THE NATIONAL SECURITY EXEMPTION IN THE AI ACT: CRITICAL PERSPECTIVES ON THE ROMANIAN LEGISLATIVE FRAMEWORK

Dragoș Alexandru MAIOR *

ABSTRACT : *Inevitably, the expansion of artificial intelligence (AI) technologies was bound to intersect with the realm of national security. Driven by this objective, the prospect of unprecedented predictive surveillance and analytical processing capabilities is undeniably compelling. Yet, while the national security exemption is enshrined at the European Union level, finding its explicit regulation within the AI Act itself, its very nature demands a strict interpretation. Addressing these emerging challenges, although government agencies might deploy AI-based technical solutions that qualify as high-risk systems, the AI Act mandates an ex-ante oversight mechanism.*
This paper traces and dissects this legal requirement through the lens of Legislative Bill 565/2025 amending Law No. 51/1991 regarding Romania's national security, a legal instrument empowering intelligence agencies to conduct mass processing of personal data via automated means. Anchored in this legislative draft, which has tacitly passed the first chamber of the Parliament, the present study argues that when dealing with this specific class of technology, traditional parliamentary oversight proves inadequate. Due to its fundamentally reactive and ex-post nature, such oversight becomes ineffective and merely illusory when confronted with the operational opacity inherent to these systems.

KEYWORDS: *artificial intelligence; AI Act; fundamental rights impact assessment (FRIA); national security; algorithmic surveillance; proportionality.*
JEL Code: *K24*

DOI: **10.62838/cjjc-2024-0081**

1. INTRODUCTION

The Normative Foundations of Algorithmic Accountability

The overarching European legal framework on artificial intelligence materialized through the concurrent adoption of Regulation (EU) 2024/1689[1] laying down harmonised

* PhD., Student, Ecological University Bucharest, Lawyer, Mureș Bar, ROMANIA.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act), published in OJ L, 2024/1689, 12 July 2024.

rules on artificial intelligence (the AI Act) on June 13, 2024, alongside the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law[2] (the AI Framework Convention) on May 17, 2024. By virtue of their legal nature and substantive content, these two harmoniously articulated instruments operate in a complementary manner. They carry significant implications for the regime governing AI deployment within the administration of justice, specifically concerning the conditions of its legitimacy, balancing between innovation, sovereignty, and the safeguarding of fundamental rights (Duțu, 2026).

Conceding that *security without liberty amounts to tyranny, while liberty without security descends into chaos* (Tănăsescu, 2025), addressing the matter at hand requires a foundational premise: the concept of national security is deeply woven into the constitutional architecture. While the Romanian Constitution stops short of providing an exhaustive definition of "national security," it projects the concept across multiple dimensions. It acts as a foundational value sustaining the constitutional order (Art. 1), an express justification for restricting the exercise of certain rights (Art. 53), and forms the basis of institutional infrastructure (Arts. 92–93, Arts. 118–119, among others). This multi-layered approach explains the growing contemporary discourse surrounding the constitutionalization of *"national security"* and its subsequent inclusion within the *"bloc of constitutionality* (E.-S. Tănăsescu, 2025)*."*

Furthermore, the debate surrounding national security against the backdrop of emerging cyber realities is hardly new. In fact, the Romanian Constitutional Court (CCR) has been seized with and has scrutinized this very issue on several occasions over recent years. Notably, through Decision No. 91/2018 and Decision No. 802/2018, the Court reviewed the provisions of Article 3 of Law No. 51/1991, which had been expanded[3] to include the following threat categories: point (n) – *"cyber threats or cyber attacks against IT and communications infrastructures of national interest"*; point (o) – *"actions, inactions, or factual circumstances with national, regional, or global consequences that affect the resilience of the Romanian state in relation to hybrid risks and threats"*; point (p) – *"actions undertaken by a state or non-state entity, through the execution in cyberspace of propaganda or disinformation campaigns, of such a nature as to affect the constitutional order."*

More recently, in 2023, the Constitutional Court, via Decision No. 70 of February 28, 2023[4], held that:

---

[2] Council of Europe, *Framework Convention on artificial intelligence and human rights, democracy and the rule of law* (CETS No. 225), adopted on May 17, 2024, and opened for signature in Vilnius on September 5, 2024.

