Metodo Giuridico
Ius et Ratio • ISSN 3103-7305
ITALIAN JOURNAL OF LAW & CASE LAW • ISSN 3103-7305
IN-DEPTH LEGAL ANALYSIS • ADMINISTRATIVE LAW & PUBLIC PROCUREMENT • 13 NOVEMBER 2026

National Security in Public Procurement: Cloud Sovereignty and ICT Veto Powers

The Convergence of the Public Contracts Code, the National Cybersecurity Perimeter, ACN Cloud Qualification, and Foreign Investment Screening in Technology Procurement

FP Federico Palumbo Administrative Law & Public Procurement 13 November 2026

Reading time 21 min

Current Legal Framework as of 11 November 2026: The intersection among the Italian Public Contracts Code, the national cybersecurity perimeter, and executive screening powers (*golden power*) has reshaped the protection of strategic assets from an exceptional derogation into a structural governing principle of digital public procurement.

ABSTRACT

The regulation of **national security in public procurement** has undergone a profound transformation, evolving from an exceptional derogation clause into a structural criterion of technical selection. This study examines the systematic integration among Article 136 of the Italian Public Contracts Code, the **national cybersecurity perimeter**, and governmental screening powers (**golden power**). Through the lens of recent administrative case law, the analysis explores mandatory qualification standards for **public sector cloud services**, geographical infrastructure localization requirements, the allocation of the burden of proof, and the boundaries of **judicial review by administrative courts** over technological exclusions and vetoes affecting ICT supply contracts.

Key Takeaways

- **Systematic Evolution:** National security has shed its traditional character as a purely exceptional exemption and consolidated its status as a structural parameter for technical qualification and price-score allocation in high-criticality ICT public procurement.
- **Allocation of Institutional Competences:** The procedural framework governing the national cybersecurity perimeter and the binding prescriptions issued by the National Evaluation and Certification Centre (CVCN) prevail over the contractual autonomy of the contracting authority, imposing mandatory compliance requirements under penalty of exclusion or termination of the contract.
- **Limits of Judicial Review:** The exercise of executive screening powers (*golden power*) and geopolitical risk assessments entail broad political and technical discretion, which may be reviewed before administrative courts solely for manifest unreasonableness, misrepresentation of material facts, or patent failure to conduct an adequate preliminary investigation.

RESEARCH DOSSIER

JURISDICTION
Italy (Civil Law)

SUBJECT AREA
Administrative Law & Public Procurement

SCOPE
Italian Civil Law System

Legal Principle / Editorial Headnote

In award procedures for digital and infrastructural public contracts, national security safeguard clauses, mandatory compliance with cybersecurity qualification tiers, and submission to special executive powers constitute intrinsic statutory limits on the contractual freedom of public authorities; judicial review over resulting exclusions is confined to an extrinsic verification of logical coherence, proportionality, and completeness of the underlying technical investigation.

01. THE EVOLUTION OF NATIONAL SECURITY IN PUBLIC PROCUREMENT ACROSS DOMESTIC AND SUPRANATIONAL SOURCES

1.1 — National Security Within the Architecture of Public Contracts Across Primary and Supranational Law

The role of **national security in public procurement** has gradually moved beyond that of a boilerplate safeguard clause to become a central regulatory pillar of the **digital transition of public administration**. Under the original architecture of the European Union procurement directives and Article 346 of the Treaty on the Functioning of the European Union (TFEU), the protection of vital State interests operated as an **exceptional derogation from competition**, strictly triggered by concrete and imminent threats to territorial sovereignty or military defence. Yet the exponential proliferation of cyber threats and the pervasive nature of networked technologies have dismantled that rigid contractual dichotomy.

The transformation of **intangible critical infrastructures** has made it unmistakable that a vulnerability embedded in a software platform or an **ICT supply chain** can compromise institutional continuity no less severely than a conventional armed attack. That realization prompted the legislature to align the entire life cycle of public tendering procedures with stringent standards of **cyber resilience** and strategic data traceability. Leading public law scholarship has observed that security no longer functions solely as an external, countervailing limit on market competition, but rather as an intrinsic qualitative parameter of contractual performance designed to ensure that public markets operate without jeopardizing collective welfare[D1].

Viewed from this perspective, **technological sovereignty** ceases to be an abstract policy aspiration and becomes an operational criterion for selecting economic operators, shaping **tender admission requirements**, technical specifications, and performance conditions governing long-term supply relationships. This development interacts systematically with the result principle in public contracts, requiring that contract awards aim not merely at the formal acquisition of an asset, but at securing reliable digital services shielded against external interference. Unlike ordinary procurement for standardized supplies—where price competition retains primary weight—in technology-intensive public contracts systemic protection takes precedence over purely budgetary cost savings.

