GIUSTIZIA INSIEME

Diritto e Processo Amministrativo" class="voce">

Appalti pubblici e cybersicurezza

di Simone Francario

28 maggio 2025

Appalti pubblici e cybersicurezza. La disciplina speciale dell'acquisto di beni e servizi informatici nei settori sensibili dopo il DPCM 30 aprile 2025

di Simone Francario

Sommario: 1. Introduzione; 2. La disciplina generale codicistica sugli appalti pubblici dei beni e servizi informatici; 3. La disciplina speciale dettata dal DPCM 30 aprile 2025; 3.1 La collocazione degli appalti pubblici di beni e servizi informatici, disciplinati dal DPCM 30 aprile 2025, nell'ambito della sistematica della disciplina codicistica; 3.2 La partecipazione degli operatori economici extra-UE agli appalti pubblici di beni e servizi informatici disciplinati dal DPCM 30 aprile 2025, con particolare riferimento ai casi di tutela della sicurezza nazionale; 4. Osservazioni conclusive

1. Introduzione

Lo scorso 5 maggio 2025 è stato pubblicato in Gazzetta Ufficiale il DPCM 30 aprile 2025 recante "*Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale*", il quale introduce una disciplina specifica per l'acquisto, da parte della p.a., di beni e servizi informatici essenziali in settori sensibili, prevedendo importanti misure di cybersicurezza[i].

Si tratta, in particolare, di contratti pubblici aventi ad oggetto tecnologie critiche -come infrastrutture di rete, software di sicurezza, sistemi di videosorveglianza e gestione dell'accesso,

piattaforme cloud e storage, strumenti di identificazione e comunicazione- destinati ad essere utilizzati in ambiti di primaria rilevanza per la vita e la sicurezza dello Stato e delle sue articolazioni.

Tale intervento si colloca all'interno di un più ampio disegno istituzionale volto al rafforzamento della resilienza cibernetica dello Stato**[ii]**.

Negli ultimi anni, infatti, non solo a livello nazionale, ma anche a livello europeo**[iii]** e globale, si è progressivamente affermata la consapevolezza che la sicurezza nazionale non può più essere garantita esclusivamente con strumenti di difesa tradizionali, ma richiede anche un controllo attivo e consapevole degli strumenti tecnologici utilizzati dalla p.a.

Nell'ordinamento italiano, ad esempio, la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN)**[iv]**, l'adozione della Strategia nazionale di cybersicurezza**[v]** 2022-2026, le misure normative in tema di Perimetro di sicurezza nazionale cibernetica (PSNC)**[vi]** e la recente legge in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici (di cui alla legge 28 giugno 2024, n. 90) rappresentano le tappe principali di questo percorso.

In tale contesto, gli appalti pubblici di beni e servizi informatici nei settori "sensibili", qualificati tali per la presenza di interessi nazionali strategici e per esigenze di difesa nazionale, assumono un'importanza cruciale e una particolare complessità che portano ad elevare la sicurezza cibernetica dello Stato al rango di un vero e proprio principio generale**[vii]** che, nella materia specifica, affianca i principi della *par condicio* e della massima partecipazione, che tradizionalmente governano le procedure di scelta del contraente.

Il DPCM 30 aprile 2025, emanato in attuazione dell'art. 14 della legge 28 giugno 2024 n. 90, come si vedrà meglio nel proseguo, si muove esattamente su questa linea: esso mira ad assicurare che alcuni beni e servizi informatici (di natura "essenziale" o "critica"), quando vengono acquistati dalla p.a. per essere utilizzati nei suddetti settori "sensibili" (qualificati tali per la presenza di interessi nazionali strategici e per esigenze di difesa nazionale), siano intrinsecamente sicuri e provengano da soggetti potenzialmente non ostili.

A tal fine, il citato DPCM, introduce per l'acquisto di tali tecnologie requisiti di sicurezza stringenti sia sotto il profilo tecnico, imponendo il rispetto di alti livelli di cybersicurezza, sia sotto il profilo soggettivo, garantendo che l'operatore economico, qualora appartenente a Stati extra-UE, provenga da Paesi ritenuti "affidabili" sulla scorta di considerazioni geopolitiche.

L'obiettivo, evidentemente, è duplice: da un lato, prevenire l'introduzione di vulnerabilità informatiche in settori pubblici altamente sensibili; dall'altro, evitare che fornitori sotto l'influenza di potenze estere non alleate accedano a dati sensibili dell'apparato statale.

Trattandosi pur sempre di contratti pubblici, la disciplina dettata dal DPCM deve comunque necessariamente coordinarsi con le disposizioni del codice dei contratti pubblici, la cui applicazione, all'apparenza scontata, risulta tuttavia problematica sotto diversi profili.

