

Goran Matic*

*Faculty of Business Studies and Law,
University "Union – Nikola Tesla", Belgrade, Republic of Serbia*

EXCESSIVE SECRECY IN DEMOCRACIES: BUREAUCRATIC REFLEX OR SECURITY ILLUSION? (Translation in *Extenso*)

Abstract

Systematic excessive classification of information within the security apparatuses of the United States, the European Union, and key NATO allies constitutes a structural anomaly within liberal democracies. Through comparative analysis, the article identifies that the principal driver of this phenomenon is the distinction between *security secrecy* (the protection of genuine security capabilities) and *political secrecy* (the protection of institutions from accountability). The research demonstrates that, despite different legal traditions, all examined systems share common structural patterns: *defensive classification* as a risk-minimization strategy, asymmetric incentives that penalize openness, and weak mechanisms of external oversight. The consequences of such practices include erosion of public trust, constrained cooperation within alliances, and reduced effectiveness in decision-making processes. The article concludes that solutions require a paradigm shift – from the logic of the *need to conceal* toward the principle of *the right to know*, grounded in the presumption of openness as the basis of democratic legitimacy. Key operational steps include the introduction of mandatory *sunset* clauses, strengthening the

* E-mail address: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

independence and competences of oversight bodies, and harmonizing standards at NATO and European Union levels to prevent misuse of secrecy for information management rather than security protection.

Keywords: overclassification, secrecy, intelligence community, democratic accountability, right to information, United States, European Union, NATO, comparative analysis.

INTRODUCTORY CONSIDERATIONS

Overclassification is not an administrative error it represents a systemic choice. In democracies founded on the principles of accountability and transparency, the mass designation of documents as “classified”, without clear and verifiable criteria, transforms secrecy from an exception into a rule. The consequence of such practice is not increased security, but weakened oversight and fragmented cooperation among allies.

This paper proceeds from the thesis that overclassification is one of the most serious, yet at the same time one of the least regulated challenges of contemporary security systems. While public and professional debates intensively focus on artificial intelligence, cyber defense, and hybrid threats, the practice of routinely restricting access to information remains largely neglected – even though it directly undermines the democratic values that these states formally uphold.

Before analyzing specific national systems, it is necessary to point to the universal frameworks of international organizations. Although the United Nations do not have a unified classification system, their bodies have, over time, articulated principles balancing security and transparency. The United Nations Educational, Scientific and Cultural Organization (UNESCO) Guidelines on Freedom of Information and National Security (United Nations Educational, Scientific and Cultural Organization 2014) require that every restriction “be lawful, necessary, and proportionate in a democratic society”. The Organization for Security and Co-operation in Europe, in the 1999 Istanbul Document (Organization for Security and Cooperation in Europe [OSCE] 1999), emphasized that secrecy must not serve as a pretext for avoiding accountability.

These universal standards constitute the normative foundation upon which more detailed and operationalized instruments were later built including the Tshwane Principles on National Security and the Right to Information (Open Society Justice Initiative 2013), the Council of Europe Convention on Access to Official Documents (Tromsø Convention 2009), the evaluation mechanisms of the Council of Europe's Group of States against Corruption (GRECO) (Council of Europe 2018), the normative framework of the European Union (EU) in the form of Council Decision 2013/488/EU on the security rules for protecting EU classified information (Decision 2013/488), and the North Atlantic Treaty Organization's NATO Glossary of Terms and Definitions, AAP-06 edition (NATO Standardization Office 2021). The common message of all these instruments is clear: a legitimate security interest must not override democratic requirements of transparency, parliamentary oversight, and public interest. Nevertheless, comparative analysis shows that the gap between normative alignment and operational practice remains the central problem of overclassification in contemporary democracies.

Although practices differ, international and regional frameworks demonstrate coherence in defining the principles of responsible classification. The Council of Europe's Group of States against Corruption has emphasized on several occasions that excessive secrecy undermines anti-corruption mechanisms and oversight, particularly in public procurement and resource management. The NATO Glossary and the EU Security Rules insist on proportionality, justification, and temporal limitation. These standards demonstrate a consensus that secrecy must be the exception, not the rule – a consensus which, as the analysis will show, often remains at the level of theory rather than practice.

At the core of the phenomenon lies the paradox of democracy and secrecy: liberal democracy, as conceptualized by Dahl and Habermas, requires openness as a condition of the legitimacy of political will (Dahl 1989; Habermas 1996). Yet within those systems, apparatuses develop whose functionality rests on controlled closure creating tension between the right to know and the need for secrecy (Fenster 2006). Secrecy within intelligence institutions is not merely

a procedural tool, but becomes part of organizational culture a “basic assumption” shaping the identity of services and the behavior of their members (Schein 2010). In this way, secrecy transforms from a technical choice into a normative imperative, creating conditions for systemic excess.

The analysis encompasses three analytical levels: the United States of America, as a global hegemon with the most developed intelligence-security apparatus; the EU as a supranational entity with layered and fragmented secrecy regimes; and three European states – the United Kingdom, France, and Germany – characterized by different approaches to secrecy, ranging from the British “culture of service” to the German legacy of the Stasi, the principal secret intelligence service of East Germany.

The theoretical framework combines the theory of bureaucratic behavior (Wilson 1989), which emphasizes the selection of minimum-risk strategies, and the theory of democratic accountability (Fenster 2006), which insists that secrecy must constitute an exception rather than a rule in the functioning of democratic institutions. Additionally, the paper relies on critical literature on the phenomenon of the “Leaky Leviathan” (Pozen 2013) and the institutional dynamics of overclassification (Aftergood 2023).

The methodological approach is based on comparative case analysis and includes consideration of the following materials: official reports of the U.S. Government Accountability Office (GAO), the European Ombudsman, and the German Bundestag’s Parliamentary Oversight Panel (*Parlamentarisches Kontrollgremium – PKGr*); relevant academic literature by authors such as Steven Aftergood and David E. Pozen; research projects of the National Security Archive at George Washington University; as well as analysis of key affairs such as the Pentagon Papers, the Snowden affair, and cases concerning the German Federal Intelligence Service (*Bundesnachrichtendienst – BND*).

The structure of the paper follows the logic of systematic comparison: the second chapter is devoted to the analysis of practice in the United States, the third to the EU, the fourth presents a comparative analysis of the three selected European states, while the fifth chapter

offers a synthetic conclusion on possible paths toward establishing accountable transparency.

The research focuses exclusively on the comparative analysis of the systems of the United States, the EU, and key NATO allies. The system of classified information protection in Serbia is not the subject of this paper.

Although NATO is mentioned in the title and in the broader context of the paper as a framework for the sharing of classified information among Western democracies, the paper does not analyze its classification system (e.g., AAP-06, Cosmic Top Secret). The reason is methodological: NATO does not possess its own intelligence capacities nor does it produce original classified information, but rather acts as a mechanism for the exchange of information generated at the national level. Accordingly, overclassification in the NATO context reflects the practices of member states, primarily the United States, the United Kingdom, France, and Germany – which are covered by this analysis. Additionally, NATO standards, including the principles of *need-to-know* and *need-to-share*, have already been incorporated into national systems and the EU framework; therefore, examining them through the prism of member states provides an adequate analytical insight into the functioning of secrecy within the Transatlantic Alliance.

Within the discourse on excessive secrecy, three approaches can be distinguished. The first, critical, characteristic of civil society organizations and right-to-information actors, focuses on abuses and consequences for transparency and democratic control. The second, defensive, characteristic of governmental bodies and security structures, proceeds from the need to preserve existing practices and emphasizes the risks that reducing secrecy could pose to security, stability, or international obligations. The third, academic, adopts a neutral position: through analysis of the normative framework, comparative practice, and implementation, it seeks to identify systemic weaknesses and possibilities for improvement.

This paper belongs to the third, academic approach. Its objective is not to take sides in existing controversies, but to offer an analytical framework that enables understanding why problems in the field of

classified information protection recur, how different approaches shape practice, and in what manner a more functional balance between security, accountability, and public interest may be achieved.

The title of the paper poses a dilemma: is overclassification the consequence of a bureaucratic reflex – a rational but narrowly instrumental response to perceived risks – or a security illusion: a strategy that conceals political opacity, avoidance of accountability, and the management of public perceptions under the pretext of national security? The analysis demonstrates that these two options are often inseparable in practice: the bureaucratic reflex becomes the mechanism through which the security illusion is produced and maintained. When fear of error, career risk, and institutional inertia are systematized as a “minimum-risk strategy”, secrecy ceases to be a technical measure and becomes an instrument of information control rather than of security protection.

THEORETICAL PARADIGMS: SECRECY BETWEEN SOVEREIGNTY AND THE DEMOCRATIC EXCEPTION

Before undertaking a comparative analysis of national systems, it is necessary to clarify the theoretical dilemmas concerning the relationship between secrecy and democracy. The paradox of liberal democracy lies in the need for openness as a source of legitimacy, but also for secrecy as a condition for the functionality of security apparatuses (Dahl 1989; Habermas 1996). This relationship can be understood through two opposing theoretical traditions.

The sovereignty paradigm – from Jean Bodin to Carl Schmitt – treats secrecy as an attribute of sovereign authority. In Bodin’s view, sovereignty implies the capacity of the state to decide independently on matters of vital importance, including the right to withhold certain information from the public domain. Schmitt radicalizes this relationship with the claim that “sovereign is he who decides on the exception” (Schmitt [1922] 2005). The exception operates outside procedures of publicity and transparency, thereby making secrecy a precondition of extraordinary decision-making. In contemporary

security states, this logic is institutionalized: the executive retains control over classified information on the assumption that secrecy is a condition of effective action in crisis situations.

The democratic paradigm is grounded in Habermas's principle that the public sphere constitutes the basis of democratic legitimation of authority. Public debate and access to information enable control of political power and transform "narrative power" into "discursive accountability" (Habermas 1996). Secrecy is not the rule, but a deviation that requires strictly limited justification. Within a democratic order, it is permissible exclusively as a controlled and temporary departure for the protection of a specific and legitimate interest. The problem arises when the exception becomes the rule, and the public sphere a secondary value.

From a legal perspective, secrecy is neither a peremptory norm (*ius cogens*) nor an absolute right of the state. It is an exception to the rule of transparency, but one strictly regulated by law. Secrecy constitutes a form of administrative discretion with clearly established legal limits. Authorities must ensure that every decision on classification is: 1) reasoned, 2) based on an assessment of harm, 3) time-limited, and 4) subject to review. This framework, shared by the Tshwane Principles (Open Society Foundations 2013) and the Tromsø Convention, forms the normative foundation of responsible classification.

A key analytical distinction lies in differentiating between the protection of genuine security capacities (security secrecy) and the "protection of institutions from accountability" (political secrecy). The former refers to safeguarding actual security capabilities (sources, methods, operational plans, cyber defense), while the latter serves to shield institutions and officeholders from accountability, oversight, or public criticism. The theoretical thesis emerging from this distinction is that overclassification is often a political, rather than a security, problem. It results from the expansion of the exception and asymmetries of power within institutions, rather than from an excess of security caution.

This distinction becomes particularly relevant when analyzing patterns of overclassification. In practice, political secrecy manifests

through: 1) the mass designation of entire documents as classified even though only a portion is sensitive; 2) retroactive classification after information has already entered the public domain – as a form of ex post censorship; 3) the preservation of “obsolete secrets” without regular risk review; and 4) the expansion of the concept of “national interest” to commercial or administrative data. These patterns, though differently formalized, are recognizable across systems – from the US to Germany – indicating a structural dynamic rather than isolated institutional errors.

Contemporary security frameworks increasingly question the traditional *need-to-know* model as the exclusive guiding principle. In an era of hybrid threats, mass surveillance, and complex challenges, this restrictive approach reveals its limitations. Consequently, the *need-to-share* principle is being affirmed – the idea that information should be made available to subjects who can effectively apply it for collective defense, even if they were not directly involved in its production. This evolution does not represent opposition, but rather an upgrade: the *need-to-know* principle protects against misuse, while *need-to-share* ensures efficiency and resilience. This dichotomy is institutionalized in the EU Security Rules and in the NATO Glossary of Terms and Definitions, AAP-06 edition, where both approaches are presented as complementary principles.

