Metodo Giuridico
Ius et Ratio • ISSN 3103-7305

RIVISTA GIURIDICA ONLINE • ISSN 3103-7305
APPROFONDIMENTO TEMATICO • DIRITTO E GIURISPRUDENZA

Sicurezza nazionale nei contratti pubblici tra cloud e veti ICT

La convergenza tra codice dei contratti, perimetro cibernetico, qualificazione ACN e golden power nella disciplina degli appalti tecnologici

FP Federico Palumbo Diritto Amministrativo & Appalti Pubblici 11 Novembre 2026 Lettura 21 min

SCHEDA APPROFONDIMENTO

TIPOLOGIA CONTRIBUTO
Approfondimento Scientifico

INQUADRAMENTO
Dottrina e Giurisprudenza

NORME DI RIFERIMENTO
Decreto legislativo 31 marzo 2023, n. 36 • Decreto-legge 21 settembre 2019, n. 105 • Decreto-legge 15 marzo 2012, n. 21

PRINCIPIO DI DIRITTO DESUMIBILE DAL SISTEMA

Nelle procedure di affidamento di committenze digitali e infrastrutturali, le clausole di salvaguardia della sicurezza nazionale, l'obbligo di conformità ai livelli di qualificazione cibernetica e l'assoggettamento ai poteri speciali statali costituiscono limiti legali intrinseci della libertà negoziale della pubblica amministrazione; il sindacato giurisdizionale sulle relative esclusioni è circoscritto alla verifica estrinseca di coerenza logica, proporzionalità e compiutezza dell'istruttoria tecnica.

Stato della questione e quadro aggiornato all'11 novembre 2026: L'intersezione tra codice dei contratti pubblici, perimetro cibernetico e golden power ha ridefinito la tutela degli asset strategici da eccezione a criterio ordinante delle committenze pubbliche digitali.

ABSTRACT (ITALIANO)

Abstract: La disciplina della **sicurezza nazionale nei contratti pubblici** ha conosciuto una radicale metamorfosi, evolvendo da clausola di deroga eccezionale a parametro strutturale di selezione tecnica. L'indagine esamina l'integrazione tra l'art. 136 del codice dei contratti, il **perimetro di sicurezza cibernetica** e i poteri governativi di **golden power**. Attraverso il prisma della giurisprudenza amministrativa, vengono approfonditi i requisiti di qualificazione dei servizi cloud, i vincoli di localizzazione infrastrutturale, il riparto dell'onere probatorio e i limiti del **sindacato del giudice amministrativo** sulle esclusioni tecnologiche e sui veti all'approvvigionamento ICT.

ABSTRACT (ENGLISH)

The regulation of national security in public contracts has undergone a structural transformation, evolving from an exceptional derogation into a primary governing principle of digital public procurement. This paper analyzes the interplay among procurement rules, the national cybersecurity perimeter, cloud qualification frameworks, and executive screening mechanisms. Examining recent administrative case law, the author addresses technical admission criteria, geographical localization requirements, evidentiary burdens, and the boundaries of judicial review over executive discretion.

Punti Chiave dell'Approfondimento

01.

Evoluzione sistematica:
La sicurezza nazionale abbandona la fisionomia di mera esimente eccezionale e si consolida quale parametro strutturale di qualificazione tecnica e di attribuzione del punteggio economico nelle committenze ICT ad alta criticità.

02.

Ripartizione delle competenze:
Il modulo procedimentale del perimetro cibernetico e le prescrizioni del Centro di Valutazione e Certificazione Nazionale prevalgono sull'autonomia contrattuale della stazione appaltante, imponendo adempimenti vincolanti a pena di esclusione o risoluzione del contratto.

03.

Limiti al sindacato giurisdizionale:
L'esercizio dei poteri governativi di golden power e le valutazioni di rischio geopolitico integrano un'ampia discrezionalità politica e tecnica, censurabile innanzi al giudice amministrativo nei soli casi di manifesta illogicità, travisamento dei fatti o palese difetto istruttorio.

01. L'EVOLUZIONE DELLA SICUREZZA NAZIONALE NEI CONTRATTI PUBBLICI TRA FONTI PRIMARIE E SOVRANAZIONALI

1.1 — La sicurezza nazionale nell'architettura dei contratti pubblici tra fonti primarie e sovranazionali

Il tema della **sicurezza nazionale nei contratti pubblici** ha progressivamente abbandonato la dimensione di mera clausola di stile per assurgere a perno regolatorio della **transizione digitale della pubblica amministrazione**. Nel disegno originario delle direttive europee e dell'art. 346 del Trattato sul Funzionamento dell'Unione Europea, la salvaguardia degli interessi statali vitali costituiva una **deroga eccezionale alla concorrenza**, azionabile unicamente a

fronte di minacce concrete e imminenti per la sovranità territoriale o la difesa militare. L'espansione esponenziale delle minacce informatiche e la pervasività delle tecnologie di rete hanno tuttavia scardinato tale rigida dicotomia negoziale.

La trasformazione delle **infrastrutture critiche immateriali** ha reso manifesto come la vulnerabilità di una piattaforma informatica o di una **catena di fornitura ICT** possa compromettere la continuità istituzionale non meno di un attacco convenzionale. Da qui è scaturita la necessità di conformare l'intero ciclo di vita dell'evidenza pubblica a canoni stringenti di **resilienza cibernetica** e tracciabilità dei dati strategici. La dottrina giuspubblicistica più attenta ha rilevato come la sicurezza non rappresenti più un limite esterno e oppositivo alla concorrenza, bensì un parametro qualitativo intrinseco della prestazione negoziale, funzionale a garantire che il mercato pubblico operi senza pregiudizio per la collettività D1.

