at risk. The highly speculative nature of mosaic theory arguments, which are particularly difficult to assess and vulnerable to abuse, exacerbates this dilemma for judges. One proposed solution is the introduction of non-judicial assistants with national security expertise, such as retired or rotating officials from intelligence agencies who are granted immunity or anonymity. These assistants could aid judges in determining the facts and assessing the credibility of mosaic arguments. Even if courts continue to recognize the risks presented by executive agencies, a specialized mechanism to evaluate mosaic theory arguments could remind them of the theory's potential for fostering excessive secrecy and the real negative consequences of such practices.[73]

Courts should consider both negative and positive mosaic scenarios—society can also create mosaics to respond more intelligently to threats. For example, public knowledge of vulnerabilities in critical infrastructure can lead to better protection schemes and advocacy for their implementation. Similarly, courts should consider not only how information technology can lead to adversarial mosaics but also how the dissemination of information can help prevent such actions. Agencies should use computerized data to process their archives and substantiate the existence of potential mosaics with stronger arguments.[74] Consequently, the disclosure of security-related information does not necessarily increase risks but may even reduce them by informing the public about threats and enabling better-informed responses.[75]

[70] Ibid, p. 668.
[71] Ibid, p. 672.
[72] Ibid, p. 664.
[73] Ibid, p. 678.
[74] Ibid, p. 677.
[75] Ibid, p. 674.

6.2. Specialized Body and Public Control

Georgia lacks a specialized body for monitoring freedom of public information, unlike many other countries, including the USA, Hungary, Serbia, and Slovenia. Such an institution plays a crucial role in mitigating excessive secrecy practices. In Hungary, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information holds the authority to change the classification of state and official secrets. Similarly, in Slovenia, the Information Commissioner is empowered to verify the accuracy of classifications. In the United States, the Information Security Oversight Office (ISOO) possesses independent authority to review classification issues.

The OSCE recommends the establishment of an independent body to ensure openness and exercise oversight. This body should be separate from the intelligence, military, or security services, have access to classified information, ensure the proper operation of the system, receive complaints about improperly classified information, and have the power to review and order the declassification of information.[76] In Georgia, these functions are assigned to the State Security Service, which lacks the critical criterion of independence.

While Georgian legislation incorporates several oversight mechanisms, the effectiveness of these mechanisms cannot be verified due to the secrecy surrounding the cases. Best practices dictate that oversight institutions should possess the authority, resources, and expertise to initiate and conduct independent investigations, as well as full and unimpeded access to necessary information, officials, and facilities. Intelligence services and law enforcement agencies should fully cooperate with supervisory bodies during witness hearings and in obtaining documentation and other evidence. [77]

In the context of ineffective control mechanisms, the active involvement of civil society is paramount. Given the evident conflict between freedom of information and privacy rules, civil society organizations should monitor to prevent the state from unjustifiably restricting the dissemination of information that is not sensitive to national security but is significant and should be freely accessible to citizens.[78] However, this task is virtually impossible without expert knowledge and access to information. As the US Supreme Court Justice Potter Stewart noted, "The only effective check on executive policy and power in the fields of national defense and international affairs can be an educated citizenry—an informed and critical public opinion capable of defending the core values of democratic government."[79]

[76] OSCE-Moldova opinion, p. 14.

[77] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight.

[78] Classified Information, A review of current legislation across 15 countries & the EU, Transparency international, p. 5.

[79] Hitoshi Nasu, op. cit., p. 403-404. Quote from the case - New York Times Co. v. United States, 1971.

Conclusion

The concepts of national security and state secrets are broad and possess a dangerous plasticity. Consequently, there is a constant temptation for the state to invoke security as a pretext to curtail civil liberties. Thus, restrictions on fundamental rights under the guise of national security should be approached with healthy skepticism.[80] This principle extends to the restriction of freedom of information through excessive secrecy. Openness must not only be central to democratic governance values, but security strategies should also acknowledge its significance.

