Artigo original

http://dx.doi.org/10.18623/rvd.v23.n1.4095

NATIONAL SECURITY LAW AND DEMOCRATIC GOVERNANCE IN TURKEY

DIREITO DA SEGURANÇA NACIONAL E GOVERNANÇA DEMOCRÁTICA NA TURQUIYE

Article received on: 8/29/2025
Article accepted on: 11/28/2025

Mehmet Recai Uygur*
*SMK College of Applied Sciences, Vilnius, Lithuania
Orcid: https://orcid.org/0000-0003-1872-0885
mehmetrecai.uygur@smk.lt

The authors declare that there is no conflict of interest

Abstract
This article argues that Türkiye's national security governance is legally fragmented across counter-terrorism, intelligence, digital surveillance and emergency regimes, producing deficits in legal certainty, accountability and rights protection. Using comparative doctrinal analysis of the United States (USA PATRIOT Act), the United Kingdom (Investigatory Powers Act 2016; National Security Act 2023) and the European Union's fundamental-rights and data-protection standards, it develops a blueprint for a holistic National Security Law (NSL) for Türkiye. The proposed design combines a narrow and justiciable threat definition, a tiered powers architecture (ordinary times/escalating risk/state of emergency), mandatory reporting to Parliament, independent oversight, and strengthened judicial authorisation. It embeds end-to-end safeguards for surveillance and data processing, data minimisation, retention limits, audit trails, delayed notification and effective remedies, while constraining emergency powers through strict time limits, qualified-majority extensions and sunset clauses. Drawing on Foucault's panopticism and Agamben's "state of exception", the article explains how vague security norms can generate chilling effects, weaken legitimacy and depress civic participation. It concludes that a rights-consistent NSL can improve security effectiveness and public trust, and address climate/disaster-related risks without securitising environmental civic space.

Keywords: National Security Law, Security Governance, Intelligence Oversight, Digital Surveillance, Emergency Powers, Sustainable Development.

Resumo
Este artigo sustenta que a governança da segurança nacional na Türkiye encontra-se juridicamente fragmentada entre os regimes de combate ao terrorismo, inteligência, vigilância digital e poderes de emergência, produzindo déficits de segurança jurídica, responsabilização e proteção de direitos. Com base em uma análise doutrinária comparativa dos Estados Unidos (USA PATRIOT Act), do Reino Unido (Investigatory Powers Act 2016; National Security Act 2023) e dos padrões da União Europeia em direitos fundamentais e proteção de dados, o estudo desenvolve um modelo para uma Lei de Segurança Nacional (LSN) holística para a Türkiye. O desenho proposto combina uma definição de ameaça restrita e judicializável, uma arquitetura escalonada de poderes (normalidade/risco crescente/estado de emergência), prestação de contas obrigatória ao Parlamento, supervisão independente e fortalecimento da autorização judicial. Integra salvaguardas de ponta a ponta para vigilância e tratamento de dados — minimização de dados, limites de retenção, trilhas de auditoria, notificação posterior e mecanismos efetivos de reparação — ao mesmo tempo em que restringe poderes de emergência por meio de prazos rígidos, prorrogações por maioria qualificada e cláusulas de caducidade. A partir do panoptismo de Foucault e do conceito de "estado de exceção" de Agamben, o artigo explica como normas de segurança vagas podem gerar efeitos de intimidação, enfraquecer a legitimidade e reduzir a participação cívica. Conclui que uma LSN compatível com direitos fundamentais pode aumentar a eficácia da segurança e a confiança pública, além de enfrentar riscos climáticos e de desastres sem securitizar o espaço cívico ambiental.

Palavras-chave: *Direito da Segurança Nacional. Governança da Segurança. Supervisão de İnteligência. Vigilância Digital. Poderes de Emergência. Desenvolvimento Sustentável.*

1 INTRODUCTION

National security is one of the oldest and most powerful words in the modern state; once uttered, the normal rhythm of the legal system often accelerates, and sometimes slows down. At times when the narrative of threat intensifies, the law becomes not only a “shield” but also a “language” through which power reorganizes itself: what is considered dangerous, who labels the danger, what powers this labeling legitimizes, and ultimately what rights can be restricted and to what extent, these are, above all, issues of legal design. For this reason, national security is not merely a policy area; it also represents a threshold where the idea of the rule of law is tested, and where the “exception” sometimes becomes the norm (Agamben, 2003).

In Turkey, security legislation has been shaped by numerous laws, KHK/CBK regulations, administrative practices, and judicial interpretations under the heavy pressure of historical and political context. counterterrorism, intelligence, law enforcement powers, regulation of the digital sphere, states of emergency, and data processing practices have taken on the appearance of a “normative mosaic” rather than a unified framework. This fragmented structure not only produces a purely technical disorder; it also creates a structural void in the fundamental promises of law: predictability, accountability, and guarantees of rights. When different sets of norms operating under the banner of “security” fail to produce compatible conceptual frameworks, the same act can lead to different legal outcomes in different contexts; the same authority can be subject to different thresholds of oversight by different institutions; similar interventions can be grounded in different regimes of justification. In such an environment, as the criteria of “law quality” and “predictability” weaken, even security effectiveness becomes less of a stable management outcome; because legitimacy erodes, social trust is undermined, and the state's security capacity risks relying increasingly on coercion and uncertainty management rather than citizen consent (The Sunday Times V. The United Kingdom (No. 1), 1979).

The starting point of this article is that it is necessary for national security in Turkey to be managed within the framework of a comprehensive National Security Law (NSL) that is compatible with rights, accountable, and has clearly defined design principles, rather than through "multiple legislative islands." Indeed, in contemporary legal systems, security laws do not merely grant authority; they also "bind" power by defining the dimensions of this authority in terms of purpose, scope, duration, procedure, and oversight. In a sense, the NSL is a proposed institutional architecture that seeks to subject the "discursive power" of security to the discipline of legal technique. In the absence of this discipline, an "asymmetry of visibility" (the state sees/monitors, while citizens cannot see the channels of oversight) of the kind that can be described by Foucault's panoptic logic easily becomes institutionalized; control can become a discursive promise, and transparency an exceptional "gift" practice (Foucault, 1975).

The comparative perspective is important here for two reasons. First, national security law produces similar tensions in different democratic regimes: there is an inevitable conflict between the demand for speed, secrecy, and effectiveness in the face of threats, and the legality, judicial oversight, and proportionality required by the regime of rights. Managing this conflict is a matter of normative design. For example, in the United Kingdom, the Investigatory Powers Act 2016 provides a detailed framework for communication surveillance and authorization processes; while the recently enacted National Security Act 2023 institutionalizes a new security language through modernized crime types and registration regimes in areas such as state threats and foreign influence (United Kingdom, 2016; United Kingdom, 2023). In the US, the USA PATRIOT Act, one of the symbolic texts of the post-September 11 security architecture, reshaped the legal basis for expanded investigation and surveillance powers in the fight against terrorism; this expansion subsequently deepened debates on oversight and limitations (United States Of America, 2001). At the European Union level, Article 52 of the EU Charter of Fundamental Rights, which centers on the "legality–substance preservation–necessity–proportionality" test regarding the limitation of fundamental rights, provides a strong normative framework for determining the threshold for the legitimacy of security-related interventions (European Union, 2012).

Second, the comparison allows for the search for transferable design principles rather than transferable institutions. This is because good design in security law is not about transferring the same text to every country; it is about establishing a minimum set

of safeguards that will work within each country's constitutional culture, judicial review tradition, and social conflict dynamics. The case law of the European Court of Human Rights on mass surveillance regimes shows what this minimum set might look like: While not ruling out mass surveillance in principle, the Court requires "end-to-end" safeguards (authorization, scope limitations, independent oversight, data processing/access restrictions, and effective remedies) would render such a regime incompatible with the ECHR (Big Brother Watch and Others V. The United Kingdom, 2021; Roman Zakharov V. Russia, 2015). Similarly, the Venice Commission's reports on democratic oversight of signals intelligence and strategic surveillance focus on the search for institutional balance that prevents security agencies from operating entirely outside the law under the pretext of "secrecy" (Venice Commission, 2015). This literature requires that "oversight" be placed at the center of the NSL design for Turkey, as much as "authority."

This study proceeds from the assumption that security must be considered not only in terms of military and counterterrorism, but also in the context of cyberspace, critical infrastructure, public health, disaster management, and increasingly visible climate/environment-based risks. Discussions on the expansion of security studies (individual/social/environmental security) have shown that the concept of "threat" cannot be reduced to a single area; however, precisely because of this expansion, legal boundaries must be drawn more carefully (Buzan; Wæver; De Wilde, 1998). Climate change is increasingly being linked to security at the political and institutional levels as a "risk multiplier" that affects social vulnerabilities, migration dynamics, food and water security, and the likelihood of local conflicts (IPCC, 2022; BRIGGS, 2012). The ongoing discussions on the climate-security nexus in the United Nations Security Council are also an indication that environmental risks are redefining the security agenda (Security Council Report, 2022). However, this link carries a two-sided risk: ignoring environmental risks undermines long-term security planning; while unlimitedly expanding environmental risks under the "security" label may restrict participatory environmental management and the civil sphere. Therefore, the place of environmental/climate-based risks in NSL design must be considered alongside the principles of sustainable development and participatory governance. Indeed, the Aarhus Convention, which guarantees access to environmental decision-making processes and public participation, emphasizes that the circulation of information and access to justice in the environmental field are part of democratic resilience (UNECE, 1998). From this

perspective, a rights-compliant NSL should include environmental risks in the security agenda without producing language that confines environmental advocacy or public dissent to the semantics of "threat."

This article seeks answers to four fundamental research questions: What rule of law risks (particularly in terms of predictability, accountability, and rights safeguards) does the fragmented security regime in Turkey generate? What design principles from the US/UK/EU examples can be transferred to Turkey? How can NSLs guarantee civil liberties through institutional safeguards while increasing security effectiveness? Finally, how can NSL design connect with a sustainable development perspective and the management of environmental/climate-based risks?

The methodology for answering these questions is based on three axes. The first axis is comparative doctrinal analysis: security powers, surveillance/intelligence architecture, and the limits of extraordinary powers will be examined through the US/UK/EU frameworks to identify principles that can be transferred to Turkey. The second axis is socio-legal and critical theory: the functioning of security within power relations will be discussed using the concepts of panoptic surveillance and the regime of exception; how the legal form is expanded by the "security discourse" and at which points it produces a normative fog will be analyzed (Foucault, 1975; Agamben, 2003). The third axis is normative design: based on the restriction regimes of international human rights law in the areas of emergency and security (ECHR art. 15; ICCPR art. 4) and relevant case law/guidance documents, a minimum institutional template for a rights-compliant NSL will be proposed for Turkey (Council of Europe, 1950; United Nations, 1966). The ethical-political basis of this framework will also be determined by the approach that public power is accountable to the idea of "secure and equal freedom" even in times of crisis (Criddle; Fox-Decent, 2012).

The contribution of this study can be summarized in a single sentence: I propose a rights-compliant NSL design template for Turkey. This template does not aim to expand security law; on the contrary, it aims to limit security by "designing" it within the law, making it controllable, and bringing it into line with long-term democratic resilience. Because national security, ultimately, is not only about eliminating threats; it is also about public life being governed by predictable rules, not fear.

2 CONCEPTUAL AND METHODOLOGICAL LIMITATIONS

This study draws two boundaries from the outset: the first is the boundary of concepts, the second is the boundary of method. Because concepts such as "national security" are not merely words that provide definitions in the lexicon of law; they are also gateways that legitimize exceptions. When the door is left wide open, it becomes unclear who can enter and on what grounds; uncertainty increases authority while diminishing control. Therefore, the aim here is to remove national security from being a "flexible metaphor of politics" and place it within a legal category that is amenable to judicial review, measurable, and compatible with legal safeguards. This limitation is based on the assumption that a language that makes national security "everything" ultimately guarantees nothing: as the security regime becomes more inclusive, legal predictability and democratic legitimacy erode; this erosion, in turn, weakens security capacity itself in the long term (Venice Commission, 2025).

2.1 Conceptual framework

(i) The concept of "national security": the need for narrowing and a proposed definition

In modern law, the concept of national security is often "the name of a thing" but not "the boundary of a thing." Where boundaries are not drawn, national security acts as a center of gravity that can draw in all areas of public order; it invokes 'extraordinary' reflexes in place of "normal" control mechanisms, particularly over rights such as freedom of expression, association, and access to information. In international human rights doctrine, this risk has been met with explicit warnings that national security should not be used as a justification to protect governments from criticism. The United Nations Human Rights Committee emphasizes that restrictions on freedom of expression must be narrow interventions that are *provided for by law*, *pursue legitimate aims*, and satisfy the *necessity–proportionality* conditions; it also stresses that the national security justification should not be expanded in an "open-ended" manner (United Nations Human Rights Committee, 2011).