[3] via Law No. 58/2023 on the cybersecurity and cyber defense of Romania, as well as amending and supplementing certain normative acts, Official Gazette No. 214 of 2023, with subsequent amendments and supplementations. This normative act also established certain definitions: 1.a) *cyber defense* - the totality of activities, means, and measures used to counter cyber threats and mitigate their effects on communications and information technology systems, weapon systems, networks, and IT systems supporting military defense capabilities; 2.b) *cyber threat* - as defined in Art. 2 letter f) of Government Emergency Ordinance No. 104/2021 regarding the establishment of the National Cyber Security Directorate, approved with amendments and supplementations by Law No. 11/2022, with subsequent amendments; 3.c) *cyber attack* - a hostile action carried out in cyberspace of such a nature as to affect cybersecurity; 4.d) *cybersecurity audit* - an activity consisting of a systematic evaluation of all policies, procedures, and protection measures implemented within networks and IT systems, aimed at identifying malfunctions and vulnerabilities and providing remedial solutions for them.

[4] concerning the objections of unconstitutionality regarding the provisions of Art. 3 para. (1) lit. c), Art. 21 para. (1), Art. 22, Art. 25, Art. 41, Art. 48, and Art. 50 of the Law on the cybersecurity and cyber defense of Romania,

147. The Court notes that, with respect to the invoked arguments, the criticism regarding the impairment of certain fundamental rights and freedoms is unfounded, since the legislator did not introduce under Article 3 points (n) to (p) any measures, competencies, or specific intelligence-gathering activities that entail the restriction of human fundamental rights or freedoms; these are expressly and exhaustively regulated under Article 14 of Law No. 51/1991. Defining the scope of threats to national security, while taking into consideration how they have evolved, transformed, and diversified, does not implicitly and necessarily entail measures restricting the exercise of fundamental rights. Only the measures expressly stipulated in Article 14 restrict rights and freedoms, and in these exhaustively provided cases, the legislator has simultaneously regulated the legal guarantees set forth in Article 15 and the subsequent articles of Law No. 51/1991. Thus, we note that Articles 14–24 of Law No. 51/1991 provide for ex ante and a posteriori procedures that guarantee the avoidance of any illegal or unauthorized interference in citizens' private lives—a protective regime applicable to any type of threat to national security specified in Article 3, as amended by the provisions of the challenged law.

148. The mere enumeration of internal or external threats to national security cannot, by way of restriction, impair fundamental rights or freedoms. The legislator neither alters the legal regime of threats to national security nor suppresses the guarantees established to ensure the observance of fundamental rights and freedoms. Rather, it merely updates the scope of threats to reflect the current realities of society, aiming—through the regulation of the protection afforded by national security mechanisms—to ultimately ensure the functioning of the Romanian state and the unhindered exercise of citizens' fundamental rights and freedoms.

149. Consequently, the Court holds that defining the threats to national security provided under Article 3 points (n)–(p) of Law No. 51/1991 falls within the Romanian state's margin of appreciation. The new threats pursue a legitimate aim, having been established in response to the realities governing cyberspace—realities which, absent adequate legal protection, could undermine the functioning of the state, the constitutional order, critical cyber infrastructures, and, implicitly, the exercise of fundamental rights and freedoms by its citizens. They are, at the same time, proportionate to the aim of the challenged law, namely ensuring the cybersecurity and cyber defense of Romania."