Access to government-held information is essential for accountable and democratic governance. It fosters an informed society, helps control the abuse of power and official corruption, strengthens electoral politics, and establishes accountability and good governance. Therefore, no public institution should be exempt from the obligation to disclose information, even if most of its functions pertain to national security. This principle applies to all branches of government and all governmental functions, including security and defense authorities. Refusals to disclose information must be justified on a case-by-case basis, and restrictions intended to conceal governmental misconduct are never justifiable.[81]

While certain information may be legitimately classified to protect national security or other vital interests, secrecy legislation must precisely define the concept of national security and clearly outline the criteria that determine the scope and extent of information secrecy. This approach helps prevent the misuse of secrecy to withhold information of legitimate public interest. The legal framework should delineate the individuals authorized to classify information and specify the duration for which information remains classified. The adoption of such legislation should be subject to public discussion.[82]

In democratic societies, the conflict between access to information and national security permits the classification of only information that is pertinent to and narrowly tailored to essential national security issues. Thus, any restriction on the right to access information based on national security must undergo strict tests of legality, legitimacy, and necessity. Additionally, it must justify the harm that the disclosure of the information would cause and weigh this harm against the public interest. This requires repealing or fundamentally altering existing rules that allow the government to withhold information without balancing the threat of harm to security against the public interest.[83] Therefore, there should be a presumption of disclosure as a standard procedure, unless there is a strictly defined exceptional case.[84]

---

[80] Thomas S. Blanton, National Security and Open Government in The United States: Beyond The Balancing Test, In "National Security and Open Government: Striking The Right Balance", Campbell Public Affairs Institute - The Maxwell School of Syracuse University, 2003, p. 66.

[81] Principle 4, https://www.article19.org/data/files/RTI_Principles_Updated_EN.pdf.

[82] International Mechanisms for Promoting Freedom of Expression 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, December 2004.

[83] David E. Pozen, op. cit., p. 630-631, Available at: https://scholarship.law.columbia.edu/faculty_scholarship/573

[84] GIPA Act section 3, 5.

Since national security arguments will always be somewhat speculative, in the sense that they describe a potential future harm rather than an actual, already occurring one, it is difficult to exercise effective judicial or other oversight.

In addition, it is important to inform citizens about the norms governing state security and secrecy. Although there is a natural conflict between invocation of the national security argument for classifying information by the government and the public's right to know, a review of recent history clearly demonstrates that legitimate national security interests are, in practice, best served when the public is well informed about state activities, including, what the government is doing to protect national security.[85]

[85] GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION ("THE TSHWANE PRINCIPLES"), finalized in Tshwane, South Africa issued on 12 June 2013.

Recommendations

- The concept of "national security" should be defined with sufficient precision to prevent that chilling effect extends to an overly broad array of information.
- The degree of harm that would result from disclosing information should be strictly defined, minimizing the discretionary power of the executive branch.
- In addition to the harm test, Georgian legislation should incorporate a balancing procedure that evaluates public interests, as a result of which the decision on secrecy should be made considering whether the harm caused by the disclosure of the information outweighs the public good brought by the publicity.
- Legislation should limit the circle of people who have the authority to classify information.
- State agencies must adequately train their personnel, develop, and finance a modern, functional, and effective archival infrastructure.
- To enhance judicial oversight, it is essential for judges to reexamine the deferential approach and critically engage with such issues. To the extent possible, the judiciary should also ensure adherence to the standard of transparency in relevant cases.
- Adoption of a separate provision for the whistleblower protection is essential in order to further strengthen the control of the protection of the right of public access to the information held by the state.
- It is crucial to establish an independent body with oversight powers responsible for ensuring legal publicity in the security sector. This entity must be autonomous from both the security and intelligence services as well as the executive branch as a whole. It should have access to classified information, ensure the proper functioning of the system, have the authority to receive complaints regarding improperly classified information, and review and order the declassification of information by relevant agencies.