Cybersecurity and the digitalisation of public administration: transforming the concept of administrative legality

Alessandra Lizzio[1,2]

[1]Scuola IMT Alti Studi Lucca, Piazza S. Ponziano 6, 55100 Lucca, LU, Italy
[2]Università di Catania, Piazza Università 2, 95124 Catania, CT, Italy

Abstract

This article examines cybersecurity as a new structural criterion of legitimacy for administrative action in the digital society. Cybersecurity can no longer be conceived as a purely technical requirement; instead, it has evolved into a principle-value that reshapes how public authorities identify, balance and protect public and private interests. Institutional trust, service continuity and the effectiveness of digital rights increasingly depend on the resilience of the digital infrastructures underpinning public activity. Consequently, administrative meritworthiness is defined not only by procedural conformity or cost-efficiency, but by the capacity to prevent systemic vulnerabilities and to safeguard integrity, transparency and data protection. Cybersecurity thus emerges as a decisive parameter of administrative performance and a meta-value guiding the balance between competition, cost-effectiveness and national security, signalling a profound transformation of the public interest within the contemporary digital ecosystem.

Keywords

Cybersecurity, Administrative Law, Digital Administration, Digital Meritworthiness, Public Interest, Data Protection, Institutional Trust, National Security, Digital Transformation,

1. Cybersecurity as an axiological and functional foundation of digital meritworthiness

Cybersecurity has assumed a structural role in determining the meritworthiness of administrative action in the context of the State's digital transformation. The digital environment in which public administrations operate has ceased to be a mere technical support; it now constitutes a legal and operational space that shapes the form, content and responsibilities of administrative activity [1].

In contemporary hyper-connected societies, digital processes underpin essential economic, social and institutional functions. The European Union Agency for Cybersecurity (ENISA) has characterised cybersecurity as the cornerstone of digital transformation, emphasising its transversal relevance across all policy domains. This perspective highlights the pivotal role of cybersecurity in enabling trustworthy digital ecosystems and sustaining confidence in digitally mediated interactions. Within this framework, digital meritworthiness may be understood as the deserved trust and credibility attributed to digital services, organisations and public authorities operating in the digital sphere. Cybersecurity constitutes both an axiological and a functional foundation of such meritworthiness. From a values-based perspective, it embodies core principles such as security, privacy protection, accountability and respect for the rule of law. From a functional standpoint, it ensures the resilience, reliability and continuity of digital infrastructures, which are indispensable to the effective delivery of public and private services. The relationship between cybersecurity and digital meritworthiness is reinforced by a growing body of academic scholarship, institutional analyses and European regulatory instruments, including the NIS2 Directive, the EU Digital Decade policy framework and the Data Act. Together, these sources reflect an emerging consensus that trust in digital systems is not an inherent attribute, but rather the outcome of sustained compliance with security, reliability and ethical standards. In this sense, digital meritworthi-

Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT
alessandra.lizzio@imtlucca.it (A. Lizzio)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-04-23

CEUR-WS.org/Vol-4198/paper17.pdf

ness operates as the digital analogue of institutional credibility or performance-based legitimacy: digital actors "earn" trust through demonstrable adherence to robust cybersecurity requirements. Empirical findings further corroborate this link. Survey data on e-government usage indicate that concerns related to cyber disruptions, data breaches and fraud significantly undermine citizens' confidence in public digital platforms, with a substantial proportion of users expressing reluctance to engage in digital public services due to perceived cybersecurity risks [2].

Perceptions that vulnerabilities "undermine the perceived security and reliability of digital governance platforms" illustrate how cybersecurity failures directly erode an entity's digital merit. Conversely, robust cybersecurity practices, those that protect personal data, ensure system integrity, and demonstrate operational resilience, enhance trust and confer "merit" within the digital domain.

From this perspective, cybersecurity cannot be reduced to a mere technical or procedural requirement; it constitutes a decisive factor shaping users' willingness to engage with digital services and to rely on technologically mediated forms of governance. Digital meritworthiness thus emerges as a conditional attribute: only actors capable of delivering secure, reliable, and resilient digital services can legitimately claim full legitimacy in the digital domain.

This conceptualisation aligns closely with broader European Union policy objectives aimed at fostering a trustworthy digital transformation. Strategic frameworks, such as the Digital Decade 2030, emphasise that secure, reliable, and user-centred digital public services are essential prerequisites for strengthening institutional trust and for ensuring societal acceptance of digitalisation processes.

Within this framework, both the fundamental right to good administration under Article 41 of the Charter of Fundamental Rights of the European Union and the constitutional principle of sound administration in Article 97 of the Italian Constitution require public authorities to operate under adequate conditions of cybersecurity. Only a protected digital environment allows individuals to exercise their rights effectively and preserves institutional trust.

This insight is consistent with the Italian constitutional tradition, which has long interpreted Article 97 as requiring the pursuit of substantively worthy interests aligned with the dignity of the person [3]. Integrity, confidentiality and availability of data and information systems therefore function not as technical parameters, but as indicators of substantive legality and compliance with constitutional and supranational values.

Digital vulnerability compromises not only the continuity and efficiency of public services but also the democratic legitimacy of the administration, insofar as it undermines citizens' ability to exercise rights in conditions of transparency and security [4]. As noted in the literature, good administration is both a principle and a fundamental right, realised in the institutions' capacity to provide adequate conditions for the quality of life of individuals (ibid.). An administration exposed to cyber-risk cannot, by definition, be regarded as good or worthy. The new Italian Public Procurement Code (Legislative Decree 36/2023) reflects this structural shift. The full digitalisation of the procurement life cycle (Arts. 19–36) is conceived as a prerequisite for the legitimacy of administrative action, as it enhances transparency, traceability, data protection and cybersecurity (Art. 19(5)). In particular, Article 108(4) stipulates that, for ICT procurements relating to strategic sectors, the economic component may not exceed 10 % of the total score, thus prioritising qualitative criteria such as reliability, resilience and security. Cybersecurity becomes a structural condition for the "principle of the result", which operationalises the constitutional requirement of sound administration (Art. 1), and a decisive element in the evaluation of bids.