2. LEGISLATIVE PERSPECTIVES ON DATA WITHIN NATIONAL SECURITY: THE ROMANIAN DRAFT LAW

A proposal to amend Law No. 51/1991 on national security[5] has recently passed the first decision-making chamber of the Romanian Parliament. This legislative draft seeks to establish an express legal framework for the processing of personal data by authorities vested with national security attributions. More specifically, this normative endeavor represents an attempt to align specific intelligence activities with the fundamental privacy guarantees that are mandatory in any democratic society.

as well as amending and supplementing certain normative acts, Legislative Draft Pl-x No. 565/2025, available at: https://www.senat.ro/legis/lista.aspx?nr_cls=L565&ancls=2025.

[5]*Pl-x nr. 565/2025* available on https://www.senat.ro/legis/lista.aspx?nr_cls=L565&an_cls=2025

Without reiterating the entire Explanatory Memorandum, the primary considerations are as follows: "*the evolutions of the European and Euro-Atlantic security climate, particularly concerning the terrorism issue, illegal migration from potential terrorist zones, as well as cyber and hybrid threats, constitute factors that mandate the updating and consolidation of the normative framework for ensuring national security. The pronounced dynamics of negative transnational phenomena, carrying aggressive or threat-level potential to security, coupled with the exacerbation of the cross-border characteristics of most threats—which would otherwise have had predominantly domestic origins and areas of manifestation—necessitate the modification and supplementation of the legislative framework in the field of national security. Concurrently, the development of new technological instruments, the incorporation of technological progress into operational endeavors, and the necessity of maintaining a high level of cooperation with internal and external partners in managing risks and threats call for a clear regulation of the means and methods of action available to the competent authorities in the field. In this regard, it is necessary to expressly regulate the capability of intelligence services and other competent authorities to create, develop, administer, and utilize databases, IT and communication systems, applications, and other online resources as modern means of accomplishing national security missions. The legislative codification of these instruments serves to ensure both operational efficiency and compliance with the principle of legality and the requirements of normative predictability, so that data subjects can reasonably anticipate the conditions under which their data may be processed for national security purposes"* [6].

In nuce, an essential first aspect deriving from this legislative initiative is the statutory enshrinement of the intelligence services' capabilities. By introducing point (e^1) to Article 13, the legislator grants an explicit mandate to create, develop, and administer databases, IT systems, and applications in the online environment. As noted *supra*, this amendment is intended to adapt the legislation to contemporary technological realities, providing the indispensable legal basis for Open-Source Intelligence (OSINT)[7] (NATO, 2001) operations and massive data processing (Big Data)—tools that have become critical in threat prevention (Stephen C. Mercado, 2007).

Nevertheless, to curb arbitrary intrusions, the newly introduced articles (also) institute a specific personal data protection regime, inspired by principles established at the European level, albeit heavily nuanced by the particularities of the field. The draft imposes the principle of storage limitation, compelling authorities to evaluate the justification for data retention at intervals of no more than five years and to erase inaccurate information. An additional safeguard concerns the regime of incidentally obtained data; such collateral information regarding intimate life, family life, or honor, obtained during specific intelligence-gathering activities, must be obligatorily destroyed or deleted when found to lack direct relevance to national security vulnerabilities or threats.

---

[6]Explanatory Memorandum of Legislative Draft Pl-x No. 565/2025, available at: https://www.cdep.ro /proiecte/2025/500/60/5/em729.pdf.

[7] OSINT represents unclassified information that has been deliberately discovered, selected, filtered, and disseminated for a specific audience in order to answer a specific request, as defined by: NATO, NATO Open Source Intelligence Handbook, November 2001, available at: http://www.oss.net/dynamaster/ file_archive /030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20%20Jan%202002 .pdf, accessed on May 24, 2026.

Regarding verification mechanisms, the draft seems anchored in the past and appears to overlook existing provisions in the field by relying on an administrative procedure where persons considering themselves aggrieved may petition the parliamentary oversight committees—effectively, an *ex-post* control. Even so, the efficacy of this democratic oversight mechanism is preemptively curtailed by the very letter of the law: competent authorities are exempted from the obligation to provide the committees with data concerning sources, ongoing operative activities, specific methods, or the identities of active personnel.