In this context, this article adopts a narrow and judicially reviewable definition of "national security": National security refers to the obligation to protect against *serious*

and concrete threats to the fundamental existence of the state and society. The phrase "fundamental conditions of existence" in this definition is linked to a core area to prevent arbitrary expansion: (a) threats to life and physical integrity on a mass scale, (b) serious threats to the territorial integrity of the country, (c) serious attempts to abolish the constitutional-democratic order through coercion/violence, (d) serious social destruction that could result from the large-scale collapse of critical infrastructure (energy, water, health, communications). The criteria of "seriousness" and "concreteness" are central to the definition, because the possibility of judicial review arises not from the poetic breadth of the concept, but from its normative measurability. The Johannesburg Principles are particularly important to prevent national security from being equated with essential elements of a democratic society such as "peaceful opposition," "public criticism," or "disturbing ideas": The approach that peaceful expression should not be considered a threat to national security and that punishment on grounds of national security can only be justified in situations closely related to violence serves as a normative compass that tightens the boundaries of the definition (Article 19, 1995).

This narrowing does not diminish the concept of "security"; it makes it controllable. Indeed, in the European human rights system, the ideas of "quality of law" and "foreseeability" are emphasized as a barrier against the arbitrariness arising from vague norms, particularly in security and surveillance measures. Documents compiled by the Council of Europe on national security and the case law of the European Court of Human Rights highlight the need for the legal framework underpinning intervention to be accessible and foreseeable, and to be surrounded by strong safeguards, particularly in areas such as surveillance (Council of Europe, n.d.).

(ii) The "sustainability" link: security regime, governance, and the long term

In this article, sustainability is addressed not only as an ethical ideal belonging to the field of environmental policy, but also as a governance capacity intertwined with the capacity of the rule of law. Sustainable development, in its classic definition, is the claim to be able to meet "today's needs without compromising the ability of future generations to meet their own needs"; this claim is only possible through resource management, institutional stability, the predictability of the law, and the continuity of public trust (World Commission on Environment and Development, 1987). Therefore, fragmented and uncertain security regimes pose a dual risk to sustainable development: on the one

hand, they perpetuate crisis management, feeding the "normality of the extraordinary," and on the other hand, they erode predictability, which is the fundamental basis of investment, planning, and participation processes. The link between the design of national security law and sustainability is established precisely at this point: establishing an institutional balance between security effectiveness and rights guarantees is a condition for long-term development capacity (McGoldrick, 1996; Venice Commission, 2025).

This approach is also consistent with the emphasis on "peaceful and inclusive societies," "accountable institutions," and "the rule of law" seen in the United Nations 2030 Agenda: sustainable development goals are not only technical policy goals, but also goals of the rule of law and institutional reliability (United Nations General Assembly, 2015).

The second pillar of the sustainability connection is the area of non-traditional risks such as climate/disasters. Climate change can act as a "risk multiplier" for security risks through channels such as extreme weather events, food–water stress, mass displacement, and deepening vulnerabilities; such relationships are discussed in both scientific synthesis reports and social science literature (Hsiang et al., 2013; Intergovernmental Panel on Climate Change, 2022). However, this observation does not automatically legitimize the "securitization" of climate. On the contrary, the intersection of climate-based risks with security law should be designed through disaster governance, resilience, transparent information flow, and public participation, rather than the expansion of extraordinary powers; because the climate crisis is long-term, and the long term can be managed through the predictability of law, not through emergency law (United Nations General Assembly, 2015).

(iii) Principles of rights restriction: the "normative grammar" of national security

The normative backbone of this study is the established 'test' logic of rights restrictions in international human rights law. The aim here is not to list principles as an abstract catalog, but to establish a "grammar" that will work wherever national security touches the sphere of rights.

The first axis of this grammar is legality and foreseeability. The Siracusa Principles emphasize that restrictions on rights must be provided for by law, must not undermine the essence of the right, and must be narrowly interpreted; this approach transforms the idea of "the limit of restriction" into a normative guarantee (United Nations Commission on

Human Rights, 1984). Similarly, Article 52 of the Charter of Fundamental Rights of the European Union explicitly states that any limitation must be provided for by law, respect the essence of the right, and meet the "necessity" condition based on the principle of proportionality (European Union, 2012). The Venice Commission's updated Rule of Law Checklist comprehensively frames "the accessibility and predictability of the law" (under legal certainty) and, particularly in exceptional circumstances, the limitation of exceptions by the guarantees of the rule of law (within legality); and positions balance-control mechanisms and the protection of "civic space" among the core elements of the rule of law (Venice Commission, 2025).

The second axis is legitimate purpose, necessity, and proportionality. Proportionality has become widespread in contemporary constitutional and human rights jurisprudence as a "global reasoning technique"; however, this technique also has its critics: proportionality sometimes carries the risk of reducing rights to a "mathematical" equation. This debate reminds us that the limitation of rights is not merely technical, but also a political-ethical area of choice (Klatt, 2012; Stone Sweet & Mathews, 2008; Tsakyrakis, 2009). Therefore, this article aims to use proportionality not as a balancing discourse that "justifies everything," but as a discipline that transparently justifies. The literature on the more transparent and structured application of the European Court of Human Rights' 'necessity' test shows that the necessity element can be strengthened by the "least restrictive means" approach; which requires considering "difficult but light" methods instead of "easy but heavy" methods in national security interventions (European Data Protection Supervisor, 2017; Gerards, 2013).

The third axis is the prohibition of discrimination and effective remedy. National security regimes can have a disproportionate impact on certain groups, particularly due to vague concepts and broad discretionary powers; therefore, both equality and access to justice are not "additional" principles of security law, but foundational safeguards. The Venice Commission's checklist regulates equality–the prohibition of discrimination and access to justice as fundamental components of the rule of law (Venice Commission, 2025).

Finally, a sharp distinction must be maintained between limitation and derogation (suspension). Article 4 of the ICCPR and General Comment No. 29 of the Human Rights Committee emphasize that derogation can only be applied in a declared state of emergency "threatening the life of the nation," to the extent strictly required by the

situation, and with due regard for the prohibition of discrimination; moreover, the overriding aim is "return to normal" (United Nations, 1966; United Nations Human Rights Committee, 2001). Similarly, Council of Europe documents concerning Article 15 of the European Convention on Human Rights highlight the conditions for derogation and the "strictly required" limit (Council of Europe, n.d.). This distinction produces a critical result in the context of Turkey's NSL design: the NSL must not be a "permanent emergency law" that perpetuates the extraordinary; it must be a normalization architecture that narrows the triggers for a state of emergency and clarifies the conditions of duration and oversight.

2.2 Method and comparison matrix

(i) Method: comparative doctrinal analysis + socio-legal theory + normative design

This study proceeds with a three-layered method. The first layer is comparative doctrinal analysis: it examines which normative tools are used to establish national security powers in the selected legal systems, which oversight mechanisms limit them, and which rights guarantees accompany their operation. The second layer is socio-legal theory: it analyzes how security law is not only a set of norms but also a technique of power; how surveillance, intelligence, and emergency measures transform "the way the state sees itself" and "the way society sees the state." This second layer will intersect with Foucault's concept of panopticism and Agamben's discussion of the state of exception in later sections of the study (only the methodological placement is indicated in this section).

The third layer is normative design: the lessons learned from the comparison are transformed into "design principles" in a manner consistent with Turkey's constitutional and social context. The purpose of comparison here is not "legal transplantation"; the context blindness of transplantation often results in the loss of the spirit of the law while carrying its text. Therefore, the comparison is conducted with an approach that follows the responses to similar problems at the "functional" level, but is also aware of the blind spots of functionalism itself. Ralf Michaels' assessment of the functional method emphasizes that the method is powerful in understanding different legal systems but limited in direct evaluation and standardization; this warning requires replacing the search for the "best model" in NSL design with the search for "transferable principles" (Michaels, 2006). Studies that recall the critical dimension of the functional approach also

show that comparison can be misleading where the function is incorrectly established; therefore, context and inter-institutional balance will be decisive in determining transferable principles for Turkey (Platsas, 2008).

This methodological preference is also consistent with the view that "comparison" is already an inevitable activity in legal thought: comparison is not just about placing different countries side by side; it is also about testing the consistency of the norm itself, the clarity of the means-ends relationship, and the functioning of safeguards (Michaels, 2006).

(ii) Why the US/UK/EU? Rationale for selection

The three selected comparative planes are not repetitive examples; they are three distinct laboratories offering different balance-and-check architectures. The US represents a system where national security law can be established with broad powers, but where strong judicial debates and institutional oversight mechanisms (especially in the area of surveillance) are also concentrated. The UK is an example where national security and intelligence powers are regulated with a greater tendency towards "codification" and where authorization-control schemes (ex ante/ex post) are clearly defined. Although not a state, the EU provides a normative framework that indirectly but powerfully influences member states' security practices through its fundamental rights regime (Article 52 of the Charter), the institutional language of data protection law, and multi-layered judicial oversight (CJEU/national courts) (European Data Protection Supervisor, 2017; European Union, 2012).

The selection of these three levels serves the purpose of bringing "different control models" side by side: they form axes that differ from each other in terms of (1) the definition of authority, (2) the technique of authorization, (3) the institutional diversity of control, and (4) the architecture of the state of emergency. Thus, the NSL template proposed for Turkey can distinguish the strengths and weaknesses of different systems at the level of "design principles" without being tied to a single model.

(iii) Comparison matrix: analysis dimensions and coding questions

To ensure that the comparative section does not become "scattered," each legal system will be examined using the same questions. The following matrix shows the

analytical scheme that will enable the US/UK/EU regulations and Turkey's current fragmented regime to be evaluated under the same lens in the following sections:

Table 1

Threat-Based Security Law Compliance Matrix

Analysis dimension	**The fundamental question asked in this study (operational)**
Definition of threat	What thresholds define a "national security threat"; is there a criterion for the seriousness/concreteness of the definition?
Intelligence authority	For what purposes and within what limits are intelligence gathering powers granted; how is purpose creep prevented?
Surveillance authorization (ex ante / ex post)	How is a balance established between prior authorization (judicial/independent administrative) and subsequent oversight?
Oversight/reporting	How are parliamentary oversight, independent authorities, oversight reports, and transparency mechanisms designed?
State of emergency triggers and duration	What are the conditions for declaring a state of emergency, the time limit, the extension procedure, and the guarantees for a "return to normal"?
Rights safeguards/judicial oversight	How are effective remedies, non-discrimination, access to justice in cases of secret proceedings, and judicial oversight ensured?

Source: Created by Author

This matrix is intended to measure not only security effectiveness but also the compatibility of security law with the rule of law. The measurement criteria are considered in conjunction with the normative grammar established above: legality–predictability; legitimate purpose; necessity and proportionality; prohibition of discrimination; effective remedy. The Venice Commission's current checklist provides institutional support for the use of these criteria as a “legal design standard” (Venice Commission, 2025).

The key point to emphasize at the close of this section is this: Comparison is not a window shopping exercise; it is established as a design discipline. The legal definition and methodological lens of national security aim to protect not only the security apparatus but also the “self-governing capacity” of democratic society. This capacity is also the silent infrastructure of sustainable development: when the rule of law weakens, not only rights but also long-term governance and social resilience weaken (McGoldrick, 1996; United Nations General Assembly, 2015).

3 COMPARATIVE EXPERIENCES

Comparative law is often practiced with an appetite for “model importation”; however, in politically sensitive areas such as national security, it is necessary to read not the institutional forms, but the design logic behind those forms. This is because security norms respond not only to “threats,” but also to how the state narrates itself, how it legitimizes its own power through words. Therefore, the practices of the US, the UK, and the EU are not “example packages” here; they are treated as testing grounds in terms of combating uncertainty, legalizing surveillance, and preventing the extraordinary from seeping into the ordinary. (European Court of Human Rights, 2025).

3.1 Defining the threat and combating “vagueness”

The first breaking point in national security law is the definition of the threat: as the definition narrows, the state's room for maneuver shrinks; as the definition broadens, the rule of law “stretches.” Stretching often promises comfort: vague concepts adapt quickly to the changing risk landscape. However, from the perspective of the rule of law, vagueness is not merely a technical flaw; it is a political opportunity that obscures the boundaries of authority. For this reason, the Strasbourg line insistently emphasizes criteria such as accessibility and predictability for intervention to be considered compatible with “law”; it seeks the concretization of minimum safeguards against arbitrariness in the norm, especially in secret surveillance regimes (European Court of Human Rights, 2025).