Il presente articolo si propone pertanto di esaminare il DPCM al fine di fornirne l'inquadramento sistematico nell'ambito della disciplina nazionale dei contratti di appalto pubblici ponendo attenzione anche alle concrete ricadute operative.

A tal fine, dopo aver inquadrato il DPCM nella cornice del vigente codice dei contratti pubblici, l'attenzione si focalizzerà su alcuni profili problematici di immediata evidenza, ravvisabili nel rapporto con in contratti esclusi o con i contratti della difesa e nel chiarimento del regime di partecipazione a tali gare da parte degli operatori economici extra-UE.

2. La disciplina generale codicistica per gli appalti di beni e servizi informatici

Le direttive europee sugli appalti pubblici e sui contratti di concessione (Direttive 2014/23-24-25/UE) non contengono disposizioni specifiche riferite al settore degli appalti di beni e servizi informatici e alle relative misure di cybersicurezza**[viii]**.

Come è noto, in attuazione delle medesime direttive, il legislatore nazionale ha adottato due distinti codici. Mentre nel primo (d.lgs. 50/2016) non vi sono norme in materia di cybersicurezza, nel vigente codice dei contratti pubblici, di cui al d.lgs. 36/2023, sono state invece introdotte due disposizioni specifiche: l'art. 19, co. 5, e l'art. 108, co. 4**[ix]**.

L'art. 19, co. 5, del d.lgs. 36/2023, allo scopo di tutelare la sicurezza cibernetica delle gare pubbliche generalmente considerate impone a tale fine una serie di obblighi in capo sia alle stazioni appaltanti, sia agli operatori economici**[x]**.

Da un lato, la norma stabilisce che le stazioni appaltanti e gli operatori economici che prendono parte alle procedure di evidenza pubblica -che, giova ricordare, devono svolgersi in forma digitalizzata- hanno l'obbligo di adottare misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali**[xi]**.

Dall'atro, rivolgendosi alle sole stazioni appaltanti, la norma stabilisce che queste ultime hanno l'ulteriore obbligo di assicurare e curare la formazione del personale addetto alle gare,

garantendone anche il costante aggiornamento**[xii]**.

L'altra disposizione codicistica che viene in rilievo, come anticipato, è l'art. 108, co. 4, specificamente dedicato all'acquisto di beni e servizi informatici da parte della p.a**[xiii]**.

Nello specifico la norma prevede che, nelle procedure di evidenza pubblica aventi ad oggetto beni e servizi informatici, le stazioni appaltanti, al fine di individuare l'offerta economicamente più vantaggiosa, devono sempre tenere in considerazione gli elementi di cybersicurezza**[xiv]**.

Ciò posto in via generale, quando l'acquisto delle predette tecnologie è connesso alla "*tutela degli interessi nazionali strategici*" l'amministrazione ha l'obbligo di attribuire alla componente della cybersicurezza una importanza ancora maggiore, o meglio uno "*specifico e peculiare rilievo*". In tali casi, infatti, le stazioni appaltanti devono limitare il peso dell'offerta economica entro il 10% del punteggio complessivo, attribuendo quindi alla componente tecnica dell'offerta (comprensiva delle misure di cybersicurezza cui deve essere dato "*specifico e peculiare rilievo*") un peso percentuale di almeno il 90% del punteggio complessivo**[xv]**.

Le disposizioni sopra esaminate esauriscono la disciplina dettata dall'attuale codice dei contratti pubblici in materia che quindi risulta contenuta essenzialmente in due soli articoli**[xvi]**.

Il primo (art. 19, co. 5) non si riferisce direttamente agli appalti pubblici di beni e servizi informatici ma mira a tutelare la sicurezza cibernetica delle procedure di *procurement* in generale.

Il secondo (art. 108, co. 4), invece, si riferisce proprio a questa particolare tipologia di contratti pubblici ed è finalizzata a garantire, in ultima analisi, che le tecnologie acquistate dalla p.a. siano "sicure" ed abbiano idonee garanzie di cybersicurezza.

L'elemento della cybersicurezza, dunque, rappresenta il nucleo centrale della disciplina già recata dal codice in materia di contratti pubblici di beni e servizi informatici, il cui acquisto non può prescindere dalla presenza di misure di sicurezza informatica, le quali dovranno essere sempre tenute in considerazione e, qualora impattino su settori connessi alla tutela di interessi nazionali strategici, dovranno essere valutate con specifico e peculiare rilievo.

Per quanto riguarda la formulazione dell'art. 108, co. 4, come visto, la norma risulta formulata in modo ampio e generico (i.e., non viene stabilito, a monte, quali sono gli elementi di cybersicurezza da tenere obbligatoriamente in considerazione oppure le modalità con cui valutare il loro impatto complessivo sull'offerta) con la conseguenza che spetterà alle singole stazioni appaltanti, nell'esercizio dei propri poteri discrezionali, il compito (assai delicato) di

"tenere in considerazione" o di attribuire "specifico e peculiare rilievo" agli elementi di cybersicurezza dei prodotti o dei servizi informatici da acquistare.