This framework is further strengthened by Law 90/2024, which transposes Directive (EU) 2022/2555 (NIS2) and introduces "essential cybersecurity elements" as techno-legal standards in strategic ICT procurement (Art. 14). The implementing decree will define requirements for security-by-design, supply chain reliability, data protection and operational continuity, thus establishing a criterion of technological merit that transcends traditional quality/price considerations and directs administrative judgment toward the systemic resilience of public digital infrastructure.

This perspective aligns with the view that good administration must ensure inclusion, equity and safe conditions for democratic participation [5]. Cybersecurity therefore assumes a dual significance:

1. Functionally, it constitutes the minimum condition for sustaining digitalised administrative action,

directly influencing the capacity of public authorities to achieve stable and reliable results;
2. Axiologically, it reflects the renewed centrality of systemic public interests (technological sovereignty, protection of digital rights, institutional trust) that guide the assessment of meritworthiness in the algorithmic society.

Accordingly, digital meritworthiness can no longer be evaluated solely in terms of procedural correctness or cost containment. It must instead be assessed through the administration's capacity to prevent systemic vulnerabilities, safeguard shared digital assets and ensure a secure, transparent and inclusive environment. Under the evolving interpretation introduced by Legislative Decree 36/2023, the "principle of the result" requires that the public interest pursued be substantively reliable, durable and protected. Cybersecurity thus emerges as a meta-criterion for evaluating public action, capable of qualifying (or disqualifying) the substantive legitimacy of administrative decisions and processes within the digital ecosystem.

2. The new Public Procurement Code as principle-Based legislation and the "result" through the lens of cybersecurity

Beyond its axiological significance, cybersecurity plays a decisive functional role by ensuring the reliable operation of digital infrastructure and services. From a practical standpoint, it constitutes an indispensable component of the technical backbone that supports economic, social, and administrative activity. Secure networks, resilient systems, and protected data are prerequisites for the functioning of e-commerce, healthcare, energy, transportation, e-government, and other essential digital services. Cyberattacks, system outages, or vulnerabilities can generate widespread disruptions, as exemplified by incidents that paralyze critical services. Investments in cybersecurity thus safeguard not only informational assets but also the operational continuity and societal functionality they underpin.

This operational importance is increasingly reflected in European Union legislation and policy. The Directive (EU) 2022/2555 on measures for high common level of cybersecurity across the Union (NIS2 Directive) establishes a harmonised framework mandating a high level of risk management across a broad spectrum of critical sectors. Member States are required to implement comprehensive cybersecurity strategies that explicitly encompass supply chain security, vulnerability management, and cybersecurity education [6]. Compared to its predecessor, the Directive significantly broadens the scope of obligations, extending them to additional domains, including public administrations, digital service providers, and space systems, thereby reinforcing systemic resilience and operational reliability.

In practical terms, this implies that numerous organizations, particularly medium-to-large entities operating in critical sectors, must adopt concrete technical and organizational measures, including:

- continuous monitoring and alerting systems for access activities and anomalies;
- periodic penetration testing and security assessments to identify vulnerabilities;
- incident response plans with clearly defined roles, responsibilities, and escalation hierarchies;
- encryption of data both in transit and at rest;
- strong authentication mechanisms and privileged access management for all platform users;
- periodic audits and certifications of ICT suppliers, ensuring compliance with international standards (e.g., ISO/IEC 27001, NIST);
- inclusion, within tender specifications, of security, interoperability, and continuous update requirements throughout the entire contractual duration;
- mandatory and ongoing training for staff and senior management on risk management, cybersecurity, and digital resilience;
- establishment of monitoring dashboards and reporting systems for management and supervisory bodies.

Complementary sector-specific regulations reinforce the functional centrality of cybersecurity. The EU Digital Operational Resilience Act (DORA) mandates robust ICT risk management and rigorous

testing for financial institutions, while the proposed EU Cloud Computing Resilience Act aims to impose resilience standards on cloud service providers. These regulatory frameworks are underpinned by the recognition that cyber resilience constitutes critical infrastructure: in its absence, neither markets nor public services can function reliably.

These operational requirements for digital services are mirrored and reinforced by institutional assessments. ENISA's strategic documentation stresses that cybersecurity considerations must permeate all policy domains and underscores the necessity of coherent, cross-sectoral implementation to ensure systemic resilience and continuity of essential digital infrastructures [7].

Its annual evaluations of the cybersecurity landscape, including the NIS Investments and NIS360 reports, consistently highlight the need for organisations to progressively enhance their cyber investments in order to comply with evolving regulatory and operational requirements. At the national level, Italy's 2022–2026 Cybersecurity Strategy, as articulated by the National Cybersecurity Agency (ACN), together with AgID guidelines, emphasises the adoption of secure cloud infrastructures, advanced encryption, CERT services, and other essential measures for public entities. Notably, the Italian Cloud Strategy for the Public Administration prioritises the migration of government data to certified cloud services that satisfy stringent security, reliability, and sovereignty criteria. The strategy underscores that, as of 2019, the majority of legacy data centres lacked adequate protection, thereby exposing public services to significant vulnerabilities [8].

Against this backdrop, Legislative Decree 36/2023 exemplifies principle-based legislation, in which the "principle of the result" serves as the organizing pillar of the entire regulatory framework. By mandating that all provisions be interpreted in light of the general principles enshrined in Articles 1, 2, and 3, the decree elevates the interpretive primacy of result, trust, and market access. This approach reflects the legislature's intent to place the realization of the public interest, now structurally dependent on the security and resilience of the digital ecosystem, at the core of public contracting decisions [9, 10].

The axiological architecture of the Code has remained unchanged even after the 2024 corrective reform, confirming the solidity of the legislative choice. The integrative amendments did not modify the discipline of principles, which retains its original formulation.

This stability aligns with the most recent constitutional case-law, which has recognised the consistency of these general principles with constitutional values and with the division of legislative competences, emphasising their coordinating function between administrative needs and the protection of digital public interests (Italian Constitutional Court, Judgments No. 77/2025 and 80/2025).

In the field of digitalised public procurement, principle-based legislation proves particularly well-suited to governing the uncertainty generated by rapid technological change. Although broad principles such as "result" or "trust" may initially raise concerns of indeterminacy, they operate as flexible guides capable of adapting the legal framework to situations unforeseen by the legislator. They thus help fill regulatory gaps in highly innovative sectors such as ICT and cybersecurity [9, 11, 12].