The issue of “definition” in counterterrorism law is a classic example that lays bare the tension between uncertainty and security. The literature, which points to the normative and political impossibility of seeking a single definition of terrorism, also shows that broad definitions create a “channel for abuse”: as the scope of the threat expands, the lines between crime and dissent; violence and protest; and organization and “danger” become blurred (Greene, 2017). This blurring is destructive not only for individual freedoms but also for security itself, as it erodes the legitimacy of security institutions by increasing the likelihood of selective and discriminatory application. Indeed, United Nations human rights mechanisms regularly emphasize that overly broad definitions of terrorism can become a tool for suppressing activism, press activity, or civil

society work, thereby creating a cycle that erodes fundamental rights "in the name of security" (United Nations Human Rights Committee, 2001; Scheinin, 2010).

US practice represents a "partially measurable" line in defining the threat. For example, the definitions of "international terrorism" and "domestic terrorism" in federal law are linked, at least, to the element of an act involving violence or danger to human life and a specific "purpose" (18 U.S.C. § 2331, 2025). This is a framework that does not leave the definition entirely to political discretion; however, phrases such as "appear to be intended" introduce an area open to interpretation into the system. Here, the uncertainty grows not at the level of words, but at the level of application: Reading the threat through the lens of "apparent intent" can, in some cases, broaden the scope of punishment and be flexible depending on the political context (Congressional Research Service, 2021).

In the United Kingdom, the recent new regime centered on "state threats" has reignited the debate on uncertainty. Topics such as espionage and "foreign interference," modernized by the National Security Act 2023, aim to establish a broader set of tools for the state to counter influence activities linked to foreign powers (National Security Act 2023, 2023). However, the breadth of the regime has been noted by independent review mechanisms themselves as posing a risk of "overreach." The independent review report emphasizes that certain types of crimes and conditions could extend to the realm of everyday political activity; in particular, it highlights that elements such as the "foreign power condition," if broadly interpreted in practice, could have a deterrent effect on journalism, academic work, protest, and political advocacy (Hall, 2025). This shows that in combating uncertainty, the "interpretation regime" is as decisive as the "definition": when the breadth of the normative text is not balanced by the triad of oversight–discretion–accountability, the law of security overshadows the law of rights.

The EU experience, however, points in a different direction: While the concept of "national security" is often left to the political discretion of member states, in areas such as the storage and access of communications data, the fundamental rights standard of Union law limits the uncertainty of the threat through its consequences. The CJEU's case law on data retention regimes has drawn a strong line against general and indiscriminate retention obligations, bringing the necessity and proportionality test closer to a "strict necessity" threshold (Tele2 Sverige AB and Others, 2016). This approach aims to systematically curb the encroachment of measures labeled as "threats" into the sphere of

rights, rather than defining the concept of threat itself; thus preventing the automatic legal consequences of vague threat language (Zalnieriute, 2021).

When read together, these three lines make it clear that "combating vagueness" is not a single technical solution: A limited and reviewable list of threats; principles that fix the interpretation of the definition in favor of rights; and the obligation of periodic review appear as fundamental design pillars that subject the political appeal of vagueness to the discipline of the rule of law (Scheinin, 2010; European Court of Human Rights, 2025).

3.2 Intelligence oversight and surveillance

Covert surveillance is the modern state's "seeing" capacity; however, when the state's seeing results in the citizen becoming invisible, the rule of law suffers a loss of balance. Therefore, the issue in the field of intelligence and surveillance is not merely the existence of powers; it is how these powers are authorized, recorded, monitored, and made subject to appeal. The Strasbourg case law's emphasis on "minimum safeguards" serves as a kind of constitutional compass here: elements such as the scope of covert measures, their duration, storage–destruction regime, independent oversight, and effective recourse are normative barriers against arbitrariness (European Court of Human Rights, 2025).

In the United Kingdom, the Investigatory Powers Act 2016 stands out with its claim to transform these barriers into an institutional architecture. The symbolic core of the regime is the "double lock" system: for the most intrusive powers, the executive's (Secretary of State) approval is filtered a second time by independent judicial oversight (Judicial Commissioners) (Investigatory Powers Act 2016, 2016; IPCO, 2025a). This two-stage structure aims to strengthen "ex ante" control, while the annual reports of the Investigatory Powers Commissioner's Office feed into the layer of transparency and accountability (IPCO, 2025b). Furthermore, complaint/appeal channels such as the Investigatory Powers Tribunal provide an institutional basis for the principle of "effective appeal," which risks being weakened due to confidentiality (Investigatory Powers Tribunal, 2024). Finally, the regime itself being subject to independent review, the assessment of the IPA 2016's reform needs in a separate report, produces a "post-legislative scrutiny" technique that supports the continuity of oversight (Anderson, 2023).

In the US, oversight is organized in a different form, more along the lines of "judicial process–congressional oversight–administrative procedure." Section 702 (50 U.S.C. § 1881a) defines the logic of a program conducted for foreign intelligence purposes, based on targeting "persons outside the United States"; at the heart of the regime is the judicial acceptance of procedures and certifications and their limitation by minimization/application rules (50 U.S.C. § 1881a, 2025). This area has been the focus of reform debates, particularly regarding "US-person queries" and the access-interrogation regime; indeed, CRS assessments show that design interventions such as limiting these queries and subjecting them to judicial approval attempt to recalibrate the tension between civil liberties and security effectiveness (Congressional Research Service, 2025).

Another institutional knot of oversight in the US is regulations aimed at reducing the transparency–representation gap in FISA processes. The USA FREEDOM Act of 2015 aimed to reform the powers at the center of the business records/metadata debate and to mitigate the problem of "unilateralism" in FISA judicial proceedings through amicus-like mechanisms (USA FREEDOM Act, 2015). Such regulations claim to enhance the normative quality of secret processes by linking oversight not only to "permission" but also to the possibility of contradictory reasoning.

At the EU level, intelligence and surveillance oversight often speaks the institutional language of data protection law. The Charter's guarantees of respect for private life and the protection of personal data (Articles 7–8), together with the GDPR's principles of data minimization and storage limitation, transform "data" from merely a technical object into a bearer of rights (Charter of Fundamental Rights of the European Union, 2012; Regulation (EU) 2016/679, 2016). In the field of electronic communications, the ePrivacy Directive's provision allowing restrictions on grounds such as national security has been transformed into "the limit of restriction" thanks to CJEU case law: The framework outlined in the Tele2 Sverige decision prohibits general and indiscriminate retention, but opens the door to targeted and strictly supervised measures under certain conditions (Directive 2002/58/EC, 2002; Tele2 Sverige AB and Others, 2016). This is a model that tightens the architecture of the surveillance regimes produced by the threat, not the EU's "definition of threat" (Zalnieriute, 2021).

The Strasbourg line stands as a higher normative layer in this picture. The Big Brother Watch decision centralizes the idea of "end-to-end safeguards" in regimes with

mass intervention capacity, focusing not only on the moment of authorization but on the entire chain of selection, filtering, storage, sharing, and control (Big Brother Watch and Others v. the United Kingdom, 2021). Thus, surveillance does not become "legitimate" with a single decision; it can only pass the democratic society test when it is made controllable throughout the entire process.

This comparison yields two critical lessons for the normative design debate in Turkey: First, the legalization of surveillance is not merely about granting authority by law, but about granting authority in a way that leaves a trace, log/audit, retention period, independent reporting, transparency. Second, placing the oversight architecture on a single institution inevitably creates blind spots; therefore, the joint establishment of a parliament–independent commissioner/inspector–judicial authorization–effective appeal line is the minimum democratic condition that makes "invisible power" visible (Anderson, 2023; European Court of Human Rights, 2025).

3.3 Extraordinary powers and limits

Extraordinary powers are the "most naked" moment of any legal system: the state speaks of a threshold at which it can suspend the law in order to save itself. Agamben's conceptualization of the "state of exception" is not merely a philosophical metaphor here; it points to a recurring technique of modern governance: the extraordinary, if it lasts long enough, becomes mixed with the ordinary; the language of the ordinary normalizes the powers of the extraordinary (Agamben, 2005). Therefore, well-designed regimes aim to tie extraordinary powers to time and oversight rather than simply "granting" them.

In the United Kingdom, the Civil Contingencies Act 2004 establishes a notable set of limitations in this context. Emergency regulations lapse automatically after a short period if they are not presented to Parliament: it is explicitly stipulated that regulations will cease to have effect if they are not approved by both Houses within seven days of being presented to Parliament (Civil Contingencies Act 2004, s. 27). Furthermore, emergency regulations generally expire after thirty days; any extension is again subject to legal and procedural conditions (Civil Contingencies Act 2004, Part 2). This framework embodies a design logic aimed at removing the extraordinary from being the "continuous reflex of the executive" and limiting it with parliamentary legitimacy.

In the US, the National Emergencies Act (NEA) makes the declaration of a state of emergency legally definable within the federal system, while also linking the termination/cancellation mechanisms to a joint decision by Congress (50 U.S.C. § 1622). The procedure envisaged by the law aims to prevent the state of emergency from continuing solely at the discretion of the president; indeed, recent status notes on the termination of certain national emergencies by congressional decision demonstrate the practical importance of this mechanism (50 U.S.C. § 1621, 2025).

The European human rights regime, on the other hand, limits extraordinary powers through the "derogation" technique. ECHR Article 15 permits derogation only in times of war or public emergency "threatening the nation," only "to the extent required by the exigencies of the situation," and only temporarily; it also keeps the door open for notification and international supervision (European Convention on Human Rights, 1950; European Court of Human Rights, 2022). This establishes a delicate balance between the legal recognition of the extraordinary and the legal limitation of the extraordinary: the exception is managed not by going beyond the norm, but by making it controllable within the norm. Similarly, the Human Rights Committee's interpretation of ICCPR Article 4 emphasizes the exceptional and temporary nature of derogation measures, along with the requirements of legality and oversight (United Nations Human Rights Committee, 2001).

Comparative literature insists on three structural tools for limiting extraordinary powers: time limits and sunset mechanisms; legislative participation (approval/extension procedures); and the "non-suspension" of judicial oversight, or at least not closing it entirely. Ferejohn and Pasquino's typology of extraordinary powers shows how different regimes use these three tools in different combinations, while the "emergency constitutions" literature reveals that the design must respond not only to the moment of crisis but also to the risk of the crisis becoming permanent (Ferejohn & Pasquino, 2004; Bjørnskov & Voigt, 2018). Current assessments also highlight the risk of "the extraordinary becoming ordinary" by showing how fragile derogation practices, particularly during the pandemic, can be within the triangle of time–parliament–judiciary (Won, 2025).

The comparative finding of this section is this: The vagueness of the threat definition, the institutional oversight of surveillance, and the perpetuation of extraordinary powers are three different facets of the same problem. The design of security law that is compatible with rights is only possible with a normative architecture

that sees these three facets simultaneously, by narrowing the definition, making oversight multi-layered, and tying the extraordinary to time.

4 DIAGNOSES OF THE NORMATIVE FRAMEWORK IN TURKEY

4.1 Mapping the current framework

The "security" sphere in Turkey is not so much a regime operating on the regular plane of a single law; but rather as a fragmented articulation between constitutional limitations, criminal norms, administrative law enforcement powers, the special status of intelligence, separate regulations for the digital sphere, and the (increasingly invoked) extraordinary thresholds of disaster and emergency management. Therefore, understanding security legislation in Turkey requires first reading its language, that is, the constitutional grammar between "limitation of rights" and "suspension of rights." The Constitution emphasizes that fundamental rights and freedoms can only be restricted by law and in accordance with the principle of proportionality (Türkiye Cumhuriyeti Anayasası, 1982, md. 13). The same text also accepts that in times of war/mobilization or states of emergency, the exercise of rights may be partially or completely suspended to the extent required by the situation, provided that international obligations are not violated (Türkiye Cumhuriyeti Anayasası, 1982, md. 15). This dual structure forces us to consider the powers of security dispersed within "normal law" alongside the powers concentrated under "emergency law": the permeable line between restriction (Article 13) and suspension (Article 15) is the most critical contour line on the normative map.