1.2 — Protection of Confidentiality and Essential State Security Interests Under the New Code

Within the statutory framework established by Legislative Decree no. 36 of 31 March 2023, the convergence between public procurement rules and strategic State interests finds institutional synthesis in **Article 136 of Legislative Decree no. 36/2023**. While establishing the general applicability of the Public Contracts Code to contracts in the defence and security sectors—without prejudice to the specific exemptions set out in Legislative Decree no. 208/2011—paragraph 2 lays down a foundational rule. Ordinary competitive procurement rules do not apply to public contracts and design contests *"where the protection of the essential security interests of the State cannot be guaranteed through less intrusive, suitable measures"*, including measures aimed at protecting the confidential nature of information made available by contracting authorities during the award procedure.

This codification enshrines a strict **principle of subsidiarity and proportionality**: a contracting authority may not automatically opt out of competitive tendering rules, but must first assess whether essential security interests can be safeguarded by adopting **proportionate protective measures**, such as enhanced non-disclosure agreements, security classification requirements, or targeted restrictions on access to tender documents. Only where such technical and legal safeguards prove insufficient to prevent unauthorized disclosure or systemic compromise does the **inapplicability of the Public Contracts Code** take effect, thereby legitimizing special regimes of direct or confidential procurement.

The scope of this provision coordinates closely with the rules governing defensive access to documents and technical trade secrets under the new Public Contracts Code, confirming that technical confidentiality and the security of the Republic prevail over ordinary disclosure claims brought by unsuccessful tenderers. In litigation, counsel representing an excluded bidder must contend with a strict demarcation of technical secrecy, raising crucial questions regarding the **burden of proof in court proceedings** as to whether less restrictive protective measures were reasonably available to the contracting authority prior to ordering exclusion.

02. THE NATIONAL CYBERSECURITY PERIMETER AND TECHNICAL VETTING BY THE CVCN

2.1 — The National Cybersecurity Perimeter and Covered Entities

Italy's digital security architecture rests primarily upon Law Decree no. 105 of 21 September 2019, converted with amendments into Law no. 133 of 18 November 2019. **Article 1 of Law Decree no. 105/2019** establishes the **National Cybersecurity Perimeter** in order to ensure a high level of security for networks, information systems, and IT services operated by public bodies and private entities *"upon which depends the exercise of an essential function of the State, or the provision of an essential service for maintaining civil, social, or economic activities fundamental to the interests of the State"*, where malfunction, interruption, or improper use could cause severe prejudice to national security.

Inclusion within the perimeter, governed at the implementing level by **Prime Ministerial Decree (D.P.C.M.) no. 131 of 30 July 2020**, encompasses central government ministries, local authorities, public utility operators, and major **private economic operators** across the strategic sectors of energy, transport, telecommunications, finance, and healthcare. Covered entities are under a statutory duty to map their **critical networks and information systems**, compiling detailed inventories of system architectures and technological components that must be updated at least annually and submitted to the **National Cybersecurity Agency** (ACN), as well as to comply with strict cyber-incident notification duties to CSIRT Italia within one hour or six hours depending on impact severity pursuant to **Prime Ministerial Decree no. 81 of 14 April 2021**.

Failure to fulfill mandatory reporting obligations or to implement prescribed security measures triggers exceptionally severe **pecuniary administrative sanctions** ranging from EUR 200,000 to EUR 1,800,000, underscoring the mandatory public-order nature of **digital public security**. Unlike ordinary administrative infringements in public tendering, perimeter sanctions do not require proof of willful misconduct (intent), resting instead upon objective non-compliance with statutory duties to map critical IT assets and notify incidents.

2.2 — The Role of the CVCN and the Impact of Technical Security Screenings on Tender Procedures

The operational core of this protective regime lies in the powers conferred upon the **National Evaluation and Certification Centre** (CVCN), housed within the ACN. Under the combined provisions of Article 1(6) of Law Decree no. 105/2019, **Presidential Decree no. 54 of 5 February 2021**, and the **Prime Ministerial Decree of 15 June 2021** (which identifies sensitive supply categories including core network routing equipment, firewalls, SCADA industrial control systems, and virtualization software), covered entities intending to award contracts for **ICT goods, systems, and services** destined for strategic networks must submit prior notification to the CVCN.

The CVCN operates within an **ordinary procedural time limit of 45 days**, extendable once by an additional 15 days for particularly complex hardware or source-code assessments, to conduct **technological security evaluations** or impose binding conditions and laboratory vulnerability tests to be completed within 60 days. The impact of this administrative screening module on public contracting is far-reaching: tender notices and supply agreements must mandatorily incorporate **express suspensive or resolutive conditions** making contractual effectiveness contingent upon compliance with CVCN prescriptions and successful completion of vulnerability testing, thereby establishing a statutory ground for **termination of the contract award**.