In an increasingly digitalized procurement environment, pursuing the principle of result means pursuing secure and resilient outcomes, through:

- contracts capable of ensuring the continuity of essential services and the protection of data;
- reliability of ICT suppliers, including the verification of certifications and periodic audits;
- hybrid or multi-cloud architectures to ensure resilience and redundancy;
- proactive risk monitoring and reporting;
- staff training and the establishment of coordination roles between procurement, IT, and oversight functions.

A contract performed punctually but built on vulnerable technological solutions cannot be said to satisfy the substantive result, as it exposes the administration and citizens to systemic risks, thereby undermining the very public interest the contract is intended to serve.

On this point, scholarship has observed that the new Code marks a shift from a traditionally pro-competitive paradigm to a neo-finalistic (sometimes described as "neo-accountability-based" paradigm) oriented toward the production of tangible and measurable outcomes, including in terms of digital

security. This evolution appears further influenced by the requirements of the National Recovery and Resilience Plan (PNRR), which demands secure, interoperable and resilient digital infrastructures. It is not surprising, therefore, that the principle of the result has generated intense academic debate: on one side, it is welcomed as a driver of effective and technologically reliable administration; on the other, some authors fear that it may lead to excessive discretion, particularly in highly innovative sectors [13].

Such concerns, however, appear mitigated when one considers the constitutional foundation of the principle. Article 1(3) of Legislative Decree 36/2023 expressly states that the principle of the result implements the constitutional requirement of sound administration, as well as the related principles of efficiency, effectiveness and economy. It is thus a sector-specific articulation of the general duty of good administration rooted in Article 97 of the Italian Constitution. Rather than signalling a shift towards private-sector logic, it reinforces the public-law function of the result as the effective satisfaction of collective interests [9, 13].

Within the digital paradigm, pursuing the result means pursuing secure results – procurements capable of ensuring the resilience of information infrastructures, data protection, platform integrity, continuity of essential services, ICT supplier reliability, and the prevention of cyber risk.

In other words, administrative result in the digital society coincides with the cyber-result: an administration that produces vulnerable results does not satisfy the principle, whereas an administration that achieves reliable, resilient and protected results fully realises the constitutional mandate of sound administration.

3. Towards a new grammar of administrative legitimacy

The innovative scope of the principle of the result becomes particularly evident when contrasted with the traditional principle of legality, which for decades constituted the exclusive foundation of administrative action. The well-established distinction in scholarship between formal legality (understood as conformity with the normative framework) and substantive legality (understood as conformity with public purposes and constitutional values) makes it possible to situate the result not as an alternative to legality but as an intra legem criterion aimed at ensuring the effectiveness of the public function [10].

Article 1 of the Code specifies that the pursuit of the result must take place "in compliance with the principles of legality, transparency and competition," thereby excluding arbitrary interpretations or forms of de-responsibilisation. The result thus operates as a dynamic criterion orienting administrative action without altering the guarantees enshrined in formal legality [13]. Legality and result are not in tension: the former defines the boundaries of the system; the latter ensures that administrative activity does not devolve into purely formal compliance but instead produces concrete, measurable and necessarily secure outcomes in the digital environment.

In a digitalised administration, substantive legality translates into cybersecurity, digital transparency and procedural reliability, as well as into the capacity of contracting authorities to prevent vulnerabilities and systemic risks. As a consequence, the procedural rules of the Code must be interpreted in an "intelligent," non-formalistic manner, so that they function as instruments of efficiency and as safeguards for the digital ecosystem. Transparency becomes a tool for civic oversight and procedural acceleration; competition becomes genuine openness to the most reliable technological solutions, free from artificial constraints; the digitalisation of the procurement life cycle becomes a guarantee of traceability, security and accountability.

The structure of the Code, such as the simplified negotiated procedures (Art. 50 of Legislative Decree 36/2023), the award incentives linked to innovation, quality and sustainability (Art. 108(7)), and the digitalisation requirements set out in Articles 19–36, illustrates how legality and result are called to operate in a mutually constitutive manner. Legality defines the limits; the result directs choices towards the solution that is technically, economically and digitally most suitable [10]. This vision is confirmed by recent scholarship, which highlights the integrative role of the principle of the result in relation to the other principles of the Code (trust, good faith, protection of legitimate expectations) within the broader framework of an increasingly "enabling" administration, capable of functioning in complex

and technologically advanced environments [14]. In this context, cybersecurity is not an ancillary element but an essential component of substantive legality: a procedure may be formally impeccable yet substantively illegitimate if it exposes public information systems to cyber risk or compromises personal data protection.

Accordingly, under the new Code, administrative legality becomes intrinsically cyber-dependent:

- The legitimacy of a procurement depends not only on procedural compliance, but also on the security of the digital infrastructures supporting its execution;
- The assessment of the public interest cannot be detached from considerations of cyber-resilience;
- Technical discretion is oriented towards choices that minimise cyber risk and maximise operational continuity.

The grammar of administrative legitimacy is thus being rewritten: there is no longer legality without result, nor result without cybersecurity. The protection of digital infrastructure becomes a constitutive element of substantive legality, while the principle of the result ensures that such protection is pursued effectively, measurably and in accordance with constitutional values.

4. Cybersecurity and the digital public interest

Within the broader context of the digital transition of public administration, it has become increasingly evident that the State must distinguish between economic interests compatible with digital resilience and those which, although legitimate in themselves, risk conflicting with cybersecurity and national technological sovereignty. This requirement does not amount to a mere technical adjustment of administrative action; rather, it constitutes a genuine organising criterion of public interests. The reason lies in the fact that cybersecurity is now regarded by authoritative scholarship as a global public good, whose absence endangers not only individual rights and sensitive economic assets, but also the stability of democratic institutions themselves [15].

The protection of critical digital infrastructures is therefore not a sectoral interest confined to ICT services; it is a condition of existence for the constitutional state in today's cyber environment, given that administrative continuity, collective trust and the proper functioning of public functions are now inseparable from the security of networks, data and systems.

From this perspective, cybersecurity generates positive and negative externalities requiring coordinated and collective protection. On the one hand, a secure digital system enhances institutional stability and fosters user trust; on the other, the vulnerability of a single node may trigger cascading effects on essential services, economic activities and critical infrastructures [16]. Consequently, interests that hinder or compromise cybersecurity cannot be deemed worthy of legal protection: in the digital context, meritworthiness operates as a negative selection criterion, applicable not only at the award stage but throughout the entire duration of the contractual relationship.