Questo approccio, che lascia ampi spazi di discrezionalità alle stazioni appaltanti, da un lato, ha il pregio di valorizzare il soddisfacimento "su misura" oppure "*taylor made*" dei fabbisogni tecnologici del soggetto pubblico**[xvii]**; dall'altro, venendo a mancare standard uniformi -seppur minimi- di cybersicurezza risulta problematico sia perché rischia di non assicurare il medesimo livello di protezione alle diverse amministrazioni, sia perché lascia margini interpretativi per la definizione degli "interessi nazionali strategici" che farebbe scattare obblighi più stringenti sul versante della cybersicurezza, con conseguente mancanza di uniformità.

3. La disciplina speciale dettata dal DPCM 30 aprile 2025

Il recente DPCM 30 aprile 2025, come anticipato, si inserisce da ultimo nell'ambito della strategia nazionale di rinforzo della sicurezza cibernetica delle tecnologie utilizzate dalla p.a. e reca una disciplina specifica per alcuni appalti pubblici di beni e servizi informatici, ritenuti "cruciali" per il corretto funzionamento dello Stato e delle sue articolazioni e dunque meritevoli di una maggior tutela sul versante cibernetico e informatico.

È opportuno chiarire fin da subito che il DPCM in oggetto non si applica indistintamente a tutti gli appalti pubblici aventi ad oggetto tecnologie. Esso si applica solamente agli appalti pubblici di beni e servizi informatici impiegati in due settori specifici, ovverosia: i) in contesti connessi alla tutela di interessi nazionali strategici**[xviii]**; ii) in contesti connessi alla tutela della sicurezza nazionale.

Ciascun contesto di riferimento, poi, è destinatario di una specifica disciplina *ad hoc* che mira a garantire che le tecnologie ivi impiegate rispettino elevati standard di cybersicurezza.

In merito al primo "contesto", relativo alla tutela di interessi nazionali strategici, il DPCM prevede, in sostanza, che le pubbliche amministrazioni**[xix]** e i soggetti privati inseriti nel PSNC, qualora intendano acquistare taluni beni e servizi informatici elencati nell'allegato 2 al DPCM, devono assicurarsi che tali tecnologie posseggano gli elementi essenziali di cybersicurezza indicati nell'allegato 1 al DPCM.

Il decreto in esame fa riferimento, più precisamente, a beni e servizi informatici**[xx]** a forte impatto sul piano cibernetico e spesso interconnessi con altre infrastrutture critiche, quali, ad esempio, software di sicurezza, apparati di rete, piattaforme di gestione dei dati, sistemi di videosorveglianza, sistemi "cloud" e di "storage", dispositivi di autenticazione e strumenti di

controllo degli accessi, la cui elencazione completa (e tassativa) è contenuta nell'allegato 2.

La natura di tali tecnologie, unitamente al loro impiego in contesti connessi alla tutela di interessi nazionali strategici rende necessaria e indispensabile la presenza di misure di cybersicurezza rafforzate.

Sotto quest'ultimo profilo il DPCM fa riferimento alla necessaria presenza di "elementi essenziali di cybersicurezza"**[xxi]**, elencati nel dettaglio all'interno dell'allegato 1 al DPCM, i quali, in via esemplificativa, ricomprendono: la protezione da accessi non autorizzati; sistemi di autenticazione e gestione dell'identità; sistemi di protezione della riservatezza e dell'integrità di dati, personali o di altro tipo; caratteristiche tecniche e funzionali che mirano a prevenire vulnerabilità informatiche; la disponibilità di aggiornamenti di sicurezza tempestivi e certificati.

Anche se sul punto il DPCM è silente, la presenza dei citati "elementi essenziali di cybersicurezza" costituisce un primo filtro selettivo per la ricerca della contraente privato per la pubblica amministrazione, introducendo, più che una modalità di valutazione delle offerte, una condizione di ammissibilità delle medesime. Il DPCM, infatti, non stabilisce che i requisiti di cybersicurezza costituiscano elementi premiali, ma al contrario impone che le tecnologie che la pubblica amministrazione intenda acquistare debbano necessariamente e inderogabilmente possedere specifici requisiti tecnici.

In sede di gara, dunque, alla luce della normativa appena esaminata, deve ritenersi che possano essere valutate esclusivamente le offerte che dimostrino la piena conformità agli standard di cybersicurezza previsti. Ne consegue, *a contrario*, che un'offerta anche economicamente più vantaggiosa rispetto alle altre, ma che difetti dei richiamati requisiti di cybersicurezza, debba essere dichiarata inammissibile in quanto non strutturalmente conforme alla disciplina speciale di settore.