Consequently, parliamentary oversight risks being confined to a formal legality check, with the committees deprived of access to the substantive material necessary for a thorough investigation. However, we will not unravel this issue in the present study, nor will we broach the final provisions of the proposal that introduce a (rather interesting) legal guarantee consisting of explicitly opening the avenue of administrative litigation. This essentially grants citizens the possibility to sue state authorities in accordance with the provisions of Law No. 554/2004, thereby shifting the center of gravity for legality control into the sphere of the judiciary.

Remaining within the realm of control and verification mechanisms, and against the European legal backdrop highlighted at the outset of this paper, the question arises: does this legislative proposal actually align with the standards of the AI Act and the GDPR?

3. THE CONVERGENCE BETWEEN ARTICLE 27 OF THE AI ACT AND ARTICLE 22 OF THE GDPR

We submit that the analysis of any national legislative endeavor aiming to implement artificial intelligence within the state architecture, including the realm of national security, must commence with delineating the European standards for the protection of fundamental rights. In this vein, a veritable "European bloc of constitutionality" concerning algorithmic surveillance is shaped by the intersection of two mandatory norms: Article 27 of the Artificial Intelligence Act (the AI Act) and Article 22 of the General Data Protection Regulation (the GDPR).

These provisions establish a dual system (preventive and remedial) of safeguards designed to prevent the citizen from being transformed into a mere object of data analysis. In essence, Article 22 of the GDPR (bearing the marginal heading *Automated individual decision-making, including profiling*) enshrines the data subject's inalienable right not to be subjected to a decision based solely on automated processing—particularly in the case of profiling—when such a decision generates legal effects or significantly affects them: *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

Although paragraph 2(b) permits exceptions[8] when the automated decision is authorized by domestic law, the European legislator strictly conditioned this derogation. The State bears a positive obligation to lay down suitable measures to safeguard rights and

[8] (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests

freedoms, guaranteeing, at an absolute minimum, the individual's right to obtain human intervention, to express their point of view, and to contest the decision. Consequently, domestic law cannot vitiate the essence of the right to defense against the algorithmic mechanism.

While the practical efficacy of Article 22 has been heavily criticized by legal scholars as being limited, we believe any research endeavor must include the turning point that shifted the interpretative paradigm, namely the CJEU judgment of December 7, 2023, in Case C-634/21 (*SCHUFA Holding*) [9]. This ruling massively expanded the applicability of Article 22, establishing that the mere generation of a probability value (scoring) by an agency constitutes an "automated individual decision."

From a strictly legal perspective, one might argue that the legislative draft would not be bound to comply with Article 22 of the GDPR. This stems from the material scope of the European Regulation, which, according to Article 2(2)(a) corroborated with Article 4(2) of the TEU—imperatively stipulating that *"[...] the Union shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State"*—expressly excludes the processing of personal data in the context of national security activities from its scope.

Thus, it could be concluded that the authorities targeted by Law No. 51/1991 operate outside European Union law in this specific domain, invoking the sovereign prerogative of the Member State as recognized by the Treaty on European Union. Even so, the Court of Justice of the European Union (CJEU) drew a very clear red line in landmark cases such as *Privacy International* (C-623/17)[10] and *La Quadrature du Net* (C-511/18)[11]. The CJEU established that if intelligence services process data directly, using their own resources, the activity escapes EU law (and, implicitly, the GDPR). However, if the State legislatively imposes an obligation on private providers (telecom companies, social media platforms, internet service providers) to retain or grant access to data for national security reasons, that obligation imposed on a private actor falls within the ambit of European Union law (specifically, the ePrivacy Directive and the GDPR).

Therefore, looking at the draft amending Law No. 51/1991 (Article 13 point e^1), the text empowers state authorities "to create, develop, administer and utilize databases...". Being an activity organized and carried out directly by the State for national security purposes, it seems to take shelter under the exemption of Article 2(2)(a) of the GDPR, which is why the draft does not address the rigors of Article 22 regarding automated decisions.