This approach follows from the very structure of cyberspace, a complex, hybrid and multi-level relational space in which public actors, private economic operators, critical infrastructures and global information flows converge. In such a scenario, security cannot be ensured by any single actor, not even by the State. It requires, as emphasised both by the NIS2 Directive and by Decree-Law 105/2019 on the National Cybersecurity Perimeter, a model of structural and permanent cooperation between public and private actors [17]. It is within this dimension that meritworthiness acquires a relational meaning: economic operators must demonstrate not only compliance with technical requirements but also a willingness to act as co-managers of the public interest, accepting stringent obligations of transparency, interoperability, continuous updating and the sharing of critical information.

The assessment of meritworthiness therefore does not end with the award phase; rather, it continues and intensifies during contract performance, where the contractor must ensure behaviour consistent with collective security, including data protection, responsible vulnerability management, system integrity and service continuity [18]. Compliance with these standards is more than a contractual obligation; it constitutes the very condition for maintaining a relationship of trust with the public

administration [19]. In this context, cybersecurity becomes a criterion of substantive legality, situated at the intersection of the principle of sound administration (Art. 97 Italian Constitution), personal data protection (Art. 8 EU Charter) and the safeguarding of electronic communications.

This framework requires a careful balance between cybersecurity and the principles of competition and economic freedom. The State may not arbitrarily restrict private economic initiative (Art. 41 Italian Constitution), yet neither may it permit the entry of technologically fragile operators whose presence would heighten exposure to cyber threats and jeopardise national security. As scholarship and existing regulations emphasise, this balancing is not an abstract value judgment but the outcome of a specific administrative evaluation distinguishing interests compatible with system resilience from those that expose it to risks and vulnerabilities.

The legislature's choice to assign a prevailing role to cybersecurity in the selection of public contractors confirms this orientation. Article 108(4) of Legislative Decree 36/2023, by introducing a maximum 10 % weight for price in high-impact strategic ICT procurements, explicitly recognises the axiological primacy of security over mere economic savings. This marks a significant departure from the traditional procurement logic in which price was commonly decisive; today, cybersecurity assumes the role of a genuine meta-value, capable of systematically orienting administrative discretion in the most technologically sensitive sectors.

This framework is further reinforced by Law 90/2024, which in Article 14 introduces "essential cybersecurity elements" for ICT goods and services used in contexts linked to the protection of national strategic interests, entrusting their technical specification to a decree of the President of the Council of Ministers proposed by the National Cybersecurity Agency (ACN).

Recent scholarship highlights the dual innovative dimension of this provision: on the one hand, it introduces a technological advantage for the use of Italian, European or NATO solutions, thereby strengthening technological sovereignty and strategic autonomy; on the other hand, it extends cybersecurity obligations to procedures awarded solely on the basis of the lowest price, thereby broadening the practical scope of Article 108 of the Code [20, 21].

The subsequent implementation of the NIS2 Directive through Legislative Decree 138/2024 completes this new regulatory triangle. Article 24 requires essential and important entities to ensure the security of their entire supply chain, including suppliers and subcontractors, confirming that security is not an internal attribute of the administration but a fiduciary relationship between public authorities and market operators. This development entails a significant shift: cybersecurity is no longer a technical burden but a substantive legal obligation, whose violation affects the validity, effectiveness and sustainability of administrative action.

A critical issue concerns the indeterminacy of the concepts of "national strategic interest" and "essential cybersecurity elements", both of which constitute general clauses with high technical content. Their broad semantic scope grants the administration substantial discretion but may also generate inconsistencies and legal uncertainty [20].

Moreover, Italian law lacks an organic definition of the national strategic interest, despite its frequent invocation in heterogeneous sources (Decree-Law 21/2012; Decree-Law 187/2022). Even the reference made by Article 14 of Law 90/2024 to Articles 5 and 7 of Decree-Law 82/2021 appears insufficient, as it identifies the National Cybersecurity Agency as guardian of such interests without articulating their precise boundaries.

From this perspective, legal certainty becomes an indispensable component of administrative meritworthiness: cybersecurity can function as a primary value only if accompanied by verifiable, proportionate and clear criteria enabling a distinction between what is essential and what is excessive or redundant. Within this framework, meritworthiness is no longer a unilateral attribute of the public interest but a relational quality recognising the participatory role of private actors in achieving collective goals. A meritorious enterprise is one that operates according to principles of cooperation, openness and transparency, contributing to the construction of a reliable digital ecosystem [22].

5. Cybersecurity, technological sovereignty and the risks of digital dependence

Having regard to the evidence outlined thus far, cybersecurity may be qualified as a structural parameter of the meritworthiness of the public interest pursued through digital procurement. The outsourcing of critical infrastructures, the management of strategic databases, and the adoption of platforms for the delivery of essential services expose public administrations to systemic risks affecting operational continuity, the protection of fundamental rights and, in certain cases, national security. In such a context, a contractual framework lacking adequate security safeguards can hardly be considered meritorious, even where it appears formally compliant and economically competitive.

This issue directly intersects with the principle of result, which, as previously noted, has now been elevated to an organizing criterion of the public procurement system. If the result cannot be reduced to the mere completion of the procedure or to immediate cost savings, but rather consists in the effective and durable achievement of the public interest underlying the award, then security, resilience and technological sustainability must be regarded as essential components thereof. A contract that generates structural dependency, systemic vulnerabilities or disproportionate migration costs in the medium term ultimately compromises the result itself, even in the presence of a formally lawful award.

From this perspective, digital meritworthiness assumes an intrinsically forward-looking dimension. It requires assessing not only the "static" security of the proposed solution, but also the contract's capacity to prevent or mitigate forms of technological dependency. Vendor lock-in, namely, the subordination of the administration to proprietary systems controlled by a single operator, represents a primary threat both to cybersecurity and to technological sovereignty, as it concentrates vulnerabilities, limits independent audits, reduces competition and hampers the autonomous evolution of systems [23].

It follows that contractual clauses aimed at ensuring data portability, interoperability among platforms, auditability of solutions and, where possible, access to or verifiability of source code acquire not merely technical, but structural relevance in relation to the pursued result. Such clauses help preserve the administration's ability to govern its digital infrastructures over time, preventing contingent choices from turning into irreversible constraints.