Per quanto riguarda il secondo ambito di applicazione del DPCM 30 aprile 2025, ovverosia quello relativo agli appalti pubblici di beni e servizi informatici ove vengono in rilievo esigenze di tutela della sicurezza nazionale, la disciplina ivi contenuta presenta un approccio diverso.

In primo luogo viene delimitato con più precisione l'ambito oggettivo di applicazione della disciplina.

Ai sensi dell'art. 4, co. 1, del DPCM, è espressamente previsto che i casi in cui vengono in rilievo esigenze di tutela della sicurezza nazionale sono quelli in cui le tecnologie di cybersicurezza sono destinate ad essere impiegate dai soggetti inclusi nel PNSC**[xxii]** e riguardano le reti, i sistemi

informativi e i servizi informatici "*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 dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica*"**[xxiii]**, ovvero che sono funzionali alla loro protezione fisica e logica.

In tali casi si applicano criteri di premialità, in maniera paritaria ed uniforme, alle proposte o alle offerte che contemplino l'uso di tecnologie di cybersicurezza provenienti, oltre che dall'Italia, da Paesi ritenuti "affidabili" e segnatamente: da Paesi appartenenti all'Unione europea; da Paesi aderenti all'Alleanza atlantica (NATO); da Paesi terzi individuati nell'allegato 3 del DPCM**[xxiv]**.

Emerge in modo chiaro che, nel contesto della sicurezza nazionale, più che sul profilo oggettivo della fornitura, il DPCM in esame pone l'accento in modo particolare sul profilo soggettivo dei fornitori, e in particolare sulla loro affidabilità e sicurezza desunte sulla base di considerazioni essenzialmente geopolitiche e diplomatiche.

Il DPCM, tuttavia, non specifica ulteriormente il contenuto dei sopra richiamati criteri di premialità né le loro modalità di applicazione, così come non contiene una disciplina specifica attraverso cui valutare l'affidabilità e la sicurezza dei predetti operatori economici.

In assenza di una specifica regolamentazione sul punto, dovrebbe trovare applicazione la relativa disciplina contenuta nel codice dei contratti pubblici oppure, eventualmente, la disciplina contenuta negli accordi internazionali che vengono in rilievo.

Infine, deve essere notato che l'art. 4 del DPCM 30 aprile 2025, che esaurisce la disciplina in materia di contratti pubblici di tecnologie in casi in cui vengono in rilievo esigenze di tutela della sicurezza nazionale, non specifica nel dettaglio (come lo stesso DPCM fa a in merito agli appalti pubblici di tecnologie impiegate in contesti connessi alla tutela di interessi nazionali strategici) quali sono le tecnologie coinvolte e/o i relativi requisiti di cybersicurezza, né richiama espressamente gli allegati 1 e 2. Esso si riferisce esclusivamente a "proposte" e "offerte che contemplino l'uso di tecnologie di cybersicurezza"**[xxv]**, senza ulteriori specificazioni.

Non è quindi chiaro se, e in che misura, l'elenco dei beni e servizi contenuti nell'allegato 2, così come gli elementi essenziali di cybersicurezza contenuti nell'allegato 1 trovino applicazione anche in tale ambito. Il silenzio del legislatore su questo punto apre a diverse opzioni interpretative. Ad esempio, una interpretazione restrittiva (ma più giustificabile in punto di diritto e coerente sotto il profilo sistematico e testuale) potrebbe sostenere, senza troppo margine

di errore, che in assenza di un richiamo esplicito gli allegati 1 e 2 del DPCM non si applichino in questo caso. Ne deriverebbe che le offerte "premiate" potrebbero riguardare anche tecnologie non tipizzate (non solo quelle indicate nell'allegato 2 del DPCM) e che i requisiti essenziali di cybersicurezza (indicati nell'allegato 1 del DPCM) non costituirebbero un requisito tecnico minimo dell'offerta. Si tratta, tuttavia, di una questione aperta, che potrà essere chiarita solo attraverso la prassi applicativa o eventuali interventi interpretativi del legislatore.

3.1. La collocazione degli appalti pubblici di beni e servizi informatici, disciplinati dal DPCM 30 aprile 2025, nell'ambito della sistematica della disciplina codicistica

Una prima questione interpretativa di un certo rilievo concerne la qualificazione giuridica degli appalti pubblici disciplinati dal DPCM 30 aprile 2025.