This theoretical framework represents an analytical “map” for examining concrete systems. It enables a distinction between legitimate security secrecy and political misuse, identification of the moment when the “exception” becomes the “rule”, and assessment of whether secrecy functions as an instrument of protection or of control. Equipped with these conceptual tools, the analysis turns to a comparative consideration of three levels: the US as a global paradigm, the EU as a supranational experiment, and key NATO allies with their differing traditions. This dichotomy is particularly relevant in the context of allied organizations such as NATO, where the principles of *need-to-know* (protection against information leakage) and *need-to-share* (ensuring collective defense) exist in constant tension. The NATO Glossary of Terms and Definitions, AAP-06 edition, explicitly recognizes this dichotomy, yet practice demonstrates that technical

standards alone are often insufficient to overcome cultural and political obstacles to information sharing.

The United States: The Paradigm of a Culture of Secrecy

The US represents the most developed, yet also the most problematic example of systemic overclassification. Although described as an “open democracy”, the US operates under a secrecy regime unprecedented in modern history. According to estimates by the Federation of American Scientists, the US security apparatus classifies over 50 million pages of documents annually – a figure that, while lower than at the peak of the Cold War, still indicates the massive application of the principle “classify everything you can” (Aftergood 2023). This practice is rooted in administrative culture, legal framework, and institutional incentives that reward caution and penalize openness.

The principal legal act regulating classification in the United States for decades was Executive Order 13526 (White House 2009). It defines three levels of classification – *Confidential*, *Secret*, and *Top Secret* – and requires classification only if unauthorized disclosure could “reasonably be expected to cause damage to national security”. On paper, the framework appears reasonable, but in practice there is no effective mechanism for verifying justification. The decision is made by an individual official, often without adequate training, oversight, or consequences in cases of excessive secrecy. The same act provides for automatic declassification after 25 years, yet permits unlimited exemptions “for enduring security interests”. As a result, more than 80% of documents older than 25 years remain classified (Public Interest Declassification Board 2022), rendering “automatic” declassification a bureaucratic fiction. In October 2022, the administration of President Joe Biden adopted Executive Order 14040 (White House 2022), intended as a “reform for a new era”. The act seeks to address chronic systemic weaknesses: it introduces standards for the “digital compatibility” of classified data, strengthens the role of the National Archives in coordinating declassification, and promotes technologies for “bulk declassification”. However, as Pozen

(Pozen 2023) emphasizes, Executive Order 14040 does not resolve the core problem: it neither limits officials' discretion in classification nor introduces sanctions for unjustified excess. The reform remains within the logic of "technocratic management" – improving processes without questioning the culture of secrecy that produces them.

Three key factors explain the persistence of overclassification in the United States:

1) Culture of secrecy – The legacy of the Cold War and the "war on terror" has created a mentality in which "it is safer to withhold than to disclose". As a former Director of the Central Intelligence Agency stated before Congress: "No one has ever lost their job for overclassifying" (US Congress 2016; Aftergood 2023; Schein 2010). Secrecy has become part of professional identity, while openness is perceived as risk.

2) Fear of accountability – Officials know they will be sanctioned if they disclose information, but almost never if they unjustifiably conceal it. The cases of Chelsea Manning and Edward Snowden demonstrated that leaking information, even in the public interest, leads to imprisonment or exile. As Fenster (Fenster 2006) observes, the system creates asymmetric incentives that undermine democratic accountability.

3) Bureaucratic inertia – The declassification process is slow, costly, and technically demanding. Instead of systematic review, agencies extend classification status "just in case". This is an example of a "minimum-risk strategy" (Wilson 1989): when the costs of error in favor of openness are high, and those in favor of secrecy negligible, the choice is always – secrecy.

Two examples particularly illustrate the consequences of excessive secrecy:

1) The Iraq War (2003–2011) – While the media and Congress debated "weapons of mass destruction", key intelligence reports indicating a lack of evidence were classified. Only later did it become clear that secrecy had prevented informed democratic debate. As the National Commission on Terrorist Attacks Upon the United States concluded, "secrecy did not protect national security – it concealed unpreparedness and poor judgment" (The National Commission on

Terrorist Attacks Upon the United States [9/11 Commission] 2004, 417).

2) NSA (National Security Agency) mass surveillance programs – As revealed by Edward Snowden in 2013, segments of the PRISM and UPSTREAM programs were classified not due to operational sensitivity, but to conceal the scope of surveillance over citizens. The consequence was a crisis of trust between the state and society. As Connelly (Connelly 2023) notes, “when even court decisions are classified, democracy loses its reflexive capacity”.

Excessive secrecy directly undermines congressional oversight as a key mechanism of democratic control. Although Congress formally has the right to access all intelligence information, in practice such access is often delayed or incomplete materials are provided. Thus, a small number of legislators are expected to oversee tens of thousands of classified activities annually – a practically impossible task. An additional problem is historical amnesia: without access to archival records, researchers and future decision-makers are deprived of the opportunity to learn from the past. As historian Matthew Connelly observed, “when the state writes its own history, it becomes myth, not lesson” (Connelly 2023).

European Union: Challenges of Supranational Secrecy

The EU represents a special case in the analysis of over-classification, not because of the scale of its intelligence apparatus, but because the protection of sensitive information is built upon national secrecy regimes. The paradox – “European transparency” based on “national closedness” – creates a layered architecture of secrecy that often functions more as a barrier than as a filter. The consequence is a system in which information can be doubly or triply classified: at the level of the member state, as EU classified information, and sometimes also through bilateral agreements with NATO or the United States. The main legal act regulating secrecy at the level of the EU is Council Decision 2013/488/EU on security rules for protecting EU classified

information. This act defines four levels of secrecy, i.e., classification: *EU Restricted*, *EU Confidential*, *EU Secret*, and *EU Top Secret*.

At the normative level, the system enables interoperability between institutions and member states. In practice, however, each state retains sovereign control over the interpretation and application of categories. Thus, a German document marked “VS – Nur für den Dienstgebrauch” (Confidential – for official use only) may be treated in Brussels as *EU Restricted*, while a French document of the same content may be elevated to *EU Secret*, due to the institutional culture of protecting information of vital importance to the French state (*secret défense*). This fragmentation in risk perception makes joint analytical activity almost impossible.

The EU has no central body for declassification. A document marked *EU Secret* retains that status until the member state or institution (e.g., the Council of the EU) explicitly declassifies it, with the consent of all actors involved in its creation. In practice, this means that most documents never lose their classified status. Theoretical alignment with standards is often not followed by consistent implementation: EU regulations require that classification be proportional, justified, time-limited, and based on concrete harm, with the principles of *need-to-know* and *need-to-share*. Yet in practice, secrecy is often treated as the default procedure, especially in public procurement, infrastructure projects, and contracts with foreign capital or European funds. Documents are often assigned a high level of secrecy without adequate risk analysis or a clearly articulated justification.

The practice of the European Union Agency for Cybersecurity (ENISA) shows that greater openness in incident management contributes substantially to systemic resilience. On the other hand, excessive secrecy makes cross-sector cooperation more difficult – both among state institutions and between the public and private sectors. Such closedness runs counter to the principle of *need-to-share*, which, according to European cybersecurity standards, is crucial for the effective exchange of technical information and indicators of compromise.

Three factors explain over-classification at the level of the EU:

1) Protection of the negotiating position – in trade negotiations (e.g., the Transatlantic Trade and Investment Partnership with the U.S., the Trade Agreement with Canada, the Common Foreign Policy), the European Commission and delegations often classify even technical analyses in order to limit public debate. The European Ombudsman has repeatedly criticized this practice, particularly in the context of negotiations with the U.S. in the field of the digital economy (European Ombudsman 2021).

2) Lack of parliamentary oversight – unlike national systems, the European Parliament has no direct oversight over documents marked as *EUCI* (EU Classified Information). The “Interinstitutional Agreement on Confidential Documents” restricts access to a narrow circle of Members of Parliament, without the right to public disclosure or debate.

3) Culture of diplomatic reserve – many EU officials come from national diplomatic services where secrecy is the rule. This mentality is transferred to Brussels, where a “security clearance” is often used as a status symbol rather than as an instrument of necessity.

Two cases clearly demonstrate systemic problems:

1) Negotiations on the Transatlantic Trade and Investment Partnership (2013–2016) – more than 90% of documents were classified, including impact assessments on health, the environment, and labor rights. When international NGOs Greenpeace and Corporate Europe Observatory published parts of the documentation, it became clear that many concerns were justified, but by then it was too late for meaningful public debate.

2) Operation “Irinì” (2020 – present) – the EU naval mission in the Mediterranean, aimed at enforcing the arms embargo on Libya, classified even geospatial data on ship movements as *EU Secret*. This prevented independent verification of the mission’s mandate and led to accusations that the EU was concealing cooperation with Libyan militias (European Parliament 2023).

Over-classification in the EU directly undermines the principle of an open and transparent Union established by the Lisbon Treaty (Article 1 TEU). Instead of clear insight into decision-making processes in the fields of security and foreign policy, citizens face

an institutionalized wall of secrecy, justified by “efficiency” or “delicacy”. The consequence is an erosion of legitimacy: according to Eurobarometer 2024, only 28% of citizens believe that institutions act in their interest, with secrecy being one of the key sources of distrust (European Commission 2024; Transparency International 2025).

Fragmented classification practices further complicate cooperation within the Union. A German service may hold information that it internally treats as “confidential”, but once it is forwarded to Europol, it becomes *EU Confidential* and is no longer accessible to the German parliamentary oversight committee. Such jurisdictional traps create gaps in the control system and increase the risk of institutional errors.

The problem is compounded by bilateral agreements with NATO, which introduce an additional layer of classification. A document marked as *EU Secret* may be reclassified as *NATO secret* if it contains information relevant to allied defense. This creates administrative barriers and the risk of “creeping classification” – the gradual and unjustified increase in the secrecy level of documents.

Comparative Analysis of Key NATO Allies: United Kingdom, France and Germany

Although they belong to the same Transatlantic alliance and face common security challenges, the United Kingdom, France, and Germany show significant differences in their approach to secrecy – not so much in regulations, but in institutional culture, the degree of parliamentary oversight, and the willingness to reassess practices. The common pattern is that over-classification is less a consequence of law and more the result of implicit norms within intelligence communities (Moran 2022). Differences in democratic tradition and historical experience lead to variations in how secrecy is subject to public and institutional scrutiny. This variability reflects deeper differences in organizational cultures (Schein 2010): the British system interprets secrecy through official loyalty, the French as an expression of sovereignty, and the German as a potential threat to the individual that must be strictly limited. These three models represent

an ideal analytical framework for examining what Habermas calls “the tension between administrative efficiency and democratic legitimacy” (Habermas 1996).

The British secrecy system is based on the Official Secrets Acts of 1989, which do not define what is “secret”, but instead sanction any unauthorized disclosure of information “in the possession of a civil servant” (Legislation 1989; Group of States against Corruption 2023). This vagueness allows for broad interpretation: anything the state considers sensitive can become subject to criminal prosecution. The consequence is a culture in which secrecy is part of professional identity, particularly in MI6, GCHQ, and the Ministry of Defence.

The key problem is limited parliamentary oversight. Although there is an Intelligence and Security Committee, its members are appointed by the Prime Minister, and the committee has no right to initiate investigations on its own. In the inquiry into British involvement in a CIA (Central Intelligence Agency) operation that included the unlawful transfer of detainees, the Committee had limited access to documents because they were marked *US Classified*, and British agencies had no authority to declassify them (Intelligence and Security Committee of Parliament 2007). Recent reform attempts – such as the Freedom of Information (Amendment) Bill of 2023 – have led to further expansion of exemptions for security services, thereby weakening the freedom of information regime even more. As investigative journalist Richard Norton-Taylor observed, “British secrecy today functions like a private club, not as part of public administration” (Norton-Taylor 2024). This metaphor illustrates a system in which secrecy is institutionalized as a means of elite self-preservation rather than as a technical security measure.