The issue of technological sovereignty, understood as the capacity to control, govern and maintain one's critical technological stack, lies at the core of the most recent European digital strategies. The European Commission has progressively integrated this concept into its policies, ultimately including, in the 2025 European Cybersecurity Strategy, the triad "resilience, technological sovereignty and leadership" among its priorities for action. Cybersecurity is thus framed within a systemic dimension in which control over deployed technologies, processed data and system update mechanisms becomes a precondition for achieving the public result.

In this vein, instruments such as the Data Act (Regulation (EU) 2023/2854), which strengthens data portability and reduces barriers to switching providers, as well as the European Commission's Cloud Sovereignty Procurement Framework, aim to guide public administrations toward open, interoperable and verifiable solutions [24]. Similarly, the Italian Cloud Strategy emphasizes digital sovereignty and the possibility of provider migration as conditions for effective control over critical infrastructures [8].

Public demand thus acquires a regulatory function in shaping the market: through procurement, administrations may steer supply toward multi-vendor architectures, open standards, federated platforms (such as GAIA-X) and solutions capable of ensuring redundancy, secure updates and operational continuity. From this perspective, technological sovereignty is not merely a political objective, but becomes a contractual design criterion consistent with the principle of result.

Accordingly, the evaluation of tenders cannot be confined to immediate economic convenience. Models such as the Most Economically Advantageous Tender (MEAT) allow for the integration of technical quality, team expertise, life-cycle costs and lock-in risk within an assessment framework that privileges the comprehensive and sustainable outcome of the award. Value for money, so understood, acquires a qualitative and strategic dimension: price must be weighed against security risks, indirect costs arising from service disruptions and the contract's capacity to ensure autonomy and resilience

over time [25].

Within this framework, the principle of result and meritworthiness do not operate as rhetorical clauses, but as criteria for rationalizing contractual choices in the digital domain. Procedural correctness and competitive award processes remain indispensable preconditions, yet they do not exhaust the assessment of the contractual arrangement's coherence with the underlying public interest.

The evaluation must extend to the technological structure of the contract, the allocation of risks, the reversibility of adopted solutions and the administration's ability to retain effective control over strategic infrastructures and data over time. In this context, cybersecurity therefore emerges as a factor directly affecting the systemic soundness of the administrative result.

Consequently, the meritworthiness of digital procurement is measured by its ability to ensure operational continuity, interoperability and the possibility of evolution without structural dependencies. The result, in turn, cannot be considered achieved where the contractual framework generates systemic vulnerabilities or technological constraints that are difficult to overcome. It is on this terrain, that of sustainability, control and resilience in the medium to long term, that the substantive quality of public decision-making in the digital sphere ultimately rests [26].

6. Cybersecurity and the principle of proportionality in administrative action

As cybersecurity becomes a structural component of administrative legality, it must be reconciled with another foundational principle of European administrative law: proportionality. This principle, codified in Article 5 TEU and deeply rooted in Italian constitutional jurisprudence, requires that administrative measures be suitable, necessary and proportionate *stricto sensu* with respect to the goals pursued.

In the procurement of ICT solutions, proportionality plays a fundamental role in assessing whether cybersecurity requirements are justified or excessive. EU procurement law explicitly mandates that technical specifications ensure equal access and do not create unjustified barriers to competition (Directive 2014/24/EU, Art. 42(2)). The Court of Justice has affirmed that security-related restrictions must be proportionate and evidence-based (CJEU, October 2020 no.123, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others).

This leads to a dual challenge:

1. Under-protection risks exposing public infrastructures to significant cyber threats;
2. Over-protection may impose technical standards so stringent or costly as to exclude SMEs, distort competition, or unjustifiably favour a narrow group of suppliers;

A proportionality analysis therefore requires administrations to demonstrate:

- The suitability of cybersecurity measures (are they technically appropriate?);
- Their necessity (do less restrictive alternatives exist?);
- Their balanced impact(does the security gain outweigh competitive restrictions?);

From this standpoint, cybersecurity obligations must be calibrated to the size, capacity and technological maturity of economic operators. NIS2 itself embraces a risk-based and proportionality-oriented approach, requiring essential and important entities to adopt measures "commensurate with the risks" (Art. 21(2)).

Cybersecurity, therefore, does not override proportionality; it operationalises it. In the digital administrative state, proportionality amounts to ensuring that cybersecurity requirements are both robust and balanced, enabling security without undermining competition, innovation or fairness in the public procurement market.

7. Guidelines and roadmap for integrating digital transformation and cybersecurity in public contracts

The ongoing digitalization of public administration and the growing importance of cybersecurity as a structural dimension of national and economic security require systematic guidelines for contracting authorities involved in cyber-sensitive procurement. These guidelines should not merely prescribe sectoral technical standards but translate the functional and ethical relevance of cybersecurity into legal and organizational criteria consistent with the existing regulatory framework.

A roadmap, in this perspective, is not a checklist of tasks but an integrated governance framework aligning technological needs, regulatory obligations, and constitutional principles of efficiency and impartiality. It should be consistent with the architecture of Legislative Decree 36/2023, emphasizing the *principle of result*, and coordinated with EU Directive 2022/2555 (NIS 2) and its implementation in Italian law via Law 90/2024.

Cybersecurity thus becomes a transversal parameter of public interest in contracts: it is not only a technical safeguard but also a substantive criterion of administrative legitimacy, influencing procurement design, contractor selection, and contract execution. These choices remain subject to proportional technical discretion aligned with sector-specific risks [27].

7.1. Strategic vision oriented to results

An effective roadmap starts from a clear, integrated strategic vision situating digital procurement within the broader digital government ecosystem. This entails:

- an end-to-end approach to the contract life cycle;
- measurable objectives in efficiency, timeliness, quality of supply, and competition;
- integration with national strategies for data governance and digital transformation.

Italy's *National Digital Procurement Ecosystem* (Legislative Decree 36/2023, arts. 19–36) exemplifies this vision, requiring procedures via certified platforms interoperable with the National Public Contracts Database (BDNCP) and the National Digital Data Platform (PDND), ensuring end-to-end digitalization. Adoption of European standards such as UBL, PEPPOL, and EN 16931 facilitates interoperability, reducing timelines, controlling spending, and preventing irregularities. Only a technically secure and standardized ecosystem allows measurement of administrative quality and performance, making public procurement a strategic infrastructure for value creation [28].