The symbolic knot of the institutional coordination architecture built upon this constitutional ground is the National Security Council: The Constitution defines the role of the NSC in terms of "taking decisions and ensuring the necessary coordination regarding the determination, identification, and implementation of the State's national security policy" (Türkiye Cumhuriyeti Anayasası, 1982, md. 118). Furthermore, the regulation on declaring a state of emergency accepts not only classic security scenarios such as "violent incidents" but also risk types such as natural disasters, dangerous epidemics, or severe economic crises as triggers for a state of emergency (Türkiye Cumhuriyeti Anayasası, 1982, md. 119). When these articles are read together, it becomes apparent that security is no longer established solely around "enemies" or "crime," but

also around 'risk' and "vulnerability", which brings the link between governance stability and legal predictability, often emphasized in sustainable development discussions, to the very center of security law.

Under this overarching framework, security norms in Turkey can be read as falling into five main categories: (i) counterterrorism and criminal law; (ii) intelligence activities and their special authority/oversight structure; (iii) "preventive" powers centered on law enforcement and administration; (iv) the separate regime shaped by access blocking, traffic information, and platform obligations in the digital sphere; (v) the personal data protection regime and its broad exceptions opened under the heading of "national security." These clusters consist of texts that constantly refer to each other but are not unified under a single "design logic": a footnote in one law opens up to another law; a regulation article points to another administrative unit; a criminal norm can become the "justification" for an administrative measure. (The mapping in this section does not claim to cover all legislation; however, it aims to show the main pillars of the fragmented regime.

The first cluster is the spread of counterterrorism norms within criminal law. Law No. 3713 on Counterterrorism establishes a special framework for combating terrorist crimes (3713 sayılı Terörle Mücadele Kanunu, 1991). This framework works in conjunction with the types of crimes related to organized crime, violent crime, and data/communication in the Turkish Criminal Code (5237 sayılı Türk Ceza Kanunu, 2004). In terms of criminal procedure, Criminal Procedure Law No. 5271 is one of the fundamental texts that defines the "procedural" limits of the security-rights balance in areas such as communication monitoring, evidence collection, and protective measures (5271 sayılı Ceza Muhakemesi Kanunu, 2004). Thus, the "security" justification is no longer merely an administrative objective; it permeates a series of normative decisions extending to the technique of investigation, the nature of evidence, and the court's standard of proof.

The second set is the specific regime of intelligence law. Law No. 2937 on State Intelligence Services and the National Intelligence Organization is the fundamental text regulating the duties and activities of state intelligence and the MIT (2937 sayılı Kanun, 1983). The logic of this law establishes a "proactive" information regime that differs from classic law enforcement activities: the institutional centrality of the MIT is strengthened not only through its own powers but also through the information production/transfer

obligations of other public institutions (Millî İstihbarat Teşkilatı, n.d.). In terms of oversight, the Security and Intelligence Commission established within the Grand National Assembly of Turkey represents the parliamentary oversight framework for intelligence (Türkiye Büyük Millet Meclisi, n.d.; 6532 sayılı Kanun, 2014). However, the nature of "information" in the intelligence field necessitates secrecy, which limits the transparency capacity of oversight tools; thus, oversight often relies on 'procedure' rather than "results," and often on closed sessions rather than public debate.

The third cluster is the area of "preventive" powers, shaped around law enforcement and civil administration. The Police Duties and Powers Law (PVSK), as one of the main texts on the duties and powers of law enforcement, produces a broad set of instruments that are effective in the daily routine of security practice (2559 sayılı Polis Vazife ve Salahiyet Kanunu, 1934). The Law on the Organization, Duties, and Powers of the Gendarmerie, on the other hand, determines the institutional distribution of law enforcement powers, particularly in rural and civil areas (2803 sayılı Kanun, 1983). In terms of social mobility and the regulation of public space, the Law on Meetings and Demonstrations No. 2911 is one of the fundamental thresholds where freedom of expression and association intersect with "security" (2911 sayılı Kanun, 1983). When combined with the administrative coordination and intervention capacity provided by the provincial administration and civil administration mechanisms under the Provincial Administration Law No. 5442 , which provides administrative coordination and intervention capacity through the mechanisms of the governor's office and local administration, the "on-the-ground" language of the security regime becomes clear: the administration regulates the use of public space on the grounds of "public order"; law enforcement becomes the instrument of this regulation; and the judiciary, most often, acts as the final link in this cycle, providing ex post facto and limited oversight.

The fourth cluster is the distinct and rapidly changing normative structure of the digital sphere. Law No. 5651 defines the obligations of content providers, hosting providers, and access providers for the purpose of regulating publications on the internet and combating certain crimes (5651 sayılı Kanun, 2007). The law defines "traffic data" and regulates the obligation of hosting providers to store traffic data for no less than one year and no more than two years (5651 sayılı Kanun, 2007, md. 2, 5). It also provides for the establishment of the Access Providers Association to implement decisions to block access and for the organization of implementation through this mechanism (5651 sayılı

Kanun, 2007, md. 6/A). This framework leads to the establishment of security in the digital sphere in a hybrid form that oscillates between "judicial measures" and "administrative intervention": tools such as access blocking, content removal, and traffic data retention bring together the logic of evidence in criminal investigations and the logic of risk in administrative regulation on the same stage.

In the field of electronic communications, Law No. 5809 on Electronic Communications, while regulating the sector, states that special provisions relating to national security, public order, and states of emergency/natural disasters remain reserved; and grants the Authority the power to determine the procedures and principles for the processing of personal data and the protection of privacy (5809 sayılı Kanun, 2008, md. 2, 51). Thus, digital surveillance and data processing practices are linked, on the one hand, to the "publication/access" regime of Law No. 5651 and, on the other hand, to the "communications infrastructure" regime of Law No. 5809; the intersections between the two texts are often filled by secondary regulations and institutional practices.

The fifth cluster is the undermining of the seemingly "rights-based" regime established in the field of personal data protection by security exceptions. The Personal Data Protection Law No. 6698 explicitly lists fundamental principles such as legality in data processing, specific–clear–legitimate purpose, relevance–limitation–proportionality, and retention for the necessary period (6698 sayılı Kanun, 2016, md. 4). However, the same law creates a broad area of exemption by excluding data processing carried out within the scope of "preventive, protective, and intelligence activities conducted by public institutions and organizations authorized by law to ensure national defense, national security, public safety, public order, or economic security." (6698 sayılı Kanun, 2016, md. 28). This exception significantly weakens the most critical promise of the data protection regime, namely, the claim to establish a controllable limit of power over personal data, in the field of security. At this point, rather than striking a balance between "data protection" and "national security," a normative asymmetry often emerges in which data protection takes a back seat to security (Kinikoglu, 2023).

Finally, the disaster–emergency and state of emergency architecture is the most direct plane on which security law in Turkey connects with environmental/climate-based risks. The fact that natural disasters and dangerous epidemics are explicitly included among the reasons for a state of emergency in the Constitution (Türkiye Cumhuriyeti Anayasası, 1982, md. 119) opens a door linking security to "sustainability" debates:

because disaster management is not only a matter of technical capacity, but also a matter of protecting rights and the accountable use of public resources. In this context, the State of Emergency Law No. 2935 establishes the framework for extraordinary management tools (2935 sayılı Kanun, 1983), while Law No. 5902 regulates the organization and duties of AFAD (5902 sayılı Kanun, 2009). The increasing frequency and scale of climate-related disasters show that these texts can be decisive not only in "exceptional moments" but also in the continuity of governance capacity; therefore, fragmentation in security legislation also creates fragility in terms of the legality of institutional coordination against disaster and climate risks.

The institutional "authority–responsibility" chain in this map does not flow in a single line; rather, it functions more like a multi-centered network. While the MGK is the constitutional hub of coordination at the policy level (Türkiye Cumhuriyeti Anayasası, 1982, md. 118) the institutional centrality of the MIT in the field of intelligence and the obligations of inter-agency information flow come to the fore (Millî İstihbarat Teşkilatı, n.d..). In the law enforcement-civil administration line, the organization of governorates and district administrations and the powers of law enforcement agencies regulate the "field" (5442 sayılı Kanun, 1949; 2559 sayılı Kanun, 1934; 2803 sayılı Kanun, 1983). In the digital sphere, the access/removal and traffic information obligations envisaged by Law No. 5651 operate through intermediary institutions such as the Access Providers Association and sectoral regulatory capacity (5651 sayılı Kanun, 2007). In the field of data protection, although the Agency/Board structure provides a theoretical guarantee, the national security exception suspends this guarantee in certain areas (6698 sayılı Kanun, 2016, md. 28). Mechanisms such as the Security and Intelligence Committee within the Grand National Assembly of Turkey represent the parliamentary dimension of oversight (Türkiye Büyük Millet Meclisi, n.d.) The result of this network is as follows: authority is fragmented in many places, responsibility is often scattered; decisions are quick, justifications are often closed; oversight is often fragmented.

4.2 Problems caused by fragmentation

The fragmented structure of security legislation in Turkey is not merely a technical "scatteredness" problem; it is a normative regime problem that directly produces consequences for the rule of law. This is because the rule of law does not a priori reject

the legitimacy of security as an "end"; however, it requires that the means used in the name of security be predictable, proportionate, and amenable to judicial oversight. The regime of restrictions established in Article 13 of the Constitution therefore places the emphasis on "legality" and "proportionality" (Türkiye Cumhuriyeti Anayasası, 1982, md. 13). In a fragmented regime, legality is often reduced to the level of "the existence of a text"; however, the essential requirement of legality is normative clarity that allows individuals to foresee their behavior and limits the arbitrariness of the administration (Venice Commission, 2016).

The first set of problems concerns predictability and equal application. When counterterrorism, intelligence, and digital regulations are established in different texts, with different purpose clauses and different conceptions of "threat," it becomes unclear under which legal regime the same phenomenon will be assessed. This uncertainty both broadens the scope of administrative application and challenges the capacity of judicial review to produce "standards." It should be recalled that in some of the European Court of Human Rights (ECHR) rulings concerning Turkey, interventions in the areas of expression and organization were found to be problematic in terms of the conditions of "predictability" and "being prescribed by law" (European Court of Human Rights [ECtHR], 2010; ECtHR, 2017). The issue here is not the existence of a norm, but rather the certainty of the norm's scope and conditions of application, and its resistance to arbitrariness. Fragmentation constantly exacerbates the tension between "legal certainty" and "discretion in application" precisely at this point.

The second set of problems becomes visible in access blocking and surveillance practices in the digital sphere. Law No. 5651 increases the "recordability" capacity of the digital sphere with provisions such as the definition of traffic data and the obligation to store it (5651 sayılı Kanun, 2007, md. 2, 5) However, interventions such as access blocking are among the most severe tools in terms of freedom of expression; therefore, justification standards and effective remedies must be robust. It is known that in its decision in Ahmet Yıldırım v. Turkey, the ECtHR emphasized the importance of legal safeguards in the context of interventions involving the blocking of internet access; in its decision in Cengiz and Others v. Turkey, it assessed the blocking of access to a video-sharing platform from the perspective of freedom of expression (ECtHR, 2012; ECtHR, 2015). In domestic legal debates on access blocking in Turkey, the Constitutional Court has also adopted an approach that points to proportionality and necessity tests in the

digital sphere, as well as the "digital public sphere" dimension of freedom of expression (Anayasa Mahkemesi, 2019). Taken together, these decisions reveal two consequences of the fragmented digital regime: (i) the risk of increased decision-making speed and decreased quality of reasoning; (ii) the fact that judicial review can often only be exercised "after the fact" and through individual applications.

The third set of problems concerns the institutional division of oversight and accountability. The existence of parliamentary oversight in the intelligence field (Türkiye Büyük Millet Meclisi, n.d.; 6532 sayılı Kanun, 2014) is normatively important; however, the justification of confidentiality limits the transparency capacity of oversight and may sever the link between oversight effectiveness and "elected representation" and "public justification." In the field of data protection, although the fundamental principles of Law No. 6698 appear strong, the scope of exceptions in Article 28 narrows the scope of the data protection regime, particularly with regard to preventive/intelligence activities (6698 sayılı Kanun, 2016, md. 28). This means that a wide range of rights-based safeguards, the duty to inform, the right of access, the right to erasure, and avenues for appeal, can be withdrawn under the label of "security." The result is that oversight cannot focus on a single "public authority"; responsibility is often fragmented between administrative, judicial, and parliamentary channels (Kinikoglu, 2023).

The fourth set of problems is the risk of "permanence" of extraordinary powers and extraordinary management techniques. Article 15 of the Constitution explicitly states that international obligations cannot be violated even in states of emergency and that the principle of "proportionality" must be observed; Article 119 links the state of emergency to specific causes (Türkiye Cumhuriyeti Anayasası, 1982, md. 15, 119). However, extraordinary governance practices may not be limited to periods when a state of emergency has been declared: administrative techniques developed during exceptional periods may later be incorporated into ordinary legislation and become "normal" governance instruments. This risk has been emphasized by international institutions, particularly in assessments of the state of emergency in the Turkish context (Venice Commission, 2016). With the increase in "non-traditional risks" such as climate-related disasters and epidemics, the more frequent emergence of the threshold for extraordinary governance makes this risk of permanence even more critical in terms of sustainable governance: sustainable development capacity is measured not only by the power to

suppress security threats, but also by predictable institutional functioning that is compatible with rights guarantees.