In questa prospettiva, la **sovranità tecnologica** cessa di essere un concetto astratto e diviene criterio operativo per la selezione dei contraenti, orientando la determinazione dei **requisiti di ammissione alle gare**, la conformazione dei capitolati e le condizioni di esecuzione dei rapporti contrattuali continuativi. Tale evoluzione dialoga sistematicamente con il principio del risultato nei contratti pubblici, imponendo che l'affidamento non miri alla mera acquisizione formale del bene ma al conseguimento di prestazioni informatiche sicure, affidabili e protette da interferenze esterne. A differenza di quanto accade negli appalti ordinari di servizi standardizzati, ove la concorrenza sul prezzo conserva un ruolo centrale, nelle committenze ad alta intensità tecnologica la salvaguardia sistemica prevale sul mero risparmio erariale.

1.2 — La tutela della riservatezza e degli interessi essenziali dello Stato nel nuovo Codice

Nel quadro delineato dal decreto legislativo 31 marzo 2023, n. 36, la convergenza tra disciplina delle committenze e interessi strategici trova composizione nell'**art. 136 del d.lgs. n. 36/2023**. La norma stabilisce il principio generale di applicazione del codice ai settori della difesa e della sicurezza, fatte salve le specifiche eccezioni previste dal decreto legislativo n. 208 del 2011, ma introduce al comma 2 un precetto cardine. L'applicazione delle ordinarie disposizioni di evidenza pubblica è esclusa per gli appalti pubblici e i concorsi di progettazione *«quando la tutela degli interessi essenziali di sicurezza dello Stato non possa essere garantita mediante misure idonee»* e volte anche a proteggere la riservatezza delle informazioni che le stazioni appaltanti rendono disponibili nella procedura di gara.

Tale previsione codicistica consacra un **criterio di sussidiarietà e proporzionalità**: l'amministrazione aggiudicatrice non può sottrarsi automaticamente alle regole del confronto concorrenziale, ma è tenuta a valutare in prima battuta l'adozione di **misure di sicurezza proporzionate**, quali accordi di riservatezza rafforzati, vincoli di secretazione o limitazioni all'accesso agli atti di gara. Solo ove tali presidi tecnici e giuridici risultino insufficienti a scongiurare dispersioni informative o compromissioni sistemiche, scatta l'**inapplicabilità del codice dei contratti pubblici**, legittimando regimi speciali di approvvigionamento diretto o fiduciario.

La portata di tale disposizione si coordina strettamente con la disciplina in tema di accesso difensivo e segreti tecnici nel nuovo Codice appalti, confermando che la riservatezza tecnica e la sicurezza della Repubblica prevalgono sulle consuete pretese di ostensione documentale dei concorrenti non aggiudicatari. In sede contenziosa, la difesa dell'operatore escluso deve misurarsi con la rigorosa perimetrazione del segreto tecnico, sollevando la questione dell'**onere della prova in giudizio** circa l'adeguatezza delle misure alternative di protezione esperibili dalla stazione appaltante prima di disporre l'esclusione.

02. IL PERIMETRO DI SICUREZZA CIBERNETICA E LE VERIFICHE DEL CVCN

2.1 — Il Perimetro di Sicurezza Nazionale Cibernetica e i soggetti inclusi

L'architettura della sicurezza digitale trova il proprio fondamento normativo nel decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133. L'**art. 1 del d.l. n. 105/2019** istituisce il **Perimetro di sicurezza nazionale cibernetica** al fine di garantire un livello elevato di protezione per le reti, i sistemi informativi e i servizi informatici di soggetti pubblici e privati *«da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato»* e il cui danneggiamento o interruzione possa arrecare grave pregiudizio alla sicurezza collettiva.

L'inclusione nel perimetro, disciplinata sul piano attuativo dal **d.P.C.M. 30 luglio 2020, n. 131**, investe amministrazioni centrali, enti locali, gestori di servizi pubblici e primari **operatori economici privati** nei comparti strategici dell'energia, dei trasporti, delle telecomunicazioni e della sanità. Tali soggetti hanno l'obbligo di censire le proprie **reti e sistemi informativi critici**, predisponendo elenchi dettagliati dell'architettura e della componentistica tecnologica soggetti ad aggiornamento almeno annuale presso l'**Agenzia per la Cybersicurezza Nazionale** (ACN), nonché di rispettare i severi obblighi di notifica degli incidenti informatici al CSIRT Italia entro una o sei ore secondo la gravità del pregiudizio, ai sensi del **d.P.C.M. 14 aprile 2021, n. 81**.

Il mancato rispetto degli obblighi di comunicazione o l'omessa adozione delle misure di sicurezza previste comporta l'irrogazione di **sanzioni amministrative pecuniarie** di eccezionale severità, oscillanti tra 200.000 euro e 1.800.000 euro, a riprova della natura inderogabile della tutela dell'**ordine pubblico digitale**. A differenza delle ordinarie violazioni amministrative in tema di appalti, le sanzioni perimetrali prescindono dall'elemento soggettivo del dolo, fondandosi sulla mera inosservanza oggettiva dei doveri di notifica e mappatura delle infrastrutture informatiche essenziali.

2.2 — Il ruolo del CVCN e l'incidenza delle verifiche tecniche sulle gare

Il cuore operativo della disciplina di tutela risiede nelle funzioni attribuite al **Centro di Valutazione e Certificazione Nazionale** (CVCN), incardinato presso l'ACN. In forza del combinato disposto dell'art. 1, comma 6, del d.l. n. 105/2019, del **d.P.R. 5 febbraio 2021, n. 54** e del **d.P.C.M. 15 giugno 2021** (che individua le categorie merceologiche di apparati di rete, firewall, sistemi SCADA e virtualizzazione sensibili), i soggetti inclusi nel perimetro che intendano affidare **forniture di beni, sistemi e servizi ICT** destinati a reti strategiche devono trasmettere preventiva comunicazione al CVCN.