Yet, looking beyond the formal mechanism of the exemption, from the perspective of democratic standards, the draft presents major deficiencies compared to the essential requirements of Article 22. Through the new Article 23^1, the draft proposes data processing "by automated means," but utterly omits the establishment of any safeguard

[9] Court of Justice of the European Union. (2023). Judgment of 7 December 2023 in Case C-634/21, OQ v Land Hessen (SCHUFA Holding), ECLI:EU:C:2023:957. https://curia.europa.eu/juris/liste.jsf?num=C-634/21.

[10] Court of Justice of the European Union. (2020). Judgment of 6 October 2020 in Case C-623/17, Privacy International, ECLI:EU:C:2020:790. https://curia.europa.eu/juris/liste.jsf?num=C-623/17.

[11] Court of Justice of the European Union. (2020). Judgment of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, ECLI:EU:C:2020:791. https://curia.europa.eu/juris/liste.jsf?num=C-511/18.

against exclusively automated decisions. Unlike the GDPR mechanism, which mandates the person's right to obtain human intervention and express their point of view, the proposed domestic text leaves a critical blind spot regarding how algorithmic profiling translates into measures with legal impact.

Perhaps this is the context and place to draw a parallel with the situation highlighted by the *Rotaru v. Romania* case[12], in which the European Court of Human Rights ruled that the right to respect for private life (Article 8 ECHR) and the right to an effective remedy (Article 13 ECHR) were violated. Among other things, the Court held that the Romanian legislation dating back to 1948 did not regulate with sufficient clarity the scope, duration, and procedures for storing information by intelligence services, meaning there were insufficient safeguards against abuses.

This legislative silence becomes critical in the scenario envisioned by Article 23^2 letter (b), concerning the clearance process for issuing a security certificate. If a massive data analysis system generates a risk profile that automatically leads to the rejection of the clearance, the absence of a legal obligation for authentic human review transforms the system into an unassailable architecture. The citizen would end up suffering severe legal consequences regarding their professional trajectory based exclusively on an unexplained algorithmic score.

Although the initiator attempted to offset these procedural loopholes by opening the avenue of administrative litigation, as provided in Article 23^8, the instrument risks remaining illusory in the absence of a genuine right to an explanation. A judge seized with a claim against the refusal of a security clearance will face the impossibility of scrutinizing the algorithm's logic, since authorities can refuse the declassification of specific methods or clearance processes by invoking the limits of their own oversight stipulated in Article 23^6 of the same draft.

In conclusion, although the proposed text evades the rigors of Article 22 of the GDPR under the protection of the national security exemption, it ignores the doctrinal substance of European safeguards. To align with the jurisprudence of the European Court of Human Rights and the exigencies of the rule of law, such legislation should expressly enshrine the prohibition of decisions founded exclusively on automated data processing, mandating the guarantee of human oversight and proportionality.

Conversely, Article 27 of the AI Act introduces a paradigm shift in public law, instituting the obligation to conduct a Fundamental Rights Impact Assessment (FRIA) prior to deploying any high-risk AI system (M. Kaminski, 2021). This norm directly targets public law bodies, mandating an ex-ante proportionality analysis.

In other words, before deploying a high-risk AI system as referred to in Article 6(2) [...]: deployers that are bodies governed by public law or private entities (NICHIFOR, 2026) providing public services, and deployers of high-risk AI systems referred to in point 5(b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such systems may produce. To that end, deployers shall perform an assessment consisting of: (a) a description of the deployer's processes in which the high-risk AI systems will be used in line with their intended purpose; (b) a description of the period of time and frequency in which each high-risk AI system is intended to be used; (c)

[12] ECtHR, Judgment of 4 May 2000, Case of Rotaru v. Romania [GC], Application no. 28341/95, §, available at https://hudoc.echr.coe.int/eng?i=001-58586.

the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to impact the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13; (e) a description of the implementation of human oversight measures, according to the instructions of use; (f) the measures to be taken in case of the materialization of those risks, including internal governance and complaint mechanisms. The deployer is obliged to map the context of use, the targeted categories of data subjects, and the specific risks of prejudice to their rights, anchoring the process in the technical information furnished by the system's developer.