The fifth set of problems is the “chilling effect” in the area of civil society and public participation. When read together, the regime governing meetings and demonstrations (2911 sayılı Kanun, 1983and the authority of local administration mechanisms to regulate public space (5442 sayılı Kanun, 1949) reveal that the justification of security and public order can become a powerful filter determining the continuity of public space. This filter is decisive not only for classic political opposition practices but also for environmental participation, climate justice demands, and local ecology struggles. This is because environmental/climate-based mobilizations often proceed along two channels: gathering in physical space and organizing in digital networks (Doğu, 2022). Studies examining how protest bans are established through space show that the state's “spatial reasoning” redraws the public sphere on security grounds (Arslanalp, 2023). In human rights literature, the connection between restrictions on freedom of assembly and strategies to “make the exercise of rights manageable” is debated (Çınar, 2017). Therefore, fragmentation in security legislation has the potential to indirectly weaken the legal guarantees of environmental participation: on the one hand, the physical boundaries of public space may narrow, and on the other, the boundaries of access and visibility in the digital sphere may shrink.

The conclusion of this diagnosis is clear: the security regime in Turkey is a “normative mosaic” of numerous texts; however, the mosaic does not only produce diversity, it also produces gaps in terms of predictability, accountability, and rights guarantees. The tension between Law No. 5651's traffic information and access blocking regime (5651 sayılı Kanun, 2007) and Law No. 6698's security exceptions (6698 sayılı Kanun, 2016, md. 28); the different oversight channels for criminal law, law enforcement, and intelligence; the thresholds of the state of emergency regime that reconnect with disaster/climate risks, all of these are negative evidence showing why a comprehensive National Security Law (NSL) framework, reconceived through “rights-compatible” and “design principles,” is necessary. From this point onward, the task is not to inventory the problems; it is to derive design principles from this inventory.

5 PROPOSED NATIONAL SECURITY LAW FOR TURKEY

This section proposes a framework law architecture to enable security law in Turkey to transition from a "piecemeal regime" logic to a "designed regime" logic. The argument here is that the legal regulation of national security is much more than just adding "more authority" to security: a good national security law defines authority but also sets limits on that authority; it speeds up the executive but also speeds up oversight; it accepts secrecy but removes secrecy as an excuse for accountability. Therefore, the proposed law should not merely be a text listing the instruments available to security agencies; it should be a normative order that does not "add" the regime of rights to the security regime, but rather makes it a constitutive element (Venice Commission, 2016; United Nations Human Rights Committee, 2011).

This approach is consistent with two fundamental tenets of contemporary human rights law. First, rights may only be restricted by law, for legitimate purposes, and subject to the conditions of necessity and proportionality; vague and broad norms structurally complicate this test because they open the door to arbitrariness (United Nations Commission on Human Rights, 1984; European Union, 2012). Second, when covert surveillance and intelligence activities become "routine" management techniques, the rule of law can only survive with end-to-end safeguards; unless a chain of authorization, recording, oversight, storage–destruction, notification, and effective recourse is designed as a whole, even a single "judicial decision" is insufficient to democratize the regime (Big Brother Watch and Others v. the United Kingdom, 2021; Roman Zakharov v. Russia, 2015).

The following proposal aims to explain the design rationale behind each article while structuring the text as an article-by-article framework. Thus, the proposal is not merely a draft; it can also be read as a normative scheme that provides a design rationale.

5.1 Purpose, scope, and definitions

The introductory provisions of the proposed National Security Law (NSL) must state what security is and, more importantly, what it is not. This is because when national security is left as an undefined concept, it becomes the "most elastic" part of the law: it encompasses every event and can legitimize every measure. Therefore, the purpose and

definition articles are not the most 'rhetorical' part of the law, but the most "technical" part.

***Article 1 (Purpose and principle clause*)** should be formulated as follows: *"The purpose of this Law is to protect the constitutional-democratic order of the Republic of Turkey, the territorial integrity of the country, and the vital conditions of society in a manner consistent with the principles of the rule of law, human rights, and sustainable development."* Two choices are important in this sentence. First, security should be understood not only as the continuity of the state but also in terms of the vital conditions of society (critical infrastructure, public health, disaster resilience); this establishes a legitimate and measured connection with the field of "non-traditional risks" such as climate/disasters (Intergovernmental Panel on Climate Change, 2022). Second, sustainable development should be made a binding principle within the purpose clause, not a "subheading"; because sustainable development is possible with predictable governance and accountable institutions (United Nations General Assembly, 2015; World Commission on Environment and Development, 1987).

Article 2 (Scope) should explicitly state that the UGK is not a "mega-law that regulates everything." In the proposed model, the UGK establishes (i) a definition of national security threats, (ii) common safeguards for intelligence and surveillance powers, (iii) a time-control architecture for extraordinary powers, (iv) inter-agency coordination and reporting, (v) rights safeguards and red lines. It does not multiply criminal law offenses; rather than "reproducing" existing criminal regimes (e.g., counterterrorism legislation) from above, it disciplines the points where they intersect with the sphere of rights through common standards based on national security justifications (Scheinin, 2010).

Article 3 (Fundamental principles) is the normative backbone of the UGK and should serve as an interpretive rule beyond being a mere "list of principles." At a minimum, the following principles should be directly linked to the text: legality and legal certainty; legitimate purpose; necessity and proportionality; non-discrimination; accountability; effective remedy; sustainability; and intergenerational justice. The logic of limitation in the Siracusa Principles and the necessity-proportionality framework in Article 52 of the EU Charter of Fundamental Rights are strong foundations for the formulation of these principles at the national level (United Nations Commission on Human Rights, 1984; European Union, 2012). To prevent proportionality from becoming

a “balance that legitimizes everything,” the “burden of justification” must be clearly placed on the administration: proportionality is the state's duty to explain (Gerards, 2013; Klatt, 2012; see also Tsakyrakis, 2009).

***Article 4 (definition of national security threat*)** is the cornerstone of the UGK. For the purposes of this article, the proposed definition should be based on two thresholds: seriousness and **concreteness**. A threat to national security should be defined as *“a serious and concrete danger to the constitutional-democratic order of the state, its territorial integrity, or the vital conditions of society, which is imminent or whose likelihood of occurrence has been demonstrated by reasonable grounds.”* The phrase “imminent threat” is necessary here to prevent national security from being unlimited by “uncertain possibilities”; The Johannesburg Principles' approach that peaceful expression should not be suppressed on grounds of national security provides normative support for this narrowing (Article 19, 1995).

Article 5 (Categories of threats) should be established with a “narrow list” logic; however, the list should not exclude real risk areas. The proposed categories can be grouped into four: (a) violence-based terrorism and mass violence; (b) foreign state-linked espionage, sabotage, and large-scale foreign interference; (c) cyber/physical disruption attempts targeting critical infrastructure and essential public services; (d) large-scale disasters and climate-induced crises that severely threaten the vital conditions of society. The fourth category does not aim to “securitize the climate”; rather, it aims to define the real impact of climate/disaster risks on critical infrastructure and public order within the legal framework (Intergovernmental Panel on Climate Change, 2022; Hsiang et al., 2013). In addition, a “negative definition” is required to prevent environmental advocacy or peaceful protest from being included in this category: *“Peaceful expression, organization, and environmental participation activities cannot be considered a threat to national security unless they are directly and closely linked to violence.”* This negative definition is consistent with both the Johannesburg Principles and UN standards on freedom of expression (Article 19, 1995; United Nations Human Rights Committee, 2011).

***Article 6 (Interpretation principle and periodic review*)** is the second safeguard against ambiguity. The law must explicitly include the rule that national security concepts will be interpreted narrowly and that, in case of doubt, the interpretation will be in favor of rights (in dubio pro libertate). Furthermore, the definition of threat and the list of

categories must be subject to periodic review (e.g., every two years) in light of independent audit reports and Turkish Grand National Assembly committee hearings. This transforms the political nature of the concept of security, which "flexes according to the period," into a legal nature that is "monitored according to the period" (Venice Commission, 2016).

5.2 Authority architecture and oversight

The second major issue for the UGK is to consolidate oversight while distributing authority. Fragmented legislation often produces authority in "many places" but does not concentrate responsibility in "any place." The proposed model does not aim to centralize security powers in a single center; rather, it aims to design each power with a counterweight that oversees it (Venice Commission, 2015).

Article 7 (Layered authority regime) must legally establish the distinction between "normal period / heightened risk / state of emergency." The goal here is to prevent responding to every risk with the same set of tools. The three layers must be differentiated not only in administrative language but also in the conditions of authority:

The normal period operates within the logic of constitutional Article 13 with restrictions on rights; surveillance and intelligence measures must be targeted, time-limited, and subject to judicial authorization (European Union, 2012; Big Brother Watch and Others v. the United Kingdom, 2021). The heightened risk period, on the other hand, should be defined as an "interim regime" that accelerates the executive but does not weaken oversight: when a specific threat meets the criteria of seriousness and concreteness, as determined by a reasoned risk assessment, certain procedures may be expedited; however, this acceleration must be balanced by immediate notification to the Grand National Assembly and ex post review by an independent auditor. A state of emergency should be kept separate, in line with Article 119 of the Constitution; the "rising risk" regime should not be designed to effectively replace a state of emergency. Otherwise, a state of emergency is experienced without being declared; the law transforms without saying its name (United Nations Human Rights Committee, 2001).

***Article 8 (National security strategy and risk assessment*)** should transform security policy from a "secret reflex" into an "accountable program." The executive branch should publish a National Security Strategy at regular intervals (e.g., every two

years), operating through a publicly available main text and a confidential annex subject to parliamentary oversight. This strategy should include a sustainability analysis in line with sustainable development goals and explicitly define institutional resilience plans regarding the impacts of climate/disaster risks on critical infrastructure, public health, and migration dynamics (United Nations General Assembly, 2015; Intergovernmental Panel on Climate Change, 2022).

Article 9 (Parliamentary oversight: strengthened committee model) should transform security/intelligence oversight within the Turkish Grand National Assembly from "symbolic" to "functional." Comparative examples show that the success of parliamentary oversight depends on two conditions: access to information and independent expertise (Venice Commission, 2015). Therefore, the commission's procedures for accessing classified documents, cross-party representation, employment of experts, and regular reporting obligations should be clearly defined. The commission should publish an annual "national security oversight report" that is open to the public and contains minimum data that cannot be withheld on grounds of confidentiality (types of powers used, numerical trends, oversight findings).

Article 10 (Independent oversight: national security and civil liberties commissioner) should be the system's most critical innovation. An "Independent National Security Auditor/Commissioner" model institutionalizes external oversight rather than expecting the executive branch to self-regulate. This commission should be empowered to oversee surveillance authorization processes, examine agencies' log/audit records, receive complaints, issue binding recommendations or limited orders in cases of administrative violations, and refer matters to the courts when necessary. Such a structure could draw inspiration from institutions like the UK's IPCO/Investigatory Powers Commissioner and oversight experiences like the US's PCLOB; however, it should be adapted to Turkey's unique constitutional administrative structure. could draw inspiration from institutions such as the IPCO/Investigatory Powers Commissioner in the United Kingdom and oversight experiences such as the PCLOB in the United States; however, it should be designed in a manner consistent with Turkey's unique constitutional administrative structure (Investigatory Powers Act 2016, 2016; USA FREEDOM Act, 2015).

Article 11 (Independent review and sunset) is the law's "self-correcting" mechanism. The greatest risk of poor design in the security field is that once established,

it becomes permanent. Therefore, the UGK should provide for an automatic sunset for certain intrusive powers (especially if there are regimes such as mass data processing or strategic surveillance) and require a "post-legislative review" by an independent panel of experts every five years (Bjørnskov & Voigt, 2018; Ferejohn & Pasquino, 2004).

5.3 Surveillance and data regime

Surveillance is the invisible architecture of national security; invisible architecture, however, is only legitimized through visible oversight. Therefore, the UGK's oversight and data regime is not only an "authorization" but also a "data lifecycle" design: collection, processing, access, storage, sharing, destruction, notification, and appeal (Big Brother Watch and Others v. the United Kingdom, 2021).