With respect to admission criteria and bid evaluation, administrative case law has clarified that contracting authorities must adhere strictly to the technical requirements set forth in the tender rules (*lex specialis*), refraining from arbitrary

conflations of distinct regulatory frameworks. Specifically, the Regional Administrative Court (*TAR*) for Campania sitting in Naples held that verifying the **technical compliance of bids** with IT reliability standards must be benchmarked exclusively against the criteria expressly specified in the call for tenders—such as holding **ISO/IEC 27001 certification**—ruling out challenges to technical scores premised on the omission of NIS2 Directive references in ordinary supply contracts unrelated to essential digital services[1]. Counsel for a competing bidder cannot therefore invoke uncodified cybersecurity standards in litigation when they were not incorporated into the tender documentation.

03. PUBLIC SECTOR CLOUD COMPUTING AND THE QUALIFICATION OF DATA AND SERVICES

3.1 — The Evolution of Cloud Qualification: From AgID Circulars to ACN Regulation No. 21007/2024

The rationalization of public administration software portfolios toward secure cloud computing paradigms has undergone a sweeping institutional overhaul. Moving beyond the pioneering soft-law regime of circulars issued by the Agency for Digital Italy (AgID), regulatory competence shifted to the National Cybersecurity Agency, culminating in the adoption of **ACN Directorial Decree no. 21007 of 27 June 2024**, which enacted the comprehensive **Regulation on Cloud Services and Technological Solutions for Public Administration**.

This regulatory framework establishes a **mandatory prior qualification regime** for any provider offering IaaS, PaaS, or SaaS solutions intended to process public sector data or support administrative functions. From a public procurement standpoint, administrative case law has laid down essential coordinates regarding the temporal and functional placement of this requirement within competitive tender procedures. As held by the Council of State (*Consiglio di Stato*), application software cloud qualification ordinarily operates as a **contract performance requirement** rather than a tender participation threshold, unless the call for tenders (*lex specialis*) expressly provides otherwise, given that the contracting authority retains full authority to verify formal ACN registry enrollment prior to executing the public contract[2].

Consequently, holding ACN qualification guarantees the **technical compliance of cloud infrastructure** with national security mandates while preventing disproportionate entry barriers at the outset of competitive bidding. Unlike general subjective integrity and public-policy requirements—whose absence entails immediate and irremediable exclusion—software qualification may be obtained and perfected during the course of the award procedure, provided that the tenderer demonstrates that formal assessment proceedings are already pending before the Agency.

3.2 — Data Taxonomy (Ordinary, Critical, Strategic) and Security Tiers (QC1–QC4 and AI1–AI4)

The current regulatory design calibrates the intensity of security scrutiny according to the substantive sensitivity of the information flows processed. **ACN Directorial Decree no. 21007/2024** classifies public sector data and digital services into three foundational categories: **ordinary data** (information whose compromise does not impair administrative continuity), **critical data** (significant institutional functions whose alteration harms socio-economic welfare or public health and safety), and **strategic data** (vital State assets whose compromise prejudices national security).

Corresponding to this tripartite taxonomy, ACN Regulation no. 21007/2024 establishes four progressive qualification tiers for commercial cloud services (**tiers QC1, QC2, QC3, and QC4**) alongside mirroring tiers of **digital infrastructure adequacy** for public sector on-premises or dedicated systems (**tiers AI1, AI2, AI3, and AI4**), as summarized in the table below:

Cloud Qualification	Infrastructure Adequacy	Data Classification	Required Security Safeguards
QC1	AI1	Ordinary Data	Baseline technical controls, ISO/IEC 27001 compliance, self-declaration of technical conformity.
QC2	AI2	Critical Data	Advanced encryption at rest and in transit, enhanced business continuity, periodic third-party security audits.
QC3	AI3	Strategic Data	Advanced logical isolation, jurisdiction and cryptographic key custody within the European Economic Area, immunity from extraterritorial reach.
QC4	AI4	Defence Strategic Data	Physical infrastructure isolation, sovereign hardware encryption, personnel holding national security clearance (NOS).

Regarding the technical compliance of cloud solutions tendered by bidders, the Council of State (*Consiglio di Stato*) has clarified that requiring **exclusive availability of the infrastructure** or primary data centre does not compel the tenderer to hold outright ownership title over the physical facility. Rather, it suffices for the economic operator to establish **full and exclusive functional control** over the computing facility through binding legal instruments—such as a capacity-borrowing agreement (*avvalimento*) or enforceable intra-group arrangements—capable of safeguarding operational continuity and public service reliability[3]. Should litigation arise, the burden of proving effective material availability of the servers rests squarely upon the bidder relying on an auxiliary undertaking.