Il CVCN dispone di un **termine procedimentale ordinario di 45 giorni**, prorogabile di ulteriori 15 giorni per accertamenti tecnici particolarmente complessi su hardware o software, per svolgere le necessarie **verifiche di sicurezza tecnologica** ovvero imporre specifiche prescrizioni o test da eseguire entro 60 giorni. L'incidenza di tale modulo procedurale sulla contrattualistica pubblica è dirompente: i bandi e i contratti devono obbligatoriamente contemplare **clausole sospensive o risolutive espresse** subordinate al rispetto delle condizioni e all'esito favorevole dei test di vulnerabilità, integrando una specifica **causa di risoluzione dell'affidamento**.

Sul piano dei requisiti di ammissione e valutazione delle offerte, la giurisprudenza amministrativa ha chiarito che la stazione appaltante deve ancorarsi con rigore alle prescrizioni formulate nella documentazione concorsuale, senza operare sovrapposizioni arbitrarie tra schemi normativi eterogenei. In particolare, il giudice di prime cure campano ha puntualizzato come la verifica della **conformità delle offerte tecniche** ai parametri di affidabilità informatica debba misurarsi sui criteri tassativamente prefissati dal bando, quale il possesso della **certificazione ISO/IEC 27001**, escludendo che l'omesso richiamo della direttiva NIS2 in commesse ordinarie estranee ai servizi informatici essenziali

possa fondare censure sul punteggio assegnato [1]. Il difensore dell'impresa concorrente non può dunque invocare in giudizio standard cyber non trasfusi nella lex specialis.

03. IL CLOUD PER LA PA E LA QUALIFICAZIONE DI DATI E SERVIZI

3.1 — L'evoluzione della qualificazione: dalle circolari AgID al Regolamento ACN n. 21007/2024

Il processo di razionalizzazione del patrimonio applicativo delle pubbliche amministrazioni verso paradigmi computazionali sicuri ha conosciuto una radicale evoluzione. Superato il pionieristico regime delle circolari dell'Agenzia per l'Italia Digitale (AgID), il baricentro regolatorio è transitato all'Agenzia per la Cybersicurezza Nazionale, culminando nell'adozione del **Decreto direttoriale ACN 27 giugno 2024, n. 21007**, recante il nuovo **Regolamento per i servizi cloud e le soluzioni tecnologiche per la pubblica amministrazione**.

Tale corpus regolamentare istituisce un **regime di qualificazione obbligatoria preventiva** per qualunque fornitore di servizi IaaS, PaaS e SaaS destinati a trattare dati o funzioni amministrative. Sotto il profilo della contrattualistica pubblica, la giurisprudenza amministrativa ha fissato coordinate essenziali circa la collocazione temporale e funzionale di tale requisito nel procedimento concorsuale. Come statuito dal Consiglio di Stato, la qualificazione del software applicativo costituisce di regola un **requisito di esecuzione del contratto** e non un vincolo di ammissione alla procedura, salvo che la lex specialis non disponga espressamente in senso contrario, atteso che l'amministrazione conserva la facoltà di verificare l'avvenuta iscrizione prima della formale stipulazione negoziale [2].

Ne discende che il possesso del titolo di abilitazione ACN garantisce la **conformità tecnica dell'infrastruttura** alle prescrizioni di sicurezza nazionale, evitando preclusioni concorrenziali sproporzionate all'avvio della contesa selettiva. A differenza di quanto si verifica per i requisiti soggettivi generali di ordine pubblico, la cui mancanza comporta l'esclusione immediata e insanabile, l'abilitazione applicativa può essere conseguita e perfezionata nel corso della procedura, a condizione che l'offerente ne dimostri la pendenza dell'istruttoria innanzi all'Agenzia.

3.2 — Tassonomia dei dati (ordinari, critici, strategici) e livelli di sicurezza (QC1-QC4 e AI1-AI4)

L'impianto regolatorio vigente correla il livello di scrutinio di sicurezza alla natura sostanziale dei flussi informativi trattati. Il **Decreto direttoriale ACN n. 21007/2024** ripartisce i dati e i servizi delle pubbliche amministrazioni in tre classi fondamentali: **dati ordinari** (informazioni la cui compromissione non pregiudica la continuità amministrativa), **dati critici** (funzioni rilevanti la cui alterazione arreca pregiudizio al benessere economico-sociale o alla salute e incolumità) e **dati strategici** (assetti vitali la cui compromissione reca pregiudizio alla sicurezza nazionale).

A fronte di tale tassonomia, il Regolamento ACN n. 21007/2024 definisce quattro livelli progressivi di qualificazione per i servizi cloud (**livelli QC1, QC2, QC3 e QC4**) e introduce speculari livelli di **adeguamento delle infrastrutture digitali** delle amministrazioni (**livelli AI1, AI2, AI3 e AI4**), secondo lo schema sintetizzato nella seguente tabella:

Qualificazione Cloud	Adeguamento Infrastrutture	Tipologia Dati	Presidi di Sicurezza Richiesti
QC1	AI1	Dati Ordinari	Requisiti tecnici di base, conformità standard ISO 27001, autodichiarazione di conformità tecnica.
QC2	AI2	Dati Critici	Crittografia evoluta a riposo e in transito, business continuity rafforzata, audit periodici di terze parti.
QC3	AI3	Dati Strategici	Isolamento logico avanzato, giurisdizione e custodia chiavi entro lo Spazio Economico Europeo, esclusione extraterritoriale.
QC4	AI4	Dati Strategici Difesa	Isolamento fisico delle infrastrutture, cifratura hardware sovrana, personale con nulla osta di sicurezza.