We might even argue that this obligation transcends bureaucratic formalism, it demands an exhaustive description of human oversight measures and internal governance mechanisms engineered for risk mitigation. However, while intended to function as a filter for institutional accountability, the provision of Article 27 is not immune to criticism. In this context, it is noteworthy that the European Center for Not-for-Profit Law (ECNL) drafted and proposed the most comprehensive methodological framework for the FRIA as early as the draft phase of the AI Act. The document, published alongside other European experts, proposes a six-step evaluation matrix for high-risk AI systems (European Center for Not-for-Profit Law, 2023).

Moreover, it contends that the FRIA is not fully mandatory for the private sector, applying instead predominantly to the public sector or entities providing public services, a limitation that heavily hampers its efficacy. The Illusion of Protection via the Provider's "Ex-Ante" Assessment The framework envisioned by the AI Act rests on the premise that the provider (developer) of the AI system has already resolved issues of bias and risk through the conformity assessment (CE) conducted prior to market placement. Consequently, the legislator considered that the private deployer no longer needs to conduct a FRIA, but merely needs to adhere to the user manual. Applying a historical-comparative approach to risk-based liability, it becomes evident that this premise is profoundly flawed from both a sociological and legal standpoint. Risks to fundamental rights are not solely intrinsic to the source code; rather, they are eminently contextual. For instance, an algorithm may remain perfectly neutral in a laboratory setting, yet become highly discriminatory depending on the local data fed into it by the private company deploying it. Essentially, by eliminating the FRIA obligation for the private sector, the law strips away the sole mechanism capable of assessing impact within the actual context of use. Nevertheless, we will halt our substantive critique of this mechanism here. When evaluating this mandatory requirement against the legislative draft currently under debate, one might say it is sublime, yet entirely absent.

The present study would remain under the mark of superficiality if we failed to specify that the European legislator appears to have foreseen a security exemption from the aforementioned requirements. Specifically, according to Article 2(3) of Regulation (EU) 2024/1689, its provisions do not apply to artificial intelligence systems if and insofar as they are placed on the market, put into service, or used exclusively for military, defense, or national security purposes:

(3) This Regulation does not apply to areas outside the scope of Union law, and in any event shall not affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences. This Regulation does not apply to AI systems if and insofar

as they are placed on the market, put into service, or used, with or without modification, exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

We thus observe that this exemption is even broader than its GDPR counterpart, as it covers not only state authorities but any entity conducting activities exclusively for these purposes. Consequently, the IT systems, applications, and databases that the Romanian intelligence services might develop or utilize under the new Article 13 point (e^1) are completely extracted from the rigors of the AI Act. From a strictly legal standpoint, the obligation to conduct a Fundamental Rights Impact Assessment (FRIA) does not arise.

However, moving beyond the formal exemption and analyzing the draft through the lens of the rule of law and proportionality, it becomes apparent that the proposed domestic text completely ignores the protective philosophy instituted by Article 27. The FRIA mechanism within the AI Act was conceived as an *ex-ante* (preventive) filter. Public institutions deploying systems with a major impact on citizens are obliged to evaluate, prior to their operationalization, how the algorithm might infringe upon human dignity, freedom of expression, the right to a fair trial, or the right to non-discrimination. In flagrant contrast, the Romanian legislative draft shifts the entire weight of oversight into the *ex-post* realm (after a potential injury has occurred).