3.3 — The National Strategic Hub (PSN) and Geographical Infrastructure Localization

At the apex of Italy's sovereign digital architecture stands the **National Strategic Hub** (*Polo Strategico Nazionale*, PSN), a high-reliability cloud infrastructure created through public-private partnership to host all strategic and critical datasets of central government administrations and regional health authorities. The PSN model directly addresses the imperative of shielding public information assets against **extraterritorial jurisdiction risks** stemming from foreign surveillance or data-access statutes, thereby achieving genuine **national technological autonomy**.

Foremost among its binding architectural constraints is the **geographical localization of data centres**, which must be sited exclusively on Italian territory with a **minimum geographical separation of 500 kilometres** between primary computing regions and disaster-recovery sites. That physical redundancy guarantees systemic resilience even in the face of large-scale natural disasters or armed conflict, preserving the continuity of essential State functions and the integrity of archived records.

Both the procedural complexity and the substantial economic value of such strategic concessions have generated major procurement litigation. Ruling on the project-financing award procedure for establishing and operating the National Strategic Hub, the Council of State (*Consiglio di Stato*) reaffirmed the **strict immutability of tender rules**, holding that pre-bid clarifications issued by the contracting authority may never introduce quantitative caps or novel obligations absent from the original tender specifications (*lex specialis*), so as to protect **equal treatment among tenderers** (*par condicio*) and administrative transparency[4]. The principle of administrative self-restraint bars public buyers from altering technological rules of engagement once bids have been submitted.

04. SPECIAL EXECUTIVE POWERS (GOLDEN POWER) AND STRATEGIC ICT CONTRACTS

4.1 — The Legislative Purpose of Law Decree No. 21/2012 Applied to ICT Public Contracts and Concessions

The friction between authoritative public-law prerogatives and competitive procurement markets reaches peak intensity with the application of Italy's foreign investment and supply screening regime, commonly known as **golden power**. Originally enacted by Law Decree no. 21 of 15 March 2012 to safeguard corporate ownership structures in the defence and energy sectors, special executive powers have been progressively expanded to encompass technological procurement contracts. Legal scholars have pointed out that national security has ceased to operate purely as an external defensive shield and has evolved into an affirmative **contract-award and contractual-shaping criterion** across cyber-intensive public procurements[D2].

Subsequent statutory reforms inserted Article 1-bis into Law Decree no. 21/2012, expressly providing that *"broadband electronic communications services based on 5G technology constitute activities of strategic relevance to the national defence and security system"*, while extending identical screening safeguards to cloud computing infrastructures and systems deploying artificial intelligence in public administration within critical environments. This expansion reshapes public procurement boundaries by compelling notifying undertakings to submit annual network rollout plans and ICT supply contracts to prior governmental clearance.

Appellate administrative courts have scrutinized how such geopolitical and industrial constraints interact with award procedures for telecommunications networks and services. In a landmark decision, the Council of State (*Consiglio di Stato*) held that tender award criteria rewarding the localization of telecommunications hardware manufacturing and research-and-development centres within the European Economic Area pursue a legitimate objective of **protecting economic public policy** and security of supply, mitigating competitive distortions associated with non-market economies[5].

4.2 — Article 1-bis: 5G Networks, Cloud Computing, and Critical Non-EU Components

Under the operational mechanism set out in Article 1-bis(2), every entity intending to procure goods or services instrumental to designing, building, or operating 5G networks and cloud infrastructures must notify an **annual ICT procurement plan** to the Presidency of the Council of Ministers. Executive screening unfolds within an **ordinary review period of 30 days**, extendable up to a total of 40 days (20 + 20 days) where in-depth technical evaluations by the CVCN and ACN are required to test for **technological vulnerability factors** linked to non-EU vendors subject to direction or influence by authoritarian foreign governments.

Building directly upon this trajectory, **Article 14 of Law no. 90 of 28 June 2024** and its implementing **Prime Ministerial Decree of 30 April 2025** establish a dual-track procurement architecture combining objective technical

cybersecurity baselines (Annexes 1 and 2, including mandatory Software Bill of Materials disclosure) with geoeconomic selectivity (Annex 3 applicable to perimeter entities). Primary legislation stipulates that, in public procurement procedures for ICT goods and services deployed in strategic contexts, contracting authorities *"shall set a maximum cap on the price score not exceeding 10 per cent"*, assigning decisive weight to **cybersecurity quality** alongside bonus award points for technologies originating in European Union Member States, NATO allies, or designated partner countries.

> Article 14 of Law no. 90/2024 curtails the price-weighting discretion of contracting authorities in critical procurements, subordinating short-term cost savings to technological sovereignty and the cyber resilience of domestic and allied industrial supply chains.