The French approach to secrecy is based on strong centralization of power and the tradition of the primacy of state interest (*raison d'État*). Law No. 91–646 on the secrecy of correspondence via electronic communications (Légifrance 1991), adopted in 1991 and amended in 2017 and 2021, gives the executive branch almost absolute control over classification. Ministers of Defense or the Interior can unilaterally declare documents “secret” without judicial or parliamentary approval, and the secrecy period can last up to 75 years.

Parliamentary oversight formally exists through the Advisory Commission on Secrecy in the Field of National Defense (*Commission consultative du secret de la défense nationale – CCSDN*), but it has no authority to order declassification, only to issue recommendations that are often ignored. An illustrative case is France's military engagement in the Sahel, where reports on civilian casualties and targeting errors remained classified for years, preventing public debate on the effects of the intervention.

French media and researchers are subject to criminal sanctions if they publish classified information, even when obtained through third parties (e.g., WikiLeaks). Thus, in 2022, journalist *Marie-Marguerite Sablon* was criminally prosecuted under the French equivalent of the British Official Secrets Act after publishing a document on cooperation between the French foreign intelligence service – the Directorate-General for External Security (*Direction Générale de la Sécurité Extérieure*) – and Moroccan intelligence services, even though the document did not originate from the French archive. Such practices not only violate principles of freedom of speech but also undermine democratic accountability: when even already obtained information becomes a criminal offense, society loses the ability to influence security policy.

The German approach to secrecy is strongly shaped by the historical legacy of the Stasi and the regime of personal data protection. The Secrecy Act (*Geheimhaltungsgesetz*) of 2016 requires that classification be proportional, time-limited, and subject to regular review. Any document older than 30 years automatically loses its classified status unless it can be proven that its disclosure would still pose a risk.

The key difference compared to the United Kingdom and France is stronger parliamentary oversight. The German Parliament's Committee for the Oversight of Federal Intelligence Services (*Parlamentarisches Kontrollgremium – PKGr*) has the right to demand access to any document, including those marked state secret (*Streng Geheim*), and to summon the directors of *Bundesnachrichtendienst* – BND, *Bundesamt für Verfassungsschutz* – BfV, and *Amt für den*

Militärischen Abschirmdienst – MAD for public or closed hearings. In the case of cooperation between the BND and the American NSA, the committee launched a comprehensive investigation in 2014 that led to legislative reform and a ban on mass data collection on EU citizens.

Germany is also not immune to over-classification. In areas such as arms exports or the deployment of the Bundeswehr abroad, documents are often classified “as a precaution”, even when they do not contain operationally sensitive information. Critics, including Transparency International Deutschland, point out that secrecy in such cases is used to conceal politically unfavorable information, such as actual costs or civilian casualties (Transparency International Deutschland 2024). This shows that even in a system with the most developed oversight mechanisms, a culture of precaution can prevail over the principles of transparency.

Table 1. Comparative conclusion: Three Models, One Problem

Country	Legal Framework	Level of Oversight	Culture of Secrecy
United Kingdom	Vaguely defined (OSA)	Weak, under executive control	Secrecy as deontology
France	Centralized (secret défense)	Formal without executive control	Raison d’État as absolute
Germany	Proportional (Geheimhaltungs-gesetz)	Strong parliamentary oversight	Secrecy as exception

Source: Author’s compilation.

What the British, French, and German systems have in common is that secrecy functions as an instrument of risk management, but primarily political rather than security risk. Overclassification in all cases prevents institutional learning from previous mistakes, undermines public trust, and complicates cooperation within NATO. It is particularly problematic when British documents cannot be shared with German partners due to differing standards in the interpretation of the concept of *secrecy*.

CONCLUDING REMARKS: TOWARDS A CULTURE OF RESPONSIBLE TRANSPARENCY

The analysis of practices in the US, the EU, the United Kingdom, France, and Germany demonstrates that overclassification is not a technical anomaly but a structural characteristic of modern democratic security apparatuses. Although the systems differ in legal form, institutional architecture, and historical context, three common causal patterns can be identified:

1) Culture of secrecy as a norm – the logic of “safer to close than to open” is internalized as a rule of behavior (Schein 2010).

2) Asymmetric incentives – officials who disclose information bear risks (career, disciplinary, legal, criminal), while those who unjustifiably expand secrecy almost never face consequences (Fenster 2006).

3) Weak external oversight mechanisms – whether the U.S. Congress, the European Parliament, the United Kingdom’s Intelligence and Security Committee, or Germany’s Parliamentary Control Panel over intelligence services, all these bodies operate with limited access to information, insufficient resources, or political silencing.

The combination of these factors produces a systemic pathology: secrecy ceases to serve the protection of national interests and becomes an instrument for shielding institutions from public and democratic accountability. The consequences are profound and multi-layered.

First, the *effectiveness of intelligence work declines*. When information is excessively fragmented and unavailable even within the same institution, the risk of duplicated activities, analytical errors, and missed critical signals increases. Such deficiencies were identified by the U.S. 9/11 Commission as one of the causes of the American systems failures (The 9/11 Commission 2004).

Second, there is an *erosion of public trust*. The legitimacy of the security apparatus is undermined when citizens see that decisions on war, mass surveillance, or international agreements are made under secrecy and later found to be based on incorrect or manipulated assumptions (e.g., the 2003 invasion of Iraq or the 2021 withdrawal from Afghanistan). According to Transparency International

(Transparency International 2025), even 62% of citizens in NATO member states believe that “secrecy is used to conceal political motives”.

Third, the *negative consequences affect international cooperation*. NATO and the EU rely on trust and information sharing, yet in practice a UK document may remain inaccessible to a German partner due to a UK Secret classification, or a French report due to the *secret défense* regime. Under such conditions, alliances lose operational value, and secrecy becomes an obstacle to collective security.

Overclassification is a structural problem, not the result of individual abuses. It arises from a systemic logic that rewards opacity, penalizes openness, and lacks effective mechanisms for retroactive review of the justification for secrecy. This pattern is present both in the US, the most powerful democracy, and in Germany, which has the most developed oversight mechanisms.

International legal frameworks provide a clear path toward responsible transparency. The Tshwane Principles on National Security and the Right to Information (Open Society Foundations 2013) require that every classification decision be accompanied by a risk assessment, proportionality justification, and the application of the lowest necessary level of protection. The OSCE Istanbul Document (OSCE 1999) prescribes prohibition of the misuse of national security as a justification for concealment of corruptive practices and institutional irregularities. The Council of Europe Tromsø Convention (Tromsø Convetion 2009) emphasizes that secrecy must be time-limited, subject to independent review, and based on an objective risk assessment.

Table 2. International Standards on Overclassification

Instrument / Organization	Key Principle	Practical Application
GRECO (Council of Europe)	Secrecy must not undermine anti-corruption mechanisms	Specifically criticizes excessive use of secrecy in public procurement and management of public resources

EU Security Rules	Proportionality, justification, and time limitation	Often applied formally, without substantive assessment of actual security risk
NATO AAP-06	Combination of “need-to-know” and “need-to-share” principles	Encourages inter-allied cooperation but often conflicts with national secrecy cultures in practice
Tshwane Principles (2013)	Specific and probable harm; democratic necessity	Serves as a reference model for reforming national classification laws and policies
OSCE Istanbul Document	Prohibition of misuse of national security	Directly relates to preventing the concealment of corruption and institutional irregularities

Source: Author’s compilation

These standards point to two mechanisms: 1) cumulative tests – access restrictions must meet the criteria of necessity, overriding interest, and specificity (specific and probable harm), with the burden of proof resting on the authority; 2) absolute prohibition of using secrecy to conceal irregularities.

However, in practice, problems arise when technical standards are applied formally, without substantive connection to these criteria. This leads to two consequences: 1) systemic undermining of protection mechanisms – excessive use diminishes the credibility of the classification; 2) limitation of democratic oversight – parliaments, oversight bodies, and media remain without access to critical information.

The solution does not lie in further tightening controls, but in a fundamental paradigm shift – from the logic of *need to hide* to the principle of *right to know*. Key steps include: 1) Introducing a legal mechanism that automatically terminates the validity of classification laws, provisions, or measures upon expiration (*sunset* clause), implying automatic declassification of information after a predefined period (e.g.,

ten years for *Confidential*, 15 years for *Secret*, except in cases where the justification for extension is explicitly and documentedly proven); 2) Strengthening independent oversight bodies – granting initiative rights, requiring public reporting, and direct access to archives; 3) systematic training of officials in the field of ethics of transparency – not only regarding the procedural application of confidentiality regimes, but also in understanding democratic responsibility and the public interest; 4) Harmonizing minimum standards at NATO and EU levels – adopting a common framework that clearly defines which types of information must not be classified (e.g., cost analyses, civilian casualty assessments, human rights documentation), in line with contemporary discussions on security sector reform in the region (Matić 2024; Starčević 2024).

The balance between security and transparency is inherently tense. However, the current state does not represent a balance but a systemic overload in favor of secrecy, often without clear and verifiable justification. If modern democracies wish to preserve their legitimacy and institutional effectiveness, they must recognize that the public's right to information is not a threat to security but one of its key foundations. As U.S. Supreme Court Justice Louis Brandeis long ago warned: "Sunlight is the best disinfectant".

In conclusion, overclassification is neither a purely bureaucratic reflex nor merely an intentional security illusion – it represents a structural coupling of both phenomena. The bureaucratic reflex (fear of accountability, institutional inertia) allows the security illusion (concealment of political motives) to become institutionalized as "normal practice".

REFERENCES

- Aftergood, Steven. 2023. "Reducing Overclassification Through Accountability and Technology." *Secrecy News, Federation of American Scientists*. October 15, 2023. <https://web.archive.org/web/20231016012102/https://fas.org/blogs/secrecy/2023/10/overclassification-accountability/>.
- Connelly, Matthew. 2023. *The Declassification Engine: What History Reveals About America's Top Secrets*. New York: Pantheon.

- Council of Europe Convention on Access to Official Documents (Tromsø Convention) CETS, June 18, 2009, CETS No. 205.
- Council of Europe. 2018. "Guidelines for GRECO Evaluation Teams (GETs)." *Group of states against Corruption – GRECO and Council of Europe*. December 7, 2018. <https://rm.coe.int/guidelines-get-eval5/16809005cd>.
- Dahl, Robert A. 1989. *Democracy and Its Critics*. New Haven: Yale University Press.
- Decision (EU) No. 2013/488/EU 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, OJ L 274, 15.10.2013, pp. 1–50. <https://eur-lex.europa.eu/eli/dec/2013/488/oj>.
- European Commission. 2024. "Standard Eurobarometer 99 – Spring 2024: Public Opinion in the European Union." *Directorate-General for Communication*. Last accessed October 20, 2025. <https://europa.eu/eurobarometer/surveys/detail/standard-eurobarometer-99>.
- European Ombudsman. 2021. "Decision of the European Ombudsman on complaint 619/98/(IJH)/GG against the European Commission." *European Ombudsman*. Last accessed October 20, 2025. <https://www.ombudsman.europa.eu/en/decision/en/1042-2020-mig>.
- European Parliament. 2023. "Report on the Implementation of Operation IRINI (2021/2206(INI)). Committee on Budgetary Control. 2023/2061(INI). PE 745.321." *European Parliament*. Last accessed October 20, 2025. http://www.europarl.europa.eu/doceo/document/A-9-2023-0232_EN.html.
- Federal Register. 2009. "Classified National Security Information." *Federal Register*. December 29, 2009. <https://www.federalregister.gov/documents/2010/01/05/E9-31418/classified-national-security-information>.
- Federal Register. 2022. "Declassification Reviews of Certain Documents Concerning the Terrorist Attacks of September 11, 2001." *Federal Register*. September 3, 2021. <https://www.federalregister.gov/documents/2021/09/09/2021-19578/declassification-reviews-of-certain-documents-concerning-the-terrorist-attacks-of-september-11-2001>.