In merito alla conformità delle soluzioni computazionali offerte dai concorrenti, il Consiglio di Stato ha chiarito che il requisito della **disponibilità esclusiva dell'infrastruttura** o del data center primario non impone necessariamente un titolo di proprietà dominicale in capo all'offerente. È sufficiente che l'operatore economico dimostri il **pieno ed esclusivo controllo funzionale** della struttura informatica mediante idonei strumenti negoziali, quali un contratto di avvalimento o accordi vincolanti di gruppo, preservando la continuità operativa e l'affidabilità del servizio pubblico[3]. In caso di contenzioso, l'onere probatorio circa l'effettività della disponibilità materiale dei server grava sul concorrente che ricorre all'ausiliaria.

3.3 — Il Polo Strategico Nazionale e la localizzazione geografica dell'infrastruttura

Il vertice dell'architettura digitale repubblicana è incarnato dal **Polo Strategico Nazionale** (PSN), infrastruttura cloud ad altissima affidabilità destinata a ospitare la totalità dei dati strategici e critici delle pubbliche amministrazioni centrali e delle autorità sanitarie. Il modello PSN risponde all'esigenza di sottrarre il patrimonio informativo dello Stato a **rischi di ingerenza extraterritoriale** derivanti da legislazioni straniere, realizzando una reale **autonomia tecnologica nazionale**.

Tra i vincoli di massima cogenza spicca la **localizzazione geografica dei data center**, per i quali è prescritta la dislocazione sul territorio nazionale a una **distanza geografica minima di 500 chilometri** tra i siti primari e quelli di disaster recovery. Ciò consente di garantire la resilienza sistemica anche a fronte di calamità naturali o eventi bellici di vaste proporzioni, salvaguardando la continuità delle funzioni pubbliche essenziali e la sicurezza dei dati archiviati.

La complessità procedurale e l'ingente valore economico di tali affidamenti strategici sono stati confermati dall'ampio contenzioso sorto in sede di gara. Chiamato a pronunciarsi sulla procedura per la realizzazione e gestione del Polo Strategico Nazionale, il Consiglio di Stato ha rimarcato la **rigida intangibilità della disciplina di gara**, chiarendo che i chiarimenti forniti dalla stazione appaltante non possono introdurre limitazioni quantitative o oneri innovativi non

contemplati dalla lex specialis, a presidio della **par condicio tra gli offerenti** e della trasparenza dell'azione amministrativa [4]. Il principio di auto-vincolo impedisce alla committenza di alterare le regole di ingaggio tecnologiche dopo la presentazione delle offerte.

04. LA DISCIPLINA DEI POTERI SPECIALI (GOLDEN POWER) E I CONTRATTI ICT

4.1 — La ratio del d.l. n. 21/2012 applicata agli appalti e concessioni ICT

L'interferenza tra prerogative pubblicistiche autoritative e dinamiche del mercato dei contratti pubblici raggiunge la massima intensità con l'applicazione della disciplina del **golden power**. Nata con il decreto-legge 15 marzo 2012, n. 21 per presidiare gli assetti proprietari nei settori della difesa e dell'energia, la normativa sui poteri speciali è stata progressivamente estesa agli approvvigionamenti tecnologici. La dottrina ha evidenziato come la sicurezza nazionale abbia cessato di operare quale mero scudo difensivo per trasformarsi in un **parametro di aggiudicazione e conformazione negoziale** nei contratti ad alta intensità cibernetica [D2].

L'evoluzione normativa ha introdotto nell'ordinamento l'art. 1-bis del d.l. n. 21/2012, disponendo espressamente che *«costituiscono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G»*, estendendo tali presidi alle infrastrutture cloud e ai sistemi di intelligenza artificiale nella pubblica amministrazione impiegati in contesti critici. Tale espansione ridefinisce la perimetrazione delle committenze, imponendo alle imprese notificanti di sottoporre preventivamente al vaglio governativo i piani di sviluppo e gli accordi contrattuali di fornitura.

La portata di tali vincoli nei confronti delle procedure di affidamento di reti e servizi di telecomunicazione è stata esaminata dalla giurisprudenza amministrativa d'appello. Il Consiglio di Stato ha chiarito che le clausole concorsuali volte a valorizzare la localizzazione della produzione degli apparati tecnici e dei centri di ricerca entro lo Spazio Economico Europeo perseguono una legittima **tutela dell'ordine pubblico economico** e della sicurezza dell'approvvigionamento, prevenendo rischi di alterazione concorrenziale derivanti da economie non di mercato [5].

4.2 — L'art. 1-bis: tecnologia 5G, cloud computing e componentistica critica extra-UE

Il meccanismo operativo disciplinato dal comma 2 dell'art. 1-bis impone a tutte le imprese che intendano acquisire beni o servizi funzionali alla realizzazione o gestione di reti 5G e cloud di notificare alla Presidenza del Consiglio dei ministri un **piano annuale di acquisti ICT**. L'istruttoria governativa si articola in un **termine ordinario di 30 giorni**, suscettibile di proroga fino a 40 giorni complessivi (20+20 giorni) per accertamenti tecnici svolti dal CVCN e dall'ACN, per saggiare la presenza di **fattori di vulnerabilità tecnologica** derivanti da fornitori extra-UE soggetti al controllo o all'influenza di governi autoritari.