Article 12 (Judicial authorization standard: necessity–proportionality and 'strict necessity') should be the fundamental threshold for targeted surveillance. Targeted communications surveillance is only possible where a reasonable justification relating to a serious and concrete national security threat is demonstrated, the inadequacy of less intrusive means is explained, and the request is narrowed in terms of duration, scope, and purpose (European Data Protection Supervisor, 2017; Gerards, 2013). Mass/strategic surveillance regimes, if envisaged at all, be linked to the "strict necessity" threshold; the CJEU's approach to general and indiscriminate data retention practices should be accepted as the "lower limit" of design at the national level (Tele2 Sverige AB and Others, 2016; Digital Rights Ireland, 2014).

Article 13 (Double lock and specialized authorization mechanism) should qualitatively strengthen the authorization procedure. The "double lock" approach in the United Kingdom embodies the idea of a second filter of executive approval by an independent judicial review (Investigatory Powers Act 2016, 2016) In Turkey, this mechanism could be adapted, for example, as "specialized judicial authorization judge" + "independent commissioner review." The aim is to improve the quality of the reasoning behind the authorization decision without overburdening a single authority. Furthermore, in order to prevent the complete absence of a "counterargument" regarding fundamental rights in the authorization process, a confidentiality-compliant "special representative/amicus" mechanism (limited and subject to security screening) could be introduced for discussion (USA FREEDOM Act, 2015).

Article 14 (Data minimization, storage, and destruction) is the "silent" but most effective guarantee of the law. The principles of minimization and storage limitations in the GDPR can be used as a design standard, even if there are security exceptions in national law: the data collected must be relevant and proportionate to the purpose; storage periods must be clearly defined; automatic deletion and destruction protocols must be mandatory (Regulation (EU) 2016/679, 2016). Furthermore, logging every access and sharing creates a regular audit trail; thus, the audit is based on what is "tracked" rather than what is "said" (Big Brother Watch and Others v. the United Kingdom, 2021).

Article 15 (Special areas of protection: journalist sources, lawyer–client, doctor–patient, academic work) protects the sensitive veins of a democratic society. European human rights case law requires stricter justification and stronger safeguards, particularly in areas such as journalist sources and lawyer-client confidentiality. Therefore, the UGK should not only subject measures targeting such communications to higher thresholds; but also make independent commissioner oversight mandatory (European Court of Human Rights, 2016; see also Szabó and Vissy v. Hungary, 2016).

Article 16 (Notification and redress mechanism) is a democratic safety valve that prevents surveillance from becoming a "permanent secret." At the core of the regime should be the principle that, once the surveillance measure has ended and it has been assessed that the national security threat will not increase upon notification, the person concerned must be notified within a reasonable time. Exceptions to notification should be narrow and justified; a delayed notification procedure and mandatory periodic reassessment should be introduced (Roman Zakharov v. Russia, 2015). The redress mechanism should not be limited to compensation alone; it should entail multi-layered consequences such as the deletion of unlawfully processed data, administrative disciplinary sanctions, and, where appropriate, criminal liability.

Article 17 (Transparency reports and statistical disclosure) is the practical counterpart of the principle of "accountability in secrecy." Institutions should publish aggregated data at least once a year on how many requests for authorization were made, how many were rejected, what measures were used, retention periods, and audit findings. This enables democratic debate without revealing operational details; the legitimacy of security is nourished precisely by this capacity for debate (Venice Commission, 2015).

5.4 State of emergency regime: duration, extension, sunset

A state of emergency is a temporary breach in the heart of the law; but if the breach becomes permanent, the law itself changes. Therefore, the UGK exists not to extend the state of emergency, but to link it to time and oversight (Ferejohn & Pasquino, 2004).

Article 18 (Triggering conditions and reasoned declaration) should free the declaration of a state of emergency from the language of "uncertain threats." The declaration decision must be submitted to the Grand National Assembly of Turkey with justification, including concrete events, a risk assessment report, a list of targeted measures, and the expected duration. Thus, the state of emergency is implemented not by "intuition" but by legal justification (Venice Commission, 2016).

***Article 19 (Time limit, qualified majority for extension, and automatic sunset*)** is the main mechanism against the normalization of the state of emergency. Comparative examples show that the time limit alone is not sufficient; the extension procedure must also generate political costs (Civil Contingencies Act 2004, 2004; National Emergencies Act, 1976). Therefore, it is recommended that extensions of the state of emergency be approved by a qualified majority (e.g., three-fifths of the total number of members of the Grand National Assembly); that the number of extensions be limited; and that a new justification and a new impact analysis be presented for each extension. Furthermore, it should be clearly stated that all regulations issued during the state of emergency that restrict rights will automatically cease to be in force when the state of emergency ends; if they are to be made permanent, they must go through the normal legislative process. This is a door lock that prevents the "exception" from seeping into the "norm" (United Nations Human Rights Committee, 2001; Gross & Aoláin, 2006).

Article 20 (Accelerated judicial review and effective remedy) is a mandatory condition for the state of emergency to remain within the rule of law. The UGK should not suspend effective remedies against emergency measures; on the contrary, it should strengthen them with special procedures that produce rapid decisions. Where derogation (ECHR Article 15; ICCPR Article 4) is concerned, the notification obligation and the compliance of measures with the principle of "strict necessity" must be subject to review (European Convention on Human Rights, 1950; United Nations, 1966). Within the theoretical framework of this field, the idea of "law accompanying the extraordinary" is

not only a normative but also an institutional necessity: if the judiciary shuts down, the extraordinary cannot find a language to constrain itself (Dyzenhaus, 2006).

***Article 21 (Post-emergency accountability: independent review and redress*)** ensures the "accountable closure" of crisis management. When the state of emergency ends, an independent review commission must report on which measures were taken and for what reasons, which measures were effective/ineffective, and how rights violations were remedied. This report creates institutional memory for future crises; sustainable security is possible precisely because of this memory (Bjørnskov & Voigt, 2018).

5.5 Red lines for expression, organization, and participation

National security law is most tested by "voices": critical speech, persistent protest, crowds filling public spaces, a small local community defending its environment... When the security regime casts a shadow over these voices, it falls into the mistake of equating security solely with "silence." Yet in a democratic society, security is not silence, but pluralism coexisting with reliable rules (United Nations Human Rights Committee, 2011).

Therefore, the UGK should not only subject rights to a "limitation test"; it should also establish red lines.

Article 22 (Test standard for restrictions on freedom of expression on grounds of security) should specifically protect the realm of political expression and public debate. The fundamental standard here is the strict application of the "necessary in a democratic society" test of ECHR Article 10, even in the case of national security grounds. The UN Human Rights Committee also explicitly emphasizes that national security justifications should not be used to shield states from criticism (United Nations Human Rights Committee, 2011). The UGK should explicitly rule that activities such as "criticizing the state," "questioning public authority," and "political advocacy" cannot be considered a threat to national security unless they are closely linked to violence (Article 19, 1995).

Article 23 (Freedom of association and assembly: prohibition of general bans and restrictive interpretation) should link the right to assembly and association to the principle of "presumed freedom." Prohibitions imposed on security grounds should be narrowed in terms of duration, location, and scope; "general and vague" prohibitions should be explicitly prohibited. This is a design choice that preserves the continuity of

civil society; because the continuity of civil society is the cornerstone not only of the political system but also of sustainable development policies (United Nations General Assembly, 2015).

Article 24 (Protection of the environmental civic space and guarantees of public participation) should be designed as an innovation directly aligned with the journal's focus on law, sustainability, and human rights. There are two normative bases here. The first is the democratic environmental governance standard set forth by the Aarhus Convention, which institutionalizes the principles of access to and participation in environmental decision-making processes (UNECE, 1998). Even though Turkey is not a party to this convention, the Aarhus principles are a global reference point in environmental governance. The second is developments related to the international recognition of the right to a clean, healthy, and sustainable environment (Human Rights Council, 2021; United Nations General Assembly, 2022). The UGK must establish both a negative definition and a special protection provision to prevent environmental protest and environmental advocacy activities from being suppressed under the label of "national security threat": it must introduce a "rights-based resilience" perspective against the securitization of environmental participation. This is because the long century ahead, marked by climate and disaster risks, will build security not only through law enforcement but also through the continuity of public participation (Intergovernmental Panel on Climate Change, 2022).

Article 25 (Abuse filter for human rights defenders and journalists) should reduce the risk of "uncontrolled accusations." The UN Declaration on the Protection of Human Rights Defenders obliges states to facilitate and protect the activities of defenders (United Nations General Assembly, 1998). The UGK may introduce automatic notification to an independent commissioner and a "reinforced justification" requirement for actions and investigations carried out by security agencies in these areas. This is a concrete test of whether security is designed to be a protector of rights rather than an enemy of rights.

These red lines separate security law from the "harsh language of politics." Because security can always produce a language of threat; but law exists to prevent the language of threat from swallowing rights. The real promise of the UGK lies here: to strengthen security without narrowing the public sphere on which democracy is based under the pretext of security.

6 CRITICAL DISCUSSIONS: SECURITIZATION, EXCEPTION, AND SUSTAINABILITY

Security is one of the most "loud" words in the modern legal order; it not only describes a danger, but also establishes a horizon of authority. The moment we say "national security," our relationship with the ordinary rhythm of law, that is, with negotiation, objection, and slow but traceable oversight mechanisms, changes. Therefore, the problematic of the security regime is not merely a table of authority-rights balance; it is a form of governance, a regime of visibility, and a technique of exception. As the securitization literature points out, "security" often functions as a discursive act: it removes a particular phenomenon from the language of ordinary politics and transfers it to the legitimacy sphere of extraordinary measures (Wæver, 1995; Buzan et al., 1998; Balzacq, 2005). The critical issue here is not whether the securitization move itself is "bad" or "good"; it is how this move, if the architecture of definition and control is weak, infiltrates the most fragile veins of the rule of law (Roe, 2012). This section justifies why the proposed National Security Law (NSL) design must be based on the triad of "transparency + oversight + limitation" through two critical lenses: Foucault's analysis of panopticism and Agamben's discussion of the state of exception. Finally, it connects this critique to the axis of sustainable development, discussing the normative limits of the relationship that the security regime will establish with "environmental/climate-based risks."

6.1 Foucault: panopticism and the political impact of surveillance

Foucault's reading of the panopticon shows that surveillance is a different form of power than brute force: power operates not only through the possibility of "being caught" but also through the constant possibility of "being seen" (Foucault, 1975/1995). In the panoptic system, the "eye" does not have to monitor individual actions; the real effect is the internalization of the possibility of being watched into the individual's behavior. This internalization is not limited to the fear of punishment: it leads to the reconfiguration of forms of speaking, writing, organizing, and participating in the public sphere based on a calculation of "possible consequences." In the digital age, surveillance is not tied to a fixed tower; it produces a "surveillant assemblage" that separates bodies and social

relations into “data flows” and reassembles them in new contexts (Haggerty & Ericson, 2000). Thus, the panoptic effect emerges not so much from the intentions of individual institutions, but rather from the overall architecture of inter-institutional data circulation.

The critical aspect of this theoretical framework in terms of legal policy is this: vague and broad surveillance powers transform not only privacy, but also the conditions of public reason. This transformation is no longer an abstract assumption; empirical studies showing that surveillance creates a “chilling effect” have identified measurable declines in information-seeking and expression behaviors following surveillance disclosures (Penney, 2016). Similarly, perceived state surveillance in online environments has been found to reduce the willingness to speak out, particularly on controversial issues, and to reinforce the “spiral of silence” (Stoycheff, 2016). More recent qualitative research also shows that the perception of surveillance can erode not only expression behavior but also trust in state institutions and the “courage to seek justice,” leading individuals to adopt “invisibility” strategies in their daily practices (Murray et al., 2024). These findings remind us that surveillance powers must be designed not only according to technical standards but also in line with democratic legitimacy.

Human rights law also translates the panoptic threat into normative language at this point: The European Court of Human Rights (ECHR), pointing to the corrosive effect of covert surveillance on democratic order, insists that systems introduced on national security grounds must include “strict and effective safeguards” (Roman Zakharov v. Russia, 2015; Szabó and Vissy v. Hungary, 2016; Big Brother Watch and Others v. the United Kingdom, 2021). The key insight here coincides with Foucault's panoptic logic: surveillance is not “merely” an intrusion into the individual's private sphere; it is a technique of power that shapes the citizen's existence in the public sphere. Therefore, in NSL design, transparency reports, independent oversight, audit/logs, data minimization, and effective appeal mechanisms are not secondary “implementation details”; they are foundational safeguards protecting the democratic sphere from panoptic effects.