- Fenster, Mark. 2006. "The Opacity of Transparency." *Administrative Law Review* 58 (3): 885–910.
- Group of States against Corruption. 2023. "Evaluation Report on the United Kingdom – Fourth Evaluation Round." *Council of Europe*. Last accessed October 20, 2025. https://rm.coe.int/16806ca4de?utm_.
- Habermas, Jürgen. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge, MA: MIT Press.
- Intelligence and Security Committee of Parliament. 2007. "Rendition: Ninth Report of Session 2006–07. HC 353." *The Stationery Office*. Last accessed October 20, 2025. <https://isc.independent.gov.uk/wp-content/uploads/2021/03/Rendition-Ninth-Report-of-Session-2006-07.pdf>.
- Légifrance. 1991. "Loi n° 91-646 du 10 juillet 1991 relative au secret de la défense nationale." *Journal Officiel de la République Française*. Last accessed October 20, 2025. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000356407>.
- Legislation. 1989. "Official Secrets Act 1989." *Legislation*. Last accessed October 20, 2025. <https://www.legislation.gov.uk/ukpga/1989/6/contents>.
- Matić, Goran. 2024. „Veleizdaja u krivičnom zakonodavstvu Republike Srbije." *Politika nacionalne bezbednosti* 26 (1): 137–154. DOI: 10.5937/pnb26-50033.
- Moran, Jon. 2022. "From Secrecy to Transparency? The UK's Intelligence and Security Committee and Parliamentary Scrutiny of Intelligence." *Parliamentary Affairs* 75 (1): 145–163. DOI: 10.1093/pa/gsab053.
- National Security Archive. 2021. "The Classification That Would Not Die: A Case Study in Overclassification." *George Washington University*. Last accessed October 20, 2025. <https://nsarchive.gwu.edu/briefing-book/2021-08-10/classification-would-not-die>.
- NATO Standardization Office. 2021. "AAP-06: NATO Glossary of Terms and Definitions (Edition 2021)." *NATO Standardization Agency*. Last accessed October 20, 2025. <https://nso.nato.int/nso/>

- ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/APP-6.pdf.
- Norton-Taylor, Richard. 2024. "British Secrecy Functions as a Private Club, Not Public Service." *The Guardian*. March 12, 2024. <https://www.theguardian.com/world/2024/mar/12/british-secrecy-private-club-not-public-service>.
- Open Society Foundations. 2013. "The Global Principles on National Security and the Right to Information (Tshwane Principles)." *Open Society Foundations*. Last accessed October 20, 2025. <https://www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf>.
- Organization for Security and Cooperation in Europe [OSCE]. 1999. "Istanbul Document 1999." *Organization for Security and Cooperation in Europe Summit*. November 19, 1999. <https://cdn.osce.org/sites/default/files/f/documents/4/2/17502.pdf>.
- Pozen, David. 2013. "The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information." *Harvard Law Review* 127 (2): 512–635.
- Pozen, David. 2023. "Executive Order 14040 and the Illusion of Secrecy Reform." *Lawfare*. November 15, 2023. Archived version. <https://web.archive.org/web/20231116000000/https://www.lawfaremedia.org/article/eo-14040-secrecy-reform>.
- Public Interest Declassification Board. 2022. "Annual Report 2022." *National Archives and Records Administration*. Last accessed October 20, 2025. <https://www.archives.gov/files/isoo/pidb/reports/pidb-annual-report-2022.pdf>.
- Schein, Edgar H. 2010. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.
- Schmitt, Carl. [1922] 2005. *Political Theology: Four Chapters on the Concept of Sovereignty*. Chicago: University of Chicago Press.
- Starčević, Srđan. 2024. „Povratak obaveznog služenja vojnog roka u Evropi – društveni determinizam i perspektive." *Politika nacionalne bezbednosti* 26 (1): 11–26. DOI: 10.5937/pnb26-50140.
- The National Commission on Terrorist Attacks Upon the United States [9/11 Commission]. 2004. "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the

- United States.” *W. W. Norton and Company*. Last accessed October 20, 2025. <https://www.9-11commission.gov/report/911Report.pdf>.
- Transparency International Deutschland. 2024. “Geheimhaltung und Demokratie: Eine Bestandsaufnahme der parlamentarischen Kontrolle.” *Transparency International Deutschland*. Last accessed October 20, 2025. <https://www.transparency.de/publikationen/geheimhaltung-und-demokratie/>.
- Transparency International. 2025. “Global Corruption Barometer – Europe & Central Asia 2025: Trust in Institutions.” *Transparency International Secretariat*. Last accessed October 23, 2025. <https://www.transparency.org/en/gcb/europe-central-asia/europe-central-asia-2025>.
- United Nations Educational, Scientific and Cultural Organization. 2014. “UNESCO Guidelines on Freedom of Expression and National Security.” *UNESCO*. Last accessed October 20, 2025. <https://unesdoc.unesco.org/ark:/48223/pf0000229381>.
- US Congress. House. Committee on Oversight and Government Reform [USC]. 2016. “Hearing on Government Secrecy and Oversight Challenges.” *114th Cong., C-SPAN*. Last accessed October 20, 2025. <https://www.c-span.org/video/?406395-1/hearing-government-secrecy-oversight-challenges>.
- Wilson, James Q. 1989. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.

Горан Матић*

Факултет за пословне студије и право, Универзитет
„Унион – Никола Тесла”, Београд, Република Србија

ПРЕКОМЕРНА ТАЈНОСТ У ДЕМОКРАТИЈАМА: БИРОКРАТСКИ РЕФЛЕКС ИЛИ БЕЗБЕДНОСНА ИЛУЗИЈА?

Резиме

„Прекомерна тајност у демократијама” анализира системску прекомерну класификацију информација у безбедносним апаратима САД, Европске уније и кључних НАТО савезника. Полазна теза рада јесте да прекомерна тајност није случајна административна девијација, већ структурирани избор који произлази из разлике између *security secrecy* – заштите оперативних капацитета и *political secrecy* – заштите институција од политичке и правне одговорности. Управо у том померању фокуса са безбедности на институционалну самозаштиту аутор препознаје суштину проблема. Компаративна анализа указује на заједничке обрасце у различитим системима: дефанзивну класификацију као стратегију минимизације ризика, асиметричне подстицаје који кажњавају отвореност, као и ограничену ефикасност спољашњих механизма надзора. Службеници су институционално мотивисани да информације класификују, јер евентуална штета од објављивања носи санкције, док прекомерна тајност ретко производи последице. Таква логика генерише културу превентивног затварања информација. У САД култура тајности и страх од одговорности доводе до класификације десетина милиона страна годишње, при чему аутоматска декласификација у пракси остаје формална норма без стварног домета. У Европској унији проблем се испољава кроз институционалну фрагментацију: различити национални режими тајности отежавају хоризонталну сарадњу, док се

* Имејл адреса: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

класификација често користи за заштиту преговарачких позиција и политичке осетљивости. Анализа Уједињеног Краљевства, Француске и Немачке показује да, упркос различитим правним традицијама, тајност функционише као инструмент политичког управљања ризиком: британски модел карактерише ограничен парламентарни надзор; француски је снажно централизован око концепта државног интереса; док немачки, иако формално снажнији у контроли, испољава бирократску инертност. Последице прекомерне тајности су вишеструке. Фрагментација информација умањује оперативну ефикасност обавештајних служби. Истовремено, еродира се јавно поверење, јер се тајност користи за прикривање политичких мотива и пропуста, што подрива демократску легитимност. Додатно, неусаглашени стандарди отежавају сарадњу унутар НАТО савеза. Закључно, рад позива на промену парадигме: од логике „потребе да се сакрије” ка принципу „права да се зна”. Предлажу се увођење обавезних *sunset* клаузула за временски ограничену класификацију, јачање независности надзорних тела и хармонизација стандарда на нивоу ЕУ и НАТО. Само системски приступ може ограничити злоупотребу тајности и обезбедити да она остане изузетак, а не правило демократског управљања.

Кључне речи: прекомерна класификација, тајност, обавештајна заједница, демократска одговорност, право на приступ информацијама, Сједињене Америчке Државе, Европска унија, НАТО, компаративна анализа.

* This paper was received on February 27, 2026, and accepted for publication at the Editorial Board meeting on February 27, 2026.

Горан Матић*

*Факултет за пословне студије и право, Универзитет
„Унион – Никола Тесла”, Београд, Република Србија*

ПРЕКОМЕРНА ТАЈНОСТ У ДЕМОКРАТИЈАМА: БИРОКРАТСКИ РЕФЛЕКС ИЛИ БЕЗБЕДНОСНА ИЛУЗИЈА?

Сажетак

Систематска прекомерна класификација информација унутар безбедносних апарата Сједињених Америчких Држава, Европске уније и кључних НАТО савезника представља структурну аномалију у оквиру либералних демократија. Кроз компаративну анализу, рад идентификује да је кључни покретач овог феномена разлика између концепта *security secrecy* (заштите стварних безбедносних капацитета) и концепта *political secrecy* (заштите институција од одговорности). Истраживање показује да, упркос различитим правним традицијама, сви анализирани системи деле заједничке структурне обрасце: *defensive classification* као стратегију минимизације ризика, асиметричне подстицаје који санкционишу отвореност и слабост механизма спољашњег надзора. Последице овакве праксе обухватају ерозију јавног поверења, отежану сарадњу унутар НАТО савеза и смањену ефикасност у процесима доношења одлука. У раду се закључује да решења захтевају промену парадигме – од логике „потребе да се сакрије” (*need to conceal*) ка принципу „права да се зна” (*the right to know*), заснованом на претпоставци отворености као основи демократске легитимности. Као кључни оперативни кораци истичу се увођење обавезног утврђивања рока истека

* Имејл адреса: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

важења класификације (*sunset* клаузула), јачање независности и надлежности надзорних тела, као и хармонизација стандарда на нивоу НАТО и Европске уније ради спречавања злоупотребе тајности у сврху управљања информацијама, а не заштите безбедности.

Кључне речи: прекомерна класификација, тајност, обавештајна заједница, демократска одговорност, право на приступ информацијама, Сједињене Америчке Државе, Европска унија, НАТО, компаративна анализа.

УВОДНА РАЗМАТРАЊА

Прекомерна класификација није административна грешка она представља системски избор. У демократијама заснованим на принципима одговорности и транспарентности, масовно означавање докумената као „тајних”, без јасних и проверљивих критеријума, трансформише тајност из изузетка у правило. Последица такве праксе није повећана безбедност, већ ослабљен надзор и фрагментирана сарадња међу савезницима.

Овај рад полази од тезе да је прекомерна класификација један од најозбиљнијих, али истовремено и најмање регулисаних изазова савремених безбедносних система. Док се јавне и стручне расправе интензивно фокусирају на вештачку интелигенцију, кибернетичку одбрану и хибридне претње, пракса рутинског затварања информација остаје у великој мери занемарена – иако директно подрива демократске вредности које те државе формално заступају.

Пре анализе специфичних националних система, неопходно је указати на универзалне оквире међународних организација. Иако Уједињене нације немају јединствен систем класификације, њихови органи су током времена артикулисали принципе равнотеже између безбедности и транспарентности. Смернице Организације Уједињених нација за образовање, науку и културу о слободи информација и националној безбедности (УНЕСКО) (United Nations Educational, Scientific and Cultural Organization 2014) захтевају да свака рестрикција буде законита, неопходна и пропорционална у демократском друштву. Организација за европску безбедност и сарадњу је у Истанбулском документу (*The*

OSCE Istanbul Document) из 1999. године (Organization for Security and Cooperation in Europe [OSCE] 1999) нагласила да тајност не сме бити изговор за избегавање одговорности.