In tale solco si inseriscono l'**art. 14 della legge 28 giugno 2024, n. 90** e l'attuativo **d.P.C.M. 30 aprile 2025**, che strutturano un doppio binario tra requisiti tecnici oggettivi (Allegati 1 e 2, inclusa la distinta base del software o *Software Bill of Materials*) e selettività geoeconomica (Allegato 3 per i soggetti del perimetro). La norma primaria prevede che, nelle procedure relative a beni e servizi ICT impiegati in contesti strategici, le stazioni appaltanti *«stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento»*, assegnando peso preponderante alla **qualità della sicurezza cibernetica** e criteri premiali per le tecnologie originarie di Paesi dell'Unione europea, della NATO o di Stati partner qualificati.

L'art. 14 della legge n. 90 del 2024 circoscrive la discrezionalità economica delle stazioni appaltanti nelle committenze critiche, subordinando la convenienza di prezzo alla sovranità tecnologica e alla sicurezza cibernetica della filiera industriale nazionale.

La giurisprudenza di merito e di legittimità ha confermato la rigorosa rispondenza di tali cautele all'interesse generale dello Stato. Da un lato, il giudice amministrativo campano ha ritenuto pienamente legittima la revoca di una gara per la sicurezza infrastrutturale e la sua successiva reindizione determinata dalla sopravvenienza di nuovi standard tecnici regolamentari, escludendo che il mero dispiegamento delle offerte economiche consolidi un affidamento tutelabile in capo ai partecipanti[6]. Dall'altro lato, il Consiglio di Stato ha sancito che le stazioni appaltanti godono della facoltà di escludere motivatamente gli operatori economici e le imprese ausiliarie provenienti da Paesi terzi non firmatari dell'Accordo sugli Appalti Pubblici (AAP), atteso che per tali soggetti l'accesso al mercato interno non è garantito in assenza di vincoli internazionali di reciprocità[7].

4.3 — Conseguenze civilistiche e amministrative: inefficacia delle clausole e risoluzione del contratto

L'inosservanza delle prescrizioni impartite in sede di golden power o l'esecuzione di contratti in violazione dei divieti governativi produce **effetti invalidanti di ordine pubblico**. Il comma 5 dell'art. 1-bis commina la **nullità testuale dei contratti** stipulati in contrasto con le prescrizioni o i veti statali, abilitando l'esecutivo a ingiungere all'impresa il ripristino a proprie spese della situazione anteriore, con l'irrogazione di **sanzioni pecuniarie fino al 3% del fatturato** globale del soggetto inadempiente.

Nel contesto della **sicurezza nazionale nei contratti pubblici**, l'insorgenza di un divieto o di una prescrizione governativa incompatibile con le soluzioni tecniche offerte dall'aggiudicatario determina la **risoluzione per impossibilità sopravvenuta** del rapporto negoziale o l'obbligo per la stazione appaltante di esercitare i poteri di autotutela decadenziale. Tuttavia, operando un doveroso **distinguishing** rispetto alle ipotesi ordinarie di esclusione morale, il Consiglio di Stato ha precisato che la valorizzazione di rischi geopolitici o di legami azionari con potenze straniere non può risolversi in presunzioni astratte: l'esclusione di un operatore per presunte ingerenze informative deve poggiare su **valutazioni giuridiche ed elementi probatori rigorosi**, non integrando di per sé la fattispecie del grave illecito professionale in difetto di un accertamento puntuale della stazione appaltante[8].

Si configura in tal modo un delicato equilibrio tra le esigenze inderogabili di **tutela della sicurezza della Repubblica** e il rispetto dei principi generali dell'azione amministrativa, imponendo una motivazione tecnica analitica e verificabile in ogni segmento procedurale, a tutela delle prerogative difensive dei concorrenti in sede giurisdizionale.

05. IL CONTENZIOSO AMMINISTRATIVO: SINDACATO GIURISDIZIONALE E TUTELE

5.1 — Il perimetro del sindacato del giudice amministrativo tra discrezionalità tecnica e politica

La tutela giurisdizionale contro i provvedimenti che precludono l'accesso alle gare pubbliche o incidono sull'esecuzione contrattuale per ragioni di **sicurezza nazionale nei contratti pubblici** sconta le peculiarità del **sindacato di legittimità sugli atti ad alta discrezionalità**. Il giudice amministrativo è chiamato a presidiare la frontiera tra conformità alla legge e insindacabile merito politico. Nel valutare le esclusioni motivate dalla tutela di interessi strategici

statali o dall'imposizione di veti cibernetici, l'organo giudicante esercita un **controllo estrinseco di ragionevolezza**, verificando che la determinazione autoritativa non risulti inficiata da palese travisamento dei fatti, manifesta illogicità o difetto istruttorio.

In questa prospettiva, il Consiglio di Stato ha chiarito che, laddove la lex specialis qualifichi determinati requisiti di sicurezza come prescrizioni mandatorie a pena di esclusione, la stazione appaltante non può degradarli a meri impegni esecutivi, dovendo accertare la **conformità tecnica dell'offerta** sin dalla fase di ammissione al confronto selettivo, ferma restando l'intangibilità dell'**apprezzamento tecnico-discrezionale** operato dalla commissione in assenza di macroscopiche incongruenze [9].

Parimenti, la giurisprudenza di prime cure ha confermato la pienezza e l'ampiezza preventiva dei poteri speciali dello Stato, statuendo che le prescrizioni governative dirette a preservare la continuità aziendale e gli **attivi strategici tecnologici** sono legittimamente imposte anche a fronte di complesse operazioni finanziarie, senza che l'operatore possa lamentare una lesione sproporzionata della libertà di impresa qualora la misura risulti funzionale a evitare **vulnerabilità sistemiche nei mercati critici** [10]. A differenza di quanto avviene nei controlli antitrust, l'intervento statale non mira a ripristinare assetti competitivi ma a prevenire minacce esterne all'incolumità economica della nazione.