One could argue that authorities are handed a blank check to create and utilize technological resources in the online environment (including systems that might integrate machine learning for OSINT or profiling), devoid of any obligation to conduct a national-level fundamental rights impact assessment. The proposed safeguards, such as the deletion of irrelevant data or parliamentary oversight, only intervene after the processing has taken place and, potentially, after harm has already been inflicted.

Moreover, Article 27(4) of the AI Act compels public deployers to publish a summary of the FRIA results, thereby ensuring a minimum threshold of democratic transparency regarding state-utilized technologies. The draft amending Law No. 51/1991 not only fails to provide for such an obligation of prior transparency, but it severely curtails the capacity for oversight even when suspicions of abuse arise. The new Article 23^6 prohibits supplying parliamentary committees with data concerning sources, methods, and specific means. Lacking an obligation to document the technology's impact on fundamental rights from its inception (a *fundamental rights by design* approach), the remedial mechanism provided through administrative litigation (Article 23^8) is left devoid of evidentiary substance for the targeted citizen.

On a more abstract level, regarding expansive surveillance—whether we speak of online monitoring or specific systems—an eloquent example is the Social Credit System (SCS) utilized in China (Liu, 2024), through which, in essence, the Chinese government quantifies and regulates citizen trust by measuring social behaviors. This system rewards and sanctions citizens based on a scoring metric with a complex calculation modality. Certainly, the SCS metrics are heavily influenced by the political interests characteristic of the regime; however, the core issue actually lies in the decontextualization of behavior. The system oversimplifies the assessment of conduct by ignoring essential factors such as the social context and the intent behind the actions, inevitably leading to a superficial

judgment. Regarding its effect on social relations, the system intensifies state control over citizens' lives, spearheading global trends of governance through quantification and algorithmic surveillance.

Venturing tangentially into the philosophy of law, it is important to note that doctrine (Schuilenburg Marc, 2015) argues how, against the backdrop of contemporary society and emerging technologies, a different consciousness emerges among people living in urban areas. Essentially, examining how surveillance technologies integrated into urban infrastructure influence the behavior and self-awareness of inhabitants, Schuilenburg concludes that in modern urban environments, a different self-consciousness develops, heavily influenced by the constant presence of surveillance and data-collection technologies. This shift impairs social cohesion, leading to a fragmented society where communities isolate themselves for protection. At the same time, securitization influences how people interact with authorities, exacerbating their dependence on state institutions for safety management (Maior, 2026).

4. CONCLUSIONS

Ultimately, although the draft appears safe from an infringement procedure due to the material exemption provided in Article 2(3) of the AI Act, it reflects an antiquated legal architecture. In an era where the European standard requires the state to justify and preventively evaluate its technological instruments, the national legislative initiative refuses to import these safeguarding principles into its security architecture.

Thus, on one hand, the AI Act norms compel the state authority to design and document the architecture of human intervention prior to the system's operationalization, evaluating the systemic impact on society. On the other hand, the GDPR provisions offer the individual the requisite legal instrument to trigger this human intervention the moment an adverse effect is felt. Yet, any legislative architecture that eludes this normative convergence risks instituting an unbalanced regime of algorithmic sovereignty, hollowing out constitutional guarantees by simultaneously eliminating preliminary risk assessments and effective avenues of material oversight.

REFERENCES

1.Books, Articles, and Academic Literature

Duțu, M., 2026. "Judicial Artificial Intelligence: Between Risks and Benefits. The European Regulatory Framework". *JURIDICE.RO.*

Tănăsescu, E.-S., 2025. *Speech by the President of the Constitutional Court at the annual roundtable organized by the Romanian Association of Constitutional Law (ARDC).* [Online]
Available at: https://www.juridice.ro/essentials/10636/securitatea-nationala-este-integrata-in-constitutie

E.-S. Tănăsescu, 2025. National Security is Integrated into the Constitution" [Securitatea națională este integrată în Constituție]. *JURIDICE.ro.*

Stephen C. Mercado, 2007. Sailing the Sea of OSINT in the Information Age. *Studies in Intelligence,* Vol. 48(3).