Ови универзални стандарди представљају нормативни темељ на којем су касније изграђени детаљнији и операционализовани инструменти укључујући Цвана принципе о националној безбедности и праву на информације (*Tshwane Principles on National Security and the Right to Information*) из 2013. године (Open Society Foundations 2013), Тромсе конвенцију Савета Европе о приступу званичним документима из 2009. године (Tromsø Convention 2009), евалуационе механизме Групе држава против корупције при Савету Европе (*Group of States against Corruption – GRECO*) (Council of Europe 2018), нормативне оквири Европске уније (ЕУ) у форми Одлуке Савета 2013/488/ЕУ о безбедносним правилима за заштиту тајних података ЕУ (Decision 2013/488) и Организације Северноатлантског уговора у форми НАТО (*North Atlantic Treaty Organization*) Глосара термина и дефиниција, издање ААП-06 (*Glossary of Terms and Definitions, AAP-06 edition*) (NATO Standardization Office 2021). Заједничка порука свих ових аката је јасна: легитиман безбедносни интерес не сме надјачати демократске захтеве транспарентности, парламентарног надзора и јавног интереса. Ипак, компаративна анализа показује да јаз између нормативне усаглашености и оперативне праксе остаје централни проблем прекомерне класификације у савременим демократијама.

Иако се праксе разликују, међународни и регионални оквири показују кохерентност у дефинисању принципа одговорне класификације. Група држава против корупције при Савету Европе у више циклуса истиче да прекомерна тајност подрива антикорупцијске механизме и надзор, нарочито у јавним набавкама и управљању ресурсима. НАТО глосар и Безбедносна правила ЕУ инсистирају на пропорционалности, образложености и временском ограничењу. Ови стандарди показују консензус да тајност мора бити изузетак, а не правило – консензус који, као што ће анализа показати, често остаје на нивоу теорије, а не праксе.

У основи феномена лежи парадокс демократије и тајности: либерална демократија, како је концептуализују Дал (*Robert Dahl*) и Хабермас (*Jürgen Habermas*), захтева отвореност као услов легитимности политичке воље (Dahl 1989; Habermas 1996). Ипак,

унутар тих система развијају се апарати чија функционалност почива на контролисаној затворености што ствара напетост између права на знање и потребе за тајношћу (Fenster 2006). Тајност у обавештајним институцијама није само процедурални алат, већ постаје део организационе културе „основна претпоставка” која обликује идентитет служби и понашање припадника (Schein 2010). Тако се тајност трансформише из техничког избора у нормативни императив, стварајући услове за системску прекомерност.

Анализа обухвата три аналитичка нивоа: САД, као глобалног хегемона са најразвијенијим обавештајно-безбедносним апаратом; ЕУ као наднационални ентитет са слојевитим и фрагментираним режимима тајности; и три европске државе – Уједињено Краљевство, Француску и Немачку – које карактеришу различити приступи тајности, у распону од британске „културе службе” до немачког наслеђа Штазија (*Stasi*), као главне тајне обавештајне службе Источне Немачке.

Теоријски оквир рада комбинује теорију бирократског понашања (Wilson 1989), у оквиру које се истиче избор стратегије минималног ризика, и теорију демократске одговорности (Fenster 2006), која инсистира на томе да тајност мора представљати изузетак, а не правило у функционисању демократских институција. Додатно, рад се ослања на критичку литературу о феномену „пропусног Левијатана” (*Leaky Leviathan*) (Pozen 2013) и институционалној динамици прекомерне класификације (Aftergood 2023).

Методолошки приступ заснива се на упоредној анализи случајева и укључује разматрање следећих материјала: званичних извештаја Врховне ревизорске институције САД (*Government Accountability Office – GAO*), Европског омбудсмана (*European Ombudsman*) и Одбора немачког Бундестага за контролу служби безбедности (*Parlamentarisches Kontrollgremium – PKGr*); релевантне академске литературе аутора, као што су Стивен Афтергуд (*Steven Aftergood*) и Дејвида И. Поузена (*David E. Pozen*), истраживачких пројеката Националног безбедносног архива при Универзитету „Џорџ Вашингтон” (*National Security Archive at George Washington University*), као и анализу кључних афера, као што су Пентагонски документи (*Pentagon Papers*), афера Сноуден (*Snowden affair*), немачке Савезне обавештајне службе (*Bundesnachrichtendienst – BND*).

Структура рада прати логику систематског поређења: друго поглавље посвећено је анализи праксе у САД, треће ЕУ, четврто доноси упоредну анализу три одабране европске државе, док пето поглавље пружа синтетички закључак о могућим путевима ка успостављању одговорне транспарентности.

Истраживање се фокусира искључиво на компаративну анализу система САД, ЕУ и кључних НАТО савезника. Систем заштите тајних података у Србији није предмет анализе овог рада.

Иако се НАТО помиње у наслову и ширем контексту рада као оквир за дељење тајних информација међу западним демократијама, рад не анализира његов систем класификације (нпр. ААР-06, *Cosmic Top Secret*). Разлог је методолошки: НАТО нема сопствене обавештајне капацитете нити производи оригиналне тајне податке, већ делује као механизам размене информација насталих на националном нивоу. Сходно томе, прекомерна класификација у контексту НАТО одражава праксе држава чланица пре свега САД, Уједињеног Краљевства, Француске и Немачке – које су обухваћене анализом. Додатно, НАТО стандарди, укључујући принципе „потребно је да зна” (*need-to-know*) и „потребно је поделити” (*need-to-share*), већ су инкорпорирани у националне системе и оквир ЕУ, па њихово разматрање кроз призму држава чланица пружа адекватан аналитички увид у функционисање тајности у Трансатлантском савезу.

Унутар дискурса о прекомерној тајности могу се разликовати три приступа. Први, критички, својствен организацијама цивилног друштва и актерима права на приступ информацијама, усмерава се на злоупотребе и последице по транспарентност и демократску контролу. Други, одбрамбени, карактеристичан за органе власти и безбедносне структуре, полази од потребе за очувањем постојећих пракси и наглашава ризике које би смањење тајности могло произвести по безбедност, стабилност или међународне обавезе. Трећи, академски, заузима неутралну позицију: кроз анализу нормативног оквира, упоредне праксе и примене настоји да идентификује слабости система и могућности унапређења.

Овај рад припада трећем, академском приступу. Његов циљ није да заузме страну у постојећим полемикама, већ да понуди аналитички оквир који омогућава разумевање зашто се проблеми у области заштите тајних података понављају, како различити

приступи обликују праксу и на који начин је могуће постићи функционалнију равнотежу између безбедности, одговорности и јавног интереса.

Наслов рада поставља дилему: да ли је прекомерна класификација последица бирократског рефлекса – рационалног, али уско инструменталног одговора на перципиране ризике – или безбедносна илузија: стратегија која прикрива политичку непрозирност, избегавање одговорности и управљање јавним перцепцијама под изговором националне безбедности? Анализа показује да су ове две опције у пракси често нераздвојиве: бирократски рефлекс постаје механизам којим се производи и одржава безбедносна илузија. Када се страх од грешке, каријерни ризик и институционална инерција систематизују као „стратегија минималног ризика” (*minimum-risk strategy*), тајност престаје да буде техничка мера и постаје инструмент контроле информација, а не заштите безбедности.

ТЕОРИЈСКЕ ПАРАДИГМЕ: ТАЈНОСТ ИЗМЕЂУ СУВЕРЕНИТЕТА И ДЕМОКРАТСКОГ ИЗУЗЕТКА

Пре компаративне анализе националних система, неопходно је разјаснити теоријске дилеме односа тајности и демократије. Парадокс либералне демократије лежи у потреби за отвореношћу као извором легитимности, али и за тајношћу као условом функционалности безбедносних апарата (Dahl 1989; Habermas 1996). Овај однос може се разумети кроз две супротстављене теоријске традиције.

Суверенитетска парадигма – од Жана Бодена (*Jean Bodin*) до Карла Шмита (*Carl Schmitt*) – третира тајност као атрибут суверене власти. Код Бодена, суверенитет подразумева способност државе да самостално одлучује о питањима од виталног значаја, укључујући право да одређене информације задржи ван домашаја јавности. Шмит овај однос радикализује тврђом да је „суверен онај ко одлучује о изузетку” (Schmitt [1922] 2005). Изузетак функционише изван процедура јавности и транспарентности, што тајност чини предусловом ванредног одлучивања. У савременим безбедносним државама ова логика је институционализована: извршна власт задржава контролу над тајним подацима, полазећи

од претпоставке да је тајност услов ефикасног деловања у кризним ситуацијама.

Демократска парадигма темељи се на Хабермасовом начелу да је јавност основ демократске легитимације власти. Јавна расправа и приступ информацијама омогућавају контролу политичке моћи и трансформишу „наративну власт” у „дискурзивну одговорност” (Habermas 1996). Тајност није правило, већ одступање које захтева строго ограничено оправдање. У демократском поретку дозвољена је искључиво као контролисано и привремено одступање ради заштите конкретног и легитимног интереса. Проблем настаје када се изузетак претвори у правило, а јавност у секундарну вредност.

Правно гледано, тајност није обавезујућа норма (*ius cogens*) нити апсолутно право државе. Она је изузетак у односу на правило транспарентности, али строго уређен законом. Тајност је облик административне дискреције са јасно утврђеним правним границама. Органи власти морају сваку одлуку о тајности: 1) образложити, 2) засновати на процени штете, 3) временски ограничити и 4) учинити подложном контроли. Овај оквир, заједнички Цвана принципима (Open Society Foundations 2013) и Тромсе конвенцији, чини нормативни темељ одговорне класификације.

Кључна аналитичка разлика лежи у дистинкцији између заштите стварних безбедносних капацитета (*security secrecy*) и „заштите институција од одговорности” (*political secrecy*). Прва се односи на заштиту стварних безбедносних капацитета (извори, методе, оперативни планови, сајбер одбрана), док друга служи заштити институција и носилаца власти од одговорности, надзора или јавне критике. Теоријска теза која произилази из ове дистинкције гласи: прекомерна тајност (*overclassification*) често је политички, а не безбедносни проблем. Она је последица ширења изузетка и асиметрије моћи унутар институција, а не вишка безбедносне пажње.

Ова дистинкција постаје релевантна при анализи образаца прекомерне класификације. Политичка тајност у пракси се манифестује кроз: 1) масовно означавање целих докумената као тајних, иако је осетљив само део; 2) ретроактивно проглашавање тајности након што су информације постале јавне – као облик

накнадне цензуре; 3) очување „застарелих тајни” без редовне ревизије ризика; и 4) проширење појма „националног интереса” на комерцијалне или административне податке. Ови обрасци, различито формализовани, препознатљиви су у свим системима – од САД до Немачке – што указује на структурну динамику, а не на изоловане институционалне грешке.

Савремени безбедносни оквири све више преиспитују традиционални модел *потребно је да зна* као искључиви принцип. У доба хибридних претњи, масовног надзора и комплексних изазова, овај рестриктивни приступ показује ограничења. Зато се афирмише принцип *потребно је поделити* – идеја да информације морају бити доступне актерима који их могу оперативно искористити за колективну одбрану, чак и ако нису директно укључени у њихово стварање. Ова еволуција није супротстављање, већ надоградња: принцип *потребно је да зна* штити од злоупотребе, а принцип *потребно је поделити* обезбеђује ефикасност и отпорност. Дихотомија је институционализована у Безбедносним правилима ЕУ и Глосару НАТО термина и дефиниција, издање ААР-06, где оба приступа представљају комплементарне принципе.

Овај теоријски оквир представља аналитичку „мапу” за испитивање конкретних система. Он омогућава да се разликује легитимна безбедносна тајност од политичке злоупотребе, идентификује тренутак када се „изузетак” претвара у „правило” и процени да ли се тајност користи као инструмент заштите или контроле. Са овим концептуалним алатима, анализа се усмерава ка компаративном разматрању три нивоа: САД као глобалне парадигме, ЕУ као наднационалног експеримента и кључних НАТО савезника са њиховим различитим традицијама. Ова дихотомија је посебно релевантна у контексту савезничких организација, као што је НАТО, у којима се принципи *need-to-know* (заштита од отицања информација) и *need-to-share* (обезбеђивање колективне одбране) налазе у сталном напону. Глосар НАТО термина и дефиниција, издање ААР-06 експлицитно препознаје ову дихотомију, али, као што показује пракса, технички стандарди сами по себи често нису довољни да превазиђу културне и политичке препреке дељењу информација.