Both first-instance and appellate administrative courts have upheld the strict alignment of these precautionary rules with overriding State interests. On the one hand, the Regional Administrative Court (*TAR*) for Campania held that revoking and re-tendering a public contract for infrastructural security equipment on account of supervening technical regulatory standards is entirely lawful, ruling that the mere opening of financial bids does not vest participants with a legally protected legitimate expectation prior to final contract award[6]. On the other hand, the Council of State (*Consiglio di Stato*) confirmed that contracting authorities enjoy discretionary power to issue reasoned exclusions against economic operators and capacity-lending auxiliaries established in third countries that are not signatories to the WTO Agreement on Government Procurement (GPA), since market access is not guaranteed absent reciprocal treaty obligations—provided, however, that exclusion does not rest on retroactive additions foreign to the tender notice[7].

4.3 — Private Law and Administrative Consequences: Unenforceability of Clauses and Contract Termination

Breaching prescriptions imposed under the *golden power* regime or performing supply contracts in defiance of governmental vetoes triggers radical **public-policy invalidity remedies**. Article 1-bis(5) expressly sanctions contracts concluded in violation of executive conditions or prohibitions with **textual nullity (voidness *ab initio*)**, empowering the Government to order the non-compliant undertaking to restore the prior factual situation at its own expense and to levy **pecuniary administrative fines of up to 3 per cent of global turnover**.

Within the framework of **national security in public procurement**, an intervening governmental prohibition or binding technical condition incompatible with the technical solution tendered by the successful bidder brings about **termination of the contract for supervening impossibility** or obliges the contracting authority to exercise statutory powers of administrative withdrawal or revocation. Drawing an important judicial distinction from ordinary discretionary exclusion grounds, however, the Council of State (*Consiglio di Stato*) has emphasized that invoking geopolitical risks or shareholding links with foreign states cannot degenerate into abstract conjecture: excluding an economic operator for alleged foreign intelligence or informational interference must rest upon **rigorous legal assessment and concrete evidentiary findings**, as such concerns do not automatically amount to grave professional misconduct absent a specific, reasoned determination by the contracting authority[8].

A delicate constitutional balance thus emerges between imperative demands of **safeguarding the security of the Republic** and adherence to general principles of administrative law, requiring detailed, verifiable technical reasoning at every procedural stage so as to preserve the procedural defence rights of competing undertakings before the courts.

05. ADMINISTRATIVE LITIGATION: SCOPE OF JUDICIAL REVIEW AND REMEDIES

5.1 — The Scope of Judicial Review by Administrative Courts Between Technical and Political Discretion

Judicial protection against administrative measures barring participation in public tenders or interfering with contractual performance on grounds of **national security in public procurement** reflects the structural constraints governing **judicial review of legality over high-discretion acts**. Administrative courts are tasked with policing the delicate boundary between statutory compliance and non-justiciable political merit. When reviewing exclusions grounded in vital State security interests or technical cyber vetoes, the reviewing court exercises an **extrinsic standard of reasonableness review**, verifying that the authoritative determination is untainted by manifest misrepresentation of material facts, patent illogicality, or defective preliminary fact-finding.

Along these lines, the Council of State (*Consiglio di Stato*) has established that where the tender specifications (*lex specialis*) classify designated security controls as mandatory requirements under penalty of exclusion, the contracting authority may not downgrade them into mere post-award performance undertakings; rather, it must verify **technical bid conformity** right from the admission stage of the competitive procedure, while the selection board's **technical-discretionary assessment** remains immune from judicial substitution absent macroscopic inconsistencies[9].

Similarly, first-instance administrative case law has upheld the broad preventive reach of special State screening powers, ruling that executive conditions aimed at preserving business continuity and safeguarding **strategic technological assets** may lawfully be imposed even upon complex corporate and financial transactions, without allowing the affected undertaking to claim a disproportionate infringement of freedom to conduct a business whenever the measure serves to avert **systemic vulnerabilities in critical markets**[10]. Unlike merger control under competition law, State screening intervention does not seek to restore market rivalry, but rather to preempt external threats to national economic security.

5.2 — Evidentiary and Duty-to-Give-Reasons Burdens Resting on Contracting Authorities and the Government

Even though executive and technical discretion in this sphere is exceptionally broad, safeguarding economic operators demands strict compliance with **duties to state reasons and procedural transparency**. As authoritative legal scholarship has underscored, generic invocations of national security cannot serve as an absolute shield for arbitrary or disguised protectionist decisions: both contracting authorities and governmental screening bodies must articulate with precision the **technical, economic, and legal grounds** justifying any restriction upon competitive market access[D3].