7.2. Data governance and interoperable architecture

Effective digital transformation requires solid data governance based on standardization, interoperability, and data quality. Obstacles include fragmented systems, legacy infrastructures, and non-machine-readable formats [29]. A roadmap should promote:

- standardization of codes, formats, and fields across the procurement life cycle;
- integration of e-procurement platforms with financial and control systems;
- adoption of interoperable, scalable, and secure data architectures.

Technical Rules by AgID (art. 26, Public Contracts Code) define functional requirements and certification for e-procurement systems, ensuring interoperability with PDND and BDNCP. Standardized, traceable, and certified data enables automated analysis, cross-administration comparisons, and real-time monitoring, constituting a foundational condition for the principle of result [30].

7.3. Gradual integration of emerging technologies

Emerging technologies (AI, machine learning, RPA, blockchain, IoT) should be introduced according to proportionality, adequacy, and organizational sustainability. Phased implementation includes:

- pilot projects in high-impact areas (spending analysis, contract performance monitoring);
- ex ante risk assessment (legal, ethical, cybersecurity);
- definition of technical and accountability standards for algorithms in decision-making.

The public procurement experience of AI systems demonstrates that such technologies can act as tools for organizational transformation. AI can support bid evaluation, contract monitoring, and optimize the delivery of public services. To ensure transparency, accountability, and non-discrimination, administrations must set strict technical requirements, implement ex ante and ex post audits, and maintain meaningful human oversight [31]. In acquiring "high-risk" systems under Regulation (EU) 2024/1689 (AI Act), administrations must ensure data governance, algorithm traceability, and adherence to accountability standards. Procurement thus becomes a regulatory and technical infrastructure that supports decision-making and service delivery, aligned with public interest and the principle of outcome.

7.4. Cybersecurity as a prerequisite for contractual results

Digital procurement exposes administrations to systemic risks affecting continuity, data integrity, and legitimacy. Strategic planning should ensure:

- structural integration of procurement and IT functions;
- cybersecurity, data protection, and incident management requirements in tender specifications;
- rigorous due diligence and supplier vetting;
- clear incident response plans with defined roles and escalation hierarchies.

Platforms such as MEF/Consip, recognized as critical national infrastructure, exemplify robust cybersecurity governance through collaboration with ACN and CSIRT Italy. Standardized, multibrand solutions enhance resilience, traceability, and risk mitigation, embedding cybersecurity as an intrinsic element of the principle of result [32].

7.5. Organizational capabilities and digital culture

Digital transformation requires structural investment in skills and cultural change. Key measures include:

- continuous training in data management, analytics, and cybersecurity;
- liaison roles connecting procurement, IT, and control functions;
- fostering a collaborative, innovation-oriented culture [33].

Compliance with Decree 36/2023, AgID technical rules, and interoperability with BDNCP (ANAC Deliberations 261/2023 and 264/2023) necessitates specialized skills in data governance, APIs, digital preservation, and cybersecurity [34], [35], [36]. The Digital Transition Officer (RTD) and the 2024–2026 Digital Plan reinforce the requirement for organizational capacity to achieve measurable, high-quality outcomes [37], [38].

7.6. Digital-by-design and human-centred approach

Roadmaps should embed digital-by-design and human-centred design principles, focusing on:

- simplification and reduced administrative burdens;
- accessibility, inclusiveness, and usability;
- transparency and traceability.

Practical applications include intuitive interfaces, automatic document checks, and integrated digital support [39]. These measures increase SME participation, reduce errors, and enhance decision-making transparency, linking the principle of result to proportionality, inclusiveness, and competition. Properly structured digitalization thus strengthens administrative rationality, reliability, resilience, and institutional legitimacy.

8. Cybersecurity as a principle-value of digital administration

The normative and scholarly framework reconstructed above reveals a profound shift in the contemporary understanding of meritworthiness within administrative law. In the twentieth-century tradition, meritworthiness was assessed in relation to the compatibility of a given interest with public purposes and its suitability to be protected by the legal order.

In the digital context, however, meritworthiness acquires a dynamic and relational nature, as it must account both for the systemic vulnerability of technological infrastructures and for the need to guarantee the resilience of administrative processes [40].

From this perspective, cybersecurity becomes the concrete measure of administrative responsibility in the digital society. It is no longer a mere technical safeguard or organisational factor, but a principle-value that profoundly influences the way the administration identifies, balances and protects the public and private interests at stake. Cybersecurity operates as a substantive criterion of legitimacy, affecting the validity, enforceability and long-term sustainability of administrative action. Accordingly, the relationship between cybersecurity and economic efficiency no longer appears as a conflict but as a functional hierarchy: security constitutes a precondition for efficiency, not an external limitation upon it. A cyber-vulnerable public administration is neither efficient nor legitimate, as it exposes data, services and ultimately citizen trust to significant risk [41]. The interest in reducing costs or accelerating procedures, although legitimate, cannot prevail over the need to guarantee the confidentiality, integrity and availability of information systems. This axiological shift overturns the traditional perspective: cybersecurity is no longer a cost to be minimised, but a public value to be optimised.

The system of legal sources confirms and crystallises this inversion. Article 14 of Law No. 90/2024, by introducing premium criteria for offers incorporating Italian or European cybersecurity technologies, establishes a new substantive parameter in the selection of public contractors: the administration evaluates not only the intrinsic quality of the offer but also the reliability and technological provenance of the proposed solutions. This constitutes a form of substantive meritworthiness, in which national security and technological sovereignty become internal dimensions of administrative judgment, rather than external or incidental considerations.

Digital administrative law thus defines the public interest not only by what the administration pursues, but also by how it pursues it: process security, data protection, infrastructure integrity and technological sustainability now constitute intrinsic components of meritworthiness [42]. A technically adequate performance lacking cybersecurity guarantees cannot be classified as meritorious, as it fails to generate trust and continuity within the public digital ecosystem.

Cybersecurity therefore emerges as a cornerstone of administrative action, both a “minimum” and “maximum” element of legitimacy, in the sense that it constitutes simultaneously the indispensable foundation and the most advanced parameter against which the quality of digital public action is measured. Its absence undermines not only administrative effectiveness but also fundamental rights and the institutional stability of public governance.