Considerato che tali contratti sono sottoposti ad una disciplina speciale e si riferiscono ad un ambito caratterizzato dalla presenza di interessi nazionali strategici e da esigenze di sicurezza nazionale, i primi dubbi da sciogliere impongono di chiarire se tali contratti rientrino nell'ambito dei c.d. contratti esclusi dall'ambito di applicazione del Codice dei contratti pubblici oppure se restino comunque all'interno del perimetro codicistico attratti nell'ambito della disciplina speciale dettata per gli appalti della difesa; ovvero se rientrino nella disciplina generale del codice pur se con le specialità recate dal DPCM.

Come è noto, il Codice contempla anche la categoria dei contratti c.d. esclusi, per tali intendendosi i contratti pubblici che, per espressa previsione legislativa, sono sottratti, in tutto o in parte, dall'ambito di applicazione del codice dei contratti pubblici**[xxvi]**.

La *ratio* alla base di tale esclusione, è altrettanto noto, si rinviene nella peculiare ed eterogenea natura degli interessi e delle ragioni sottese alla loro aggiudicazione, quali, ad esempio, il carattere *intuitu personae* del contratto, motivi di riservatezza o segretezza, la dimensione internazionale del mercato nonché il rispetto di delicati equilibri politico-diplomatici.

La rilevanza di tali interessi può giustificare che la disciplina di tali contratti sia demandata a fonti normative autonome e settoriali, estranee al codice.

Come si è visto nei paragrafi che precedono, gli appalti pubblici di beni e servizi informatici regolati dal DPCM 30 aprile 2025 presentano effettivamente molte di queste caratteristiche: sono caratterizzati dalla presenza di rilevanti e sensibili interessi nazionali, si rivolgono ad una platea internazionale, coinvolgono delicate considerazioni di carattere politico-diplomatico e sono soggetti ad una disciplina specifica dettata ad hoc dallo stesso DPCM.

La compresenza di tutti questi elementi e considerazione potrebbe indurre a collocare tali contratti al di fuori della disciplina codicistica.

Tuttavia, né il codice dei contratti pubblici, né le direttive comunitarie cui esso dà attuazione, né il DPCM 30 aprile 2025, prevedono, espressamente o implicitamente, che tali contratti rientrino nell'ambito dei contratti esclusi e che debbano essere conseguentemente assoggettati ad una diversa disciplina extracodicistica.

Non potendosi prescindere da una espressa indicazione legislativa in tal senso, è quindi evidente che i contratti pubblici regolati dal DPCM in esame, sebbene posseggano spiccati elementi di specialità, rientrano nel perimetro della disciplina codicistica la cui inclusione, tra l'altro, è del tutto coerente con la disciplina speciale recata dallo stesso DPCM che non introduce, ad esempio, diverse modalità o procedure di aggiudicazione, ma insiste, essenzialmente, sui requisiti tecnici minimi delle offerte e sui requisiti soggettivi premiali da attribuire ad alcuni operatori economici.

Rimanendo nell'ambito della disciplina codicistica, è poi comunque da escludere che il richiamo fatto agli interessi nazionali strategici e alle esigenze di sicurezza nazionale valga a consentire la collocazione degli appalti disciplinati dal DPCM 30 aprile 2025 nella categoria degli appalti nel settore della difesa e della sicurezza regolati dall'art. 136 del d.lgs. 36/2023.

Sia l'espresso riferimento a "interessi strategici nazionali" ed a "esigenze di sicurezza nazionale", sia il fatto che molti beni e servizi informatici oggetto del DPCM potrebbero essere impiegati in contesti militari o "*dual use*", possono originare il dubbio che tali appalti rientrino nella disciplina del citato art. 136, il quale prevede che "*le disposizioni del codice si applicano ai contratti aggiudicati nei settori della difesa e della sicurezza*" ad eccezione dei contratti che: a) rientrano nell'ambito di applicazione del d.lgs. 15 novembre 2011 n. 208 (recante "Disciplina dei contratti pubblici relativi ai lavori, servizi e forniture nei settori della difesa e sicurezza, in attuazione della direttiva 2009/81/CE"); b) ai quali non si applica nemmeno il d.lgs. 208/2011, in virtù dell'art. 6 del medesimo.

Tuttavia, l'ambito oggettivo del DPCM appare più ampio e generale: non riguarda necessariamente beni o servizi tecnologici progettati in modo specifico per scopi militari, né si limita a forniture destinate al Ministero della Difesa o ad altri enti del comparto difensivo. Al contrario, il decreto si rivolge alla generalità delle amministrazioni pubbliche, nonché ai soggetti privati inseriti nel PSNC.

Non pare dunque che i contratti regolati dal DPCM 30 aprile 2025 possano essere di per sé ricompresi in quelli della difesa, salvo ovviamente il caso che l'oggetto della fornitura sia costituito da beni o servizi tecnologici espressamente progettati per fini difensivi.