6.2 Agamben: the normalization of the state of exception

Agamben's discussion of the “state of exception” focuses on the most critical breaking point between law and politics: what happens when the extraordinary becomes established not as a temporary measure but as a continuous technique of governance?

(Agamben, 2005). Agamben argues that the exception is not merely the "suspension of law"; rather, law produces a threshold area that includes its own suspension. Humphreys' reading of Agamben emphasizes that this threshold area opens the door to "anomie," but that even anomie is attempted to be made governable by being legalized (Humphreys, 2006). The issue here is not the existence of extraordinary powers; it is their becoming the silent ground of everyday governance. Once the "exception" becomes commonplace, the rule of law is no longer merely a collection of texts that limit rights; it can become a mechanism that "proceduralizes" the suspension of rights.

The reason this risk is constantly on the agenda in modern constitutional states is that "crisis" has become an increasingly broad category in contemporary governance: terrorist threats, cyber risks, pandemics, mass migration, climate-related disasters... As the repertoire of crises expands, so do the politically persuasive justifications for extraordinary powers. Therefore, the normative core of emergency law is not just the question of "should we grant authority?" but also "how will we take back authority, how will we limit it, how will we keep it open to judicial and democratic oversight?" (Ferejohn & Pasquino, 2004; Gross & Aoláin, 2006; Dyzenhaus, 2006). The international human rights regime also establishes this core with procedural and substantive limits: derogation regimes, necessity–proportionality, non-discrimination, and the inviolability of core rights produce thresholds (Human Rights Committee, 2001; European Convention on Human Rights, 1950, art. 15; International Covenant on Civil and Political Rights, 1966, art. 4). Thus, the "exception" can only be accepted within the law under the conditions of "temporariness and controllability."

In this context, elements of the NSL design such as sunset (automatic expiry), time limits, qualified majority for extension, accelerated judicial review, and regular parliamentary reporting are not merely administrative techniques but serve as a "constitutional brake" against the risk of normalization described by Agamben. The exception tends to produce its own language: the discourse of "urgency" obscures "time"; the discourse of 'secrecy' weakens oversight; the discourse of "threat" expands scope. Therefore, duration, oversight, and transparency are rules that security "limits" rather than "enables" in NSL design.

6.3 The sustainable development dimension

Sustainable development is often equated with environmental policies; however, sustainability is concerned not only with the continuity of natural resources, but also with the continuity of institutional trust and legal predictability. Legal certainty and accountability are the most invisible infrastructure of long-term public policies: without "predictable rules" and "appealable decisions" across a wide range of areas, from investment decisions to local participation, disaster management to climate adaptation policies, sustainability becomes fragile (Mahmutovic & Alhamoudi, 2023; Gu et al., 2024). Indeed, the SDG 16 strand of the 2030 Agenda considers sustainable development alongside "peaceful, inclusive societies; accessible justice; effective, accountable, and inclusive institutions" (United Nations, 2015; United Nations, n.d.). This link removes security law from being an "unsustainable" area: the predictability of security legislation is the institutional production of public trust; public trust, in turn, is the social fuel for sustainable policy capacity.

However, the sustainability–security relationship oscillates between two extremes. At one extreme, climate change and disaster risks are incorporated into the "national security" repertoire, aiming to mobilize state capacity; at the other extreme, this language can render the "environmental civil sphere" fragile by transforming environmental issues into a legitimizing ground for extraordinary measures. The second risk is explicitly discussed in the critical literature on the securitization of climate: the discourse of "climate security" can sometimes make invisible forms of violence visible, while at other times it can reproduce power relations regarding whose security will be protected (Cusato, 2022). Therefore, NSL design must establish normative "safety valves" that protect democratic participation and environmental rights while incorporating climate/disaster risks into national security categories.

This necessity is also becoming increasingly clear in current international documents. On the one hand, the United Nations General Assembly's resolution recognizing a clean, healthy, and sustainable environment as a human right (United Nations General Assembly, 2022) increases the normative weight of environmental rights, while on the other hand, the advisory opinion of the International Court of Justice dated July 23, 2025, establishes a framework that explicitly references principles such as sustainable development, precaution, equity, and intergenerational justice when

interpreting state obligations related to climate change (International Court of Justice, 2025). In this context, incorporating climate/disaster-based risks into security policies requires placing the protection of rights at the center of climate governance, not the "suspension of rights."

Finally, the political conditions for sustainable development are directly linked to the public participation of environmental advocates and local communities. Precisely for this reason, examples where environmental mobilization is pushed into "threat" categories, protest is criminalized, and surveillance is used to suppress it, produce a kind of "institutional climate crisis" for sustainability: when actors defending the environment are at risk, climate policy loses its social legitimacy. This risk has become visible both in the reports of international human rights mechanisms and in global data: Global Witness documents that at least 146 land and environmental defenders were killed or forcibly disappeared in 2024 (Global Witness, 2025). The United Nations human rights system also highlights structural gaps in the protection of defenders working in rural/isolated areas and the location-specific concentration of attacks/threats (Lawlor, 2025). Current reporting on the Aarhus Convention's environmental defenders rapporteurship points to a common trend across different countries of suppressing environmental protest and civil disobedience (Forst, 2025). These data show why "red lines protecting the environmental civil space" in NSL design are not merely a liberal gesture, but an institutional condition for sustainable development: if security law creates a climate that cools environmental participation, climate governance itself loses its social foundation.

The conclusion reached in this section is normatively clear: NSL is not merely a law that organizes security; it is the technique for keeping security itself within the rule of law. Foucault's panoptic warning recalls the public sphere that surveillance "makes impossible" as much as the security it "makes possible." Agamben's diagnosis of the exception shows that when the extraordinary does not remain "temporary," the law can turn into its own shadow. The sustainability perspective links these two warnings to the future: predictability, participation, and trust are the minimum institutional climate for long-term environmental and climate policies. Therefore, the transparency–control–limitation triad in NSL design is essential not only for the protection of rights but also for the possibility of a sustainable state mind.

7 CONCLUSION

This study was based on the finding that national security in Turkey is managed within a regime that is legally "multitextual" but institutionally lacking a "single design rationale." This finding is not merely a technical observation regarding the abundance of legislation: the fragmented structure generates constant tension on the three fundamental pillars that carry the democratic legitimacy of security, predictability, accountability, and rights guarantees. The rule of law is not a system that rejects security; rather, it is a system that places security within a "system of checks and balances" against the possibility of unlimited power. Therefore, the fundamental question in the field of national security is not the existence of the powers of security institutions, but how these powers are limited by their definition, procedure, duration, oversight, and redress mechanisms (Venice Commission, 2016; United Nations Commission on Human Rights, 1984).

This article answers the first research question, What risks does the fragmented security regime in Turkey pose to the rule of law?, with the following conclusion: Fragmentation not only erodes legal certainty; it also produces an ecosystem of practices where similar interventions can be subject to different justifications and oversight thresholds. The most visible consequences of this are particularly evident in the digital sphere, in surveillance and access interventions and data processing practices: once the "security" justification is invoked, data protection and freedom of expression safeguards sometimes weaken in areas outside the scope of the justification; at other times, judicial oversight is largely confined to post-event and individual application channels. However, international human rights standards clearly establish that the tests of legality, legitimate purpose, necessity, and proportionality in rights restrictions are not a "formal ritual" but a logic of oversight that creates a burden of concrete justification (United Nations Human Rights Committee, 2011; European Union, 2012).

The second research question, what design principles can be transferred to Turkey from the examples of the US, the UK, and the EU?, was answered by conducting a comparative reading as a "principle separation" rather than a "model transfer." This comparison highlighted three main design principles. First, clarity in the definition of threats: vague and broad definitions create a channel for arbitrary application and erode the legitimacy of security agencies in the long term. Second, end-to-end safeguards in surveillance and intelligence: when permission, recording (audit/log), storage–

destruction, independent oversight, transparency reports, and an effective chain of appeal are not established together, individual permission mechanisms are insufficient to produce democratic safeguards (Big Brother Watch and Others v. the United Kingdom, 2021; Roman Zakharov v. Russia, 2015). Third, temporality and reversibility in extraordinary powers: time limits, extension procedures, sunset mechanisms, and accelerated judicial review are structural brakes that prevent exceptions from becoming permanent (Ferejohn & Pasquino, 2004; Gross & Aoláin, 2006).

The third research question, how does the NSL ensure civil liberties while enhancing security effectiveness?, was discussed in this study based on the assumption that "security effectiveness and rights protection" are not a zero-sum equation. Rights protections are not a "luxury" that weakens security; they are an infrastructure that produces the social legitimacy and institutional sustainability of security. Unclear powers may provide short-term speed; however, in the long term, they erode the capacity for dissent, public trust, and opportunities for cooperation. Therefore, the proposed National Security Law template aimed to strengthen security not with "more authority" but with better designed authority: a narrow and judicially reviewable definition of threat; a layered authority regime (normal period / rising risk / state of emergency); mandatory reporting and parliamentary briefing; an independent auditor/commissioner model; tightening judicial authorization standards along the necessity-proportionality axis; and a minimization-storage-destruction-notification-remedy chain throughout the data life cycle (European Data Protection Supervisor, 2017; United Nations Human Rights Committee, 2011).

The fourth research question, how can the design of NSLs be linked to sustainable development and environmental/climate-based risks?, required a two-pronged approach in this study. On the one hand, climate change and disasters are risk areas that directly affect security governance through critical infrastructure, public health, and social vulnerabilities; therefore, national security law's disregard for the "age of risk" weakens institutional preparedness capacity (Intergovernmental Panel on Climate Change, 2022). On the other hand, the securitization of climate and environmental issues can produce a chilling effect in the areas of public participation and environmental rights, eroding the democratic conditions for sustainable development. The 2030 Agenda's emphasis on "strong institutions, accessible justice, and inclusive societies" reminds us that sustainable development is not only a technical but also an institutional-legal project (United Nations

General Assembly, 2015). Therefore, in the design of NSL, environmental/climate-based risks should not be used as a pretext for extraordinary authority; rather, they should be positioned as a public policy area consistent with resilience, transparent information flow, and participatory governance. Provisions protecting the environmental civil sphere are not “extra” in this context, but rather the legal insurance of sustainable development (UNECE, 1998; United Nations General Assembly, 2022).

On a critical level, Foucault's analysis of panopticism reminded us that surveillance is not merely a violation of privacy but a technique of power that reconfigures the behaviors of public life; the perception of surveillance can generate self-censorship and withdrawal from participation (Foucault, 1995; Penney, 2016; Stoycheff, 2016). Agamben's discussion of the state of exception, meanwhile, showed that where extraordinary measures do not remain “temporary,” the law can become a threshold that normalizes the extraordinary (Agamben, 2005). Together, these two lenses substantiate why the proposed NSL design's triad of “transparency + oversight + limitation” is not merely technical but a constitutive condition of democratic rule.

This article's main contribution is to show that a National Security Law compatible with rights for Turkey can be established not merely as a “general call” but as a concrete design architecture. The framework proposed here claims not so much to consolidate the institutional tools of security into a single text, but rather to mandate minimum design standards wherever security touches on rights: specificity, accountability, time-boundness, burden of justification, and effective recourse. Such a design strengthens security's capacity to produce “legitimacy through predictability” rather than its capacity to produce “consent through fear.”

Of course, this work also has limitations. First, the proposed NSL template, as a normative design proposal, will succeed depending on factors such as implementation capacity, institutional resources, judicial specialization, and the actual effectiveness of oversight bodies. Second, it is clear that comprehensive “harmonization” of existing legislation in Turkey will be required: unless the framework norms of the NSL are systematically linked to counterterrorism, criminal procedure, data protection, and digital regulations, a new text may simply reproduce the old fragmentation. Third, the social acceptance of the transparency-privacy balance in the field of surveillance and intelligence is not only a matter of legal formulae but also of long-term institutional culture. Therefore, further studies should (i) produce empirical data on the justification

practices of security interventions in Turkey, (ii) measure the capacity and independence conditions of oversight bodies, and (iii) reveal how environmental participation intersects with securitization discourses through field-based research.

Ultimately, national security law asks the slowest question of law in the area where the state wants to act the fastest: "At what cost?" The conclusion of this article is this: The way to manage national security in Turkey with democratic legitimacy is not to take security outside the law; it is to make security the subject of a more sophisticated design within the law. A rights-compliant NSL not only protects the individual against the state; it also protects the state against the institutional and political costs of its own reflex to make exceptions. And a sustainable future can only be built on this foundation of dual protection.

REFERENCES

2559 sayılı Polis Vazife ve Salahiyet Kanunu. (1934). Emniyet Genel Müdürlüğü mevzuat yayımları.