This transformation produces a new balance between public and private interests. Meritworthiness is no longer limited to assessing whether an interest deserves legal protection; it becomes a criterion of prioritisation that reorganises administrative objectives according to cybersecurity needs. In other words, cybersecurity appears as a prevailing public interest, capable of reshaping the weight of competing values (competition, cost-effectiveness, speed) in light of the need to protect technological reliability.

As shown, this evolution finds its most evident application in the field of public procurement, the main interface between administration and market. The assessment of digital security decisively influences not only the award stage (through criteria such as those in Art. 108 of Legislative Decree 36/2023), but also the execution phase, during which the economic operator remains bound to maintain adequate security standards throughout the contractual relationship.

From this perspective, digital procurement becomes an instrument for giving effect to the right to good administration [43], as it enables efficiency, transparency and technological reliability to be pursued simultaneously. The meritworthiness of the interest at stake thus consists in the system’s capacity to ensure public decisions that are secure, competitive and consistent with constitutional

values.

EU law reinforces this approach. Article 42(2) of Directive 2014/24/EU requires that technical specifications ensure equal access and do not create unjustified obstacles to competition. Cyber-resilience therefore cannot justify arbitrary discrimination; it must rest on objective, proportionate and technically verifiable parameters [19].

The new paradigm nonetheless raises significant questions. On the one hand, the effectiveness of the legal provisions will depend on administrative practice and on judicial developments, particularly regarding the verification of cybersecurity requirements and the assessment of their technical adequacy [16]. On the other hand, the proportionality of security obligations *vis-à-vis* the size and capabilities of economic operators, especially SMEs, must be considered to prevent cybersecurity from becoming a tool of exclusion or market concentration.

In conclusion, cybersecurity is no longer a purely technical or regulatory field; it is the benchmark through which the criteria of administrative meritworthiness are being redefined. Meritorious is that which strengthens the resilience of digital infrastructures, reduces information asymmetries, ensures operational continuity and promotes technological sovereignty. Not meritorious is that which generates dependence, opacity or vulnerability. The new meritworthiness is thus measured by the State's capacity to protect its digital dimension, as the security of cyberspace has become the benchmark of public decision-making, the criterion for awarding procurement, and the ultimate guarantee of citizen trust.

Declaration on Generative AI

During the preparation of this work, the author used ChatGPT and DeepL in order to: grammar, spelling check, transaltion and to improve the writing style. After using these tools the author reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] E. Gamero Casado, R. Martínez Gutiérrez, El derecho administrativo ante la era de la información, in: E. Gamero Casado, J. Valero Torrijos (Eds.), La ley de administración electrónica. Comentario sistemático a la Ley 11/2007, Thomson Aranzadi, Navarra, 2010, pp. 35–88.

[2] J. Preecha, Cybersecurity and public trust in digital governance: Focusing on citizen trust, in: Proceeding of International Conference on Social Science and Humanity, volume 2, 2025, pp. 26–37.

[3] A. Andreani, Il principio costituzionale di buon andamento della pubblica amministrazione, CEDAM, Padova, 1979.

[4] J. Rodríguez-Arana, La buena administración como principio y como derecho fundamental en europa, Revista Misión Jurídica 6 (2013) 23–56.

[5] J. Barnes, Buena administración, principio democrático y procedimiento administrativo, Revista Digital de Derecho Administrativo (2018) 77–123.

[6] European Commission, Nis2 directive: securing network and information systems, Shaping Europe's Digital Future, 2026. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20directive%20mandates%20that%20each,comply%20with%20the%20directive%27s%20requirements.

[7] European Union Agency for Cybersecurity (ENISA), A trusted and cyber secure europe: Enisa strategy, PDF Strategy Document, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-02/a-trusted-and-cyber-secure-europe-enisa-strategy.pdf#:~:text=Context%20Cybersecurity%20is%20the%20cornerstone,specificities%20of%20each%20sector%20is.

[8] Dipartimento per la trasformazione digitale and Agenzia per la Cybersicurezza Nazionale, Strategia cloud italia: la strategia nazionale del cloud per la pubblica amministrazione, Cloud Italia, n.d. URL: https://cloud.italia.it/strategia-cloud-pa/#:~:text=,e%20pubbliche%20e%20medie%20imprese, accessed: 2026-02-08.