In linea generale la disciplina prevista dal DPCM 30 aprile 2025 non è dunque riconducibile nel perimetro degli appalti della difesa almeno fintanto che riguardi specificamente forniture di natura militare in senso stretto.

I contratti d'appalto disciplinati dal DPCM 30 aprile 2025, quindi, pur se caratterizzati dalla presenza di interessi nazionali strategici e di esigenze di difesa nazionale non sono dunque riconducibili nell'ambito dei c.d. contratti esclusi, né in quello degli appalti nei settori della difesa e sicurezza atteso che l'ambito oggettivo del DPCM è più ampio.

Alla luce delle considerazioni svolte, dunque, a livello di inquadramento sistematico, gli appalti pubblici presi in considerazione dal DPCM 30 aprile 2025 rientrano nell'ambito della disciplina generale dettata dal codice dei contratti pubblici, con la conseguenza che, in linea di principio, le procedure di aggiudicazione di tali contratti saranno disciplinate dai principi e dalle norme ordinarie contenute nel d.lgs. 36/2023.

Si deve tuttavia considerare che il DPCM, per quanto sia una fonte secondaria, introduce elementi di specialità della disciplina con specifico riferimento all'introduzione di requisiti minimi di cybersicurezza in punto di presentazione delle offerte e di un maggior *favor* verso la partecipazione di operatori economici appartenenti a Paesi ritenuti sicuri sulla scorta di valutazioni diplomatiche e geopolitiche.

Non si può pertanto ignorare che sotto tale profilo le disposizioni del DPCM integrano con carattere di specialità la disciplina generalmente dettata dal codice dei contratti pubblici. Si può tuttavia ritenere che la disciplina in parte derogatoria introdotta dal DPCM si muova comunque nel rispetto del principio di legalità e della gerarchia del sistema delle fonti in quanto il decreto è stato emanato in attuazione di una specifica norma di legge, l'art. 14 della l. 90/2024, che sotto questo profilo offre idonea copertura legislativa.

3.2. La partecipazione degli operatori economici extra-UE agli appalti pubblici di beni e servizi informatici disciplinati dal DPCM 30 aprile 2025, con particolare riferimento ai casi di tutela della sicurezza nazionale

Una seconda questione interpretativa di rilievo concerne l'individuazione delle condizioni di partecipazione delle imprese stabilite in Paesi extra-UE alle gare pubbliche per l'affidamento dei

contratti disciplinati dal DPCM 30 aprile 2025, soprattutto in contesti connessi alla tutela della sicurezza nazionale ove il decreto in esame introduce un chiaro *favor* nei confronti di alcuni Paesi che possono anche non appartenere alla UE**[xxvii]**.

L'art. 4 del DPCM, come visto, introduce un sistema di premialità selettiva fondato sul Paese di origine delle tecnologie utilizzate nelle offerte. In base a tale disposizione, sono previsti criteri premiali per le proposte che contemplino l'uso di tecnologie di cybersicurezza provenienti da:

i) operatori economici stabiliti in Italia;

ii) operatori economici stabiliti in altri Stati membri dell'Unione europea;

iii) operatori economici stabiliti in Paesi aderenti alla NATO;

iv) operatori economici stabiliti in Paesi terzi indicati nell'allegato 3 del DPCM.

Con riguardo ai punti i) e ii) non sorgono particolari problemi di sorta: è noto che in base al codice dei contratti pubblici, tanto gli operatori economici nazionali, quanto quelli comunitari, possono partecipare alle procedure di affidamento dei contratti pubblici in condizioni di parità **[xxviii]**.

Più problematica potrebbe risultare la partecipazione degli operatori economici appartenenti ai Paesi extra-UE richiamati dal DPCM che, nello specifico, fa riferimento a Stati Uniti e Canada (quali Paesi aderenti alla NATO e non facenti parte dell'Unione europea), nonché ad Australia, Corea del Sud, Giappone, Israele, Nuova Zelanda e Svizzera (quali Paesi elencati nell'allegato 3 del DPCM).

È altrettanto noto, infatti, che la partecipazione degli operatori economici extracomunitari, al contrario di quanto avviene con gli operatori economici stabiliti nell'Unione europea, non è "automatica": la *lex specialis*, infatti, potrebbe prevedere un generale divieto di partecipazione per tali operatori; potrebbe imporre condizioni di partecipazione più gravose; oppure, al ricorrere di determinate condizioni, potrebbe garantire loro la partecipazione in condizioni di parità con gli operatori nazionali e comunitari.