5.2 — Gli oneri probatori e motivazionali gravanti sulla stazione appaltante e sul governo

Sebbene la discrezionalità esecutiva sia particolarmente intensa, la tutela dell'operatore economico esige il rispetto di rigorosi **oneri di motivazione e trasparenza**. Come autorevolmente osservato dalla dottrina, l'evocazione generica della sicurezza nazionale non può fungere da esimente assoluta per decisioni arbitrarie o protezionistiche: la stazione appaltante e l'autorità governativa sono tenute a delineare con puntualità le **ragioni tecniche ed economico-giuridiche** che giustificano il sacrificio del principio di concorrenza [D3].

Sul piano governativo, il Consiglio di Stato ha evidenziato la natura bifasica del procedimento di golden power, distinguendo la fase propedeutica di carattere istruttorio dalla **valutazione politica collegiale** del Consiglio dei ministri. Il massimo organo di vertice è legittimato a ponderare le ripercussioni strategiche dell'operazione sulla scorta della postura internazionale del Paese, senza che lo scostamento dalle proposte ministeriali integri di per sé un **vizio di eccesso di potere**, purché emerga un'istruttoria approfondita circa la rilevanza degli asset coinvolti [11].

Nei procedimenti in cui rilevino atti classificati o **informazioni coperte da riservatezza**, la giurisprudenza amministrativa ha delineato un equilibrato contemperamento: se da un lato la motivazione del provvedimento può legittimamente richiamare *per relationem* le informative secretate, dall'altro lato la garanzia del giusto processo impone che la **documentazione secretata sia ostesa in giudizio** al collegio e ai difensori costituiti con idonee cautele formali, assicurando l'effettività della difesa e il **principio della parità delle armi** [12]. L'onere della prova grava sulla parte pubblica, che non può sottrarsi al controllo giudiziale eccependo mere esigenze astratte di tutela.

5.3 — Quali tutele effettive residuano per l'operatore economico escluso per ragioni di sicurezza nazionale?

L'operatore economico escluso per ragioni di sicurezza nazionale può esperire l'impugnazione giurisdizionale innanzi al giudice amministrativo per contestare vizi di eccesso di potere, travisamento o difetto istruttorio, richiedendo l'accesso documentale anche con stralcio difensivo; tuttavia, l'annullamento dell'atto determina esclusivamente la riedizione del potere valutativo della stazione appaltante, escludendo automatismi risarcitori.

Il quadro dei rimedi processuali azionabili dal concorrente o dal fornitore attinto da determinazioni escludenti o veti governativi si riassume schematicamente nella seguente tabella comparativa:

Strumento di Tutela	Presupposti e Contenuto dell'Azione	Portata ed Effetti della Decisione Giudiziale
Annullamento Giurisdizionale	Impugnazione ex art. 120 c.p.a. per travisamento dei fatti, difetto di istruttoria o carenza motivazionale.	Caducazione del provvedimento con riserva di riesame e riesercizio motivato del potere amministrativo.
Accesso Difensivo agli Atti	Istanza di ostensione delle relazioni tecniche e dei pareri CVCN o del gruppo di coordinamento.	Visione documentale con oscuramento o trasmissione riservata al solo difensore tecnico nominato.
Subentro nel Contratto	Domanda ex art. 124 c.p.a. subordinata all'accertamento della conformità della propria offerta tecnica.	Precluso o subordinato alla compatibilità con i presidi di sicurezza nazionale e alla riedizione della gara.
Risarcimento per Equivalente	Dimostrazione della colpa grave dell'amministrazione e della spettanza certa del bene della vita.	Di regola escluso stante l'ampia discrezionalità tecnica e politica rimessa all'autorità pubblica.

Sul versante dell'opposizione governativa alle operazioni tecnologiche transfrontaliere, il Consiglio di Stato ha precisato che la natura strategica e potenzialmente duale dei beni va accertata secondo un **criterio oggettivo e sostanzialistico**, svincolato dalle qualificazioni formali della parte privata; ove l'attività produttiva sia destinata a svolgersi sotto la giurisdizione di uno Stato terzo con conseguente impossibilità pratica di vigilare sull'osservanza di prescrizioni mitigative, risulta pienamente legittimo l'esercizio del **potere di veto integrale**, restando precluse le pretese indennitarie o risarcitorie dell'operatore [13].

Infine, nell'ipotesi in cui l'amministrazione governativa abbia imposto prescrizioni sproporzionate o prive di adeguato supporto istruttorio, il T.A.R. Lazio ha precisato che il giudice annulla il decreto nei limiti delle misure non sorrette da idonea base fattuale, restituendo alla Presidenza del Consiglio la **facoltà di rinnovare l'esercizio del potere** speciale previa corretta ponderazione degli elementi informativi acquisiti [14]. Si conferma così la centralità di una difesa tecnica rigorosa in grado di contestare la congruità dell'istruttoria senza pretendere una sostituzione diretta del giudice nell'apprezzamento dell'interesse nazionale.

06. CONCLUSIONI: VERSO UN MODELLO INTEGRATO DI PROCUREMENT PUBBLICO ORIENTATO ALLA SOVRANITÀ DIGITALE

Il quadro ricostruttivo delineato dimostra come la **sicurezza nazionale nei contratti pubblici** abbia superato la configurazione tradizionale di mera deroga episodica per assurgere a **principio regolatore strutturale** delle

committenze telematiche e digitali. La convergenza coordinata tra il codice dei contratti pubblici, il perimetro di sicurezza cibernetica, i livelli di qualificazione cloud dell'ACN e i poteri speciali governativi di golden power testimonia il passaggio verso un modello avanzato di **sovranità tecnologica repubblicana**.