[9] M. R. Spasiano, La codificazione dei principi del codice dei contratti pubblici e, in particolare, del risultato, alla prova del correttivo, federalismi.it (2025) 191–234.
[10] L. Martini, Il principio del risultato nel codice dei contratti pubblici: un cambio di paradigma, Il Diritto Amministrativo (2025).
[11] R. Ursi, Studi sui principi generali del Codice dei contratti pubblici, Percorsi di diritto amministrativo – Monografie, Editoriale Scientifica, Napoli, 2024.
[12] M. Macchia, Costruire e acquistare. Lezioni sul nuovo codice dei contratti pubblici, Giappichelli, Torino, 2024.
[13] F. D'Abronzo, Il principio del risultato nel nuovo codice dei contratti pubblici, De Iustitia (2025).
[14] L. Randazzo, Il nuovo codice dei contratti pubblici: il rapporto tra principi e esigenze di mercato, solidarietà e sussidiarietà orizzontale, Il Diritto Amministrativo (2024).
[15] R. Brighi, P. G. Chiara, La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'unione europea, federalismi.it (2021) 18–42.
[16] S. Rossa, Cybersicurezza e Pubblica Amministrazione, Contributi di Diritto Amministrativo – Studi e Monografie, Editoriale Scientifica, Napoli, 2023.
[17] A. Sandulli, Pubblico e privato nelle infrastrutture digitali nazionali strategiche, Rivista trimestrale di diritto pubblico (2021).
[18] L. Nannipieri, Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio, Rivista Italiana di Informatica e Diritto (2024) 19–23.
[19] M. A. Sandulli, R. De Nictolis (Eds.), Trattato sui contratti pubblici. Volume III, Giuffrè Francis Lefebvre, Milano, 2019.
[20] L. Nannipieri, Cybersicurezza e appalti. interventi legislativi e prime criticità, Rivista Italiana di Informatica e Diritto (2024) 72–79.
[21] S. Rossa, Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività, CERIDAP (2024) 338 – 373.
[22] Presidenza del Consiglio dei Ministri, Strategia nazionale di cybersicurezza, 2022.
[23] J. Svoboda, Public procurement and vendor lock-in within the area of data migration, Milan Law Review 3 (2022).
[24] Orrick, Herrington & Sutcliffe LLP, European data act: The eu data act is in force — what should businesses do?, 2025. URL: https://www.orrick.com/en/Insights/2025/09/The-EU-Data-Act-is-in-Force-What-Should-Businesses-Do.
[25] Nortal, Best practices in public procurement for continuous modernization : Using outcome-driven public procurement as an instrument for innovation, resilience and efficiency, Playbook, Nortal, 2025.
[26] European Commission, Directorate-General for Digital Services, Cloud sovereignty framework, version 1.2.1, European Commission Technical Document, 2025. URL: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en#:~:text=Technology%20sovereignty%20evaluates%20the%20degree,in%20to%20foreign%20proprietary%20systems.
[27] G. Sferrazzo, La cybersecurity nel nuovo codice dei contratti pubblici: l'art. 108 co. 4 e le criticità per le stazioni appaltanti, Teoria e Critica della Regolazione Sociale / Theory and Criticism of Social Regulation 1 (2025). URL: https://mimesisjournals.com/ojs/index.php/tcrs/article/view/5071. doi:10.7413/197054760166.
[28] Team per la Trasformazione Digitale & Agenzia per l'Italia Digitale, Il procurement per la trasformazione digitale, Piano triennale per l'informatica nella Pubblica Amministrazione 2024–2026, aggiornamento 2025, 2025. URL: https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2024-2026-agg-2025/capitolo-2_il-procurement-per-la-trasformazione-digitale/il-procurement-per-la-trasformazione-digitale.html.
[29] OECD Publishing, Digital Transformation of Public Procurement: Good Practice Report, Technical Report 77, OECD Publishing, Paris, 2025. URL: https://www.oecd.org/en/publications/digital-transformation-of-public-procurement_79651651-en.html. doi:10.1787/79651651-en.
[30] Agenzia per l'Italia Digitale (AgID), Regole tecniche: requisiti tecnici e modalità di certificazione delle piattaforme di approvvigionamento digitale, Documento PDF pubblicato nella sezione "Am-

ministrazione Trasparente" di AgID, 2023. URL: https://trasparenza.agid.gov.it/download/6224.html.
[31] G. F. Licata, Transformative public procurement of artificial intelligence, Laws 14 (2025) 97. URL: https://www.mdpi.com/2075-471X/14/6/97. doi:10.3390/laws14060097.
[32] Corriere Comunicazioni, Cybersecurity, consip affila le armi. ecco tutte le iniziative, Articolo pubblicato su Corriere Comunicazioni, 2022.
[33] M. Burtscher, S. Piano, B. Welby, Developing Skills for Digital Government: A Review of Good Practices Across OECD Governments, Technical Report 303, OECD Publishing, Paris, 2024. URL: https://www.oecd.org/en/publications/developing-skills-for-digital-government_f4dab2e9-en.html. doi:10.1787/f4dab2e9-en, oECD Social, Employment and Migration Working Papers No. 303; Accessed 2026.
[34] Agenzia per l'Italia Digitale, Adozione del provvedimento "Requisiti tecnici e modalità di certificazione delle Piattaforme di Approvvigionamento Digitale (PAD)" ai sensi dell'art. 26 del decreto legislativo 31 marzo 2023, n. 36 e s.m.i. recante Codice dei contratti pubblici, Determinazione AgID n. 0000267/2025, 2025. https://trasparenza.agid.gov.it/page/103/details/5521/adozione-del-provvedimento-requisiti-tecnici-e-modalita-di-certificazione-delle-piattaforme-di-approvvigionamento-digitale-pad-ai-sensi-dellart-26-del-decreto-legislativo-31-marzo-2023-n-36-e-smi-recante-codice-dei-contratti-pubblici.html.
[35] Autorità Nazionale Anticorruzione, Delibera anac n. 261 del 20 giugno 2023 – banca dati nazionale dei contratti pubblici, https://biblus.acca.it/download/delibera-anac-n-261-banca-dati-nazionale-dei-contratti-pubblici/, 2023. Provvedimento ai sensi dell'art. 23 del d.lgs. 31 marzo 2023, n. 36, che individua le informazioni da trasmettere alla BDNCP e i tempi di integrazione con i servizi dell'ecosistema digitale.
[36] Autorità Nazionale Anticorruzione, Delibera n. 264 del 20 giugno 2023 – modificata da delibera n. 601 del 19 dicembre 2023, https://www.anticorruzione.it/documents/91439/94538987/Delibera+n.+264+del+20+giugno+2023+-+modificata+da+Del.601-19.12.2023.pdf/7672629f-287e-e776-8854-a454d922027f?t=1704374287877, 2023. Delibera ANAC n. 264/2023, modificata da Delibera n. 601/2023, concernente disciplina della Banca Dati Nazionale dei Contratti Pubblici (BDNCP).
[37] Agenzia per l'Italia Digitale, Responsabile per la transizione digitale, https://www.agid.gov.it/it/agenzia/responsabile-transizione-digitale, 2026. Pagina informativa sull'istituzione, funzioni e responsabilità del Responsabile per la Transizione Digitale nella Pubblica Amministrazione.
[38] Agenzia per l'Italia Digitale, Piano triennale per l'informatica nella pubblica amministrazione, https://www.agid.gov.it/it/agenzia/piano-triennale, 2026. Pagina istituzionale dedicata al Piano Triennale per l'informatica nella Pubblica Amministrazione, con riferimenti alle edizioni 2024-2026 e aggiornamenti.
[39] Agenzia per l'Italia Digitale (AgID), Regole tecniche e-procurement, Pagina web istituzionale di AgID sul procurement digitale, 2023. URL: https://www.agid.gov.it/it/piattaforme/procurement/regole-tecniche-procurement.
[40] G. Mancini Palamoni, Il paradigma digitale dell'evidenza pubblica, CERIDAP (2024) 64–100.
[41] T. Cocchi, La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione, Munus – Rivista Giuridica dei Servizi Pubblici (2024) 177–207.
[42] V. Neri, Diritto amministrativo e intelligenza artificiale: un amore possibile, 2021.
[43] D. U. Galetta, Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte dal pnrr e problemi ancora da affrontare, federalismi.it (2022) 103–125.