Сједињене Америчке Државе: парадигма културе тајности

САД представљају најразвијенији, али и најпроблематичнији пример системске прекомерне класификације. Иако се описују као „отворена демократија”, САД функционишу под режимом тајности без преседана у модерној историји. Према проценама Федерације америчких научника (*Federation of American Scientists*), амерички безбедносни апарат годишње класификује преко 50 милиона страница докумената – бројка која, иако нижа него у врхунцу Хладног рата, и даље указује на масовну примену принципа „класификуј све што можеш” (Aftergood 2023). Ова пракса је утемељена у административној култури, правном оквиру и институционалним подстицајима који награђују предострожност, а кажњавају отвореност.

Основни правни акт који је деценијама регулисао класификацију у САД била је Уредба 13526 (*Executive Order 13526*) (Federal Register 2009). Она дефинише три нивоа класификације – поверљиво (*Confidential*), строго поверљиво (*Secret*) и државна тајна (*Top Secret*) – и захтева класификацију само ако њено неовлашћено откривање може „очигледно угрозити националну безбедност”. На папиру оквир делује разумно, али у пракси не постоји ефикасан механизам за проверу оправданости. Одлуку доноси појединачни службеник, често без адекватне обуке, надзора или последица у случају прекомерне тајности. Исти акт предвиђа аутоматску декласификацију након 25 година, али дозвољава неограничене изузетке „због трајних безбедносних интереса”. Последица је да више од 80% докумената старијих од 25 година остаје класификовано (Public Interest Declassification Board 2022), па „аутоматска” декласификација постаје бирократска фикција. У октобру 2022. администрација председника Џоа Бајдена (*Joe Biden*) донела је Уредбу 14040 (*Executive Order 14040*) (Federal Register 2022), која је требало да представља „реформу за нову еру”. Акт настоји да ублажи хроничне слабости система: уводи стандарде за „дигиталну компатибилност” класификованих података, повећава улогу Националне архиве у координацији декласификације и подстиче технологије за „масовну декласификацију”. Међутим, како истиче Поузен (Pozen 2023), Уредба 14040 не решава кључни

проблем: не ограничава дискрецију службеника у класификацији нити уводи санкције за неоправдану прекомерност. Реформа остаје унутар логике „технократског управљања” – унапређује процесе, али не преиспитује културу тајности која их производи.

Постоје три кључна фактора који објашњавају опстанак прекомерне класификације у САД:

1) Култура тајности – наслеђе Хладног рата и „рата против тероризма” створило је менталитет у коме је „сигурније затворити него објавити”. Како је један бивши директор Централне обавештајне агенције (*Central Intelligence Agency – CIA*) изјавио пред Конгресом: „Нико никада није изгубио посао зато што је прекорачио у тајности” (US Congress 2016; Aftergood 2023; Schein 2010). Тајност је постала део професионалног идентитета, док се отвореност перципира као ризик.

2) Страх од одговорности – службеници знају да ће бити санкционисани ако нешто открију, али готово никада ако неоправдано сакрију. Случајеви Челси Менинг (*Chelsea Manning*) и Едварда Сноудена (*Edward Snowden*) показали су да цурење информација, чак и у јавном интересу, води затвору или егзилу. Како примећује Фенстер (Fenster 2006), систем ствара асиметричне подстицаје који поткопавају демократску одговорност.

3) Бирокупатска инертност – процес декласификације је спор, скуп и технички захтеван. Уместо систематске ревизије, агенције продужавају статус тајности „за сваки случај”. То је пример „стратегије минималног ризика” (Wilson 1989): када су трошкови грешке у корист отворености високи, а у корист тајности занемарљиви, избор је увек – тајност.

Два примера посебно илуструју последице прекомерне тајности:

1) Рат у Ираку (2003–2011) – док су медији и Конгрес расправљали о „оружју за масовно уништење”, кључни извештаји обавештајних служби који су указивали на недостатак доказа били су класификовани. Тек касније постало је јасно да је тајност онемогућила информисану демократску дебату. Како је закључила Комисија за истраживање терористичког напада 11. септембра 2001, „тајност није штитила националну безбедност – она је прикривала неспремност и лош суд” (The National Commission on Terrorist Attacks Upon the United States [9/11 Commission] 2004, 417).

2) Програми масовног надзора НСА (*National Security Agency – NSA*) – како је показао случај Едварда Сноудена (*Edward Snowden*) 2013, сегменти програма *PRISM* и *UPSTREAM* били су класификовани не због оперативне осетљивости, већ ради прикривања обима надзора над грађанима. Последица је била криза поверења између државе и друштва. Како истиче Метју Конели (*Matthew Connolly*), „када се чак и судске одлуке класификују, демократија губи свој рефлексивни капацитет” (*Connolly 2023*).

Прекомерна тајност директно подрива надзор Конгреса као кључни механизам демократске контроле. Иако Конгрес формално има право на приступ свим обавештајним информацијама, у пракси се тај приступ често одлаже или се достављају непотпуни материјали. Тако мали број законодаваца треба да надзире десетине хиљада класификованих активности годишње, што је практично немогуће. Додатни проблем је историјска амнезија: без приступа архивској грађи, истраживачи и будући доносиоци одлука лишени су могућности да уче из прошлости. Како је приметио историчар Метју Конели, „када држава сама пише сопствену историју, она постаје мит, а не лекција” (*Connolly 2023*).

Европска унија: изазови наднационалне тајности

ЕУ представља посебан случај у анализи прекомерне класификације, не због обима обавештајног апарата, већ зато што заштиту осетљивих информација гради на националним режимима тајности. Парадокс – „европска транспарентност” заснована на „националној затворености” – ствара слојевиту архитектуру тајности која често делује као баријера, а не као филтер. Последица је систем у којем информације могу бити двоструко или троструко класификоване: на нивоу државе чланице, као тајни податак ЕУ, а понекад и кроз билатералне споразуме са НАТО или САД. Основни правни акт који уређује тајност на нивоу ЕУ јесте Одлука Савета 2013/488/ЕУ о безбедносним мерама за заштиту тајних података Европске уније (*Council of the European Union 2013*). Она дефинише четири степена тајности, односно нивоа класификације: ЕУ интерно (*EU Restricted*), ЕУ поверљиво (*EU Confidential*), ЕУ строго поверљиво (*EU Secret*) и ЕУ државна тајна (*EU Top Secret*).

На нормативном нивоу систем омогућава интероперабилност институција и држава чланица. У пракси, међутим, свака

држава задржава суверену контролу над тумачењем и применом категорија. Тако немачки документ означен као *VS – Nur für den Dienstgebrauch* (Тајно – само за службену употребу) у Бриселу може бити третиран као *EU Restricted*, док француски документ истог садржаја може бити подигнут на ниво *EU Secret*, услед институционалне културе заштите података од виталног значаја за француску државу *secret défense*. Оваква фрагментација у перцепцији ризика чини заједничку аналитичку делатност готово немогућом.

ЕУ нема централни орган за декласификацију. Документ означен као *EU Secret* задржава тај статус све док га држава чланица или институција (нпр. Савет ЕУ) изричито не декласификује, уз сагласност свих актера укључених у његово креирање. У пракси то значи да већина докумената никада не губи статус тајности. Теоријска усаглашеност са стандардима често није праћена доследном применом: прописи ЕУ захтевају да класификација буде пропорционална, образложена, временски ограничена и заснована на конкретној штети, уз принципе *need-to-know* и *need-to-share*. Ипак, у пракси тајност се често третира као подразумевани поступак, нарочито у јавним набавкама, инфраструктурним пројектима и уговорима са страним капиталом или европским фондовима. Документи понекад добијају висок степен тајности без адекватне процене ризика или јасно дефинисаног интереса.

Пример праксе Европске агенције за сајбер безбедност (*European Union Agency for Cybersecurity – ENISA*) показује да повећана транспарентност у управљању инцидентима значајно повећава отпорност система. Насупрот томе, прекомерна тајност смањује међусекторску сарадњу – како између државних институција, тако и између јавног и приватног сектора. Оваква затвореност је у супротности са принципом *потребно је поделити* који је према европским стандардима сајбер безбедности кључан за ефикасну размену техничких информација и индикатора компромитовања.

Три фактора објашњавају прекомерну класификацију на нивоу ЕУ:

- 1) Заштита преговарачке позиције – у трговинским преговорима (нпр. Трансатлантски трговинско-инвестициони споразум са САД, Трговински споразум са Канадом, Заједничка

спољна политика) Европска комисија и делегације често класификују чак и техничке анализе како би ограничиле јавну расправу. Европски омбудсман више пута је критиковао ову праксу, нарочито у контексту преговора са САД у области дигиталне привреде (European Ombudsman 2021).

2) Недостатак парламентарног надзора – за разлику од националних система, Европски парламент нема директан надзор над документима означеним као тајни подаци ЕУ (*EU Classified Information – EUCI*). „Међуинституционални споразум о поверљивим документима” ограничава приступ на уски круг посланика, без права на јавно објављивање или расправу.

3) Култура дипломатске резерве – многи званичници ЕУ долазе из националних дипломатских служби где је тајност правило. Та менталност преноси се у Брисел, где се „безбедносна дозвола” често користи као статусни симбол, а не као инструмент нужности.

Два случаја јасно показују системске проблеме:

1) Преговори о Трансатлантском трговинско-инвестиционом споразуму (*Transatlantic Trade and Investment Partnership*) (2013–2016) – више од 90% докумената било је класификовано, укључујући анализе утицаја на здравство, животну средину и радна права. Када су међународне невладине организације Гринпис (*Greenpeace*) и Опсерваторија корпоративне Европе (*Corporate Europe Observatory*) објавиле делове документације, показало се да су бројни разлози за забринутост били оправдани, али је већ било прекасно за смислену јавну дебату.

2) Операција „Ирини” (*Operation IRINI*) (2020 – до данас) – поморска мисија ЕУ у Медитерану, усмерена на спровођење ембарга на оружје према Либији, класификовала је чак и геопросторне податке о кретању бродова као *EU Secret*. То је онемогућило независну верификацију мандата мисије и довело до оптужби да ЕУ прикрива сарадњу са либијским милицијама (European Parliament 2023).

Прекомерна класификација у ЕУ директно подрива принцип отворене и транспарентне Уније утврђен Лисабонским уговором (члан 1 Уговора о ЕУ). Уместо јасног увида у процесе одлучивања у области безбедности и спољне политике, грађани се суочавају са институционализованим зидом тајности, оправданим „ефикасношћу” или „деликатношћу”. Последица је

ерозија легитимитета: према Евробарометру 2024. године, само 28% грађана верује да институције делују у њиховом интересу, при чему је управо тајност један од кључних извора неповерења (European Commission 2024; Transparency International 2025).

Фрагментирана пракса класификације додатно отежава сарадњу унутар Уније. Немачка служба може располагати информацијом коју интерно третира као „поверљиву”, али када је проследи Европолу (*European Union Agency for Law Enforcement Cooperation – EUROPOL*), она постаје *EU Confidential* и више није доступна немачком парламентарном одбору за надзор. Такве јурисдикцијске замке стварају празнине у систему контроле и повећавају ризик од институционалних грешака.

Проблем се усложњава билатералним споразумима са НАТО, који уводе додатни слој класификације. Документ означен као *EU Secret* може бити прекласификован у *NATO Secret* ако садржи информације од значаја за савезничку одбрану. То ствара административне баријере и ризик од „пузајуће класификације” – постепеног и неоправданог повећања степена тајности докумената.

Упоредна анализа кључних НАТО савезника: Уједињено Краљевство, Француска, Немачка

Иако припадају истом трансатлантском савезу и суочавају се са заједничким безбедносним изазовима, Уједињено Краљевство, Француска и Немачка показују значајне разлике у приступу тајности – не толико у прописима, колико у институционалној култури, степену парламентарног надзора и спремности на преиспитивање пракси. Заједнички образац је да је прекомерна класификација мање последица закона, а више резултат имплицитних норми унутар обавештајних заједница (Morgan 2022). Разлике у демократској традицији и историјском искуству доводе до варијација у томе колико је тајност подложна јавној и институционалној провери. Ова варијабилност одражава дубље разлике у организационим културама (Schein 2010): британски систем тумачи тајност кроз службену лојалност, француски као израз суверенитета, а немачки као потенцијалну претњу појединцу коју треба строго ограничити. Ова три модела представљају идеалан аналитички оквир за испитивање онога што Хабермас

назива „тензијом између административне ефикасности и демократске легитимности” (Habermas 1996).