In tale nuovo assetto ordinamentale, l'autonomia negoziale delle stazioni appaltanti si trova conformata da stringenti **obblighi di conformità tecnica** e vincoli di interoperabilità sovrana, mentre gli operatori economici sono chiamati a garantire la **tracciabilità della catena di fornitura ICT** e la trasparenza degli assetti proprietari. L'affermazione di vincoli inderogabili sui flussi informativi e la valorizzazione della localizzazione geografica delle infrastrutture computazionali costituiscono presidi irrinunciabili per prevenire **rischi di compromissione sistemica** e ingerenze esterne ostili.

Al contempo, l'intensa discrezionalità riconosciuta alle autorità pubbliche impone un rigoroso rispetto dei canoni di **proporzionalità dell'azione amministrativa** e un puntuale assolvimento dell'onere motivazionale. Il contenzioso giurisdizionale conferma che l'equilibrio tra salvaguardia degli interessi vitali dello Stato e tutela della concorrenza risiede nell'effettività del **sindacato di legittimità estrinseco**, assicurando che la discrezionalità tecnica non trasmodi in arbitrio escludente e garantendo al professionista del diritto percorsi di tutela effettivi e calibrati sulla natura sostanziale degli interessi in conflitto.

FONTI UTILIZZATE

NORMATIVA DI RIFERIMENTO

Decreto legislativo 31 marzo 2023, n. 36
— Codice dei contratti pubblici, in particolare l'art. 136 sulla tutela degli interessi essenziali di sicurezza dello Stato e l'esclusione dall'applicazione del codice.

Decreto-legge 21 settembre 2019, n. 105
— Convertito con modificazioni dalla Legge 18 novembre 2019, n. 133, istitutivo del Perimetro di sicurezza nazionale cibernetica e degli obblighi di notifica al CVCN.

Decreto-legge 15 marzo 2012, n. 21
— Convertito con modificazioni dalla Legge 11 maggio 2012, n. 56, recante la disciplina dei poteri speciali dello Stato (golden power), con particolare riferimento all'art. 1-bis su reti 5G e cloud.

Legge 28 giugno 2024, n. 90
— Disposizioni in materia di rafforzamento della cybersicurezza nazionale e reati informatici, con il vincolo del tetto al 10% per il punteggio economico ex art. 14.

Decreto direttoriale Agenzia per la Cybersicurezza Nazionale 27 giugno 2024, n. 21007
— Regolamento per i servizi cloud della pubblica amministrazione (qualificazione dei servizi cloud QC1-QC4 e adeguamento delle infrastrutture digitali AI1-AI4).

Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131

— Regolamento recante criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro cibernetico.

Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54

— Regolamento attuativo sulle procedure di notifica degli affidamenti ICT e sulle verifiche tecniche del CVCN.

Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81

— Regolamento sulle notifiche degli incidenti cibernetici al CSIRT Italia e sulle misure di sicurezza del perimetro.

Decreto del Presidente del Consiglio dei Ministri 15 giugno 2021

— Individuazione delle categorie di beni, sistemi e servizi ICT destinati a essere impiegati nel perimetro di sicurezza nazionale cibernetica.

Decreto del Presidente del Consiglio dei Ministri 30 aprile 2025

— Definizione degli elementi essenziali di cybersicurezza e dei criteri di premialità per i contratti pubblici di beni e servizi informatici impiegati in contesti strategici (in attuazione dell'art. 14 della legge n. 90/2024).

GIURISPRUDENZA CITATA

1. **T.A.R. Campania, Napoli, sentenza 21 ottobre 2025, n. 6866**

— Esito: respinge il ricorso principale introduttivo, dichiara in parte inammissibile e in parte respinge il ricorso per motivi aggiunti e dichiara improcedibile il ricorso incidentale. Punto: I punteggi premiali sulla sicurezza informatica devono attenersi strettamente ai criteri prefissati dalla lex specialis (certificazione ISO 27001), senza estendere indebitamente obblighi NIS2 se non espressamente richiamati.

2. **Consiglio di Stato, sentenza 7 ottobre 2024, n. 8046**

— Esito: respinge l'appello principale e dichiara improcedibile l'appello incidentale. Punto: La qualificazione cloud dei software applicativi per la PA costituisce ordinariamente un requisito di esecuzione e non di partecipazione alla gara, salvo contraria ed espressa disposizione del bando.

3. **Consiglio di Stato, sentenza 2 luglio 2024, n. 5871**

— Esito: rigetta l'appello principale e dichiara improcedibile l'appello incidentale, confermando la sentenza di primo grado. Punto: Il requisito della disponibilità del data center primario non esige un titolo di proprietà dominicale, essendo sufficiente il pieno ed esclusivo controllo funzionale e operativo della struttura informatica mediante avvalimento o accordi infragruppo.

4. **Consiglio di Stato, sentenza 24 ottobre 2023, n. 9210**

— Esito: respinge in parte e dichiara improcedibile l'appello autonomo, accoglie in parte l'incidentale, respinge l'appello principale, conferma la sentenza e trasmette gli atti alla Corte dei conti. Punto: Nella procedura per il Polo Strategico Nazionale, i chiarimenti della stazione appaltante non possono modificare o integrare la disciplina di gara introducendo limitazioni o oneri innovativi a carico degli offerenti.

5. **Consiglio di Stato, sentenza 18 dicembre 2023, n. 10889**

— Esito: respinge l'appello principale e conferma la sentenza impugnata. Punto: Sono legittimi i criteri premiali correlati alla localizzazione europea o convenzionata della produzione degli apparati tecnici di telecomunicazione e dei centri di ricerca.