L'attuale codice dei contratti pubblici, all'art. 69, prevede che "*se sono contemplati dagli allegati 1, 2, 4 e 5 e dalle note generali dell'appendice 1 dell'Unione europea dell'Accordo sugli Appalti Pubblici (AAP) e dagli altri accordi internazionali cui l'Unione è vincolata, le stazioni appaltanti applicano ai lavori, alle forniture, ai servizi e agli operatori economici dei Paesi terzi firmatari di tali accordi un trattamento non meno favorevole di quello concesso ai sensi del codice*."**[xxix]**

In altre parole, l'art. 69 del d.lgs. 36/2023 stabilisce che gli operatori economici extracomunitari possono partecipare e gareggiare in condizioni di parità con gli operatori nazionali e comunitari solamente al ricorrere di uno dei seguenti requisiti: i) l'appalto in questione rientra nell'ambito del Government Procurement Agreement (GPA; detto anche accordo internazionale sugli appalti pubblici: AAP); oppure, ii) l'appalto in questione rientra nell'ambito di un altro accordo internazionale firmato dall'Unione europea.

Il GPA**[xxx]**, richiamato dall'art. 69 del d.lgs. 36/2023, rappresenta una delle principali fonti normative sovranazionali che disciplinano la materia dei contratti pubblici e costituisce un accordo internazionale plurilaterale stipulato all'interno della World Trade Organization (WTO) **[xxxi]**. Tuttavia, tale accordo non è vincolante nei confronti di tutti i membri della WTO, ma solamente nei confronti delle parti (ovverosia degli Stati) che lo hanno espressamente sottoscritto.

Ad oggi, come risulta anche dal database ufficiale della WTO, tale accordo risulta sottoscritto da 22 Paesi**[xxxii]** tra cui, oltre all'Unione europea e i suoi Stati membri, si rinvengono anche Australia, Canada, Israele, Giappone, Corea del Sud, Nuova Zelanda, Svizzera e Stati Uniti.

Nel delimitare l'ambito oggettivo di applicazione dell'accordo occorre fare riferimento all'articolo 2 del GPA in base al quale è previsto che: i) l'accordo non si applica indistintamente a tutti gli appalti aggiudicati dagli Stati firmatari; ii) al contrario, l'accordo si applica solamente a quegli appalti specifici che ciascuno Stato firmatario, al momento della propria adesione, inserisce nell'Appendice I del GPA (c.d. "*covered procurement*").

L'Appendice I è suddivisa in più allegati ove gli Stati firmatari devono ulteriormente specificare l'ambito di applicazione oggettiva dell'accordo e, in particolare, devono indicare: i) le amministrazioni cui si applica il GPA e le relative soglie di rilevanza per l'acquisto di beni e servizi**[xxxiii]**; ii) i beni e i servizi ricompresi nell'ambito di applicazione del GPA**[xxxiv]**; iii) eventuali eccezioni all'applicazione del GPA.

Ebbene, in una gara pubblica bandita da uno dei Paesi sopra evidenziati, qualora detta gara rientri nell'ambito dei "*covered procurement*", troveranno applicazione, oltre alla normativa nazionale, anche le disposizioni contenute nel GPA, tra cui, in particolare, per quanto qui interessa, l'articolo 4.

L'articolo 4 del GPA, rubricato "*general principles*", costituisce una norma fondamentale dell'accordo in quanto reca i principi fondamentali che si applicano alle procedure di evidenza pubblica governate dal trattato.

Nello specifico, l'art. 4, ai commi 1 e 2**[xxxv]**, riporta due fondamentali regole del commercio internazionale, ovverosia: la *National treatment rule* (c.d. *Nt rule*), in base alla quale l'amministrazione deve concedere agli operatori economici degli Stati firmatari del GPA un trattamento non meno favorevole di quello che lo Stato banditore riserva alle proprie imprese e ai propri beni e servizi; e la *Most favoured nation rule* (c.d. *Mfn rule*) in base alla quale l'amministrazione non deve effettuare discriminazioni tra le imprese straniere provenienti da diversi Stati firmatari del GPA.

Quanto affermato dall'articolo 4, commi 1 e 2, del GPA si riflette (anche e soprattutto) in punto di partecipazione delle imprese extracomunitarie agli appalti aggiudicati da stazioni appaltanti italiane: in questo caso, infatti, se l'appalto bandito rientra tra i "*covered procurements*", allora, anche gli operatori economici extracomunitari potranno accedervi, in quanto destinatari di un trattamento non meno favorevole di quello riservato agli operatori economici nazionali.

Ricostruiti i tratti essenziali del quadro normativo di riferimento, a livello nazionale e internazionale, occorre a questo punto verificare se e in che modo i principi sopra richiamati si possano applicare agli operatori economici extra-UE, nei confronti dei quali il DPCM 30 aprile 2025 prevede l'applicazione di elementi premiali, nel caso in cui intendano partecipare agli appalti pubblici di beni e servizi informatici in settori connessi a esigenze di tutela della sicurezza nazionale.