At the governmental level, the Council of State (*Consiglio di Stato*) has highlighted the two-stage structure of *golden power* proceedings, distinguishing the preparatory technical investigation conducted by the inter-ministerial coordination group from the subsequent **collegiate political evaluation** vested in the Council of Ministers. As the supreme executive body, the Cabinet is entitled to weigh the strategic repercussions of a transaction in light of Italy's international posture, and departing from preparatory ministerial proposals does not in itself constitute **misuse or excess of power** (*eccesso di potere*), provided that the record reflects a thorough investigation into the strategic nature of the assets involved[11].

Where administrative proceedings rely upon classified records or **confidential intelligence reports**, administrative jurisprudence has struck a careful procedural balance: while the statement of reasons in the final measure may lawfully incorporate classified assessments by reference (*per relationem*), constitutional due process guarantees require that **classified documentation be disclosed in court** to the judicial panel and to counsel of record under appropriate confidentiality safeguards, thereby preserving effective judicial protection and the **principle of equality of arms**[12]. The

burden of proof rests upon the public authority, which cannot evade judicial scrutiny merely by asserting abstract security concerns.

5.3 — What Effective Legal Remedies Remain Available to an Economic Operator Excluded on National Security Grounds?

An economic operator excluded on national security grounds may bring an action for annulment before the Regional Administrative Court to challenge defects of excess of power, factual misrepresentation, or inadequate investigation, while seeking defensive access to redacted or restricted technical files; however, judicial annulment ordinarily entails only a remand requiring the public authority to re-exercise its discretionary power, precluding automatic damages awards.

The array of procedural remedies available to a tenderer or ICT supplier affected by exclusionary determinations or governmental vetoes is systematically compared in the table below:

Judicial Remedy	Prerequisites and Scope of the Claim	Legal Reach and Effects of Judgment
Judicial Annulment	Challenge under Article 120 of the Code of Administrative Procedure for factual error, defective investigation, or insufficient reasoning.	Quashing of the contested measure without prejudice to fresh evaluation and reasoned re-exercise of administrative power.
Defensive Access to Records	Motion for disclosure of technical inspection reports and opinions issued by the CVCN or inter-ministerial coordination group.	In-camera or redacted inspection, or restricted disclosure solely to appointed legal counsel and cleared technical experts.
Contractual Substitution (*Subentro*)	Application under Article 124 of the Code of Administrative Procedure contingent upon proving full technical compliance of the claimant's bid.	Ordinarily barred or strictly subordinated to compatibility with national security safeguards and potential re-tendering.
Compensatory Damages	Proof of gross negligence or inexcusable error by the authority and certainty of substantive entitlement to the contract award.	Generally excluded given the wide margin of technical and political appreciation vested in public security authorities.

With respect to governmental opposition against cross-border technology transactions, the Council of State (*Consiglio di Stato*) has clarified that the strategic and potentially dual-use nature of technological assets must be assessed under an **objective, substantive criterion** detached from formalistic labels advanced by private parties; where manufacturing operations are slated to relocate under the jurisdiction of a non-allied third country—rendering ongoing monitoring of behavioral mitigation conditions practically impossible—exercising an **outright executive veto** is wholly lawful, barring any claim for statutory indemnification or tortious damages by the operator[13].

Finally, where the Government imposes disproportionate conditions or restrictions unsupported by an adequate technical record, the Regional Administrative Court (*TAR*) for Lazio sitting in Rome has held that partial judicial annulment strikes down the Prime Ministerial Decree solely insofar as the contested prescriptions lack factual substantiation, while leaving the Presidency of the Council of Ministers **free to re-exercise its special screening power** upon properly weighing the evidentiary record[14]. This jurisprudence confirms the decisive role of specialized litigation strategies focused on testing the methodological rigor of technical investigations without inviting courts to usurp executive assessments of national interest.

06. CONCLUSIONS: TOWARD AN INTEGRATED PUBLIC PROCUREMENT MODEL ORIENTED TOWARD DIGITAL SOVEREIGNTY

The systematic reconstruction conducted above demonstrates that **national security in public procurement** has outgrown its historical confines as an episodic derogation to become a **structural governing principle** of digital and IT public contracting. The coordinated interplay among the Public Contracts Code, the national cybersecurity perimeter, ACN cloud qualification tiers, and special executive *golden power* screening marks a decisive shift toward an advanced model of **republican technological sovereignty**.

Within this transformed legal order, the contractual autonomy of contracting authorities is shaped by binding **technical compliance obligations** and sovereign interoperability mandates, while economic operators are required to ensure end-to-end **ICT supply-chain traceability** and corporate ownership transparency. Enforcing non-derogable safeguards over public data flows and rewarding secure geographical localization of computing infrastructures serve as indispensable bulwarks against **systemic compromise risks** and hostile foreign interference.