Британски систем тајности темељи се на Закону о службеним тајнама (*Official Secrets Acts*) из 1989. године, који не дефинише шта је „тајно”, већ санкционише свако неовлашћено откривање информација које су „у поседу државног службеника” (Legislation 1989; Group of States against Corruption 2023). Та неодређеност омогућава широку интерпретацију: све што држава сматра осетљивим може постати предмет кривичног гоњења. Последица је култура у којој је тајност део професионалног идентитета, нарочито у *Secret Intelligence Service – MI6, Government Communications Headquarters – GCHQ* и Министарству одбране.

Кључни проблем је ограничен парламентарни надзор. Иако постоји Комитет за обавештајне и безбедносне послове (*Intelligence and Security Committee*), његове чланове именује премијер, а комитет нема право да покрене истраге по сопственој иницијативи. У истрази британског учешћа у операцији Централне обавештајне агенције која је обухватила противправни трансфер притвореника, Комитет је имао ограничен приступ документима, јер су били означени као САД тајно (*US Classified*), а британске агенције нису имале овлашћења за њихову декласификацију (*Intelligence and Security Committee of Parliament 2007*). Недавни покушаји реформе – попут Нацрта закона о изменама и допунама Закона о слободи приступа информацијама (*Freedom of Information (Amendment) Bill*) из 2023. године – довели су до даљег проширења изузетака за безбедносне службе, чиме је режим слободе приступа информацијама додатно ослабљен. Како је приметио истраживачки новинар Ричард Нортон-Тејлор (*Richard Norton-Taylor*), „британска тајност данас функционише као приватни клуб, а не као део јавне управе” (Norton-Taylor 2024). Ова метафора осликава систем у којем је тајност институционализована као средство самоодржања елите, а не као техничка мера безбедности.

Француски приступ тајности заснован је на снажној централизацији власти и традицији примата државног интереса (*raison d’État*). Закон бр. 91–646 о тајности преписке путем електронских комуникација (*Légifrance 1991*), донет 1991. године и допуњен 2017. и 2021, даје извршној власти готово апсолутну контролу над класификацијом. Министри одбране или унутрашњих послова могу једнострано прогласити документе

„тајним” без судског или парламентарног одобрења, а рок тајности може трајати до 75 година.

Парламентарни надзор формално постоји кроз Саветодавну комисију за питања тајности у области националне одбране (*Commission consultative du secret de la défense nationale – CCSDN*), али она нема овлашћење да наложи декласификацију, већ само даје препоруке које се често игноришу. Илустративан је случај француског војног ангажмана у Сахелу, где су извештаји о цивилним жртвама и грешкама у циљању остајали класификовани годинама, онемогућавајући јавну расправу о ефектима интервенције.

Француски медији и истраживачи изложени су кривичним санкцијама ако објаве класификоване информације, чак и када су до њих дошли преко трећих страна (нпр. Викиликс – *WikiLeaks*). Тако је 2022. године новинарка Мари-Маргерит Саблон (*Marie-Marguerite Sablon*) кривично гоњена према француском еквиваленту британског Закона о службеним тајнама, након објављивања документа о сарадњи француске спољне обавештајне службе – Генералне дирекције за спољну безбедност (*Direction Générale de la Sécurité Extérieure*) са мароканским обавештајним службама, иако документ није потицао из француске архиве. Оваква пракса не само да крши принципе слободе говора, већ и подрива демократску одговорност: када чак и већ прибављене информације постану кривично дело, друштво губи могућност да утиче на безбедносну политику.

Немачки приступ тајности снажно је обликован историјским наслеђем Штазија и режимом заштите личних података. Закон о тајности (*Geheimhaltungsgesetz*) из 2016. године захтева да класификација буде пропорционална, временски ограничена и подложна редовној ревизији. Сваки документ старији од 30 година аутоматски губи статус тајности, осим ако се докаже да би његово објављивање и даље представљало ризик.

Кључна разлика у односу на Уједињено Краљевство и Француску је снажнији парламентарни надзор. Комисија немачког Парламента за надзор рада савезних обавештајних служби (*Parlamentarisches Kontrollgremium – PKGr*) има право да захтева приступ било ком документу, укључујући и оне означене као државна тајна (*Streng Geheim*), као и да позива на јавна или затворена саслушања директоре *Bundesnachrichtendienst – BND*,

BfV – Bundesamt für Verfassungsschutz и *Amt für den Militärischen Abschirmdienst – MAD*. У случају сарадње *BND* и америчке *HSA*, комисија је 2014. покренула обимну истрагу која је довела до реформе законодавства и забране масовног прикупљања података о грађанима ЕУ.

Немачка такође није имуна на прекомерну класификацију. У областима као што су извоз наоружања или ангажман Оружаних снага Савезне Републике Немачке (*Bundeswehr*) у иностранству, документи се често класификују „из предострожности”, иако не садрже оперативну осетљиву податке. Критичари, укључујући *Transparency International Deutschland*, указују да се тајност у таквим случајевима користи ради прикривања политички неповољних информација, попут стварних трошкова или цивилних жртава (*Transparency International Deutschland* 2024). То показује да чак и у систему са најразвијенијим надзорним механизмима култура предострожности може преовладати над принципима транспарентности.

Табела 1. Компаративни закључак: три модела, један проблем

Земља	Правни оквир	Ниво надзора	Култура тајности
Уједињено Краљевство	Нејасно дефинисан (OSA)	Слаб (под контролом извршне власти)	Тајност као деонтологија
Француска	Централизован (secret défense)	Формалан, без извршне моћи	Raison d’État као апсолут
Немачка	Пропорционалан (Geheimhaltungsgesetz)	Јак парламентарни надзор	Тајност као изузетак

Извор: Обрада аутора.

Заједничко за британски, француски и немачки систем јесте да тајност функционише као инструмент управљања ризиком, али преваходно политичким, а не безбедносним. Прекомерна класификација у свим случајевима спречава институционално учење из претходних грешака, подрива јавно поверење и отежава сарадњу унутар НАТО. Нарочито је проблематично када британски документи не могу бити дељени са немачким партнерима због различитих стандарда у тумачењу појма „тајности”.

ЗАКЉУЧНА РАЗМАТРАЊА: КА КУЛТУРИ ОДГОВОРНЕ ТРАНСПАРЕНТНОСТИ

Анализа праксе у САД, ЕУ, Уједињеном Краљевству, Француској и Немачкој показује да прекомерна класификација није техничка аномалија, већ структурна карактеристика савремених демократских безбедносних апарата. Иако се системи разликују по правној форми, институционалној архитектури и историјском контексту, могу се идентификовати три заједничка узрочна обрасца:

1) Култура тајности као норма – логика „сигурније је затворити него отворити” интернализована је као правило понашања (Schein 2010).

2) Асиметрични подстицаји – службеници који откриву информацију сnose ризике (каријерне, дисциплинске, правне, кривичне), док они који неоправдано проширују тајност готово никада не сnose последице (Fenster 2006).

3) Слабост механизма спољашњег надзора – било да је реч о Конгресу САД, Европском парламенту, Комитету за обавештајне и безбедносне послове у Уједињеном Краљевству или Комисији немачког Парламента за надзор рада обавештајних служби, сва ова тела делују уз ограничен приступ информацијама, недовољне ресурсе или политичко прећуткивање.

Комбинација ових фактора производи системску патологију: тајност престаје да служи заштити националних интереса и постаје инструмент заштите институција од јавне и демократске одговорности. Последице су дубоке и вишеслојне.

Прво, опада ефикасност обавештајног рада. Када су информације прекомерно фрагментиране и недоступне чак и унутар исте институције, расте ризик од дуплирања активности, аналитичких грешака и пропуштања критичних сигнала. Управо такве недостатке Комисија за истрагу терористичких напада на САД (Комисија 9/11) идентификовала је као један од узрока неуспеха америчког система (9/11 Commission 2004).

Друго, долази до ерозије јавног поверења. Легитимитет безбедносног апарата нарушава се када грађани виде да се одлуке о рату, масовном надзору или међународним споразумима доносе у режиму тајности, а накнадно се покаже да су засноване

на погрешним или манипулисаним претпоставкама (нпр. инвазија на Ирак 2003. или повлачење из Авганистана 2021). Према Транспаренси интернешнл (*Transparency International*) (Transparency International 2025), чак 62% грађана у државама чланицама НАТО сматра да се „тајност користи како би се прикрили политички мотиви”.

Треће, негативне последице погађају међународну сарадњу. НАТО и ЕУ почивају на поверењу и дељењу информација, али у пракси британски документ може остати недоступан немачком партнеру због ознаке строго поверљиво УК (*UK Secret*), или француски извештај услед режима *secret défense*. У таквим условима савезништво губи оперативну вредност, а тајност постаје препрека колективној безбедности.

Прекомерна класификација је структурни проблем, а не последица индивидуалних злоупотреба. Она произлази из системске логике која награђује затвореност, санкционише отвореност и нема ефикасне механизме ретроактивне провере оправданости тајности. Овај образац присутан је и у САД, као најмоћнијој демократији, и у Немачкој, која има најразвијеније механизме надзора.

Међународно-правни оквири пружају јасан пут ка одговорној транспарентности. Цвана принципи националне безбедности и права на информације из 2013. године (Open Society Foundations 2013) захтевају да свака одлука о класификацији буде праћена проценом ризика, образложењем пропорционалности и применом најнижег неопходног степена заштите. Истанбулски документ ОЕБС из 1999. године (OSCE 1999) забрањује злоупотребу националне безбедности као изговора за прикривање корупције и неправилности. Тромсе конвенција Савета Европе из 2009. године (Tromsø Convention 2009) наглашава да тајност мора бити временски ограничена, подложна независној ревизији и заснована на објективној процени ризика.

Табела 2. Међународни стандарди у области прекомерне тајности

Инструмент / организација	Кључни принцип	Практична примена
GRECO (Савет Европе)	Тајност не сме подривати антикорупцијске механизме	Посебно критикује прекомерну употребу тајности у области јавних набавки и управљања јавним ресурсима
EU Security Rules	Пропорционалност, образложеност и временско ограничење	Често се примењује формално, без суштинске процене стварног безбедносног ризика
NATO AAP-06	Комбинација принципа „need-to-know” и „need-to-share”	Подстиче међусавезничку сарадњу, али се у пракси често сукобљава са националним културама тајности
Tshwane Principles (2013)	Конкретна и вероватна штета; демократска неопходност	Служе као референтни модел за реформу националних законодавстава и политика класификације
OSCE Istanbul Document	Забрана злоупотребе националне безбедности	Директно се односи на спречавање прикривања корупције и институционалних неправилности

Извор: Обрада аутора

Ови стандарди указују на два механизма: 1) кумулативне тестове – ограничење приступа мора испунити услове неопходности, претежног интереса и специфичности (конкретне и вероватне штете), при чему терет доказивања лежи на органу; 2) апсолутну забрану коришћења тајности за прикривање неправилности.

Ипак, проблем у пракси настаје када се технички стандарди спроводе формално, без суштинског повезивања са овим критеријумима. То доводи до две последице: 1) обесмишљавања система заштите – прекомерна употреба умањује кредибилитет ознаке; 2) ограничења демократског надзора – парламент, надзорна тела и медији остају без приступа кључним подацима.