NATO, 2001. *NATO Open Source Intelligence Handbook, November 2001,* s.l.: s.n.

M. Kaminski, G. M., 2021. Algorithmic Impact Assessments under the GDPR and the AI Act: producing protection or performative compliance?. *International Data Privacy Law*, 11(1).

NICHIFOR, A., 2026. Suprapunerea dintre AI Act și GDPR. Provocări de conformare pentru companii românești care utilizează inteligență artificială. *JURIDICE.ro*,.

European Center for Not-for-Profit Law, 2023. *Framework for a Fundamental Rights Impact Assessment for AI*, The Hague: s.n.

Liu, C. &. R.-T. A., 2024. Trusting by Numbers: An Analysis of a Chinese Social Credit System Governance Infrastructure. *Critical Sociology*.

Schuilenburg Marc, G. H., 2015. he Securitization of Society: Crime, Risk, and Social Order.

Maior, A. D., 2026. *FROM PSYCHOPOWER TO PROHIBITED PRACTICES: THE PROTECTION OF COGNITIVE LIBERTY IN THE CONTEXT OF ART. 5 OF THE AI REGULATION AND ECtHR JURISPRUDENCE*. Craiova, Universitaria Publishing House, pp. 297-309.

2. International and European Legislation

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. OJ L 119, 4.5.2016, p. 1–88.

Note: Analyzed specifically with regard to Article 22(2)(b) concerning automated individual decision-making authorized by Union or Member State law.

European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act)*. OJ L, 2024/1689, 12 July 2024.

Council of Europe. (2024). *Framework Convention on artificial intelligence and human rights, democracy and the rule of law*. CETS No. 225, adopted on May 17, 2024, opened for signature in Vilnius on September 5, 2024.

3. National Legislation and Preparatory Acts (Romania)

Parliament of Romania. (2023). *Law No. 58/2023 on the cybersecurity and cyber defense of Romania, as well as amending and supplementing certain normative acts*. Official Gazette of Romania, No. 214 of 2023.

Note: Statutory definitions reviewed from Article 3: point (1)(a) cyber defense; point (2)(b) cyber threat; point (3)(c) cyber attack; point (4)(d) cybersecurity audit.

Parliament of Romania. (2025). *Legislative Draft Pl-x No. 565/2025 concerning the amendment and supplementation of certain normative acts regarding national security*. Available at: https://www.senat.ro/legis/lista.aspx?nr_cls=L565&an_cls=2025.

Parliament of Romania. (2025). *Explanatory Memorandum of Legislative Draft Pl-x No. 565/2025*. Available at: https://www.cdep.ro/proiecte/2025/500/60/5/em729.pdf.

Note: Investigated in relation to the constitutional objections raised regarding Articles 3(1)(c), 21(1), 22, 25, 41, 48, and 50 of the Cybersecurity Law.

4. Jurisprudence

Court of Justice of the European Union. (2020). *Judgment of the Court (Grand Chamber) of 6 October 2020, Privacy International v Ministre des Affaires étrangères and Others*. Case C-623/17, ECLI:EU:C:2020:790. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-623/17.

Court of Justice of the European Union. (2020). *Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others v Premier Ministre and Others*. Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-511/18.

Court of Justice of the European Union. (2023). *Judgment of the Court (First Chamber) of 7 December 2023, OQ v Land Hessen (SCHUFA Holding)*. Case C-634/21, ECLI:EU:C:2023:957. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-634/21.

European Court of Human Rights. (2000). *Judgment of 4 May 2000, Case of Rotaru v. Romania* [Grand Chamber]. Application No. 28341/95. Available at: https://hudoc.echr.coe.int/eng?i=001-58586.

5. Institutional Reports and Technical Standards

NATO. (2001). *NATO Open Source Intelligence Handbook*. Intelligence Liaison Section, NATO Headquarters. Available at: http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20%20Jan%202002.pdf [Accessed on May 24, 2026].