At the same time, the broad margin of appreciation conferred upon public security authorities requires strict adherence to **administrative proportionality** and rigorous fulfillment of the duty to state reasons. Administrative litigation confirms that reconciling vital State security imperatives with market openness ultimately hinges upon effective **extrinsic judicial review of legality**, ensuring that technical discretion never degenerates into arbitrary exclusion while affording legal practitioners structured, predictable avenues of judicial redress calibrated to the substantive interests at stake.

References & Authorities Cited

Statutory Provisions

Legislative Decree no. 36 of 31 March 2023 — Italian Public Contracts Code, specifically Article 136 governing the protection of essential State security interests and exclusion from the scope of ordinary procurement rules.

Law Decree no. 105 of 21 September 2019 — Converted with amendments by Law no. 133 of 18 November 2019, establishing the National Cybersecurity Perimeter and mandatory prior notification duties to the CVCN.

- Law Decree no. 21 of 15 March 2012 — Converted with amendments by Law no. 56 of 11 May 2012, governing special executive screening powers (*golden power*), with particular reference to Article 1-bis on 5G broadband networks and cloud computing.

- Law no. 90 of 28 June 2024 — Provisions strengthening national cybersecurity and combating cybercrime, introducing under Article 14 a mandatory 10% cap on price-score weighting in strategic ICT procurement.

- National Cybersecurity Agency (ACN) Directorial Decree no. 21007 of 27 June 2024 — Regulation on Cloud Services for Public Administration (cloud service qualification tiers QC1–QC4 and digital infrastructure adequacy tiers AI1–AI4).

- Prime Ministerial Decree (D.P.C.M.) no. 131 of 30 July 2020 — Implementing regulation establishing criteria and procedures for identifying public and private entities included within the National Cybersecurity Perimeter.

- Presidential Decree no. 54 of 5 February 2021 — Implementing regulation governing ICT procurement notification procedures and technical security assessments carried out by the CVCN.

- Prime Ministerial Decree (D.P.C.M.) no. 81 of 14 April 2021 — Regulation governing mandatory cyber-incident reporting to CSIRT Italia and baseline security measures within the perimeter.

- Prime Ministerial Decree (D.P.C.M.) of 15 June 2021 — Identification of sensitive categories of ICT goods, systems, and services intended for deployment within the National Cybersecurity Perimeter.

- Prime Ministerial Decree (D.P.C.M.) of 30 April 2025 — Definition of essential cybersecurity elements and geoeconomic bonus award criteria for public contracts concerning IT goods and services deployed in strategic contexts (implementing Article 14 of Law no. 90/2024).

Case Law Cited

1. **Regional Administrative Court (TAR) Campania, Naples, Judgment of 21 October 2025, no. 6866** — Bonus technical scores for IT security must adhere strictly to the criteria expressly specified in the tender rules (ISO/IEC 27001 certification), without improperly extending NIS2 Directive obligations where not incorporated into the call for tenders. Outcome: main application dismissed; supplemental grounds declared partly inadmissible and partly dismissed; cross-application declared moot. Para.: technical evaluation grounds.

2. **Council of State, Judgment of 7 October 2024, no. 8046** — Cloud qualification of application software for public administration ordinarily operates as a contract performance requirement rather than a tender participation threshold, absent an express contrary stipulation in the tender notice. Outcome: main appeal dismissed; cross-appeal declared moot. Para.: cloud qualification requirements.

3. **Council of State, Judgment of 2 July 2024, no. 5871** — The requirement of exclusive availability of the primary data centre does not demand full ownership title, as full and exclusive functional and operational control over the computing facility via capacity-borrowing (*avvalimento*) or binding intra-group agreements suffices. Outcome: main appeal dismissed and cross-appeal declared moot, upholding first-instance judgment. Para.: data-centre availability.

4. **Council of State, Judgment of 24 October 2023, no. 9210** — In the award procedure for the National Strategic Hub (PSN), clarifications issued by the contracting authority may neither amend nor supplement the tender specifications by introducing novel caps or obligations upon tenderers. Outcome: independent appeal partly dismissed and partly declared moot; cross-appeal upheld in part; main appeal dismissed; case file referred to the Court of Auditors. Para.: scope of contracting-authority clarifications.

5. **Council of State, Judgment of 18 December 2023, no. 10889** — Bonus award criteria tied to European or treaty-partner localization of telecommunications hardware production and research-and-development centres lawfully safeguard economic public policy and supply security. Outcome: main appeal dismissed, upholding contested judgment. Para.: geographical localization award criteria.

6. **Regional Administrative Court (TAR) Campania, Naples, Judgment of 16 June 2026, no. 3822** — Revocation and subsequent re-tendering of a procurement procedure for security equipment prompted by supervening sector-specific technical standards is lawful, as no protected legitimate expectation vests prior to final contract award. Outcome: main application and supplemental grounds dismissed; cross-applications declared moot. Para.: revocation on grounds of supervening security standards.