6. **T.A.R. Campania, Napoli, sentenza 16 giugno 2026, n. 3822**

— Esito: rigetta il ricorso principale e i motivi aggiunti e dichiara improcedibili i ricorsi incidentali. Punto: È legittima la revoca e la successiva reindizione della gara per l'approvvigionamento di apparati di sicurezza determinata da sopravvenuti standard tecnici di settore, non radicandosi alcun legittimo affidamento prima dell'aggiudicazione definitiva.

7. **Consiglio di Stato, sentenza n. 3721/2025**

— Esito: accoglie l'appello e, in riforma della sentenza impugnata, accoglie il ricorso di primo grado nei termini di cui in motivazione. Punto: L'accesso agli appalti pubblici degli operatori e ausiliarie di Paesi terzi non firmatari dell'accordo internazionale non è garantito e la stazione appaltante può motivatamente escluderli, ma tale esclusione non può basarsi su automatismi o integrazioni postume non previste dal bando.

8. **Consiglio di Stato, sentenza 7 novembre 2025, n. 8661**

— Esito: respinge l'appello nei sensi di cui in motivazione e conferma la sentenza impugnata. Punto: Le contestazioni riguardanti la sicurezza nazionale e le ingerenze informative estere devono fondarsi su accertamenti probatori rigorosi, non integrando automaticamente un grave illecito professionale in assenza di un puntuale apprezzamento discrezionale dell'amministrazione.

9. **Consiglio di Stato, sentenza 31 luglio 2026, n. 6153**

— Esito: accoglie l'appello, annulla l'aggiudicazione, dichiara inefficace il contratto stipulato disponendo il subentro dell'appellante e trasmette gli atti alla Procura della Repubblica. Punto: I requisiti tecnici di conformità e sicurezza qualificati come mandatori dalla lex specialis hanno natura di requisiti di partecipazione e non possono essere degradati a prescrizioni esecutive per sanare l'offerta non conforme.

10. **T.A.R. Lazio, Roma, sentenza 22 maggio 2024, n. 10275**

— Esito: respinge il ricorso introduttivo e conferma il decreto governativo impugnato. Punto: La finalità preventiva del golden power legittima l'imposizione di prescrizioni volte ad assicurare la continuità degli investimenti e la tutela degli asset tecnologici strategici anche su operazioni societarie e finanziarie complesse.

11. **Consiglio di Stato, sentenza 9 gennaio 2023, n. 289**

— Esito: respinge l'appello principale e conferma la sentenza di primo grado. Punto: La decisione governativa di esercizio dei poteri speciali assume una marcata discrezionalità politica strategica, non censurabile in sede giurisdizionale ove sia sorretta da un'istruttoria approfondita sulla strategicità degli attivi.

12. **Consiglio di Stato, sentenza 19 novembre 2019, n. 7904**

— Esito: respinge l'appello principale e conferma la sentenza di primo grado. Punto: Nei procedimenti fondati su informative riservate o secretate a tutela della sicurezza della Repubblica, la motivazione per relationem è legittima a condizione che sia garantita l'ostensione documentale riservata in sede giurisdizionale.

13. **Consiglio di Stato, sentenza n. 2180/2026**

— Esito: respinge l'appello principale e conferma la sentenza impugnata. Punto: L'esercizio del veto statale su investimenti tecnologici all'estero poggia su valutazioni sostanzialistiche della fungibilità militare e duale dei beni, precludendo il risarcimento del danno e l'automatismo delle pretese private.

14. **T.A.R. Lazio, Roma, sentenza n. 13748/2025**

— Esito: accoglie in parte il ricorso introduttivo annullando nei limiti il decreto governativo con riserva di rinnovato esercizio del potere, dichiarando inammissibili i motivi aggiunti. Punto: L'imposizione di prescrizioni golden power deve poggiare su un'adeguata e congruente base istruttoria tecnica, restituendo all'amministrazione la facoltà di riesaminare l'operazione in caso di annullamento parziale.

DOTTRINA RICHIAMATA

D1. **Antonio Cassatella**

, *Sicurezza e mercato: difficili equilibri*, in *Urbanistica e appalti*, 2026, n. 5, pp. 565-589 — Punto: Ricostruisce la transizione della sicurezza nazionale da limite esterno ed eccezionale a parametro intrinseco di qualificazione tecnica e resilienza nelle committenze pubbliche.

D2. **Manfredi Matassa**

, *Cibersicurezza, intelligenza artificiale e contratti pubblici. La sicurezza nazionale come parametro di aggiudicazione*, in *Urbanistica e appalti*, 2026, n. 5, pp. 601-615 — Punto: Analizza l'impiego della cibersicurezza e dell'intelligenza artificiale come criteri qualitativi premiali e requisiti minimi di partecipazione alle gare pubbliche.

D3. **Lorenzo Marilotti**

, *L'incidenza dei poteri di sicurezza nazionale sui contratti pubblici*, in *Urbanistica e appalti*, 2026, n. 5, pp. 590-600 — Punto: Esamina i confini applicativi dei poteri speciali dello Stato sugli affidamenti ICT e gli oneri motivazionali a carico dell'amministrazione nel contemperamento tra sicurezza e concorrenza.

FP

Federico Palumbo

AUTORE • METODO GIURIDICO

Avvocato del Foro di Roma

Si occupa di diritto civile, diritto amministrativo e diritto del lavoro. Per Metodo Giuridico firma approfondimenti e note a sentenza sui profili sostanziali e processuali del contenzioso civile e amministrativo.