Решење овог проблема не лежи у додатном пооштравању контрола, већ у суштинској промени парадигме – од логике „потребе да се сакрије” (*need to hide*) ка принципу „права да се зна” (*right to know*). У том смислу, кључни кораци обухватају: 1) увођење правног механизма који аутоматски укида важење закона, одредаба или мера о тајности по истеку њиховог важења (*sunset* клаузула), што би подразумевало аутоматску декласификацију информација након унапред дефинисаног рока (нпр. десет година за степен *Confidential*, 15 година за степен *Secret*, осим у случајевима у којима се оправданост продужетка експлицитно и документовано докаже; 2) јачање независних надзорних тела – кроз давање права иницијативе, обавезу објављивања јавних извештаја и директан приступ архивама; 3) систематску обуку службеника у области етике транспарентности – не само у погледу процедуралне примене режима тајности, већ и у разумевању демократске одговорности и јавног интереса; 4) хармонизацију минималних стандарда на нивоу НАТО и ЕУ – усвајањем заједничког оквира који јасно дефинише које врсте информација не смеју бити предмет класификације (нпр. анализе трошкова, процене цивилних жртава, документација о људским правима), што је у складу са савременим дискусијама о реформи безбедносног сектора у региону (Matić 2024; Starčević 2024).

Равнотежа између безбедности и транспарентности по својој природи увек остаје напета. Међутим, постојеће стање не представља равнотежу, већ системско преоптерећење у корист тајности, често без јасног и проверљивог оправдања. Уколико савремене демократије желе да очувају сопствену легитимност и институционалну ефикасност, неопходно је да препознају да право јавности на информисање није претња безбедности, већ један од њених кључних темеља. Јер, како је још давно упозорио амерички судија Луис Брендис (*Louis Brandeis*): „Сунце је најбоље дезинфекционо средство”.

Закључно, прекомерна класификација није ни чисто бирократски рефлекс, ни само намерна безбедносна илузија – она представља структурну спрегу ова два феномена. Бирократски рефлекс (страх од одговорности, институционална инерција) омогућава да се безбедносна илузија (прикривање политичких мотива) институционализује као „нормална пракса”.

РЕФЕРЕНЦЕ

- Aftergood, Steven. 2023. “Reducing Overclassification Through Accountability and Technology.” *Secrecy News, Federation of American Scientists*. October 15, 2023. <https://web.archive.org/web/20231016012102/https://fas.org/blogs/secrecy/2023/10/overclassification-accountability/>.
- Connelly, Matthew. 2023. *The Declassification Engine: What History Reveals About America's Top Secrets*. New York: Pantheon.
- Council of Europe Convention on Access to Official Documents (Tromsø Convetion) CETS, June 18, 2009, CETS No. 205.
- Council of Europe. 2009. “Convention on Access to Official Documents (CETS No. 205).” *Treaty Office*. June 18, 2009. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyenum=205>.
- Council of Europe. 2018. “Guidelines for GRECO Evaluation Teams (GETs).” *Group of states against Corruption – GRECO and Council of Europe*. December 7, 2018. <https://rm.coe.int/guidelines-get-eval5/16809005cd>.
- Dahl, Robert A. 1989. *Democracy and Its Critics*. New Haven: Yale University Press.
- Decision (EU) No. 2013/488/EU 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, OJ L 274, 15.10.2013, pp. 1–50. <https://eur-lex.europa.eu/eli/dec/2013/488/oj>.
- European Commission. 2024. “Standard Eurobarometer 99 – Spring 2024: Public Opinion in the European Union.” *Directorate-General for Communication*. Last accessed October 20, 2025. <https://europa.eu/eurobarometer/surveys/detail/standard-eurobarometer-99>.
- European Ombudsman. 2021. “Decision of the European Ombudsman on complaint 619/98/(IJH)/GG against the European Commission.” *European Ombudsman*. Last accessed October 20, 2025. <https://www.ombudsman.europa.eu/en/decision/en/1042-2020-mig>.

- European Parliament. 2023. "Report on the Implementation of Operation IRINI (2021/2206(INI)). Committee on Budgetary Control. 2023/2061(INI). PE 745.321." *European Parliament*. Last accessed October 20, 2025. http://www.europarl.europa.eu/doceo/document/A-9-2023-0232_EN.html.
- Federal Register. 2009. "Classified National Security Information." *Federal Register*. December 29, 2009. <https://www.federalregister.gov/documents/2010/01/05/E9-31418/classified-national-security-information>.
- Federal Register. 2022. "Declassification Reviews of Certain Documents Concerning the Terrorist Attacks of September 11, 2001." *Federal Register*. September 3, 2021. <https://www.federalregister.gov/documents/2021/09/09/2021-19578/declassification-reviews-of-certain-documents-concerning-the-terrorist-attacks-of-september-11-2001>.
- Fenster, Mark. 2006. "The Opacity of Transparency." *Administrative Law Review* 58 (3): 885–910.
- Group of States against Corruption. 2023. "Evaluation Report on the United Kingdom – Fourth Evaluation Round." *Council of Europe*. Last accessed October 20, 2025. https://rm.coe.int/16806ca4de?utm_.
- Habermas, Jürgen. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge, MA: MIT Press.
- Intelligence and Security Committee of Parliament. 2007. "Rendition: Ninth Report of Session 2006–07. HC 353." *The Stationery Office*. Last accessed October 20, 2025. <https://isc.independent.gov.uk/wp-content/uploads/2021/03/Rendition-Ninth-Report-of-Session-2006-07.pdf>.
- Légifrance. 1991. "Loi n° 91-646 du 10 juillet 1991 relative au secret de la défense nationale." *Journal Officiel de la République Française*. Last accessed October 20, 2025. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT0000000356407>.
- Legislation. 1989. "Official Secrets Act 1989." *Legislation*. Last accessed October 20, 2025. <https://www.legislation.gov.uk/ukpga/1989/6/contents>.
- Matić, Goran. 2024. „Veleizdaja u krivičnom zakonodavstvu Republike Srbije." *Politika nacionalne bezbednosti* 26 (1): 137–154. DOI: 10.5937/pnb26-50033.

- Moran, Jon. 2022. "From Secrecy to Transparency? The UK's Intelligence and Security Committee and Parliamentary Scrutiny of Intelligence." *Parliamentary Affairs* 75 (1): 145–163. DOI: 10.1093/pa/gsab053.
- National Security Archive. 2021. "The Classification That Would Not Die: A Case Study in Overclassification." *George Washington University*. Last accessed October 20, 2025. <https://nsarchive.gwu.edu/briefing-book/2021-08-10/classification-would-not-die>.
- NATO Standardization Office. 2021. "AAP-06: NATO Glossary of Terms and Definitions (Edition 2021)." *NATO Standardization Agency*. Last accessed October 20, 2025. https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/APP-6.pdf.
- Norton-Taylor, Richard. 2024. "British Secrecy Functions as a Private Club, Not Public Service." *The Guardian*. March 12, 2024. <https://www.theguardian.com/world/2024/mar/12/british-secrecy-private-club-not-public-service>.
- Open Society Foundations. 2013. "The Global Principles on National Security and the Right to Information (Tshwane Principles)." *Open Society Foundations*. Last accessed October 20, 2025. <https://www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf>.
- Organization for Security and Cooperation in Europe [OSCE]. 1999. "Istanbul Document 1999." *Organization for Security and Cooperation in Europe Summit*. November 19, 1999. <https://cdn.osce.org/sites/default/files/f/documents/4/2/17502.pdf>.
- Pozen, David. 2013. "The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information." *Harvard Law Review* 127 (2): 512–635.
- Pozen, David. 2023. "Executive Order 14040 and the Illusion of Secrecy Reform." *Lawfare*. November 15, 2023. Archived version. <https://web.archive.org/web/20231116000000/https://www.lawfaremedia.org/article/eo-14040-secrecy-reform>.
- Public Interest Declassification Board. 2022. "Annual Report 2022." *National Archives and Records Administration*. Last accessed October 20, 2025. <https://www.archives.gov/files/isoo/pidb/reports/pidb-annual-report-2022.pdf>.
- Schein, Edgar H. 2010. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.

- Schmitt, Carl. [1922] 2005. *Political Theology: Four Chapters on the Concept of Sovereignty*. Chicago: University of Chicago Press.
- Starčević, Srđan. 2024. „Povratak obaveznog služenja vojnog roka u Evropi – društveni determinizam i perspektive.” *Politika nacionalne bezbednosti* 26 (1): 11–26. DOI: 10.5937/pnb26-50140.
- The National Commission on Terrorist Attacks Upon the United States [9/11 Commission]. 2004. “The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.” *W. W. Norton and Company*. Last accessed October 20, 2025. <https://www.9-11commission.gov/report/911Report.pdf>.
- Transparency International Deutschland. 2024. “Geheimhaltung und Demokratie: Eine Bestandsaufnahme der parlamentarischen Kontrolle.” *Transparency International Deutschland*. Last accessed October 20, 2025. <https://www.transparency.de/publikationen/geheimhaltung-und-demokratie/>.
- Transparency International. 2025. “Global Corruption Barometer – Europe & Central Asia 2025: Trust in Institutions.” *Transparency International Secretariat*. Last accessed October 23, 2026. <https://www.transparency.org/en/gcb/europe-central-asia/europe-central-asia-2025>.
- United Nations Educational, Scientific and Cultural Organization. 2014. “UNESCO Guidelines on Freedom of Expression and National Security.” *UNESCO*. Last accessed October 20, 2025. <https://unesdoc.unesco.org/ark:/48223/pf0000229381>.
- US Congress. House. Committee on Oversight and Government Reform [USC]. 2016. “Hearing on Government Secrecy and Oversight Challenges.” *114th Cong., C-SPAN*. Last accessed October 20, 2025. <https://www.c-span.org/video/?406395-1/hearing-government-secrecy-oversight-challenges>.
- Wilson, James Q. 1989. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.

Goran Matic*

*Faculty of Business Studies and Law,
University "Union – Nikola Tesla", Belgrade, Republic of Serbia*

EXCESSIVE SECRECY IN DEMOCRACIES: BUREAUCRATIC REFLEX OR SECURITY ILLUSION?

Resume

“Excessive Secrecy in Democracies” examines the systemic over-classification of information within the security apparatuses of the United States, the European Union, and key NATO allies. The central thesis of the study is that excessive secrecy does not represent an incidental administrative deviation, but rather a structured institutional choice arising from the distinction between *security secrecy* – the protection of operational capabilities and *political secrecy* – the shielding of institutions from political and legal accountability. It is precisely in this shift of focus from security protection to institutional self-preservation that the author locates the core of the problem. The comparative analysis identifies common patterns across different systems: defensive classification as a strategy of risk minimization, asymmetric incentives that penalize openness, and the limited effectiveness of external oversight mechanisms. Public officials are institutionally incentivized to classify information, as potential harm resulting from disclosure carries sanctions, whereas excessive secrecy rarely entails consequences. Such a logic generates a culture of preventive information closure. In the United States, a deeply embedded culture of secrecy and fear of accountability results in the classification of tens of millions of pages annually, while automatic declassification remains, in practice, a largely formal norm without substantial effect. Within the European Union, the problem manifests through institutional fragmentation: divergent national secrecy regimes impede horizontal cooperation, and classification is frequently employed to protect negotiating positions and political sensitivities. The analysis of the United Kingdom, France, and Germany demonstrates that,

* E-mail address: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797.

despite differing legal traditions, secrecy functions as an instrument of political risk management. The British model is characterized by limited parliamentary oversight; the French system is strongly centralized around the concept of state interest; and the German system, although formally more robust in terms of control, exhibits pronounced bureaucratic inertia. The consequences of excessive secrecy are multifaceted. The fragmentation of information diminishes the operational effectiveness of intelligence services. Simultaneously, public trust erodes, as secrecy is used to conceal political motives and errors, thereby undermining democratic legitimacy. Moreover, the lack of harmonized standards complicates cooperation within the NATO alliance. In conclusion, the study calls for a paradigmatic shift: from the logic of the *need to conceal* toward the principle of the *right to know*. It proposes the mandatory introduction of time-bound *sunset* clauses for classification, the strengthening of the independence of oversight bodies, and the harmonization of standards at the EU and NATO levels. Only a systemic approach can effectively limit the misuse of secrecy and ensure that it remains an exception rather than the governing rule of democratic governance.

Keywords: overclassification, secrecy, intelligence community, democratic accountability, right to information, United States, European Union, NATO, comparative analysis.

* Овај рад је примљен 27. фебруара 2026. године, а прихваћен за штампу на састанку Редакције 27. фебруара 2026. године.