7. **Council of State, Judgment no. 3721/2025** — Market access to public procurement for economic operators and capacity-lending auxiliaries established in third countries not party to international procurement agreements is not guaranteed and contracting authorities may issue reasoned exclusions, provided such exclusions do not rely on automatic bars or retroactive additions absent from the tender notice. Outcome: appeal upheld, reversing contested judgment and upholding first-instance application within the terms stated in the reasoning. Para.: third-country operators and reciprocity.

8. **Council of State, Judgment of 7 November 2025, no. 8661** — Allegations concerning national security risks and foreign informational interference must rest upon rigorous evidentiary findings and do not automatically constitute grave professional misconduct absent a specific discretionary assessment by the contracting authority. Outcome: appeal dismissed on the grounds set out in the reasoning, upholding contested judgment. Para.: evidentiary threshold for geopolitical exclusion.

9. **Council of State, Judgment of 31 July 2026, no. 6153** — Technical conformity and security controls designated as mandatory by the tender specifications constitute participation requirements and cannot be downgraded to post-award performance conditions so as to cure a non-compliant bid. Outcome: appeal upheld; contract award annulled; executed contract declared ineffective with substitution (*subentro*) of appellant ordered and file referred to the Public Prosecutor's Office. Para.: mandatory technical security requirements.

10. **Regional Administrative Court (TAR) Lazio, Rome, Judgment of 22 May 2024, no. 10275** — The preventive rationale of *golden power* screening legitimizes executive conditions designed to safeguard investment continuity and strategic technological assets even within complex corporate and financial transactions. Outcome: application dismissed, upholding contested governmental decree. Para.: preventive scope of special executive powers.

11. **Council of State, Judgment of 9 January 2023, no. 289** — Executive decisions exercising special screening powers involve broad strategic political discretion that is not open to judicial substitution where supported by a thorough investigation into asset criticality. Outcome: main appeal dismissed, upholding first-instance judgment. Para.: two-stage structure and standard of review.

12. **Council of State, Judgment of 19 November 2019, no. 7904** — In administrative proceedings grounded upon confidential or classified intelligence reports protecting the security of the Republic, reasoning by reference (*per relationem*) is lawful provided that restricted in-court documentary disclosure is guaranteed to preserve defence rights. Outcome: main appeal dismissed, upholding first-instance judgment. Para.: classified records and judicial due process.

13. **Council of State, Judgment no. 2180/2026** — Exercising an outright governmental veto over outbound technological investments rests upon substantive assessments of military and dual-use asset fungibility, precluding damages claims and automatic private entitlements. Outcome: main appeal dismissed, upholding contested judgment. Para.: dual-use technology veto and exclusion of damages.

14. **Regional Administrative Court (TAR) Lazio, Rome, Judgment no. 13748/2025** — Imposing *golden power* prescriptions requires an adequate and coherent technical evidentiary basis, leaving the executive authority free to re-examine the transaction following partial judicial annulment. Outcome: introductory application upheld in part, partially annulling governmental decree without prejudice to fresh exercise of screening power; supplemental grounds declared inadmissible. Para.: proportionality and adequacy of technical investigation.

Legal Scholarship Cited

D1. **Antonio Cassatella**, *Sicurezza e mercato: difficili equilibri* [Security and the Market: Difficult Balances], in *Urbanistica e appalti*, 2026, no. 5, pp. 565–589 — Reconstructs the transition of national security from an external, exceptional derogation into an intrinsic parameter of technical qualification and systemic resilience in public procurement.

D2. **Manfredi Matassa**, *Cibersicurezza, intelligenza artificiale e contratti pubblici. La sicurezza nazionale come parametro di aggiudicazione* [Cybersecurity, Artificial Intelligence, and Public Contracts: National Security as an Award Criterion], in *Urbanistica e appalti*, 2026, no. 5, pp. 601–615 — Examines the deployment of cybersecurity standards and artificial intelligence governance as qualitative bonus award criteria and minimum participation requirements in public tenders.

D3. **Lorenzo Marilotti**, *L'incidenza dei poteri di sicurezza nazionale sui contratti pubblici* [The Impact of National Security Powers on Public Contracts], in *Urbanistica e appalti*, 2026, no. 5, pp. 590–600 — Analyzes the operational reach of special executive screening powers over ICT public contracts and the heightened duty to state reasons incumbent upon public authorities when balancing security imperatives against competition.

FP

Federico Palumbo

AUTHOR • METODO GIURIDICO

Attorney at the Rome Bar

Practises civil law, administrative law, and labour law. For Metodo Giuridico he authors in-depth analyses and case notes on the substantive and procedural aspects of civil and administrative litigation.