2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu. (1983). T.C. İçişleri Bakanlığı mevzuat yayımları.

2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu. (1983). Türkiye Büyük Millet Meclisi.

2935 sayılı Olağanüstü Hal Kanunu. (1983). UYAP Mevzuat.

2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu. (1983). UYAP Mevzuat.

3713 sayılı Terörle Mücadele Kanunu. (1991). UYAP Mevzuat.

50 U.S.C. § 1881a (USA). (n.d.).

5237 sayılı Türk Ceza Kanunu. (2004). T.C. Adalet Bakanlığı (Mevzuat yayını).

5271 sayılı Ceza Muhakemesi Kanunu. (2004). T.C. Adalet Bakanlığı (Mevzuat yayını).

5442 sayılı İl İdaresi Kanunu. (1949). UYAP Mevzuat.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. (2007). Resmî Gazete metni (konsolide).

5809 sayılı Elektronik Haberleşme Kanunu. (2008). T.C. Ulaştırma ve Altyapı Bakanlığı.

5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun. (2009). AFAD mevzuat yayımları.

6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun. (2014). Türkiye Büyük Millet Meclisi.

6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016). T.C. Adalet Bakanlığı.

Agamben, G. (2003). *Lo stato di eccezione*. Bollati Boringhieri.

Agamben, G. (2005). *State of exception* (K. Attell, Trans.). University of Chicago Press.

Anayasa Mahkemesi. (2019). Basın duyurusu: Wikipedia'ya erişim engeli hakkında bireysel başvuru kararı.

Anderson, D. (2023). *Independent Review of the Investigatory Powers Act 2016*. Home Office.

Arslanalp, S. (2023). Spatial reason of the state: The role of space in protest bans in Turkey. *Space and Polity*.

Article 19. (1995). *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*.

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. *European Journal of International Relations, 11*(2), 171–201. doi:10.1177/1354066105052960

Big Brother Watch and Others v. the United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (European Court of Human Rights Grand Chamber, May 25, 2021).

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives, 27*(1_suppl), 63–92. doi:10.1177/03043754020270S105

Bjørnskov, C., & Voigt, S. (2018). The architecture of emergency constitutions. *International Journal of Constitutional Law, 16*(1), 101–127.

Briggs, C. M. (2012). Climate security, risk assessment and military planning. *International Affairs, 88*(5).

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Civil Contingencies Act 2004 (UK). (2004).

Congressional Research Service. (2021). *Domestic Terrorism: Overview of Federal Criminal Law and Investigative Authorities* (R46829).

Congressional Research Service. (2025). *FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act (RISAA)* (R48592).

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)* (ETS No. 5).

Council of Europe. (n.d.). *Derogation in time of emergency (Article 15 of the European Convention on Human Rights)*(Factsheet).

Council of Europe. (n.d.). *Guide on Article 15 of the Convention – Derogation in time of emergency*.

Council of Europe. (n.d.). *National security and European case-law*.

Criddle, E. J., & Fox-Decent, E. (2012). Human rights, emergencies, and the rule of law. *Human Rights Quarterly, 34*(1), 39–87.

Cusato, E. (2022). Of violence and (in)visibility: The securitisation of climate change in international law. *London Review of International Law, 10*(2), 203–242. doi:10.1093/lril/lrac015

Çınar, Ö. H. (2017). Turkey's human rights agenda: Toplantı özgürlüğü ve güvenlik ekseninde tartışmalar. *Journal of Human Rights*.

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12 (Court of Justice of the European Union, 2014).

Directive 2002/58/EC (ePrivacy Directive), OJ L 201, 31.7.2002. (2002).

Directive (EU) 2016/680 (Law Enforcement Directive), OJ L 119, 4.5.2016. (2016).

Directive (EU) 2017/541 on combating terrorism, OJ L 88, 31.3.2017. (2017).

Doğu, B. (2022). Environmental mobilizations through online networks: Digital activism and collective action in Turkey. *International Journal of Communication*.

Dyzenhaus, D. (2006). *The constitution of law: Legality in a time of emergency*. Cambridge University Press.

European Court of Human Rights. (2010). *Gözel and Özer v. Turkey* (Judgment). HUDOC.

European Court of Human Rights. (2012). *Ahmet Yıldırım v. Turkey* (Judgment). HUDOC.

European Court of Human Rights. (2015). *Cengiz and Others v. Turkey* (Judgment). HUDOC.

European Court of Human Rights. (2017). *Işıkırık v. Turkey* (Judgment). HUDOC.

European Court of Human Rights. (2022). *Factsheet – Derogation in time of emergency* (February 2022).

European Court of Human Rights. (2025). *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Updated August 31, 2025).

European Data Protection Supervisor. (2017). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit*.

European Union. (2012). *Charter of Fundamental Rights of the European Union* (2012 O.J. C 326/391, Art. 52).

Ferejohn, J., & Pasquino, P. (2004). The law of the exception: A typology of emergency powers. *International Journal of Constitutional Law, 2*(2), 210–239. doi:10.1093/icon/2.2.210

Forst, M. (2025, October 29). New report: UN Special Rapporteur reveals global complaints on environmental defender harassment under the Aarhus Convention. *Business & Human Rights Resource Centre*.

Foucault, M. (1975). *Surveiller et punir: Naissance de la prison*. Gallimard.

Foucault, M. (1995). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books. (Original work published 1975)

Gerards, J. (2013). How to improve the necessity test of the European Court of Human Rights. *International Journal of Constitutional Law, 11*(2), 466–490.

Global Witness. (2025). *Roots of resistance: Documenting the killings and disappearances of land and environmental defenders*.

Greene, A. (2017). Defining terrorism: One size fits all? *International and Comparative Law Quarterly, 66*(2), 411–440.

Gross, O., & Aoláin, F. N. (2006). *Law in times of crisis: Emergency powers in theory and practice*. Cambridge University Press.

Gu, W., Yan, W., & Yu, S. (2024). Rule of law, corruption and transparency impacts on green growth of East Asian economies. *Humanities and Social Sciences Communications, 11*(1). doi:10.1057/s41599-024-03659-1

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622. doi:10.1080/00071310020015280

Hall, J. (2025). *State threats legislation in 2024*. Independent Reviewer of Terrorism Legislation (Report laid before Parliament).

Hsiang, S. M., Burke, M., & Miguel, E. (2013). Quantifying the influence of climate on human conflict. *Science, 341*(6151).

International Court of Justice. (2025, July 23). *Obligations of States in respect of climate change* (Advisory Opinion, General List No. 187).

Intergovernmental Panel on Climate Change. (2022). *Climate Change 2022: Impacts, adaptation and vulnerability (WGII AR6)*. Cambridge University Press.

Investigatory Powers Act 2016 (UK). (2016).

Investigatory Powers Commissioner's Office. (2025a). *The double lock*.

Investigatory Powers Commissioner's Office. (2025b). *Annual Report 2023* (HC 603).

Investigatory Powers Tribunal. (2024). *Report 2021–2023*.

Kinikoglu, D. (2023). Implementing a new data protection law in Turkey: Opportunities, gaps, and enforcement. *International Data Privacy Law*.

Klatt, M. (2012). Proportionality—a benefit to human rights? Remarks on the I•CON controversy. *International Journal of Constitutional Law, 10*(3), 687–708.

Lawlor, M. (2025). *Out of sight: Human rights defenders working in isolated, remote and rural contexts* (A/HRC/58/53). United Nations Human Rights Council.

Mahmutovic, A., & Alhamoudi, A. (2023). Understanding the relationship between the rule of law and sustainable development. *Access to Justice in Eastern Europe*.

McGoldrick, D. (1996). Sustainable development and human rights: An integrated conception. *International and Comparative Law Quarterly, 45*(4), 796–818.

Michaels, R. (2006). The functional method of comparative law. In M. Reimann & R. Zimmermann (Eds.), *The Oxford Handbook of Comparative Law* (pp. 339–382). Oxford University Press.

Millî İstihbarat Teşkilatı. (n.d.). Faaliyetler (2937 sayılı Kanun kapsamında kurumlar arası yükümlülükler).

Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2024). The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe. *Journal of Human Rights Practice, 16*(1), 397–412. doi:10.1093/jhuman/huad020

National Emergencies Act, 50 U.S.C. §§ 1601–1651 (USA). (1976).

National Security Act 2023 (UK). (2023).

OSCE Representative on Freedom of the Media. (2009). *Access blocking in Turkey: The law on "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication" (Law No. 5651)*. OSCE.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117–182.

Platsas, A. E. (2008). The functional and the dysfunctional in the comparative method of law: Some critical remarks. *Electronic Journal of Comparative Law, 12*(3).

Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4.5.2016. (2016).

Roe, P. (2012). Is securitization a 'negative' concept? Revisiting the normative debate over normal politics. *Security Dialogue, 43*(3), 249–266. doi:10.1177/0967010612443723

Roman Zakharov v. Russia, App. No. 47143/06 (European Court of Human Rights Grand Chamber, December 4, 2015).

Scheinin, M. (2010). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Ten areas of best practices in countering terrorism* (A/HRC/16/51).

Security Council Report. (2022, December 30). *The UN Security Council and Climate Change*.

Stone Sweet, A., & Mathews, J. (2008). Proportionality balancing and global constitutionalism. *Columbia Journal of Transnational Law, 47*, 68–149.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly, 93*(2), 296–311. doi:10.1177/1077699016630255

Szabó and Vissy v. Hungary, App. No. 37138/14 (European Court of Human Rights, January 12, 2016).

Tele2 Sverige AB and Others, Joined Cases C-203/15 and C-698/15 (Court of Justice of the European Union, 2016).

The Sunday Times v. the United Kingdom (No. 1), App. No. 6538/74 (European Court of Human Rights, April 26, 1979).

Tsakyrakis, S. (2009). Proportionality: An assault on human rights? *International Journal of Constitutional Law, 7*(3), 468–493.

Türkiye Büyük Millet Meclisi. (n.d.). Güvenlik ve İstihbarat Komisyonu (kuruluş ve görevler).

Türkiye Cumhuriyeti Anayasası. (1982). T.C. Anayasa Mahkemesi mevzuat sayfası (konsolide metin).

UNECE. (1998). *Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Aarhus Convention)*.

United Nations. (1966). *International Covenant on Civil and Political Rights* (999 U.N.T.S. 171).

United Nations. (n.d.). *Goal 16: Peace, justice and strong institutions*.

United Nations Commission on Human Rights. (1984). *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (E/CN.4/1985/4).

United Nations General Assembly. (1998). *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms*(A/RES/53/144).

United Nations General Assembly. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*(A/RES/70/1).

United Nations General Assembly. (2022). *The human right to a clean, healthy and sustainable environment*(A/RES/76/300).

United Nations Human Rights Committee. (2001). *General comment No. 29: States of emergency (Article 4)*(CCPR/C/21/Rev.1/Add.11).

United Nations Human Rights Committee. (2011). *General comment No. 34: Freedoms of opinion and expression (Article 19)* (CCPR/C/GC/34).

United Nations Human Rights Council. (2021). *The human right to a clean, healthy and sustainable environment*(Resolution 48/13).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (USA). (2001).

U.S. Congress. (2009). *18 U.S.C. § 2331: Definitions*. U.S. Government Publishing Office. https://www.govinfo.gov/app/details/USCODE-2009-title18/USCODE-2009-title18-partI-chap113B-sec2331

USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (USA). (2015).

Venice Commission. (2015). *Report on the democratic oversight of signals intelligence agencies* (CDL-AD(2015)011). Council of Europe.

Venice Commission. (2016). *Opinion on emergency decree laws in Turkey* (CDL-AD series). Council of Europe.

Venice Commission. (2016). *Opinion on Turkish legislation relevant to the internet (Law No. 5651)*. Council of Europe.

Venice Commission. (2016). *Rule of law checklist* (CDL-AD(2016)007). Council of Europe.

Venice Commission. (2025). *The Updated Rule of Law Checklist* (CDL-AD(2025)002). Council of Europe.

Wæver, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On security*. Columbia University Press.

Won, Y. (2025). Emergency powers and COVID-19 derogations. *International Journal of Constitutional Law, 23*(1), 113–147.

World Commission on Environment and Development. (1987). *Our common future*. Oxford University Press.

Zalnieriute, M. (2021). A struggle for competence: National security, surveillance and the scope of EU law at the Court of Justice. *The Modern Law Review, 85*(1), 198–217.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Uygur, M. R. NATIONAL SECURITY LAW AND DEMOCRATIC GOVERNANCE IN TURKEY. Veredas Do Direito, e234095. https://doi.org/10.18623/rvd.v23.n1.4095