Punto di partenza è l'art. 69 del d.lgs. 36/2023 il quale, in merito, rinvia al GPA.

In primo luogo, dunque, bisogna verificare se la commessa pubblica da aggiudicare rientri nell'ambito dei "*covered procurements*" del GPA, sia sotto il profilo soggettivo che sotto il profilo oggettivo.

In merito al rispetto dell'ambito soggettivo di applicazione del GPA non dovrebbero sorgere particolari problemi in quanto, si è visto, il GPA è stato sottoscritto anche da Australia, Canada, Israele, Giappone, Corea del Sud, Nuova Zelanda, Svizzera e Stati Uniti, ovverosia i Paesi ritenuti "più sicuri e affidabili" da parte del DPCM 30 aprile 2025.

Per quanto riguarda l'ambito oggettivo di applicazione del GPA, la questione non può essere risolta in via teorica in quanto occorre verificare, nel concreto, una serie di elementi fondamentali della commessa pubblica quali il valore della commessa (che deve rispettare le soglie di rilevanza indicate nell'Appendice 1), le tecnologie o i servizi richiesti (che devono coincidere con i beni e i servizi indicati nell'Appendice 1) e l'assenza di eventuali esclusioni.

Se entrambi questi profili risultano soddisfatti e l'appalto rientra nell'ambito dei "*covered procurements*" del GPA, allora nei confronti degli operatori economici extra-UE presi in considerazione dal DPCM 30 aprile 2025 troveranno applicazione, in punto di partecipazione alla procedura di evidenza pubblica, la *Mfn rule* e la *Nt rule* contenute nell'art. 4 del GPA, la cui applicazione, come visto, garantisce la partecipazione di tali operatori economici in condizioni di sostanziale parità con gli operatori economici nazionali ed UE.

Nel caso in cui non dovesse applicarsi il GPA e non dovessero trovare applicazione neanche eventuali altri accordi internazionali -stipulati tra gli Stati coinvolti nella predetta procedura di procurement ed aventi ad oggetto la reciproca apertura dei rispettivi mercati dei contratti pubblici- allora la partecipazione degli operatori economici extra-UE contemplati dal DPCM 30 aprile 2025 sarà rimessa alla discrezionalità delle singole stazioni appaltanti, le quali potranno decidere di vietarne la partecipazione, renderla più gravosa oppure consentirla in condizione di parità con gli operatori economici nazionali e comunitari.

4. Osservazioni conclusive

Il DPCM 30 aprile 2025 si inserisce in una traiettoria normativa e strategica che riflette la crescente centralità degli interessi di sicurezza cibernetica nello spazio pubblico. Il provvedimento rappresenta un primo esempio concreto di disciplina attuativa in materia di appalti pubblici di tecnologie informatiche impiegate in contesti sensibili, e come tale costituisce un tassello essenziale del nuovo assetto multilivello della sicurezza tecnologica nazionale.

Come emerso dall'analisi condotta, il DPCM delinea un doppio regime: da un lato, quello relativo ai contesti connessi alla tutela degli interessi nazionali strategici, per i quali vengono specificamente individuati beni e servizi informatici soggetti a obblighi stringenti in termini di cybersicurezza e affidabilità tecnica dell'offerta; dall'altro, quello afferente alla tutela della sicurezza nazionale, che introduce meccanismi premiali selettivi basati sull'origine geografica delle tecnologie impiegate, con chiaro riferimento alla loro provenienza da Stati ritenuti affidabili in chiave geopolitica.

È stato inoltre chiarito che, sebbene gli appalti disciplinati dal DPCM in oggetto siano caratterizzati de esigenze di tutela di interessi nazionali sensibili e di tutela della difesa nazionale, ciò non vale ad assoggettare tali contratti alla disciplina dei "contratti esclusi" o dei contratti "della difesa e sicurezza" (salvo, in quest'ultimo settore, casi particolari), ragion per cui rimangono assoggettati alle norme ordinarie dettate dal codice dei contratti pubblici integrato con la disciplina speciale prevista dal DPCM grazie alla copertura legislativa contenuta nell'art.

14 della l. 90/2024.

Non mancano, tuttavia, alcuni aspetti problematici che il DPCM 30 aprile 2025 lascia irrisolti. Tra questi, l'ampia discrezionalità riconosciuta alle stazioni appaltanti nella definizione del concetto di "interessi strategici nazionali", con il rischio di applicazioni disomogenee, e la mancata esplicita previsione, nel contesto della sicurezza nazionale, di requisiti tecnici minimi di cybersicurezza, che il DPCM sembra sostituire accontentandosi di una valutazione fondata unicamente sulla provenienza geopolitica dell'operatore economico. Lo stesso tema della partecipazione degli operatori economici extra-UE, rispetto al quale il DPCM introduce un sistema di premialità fondato su criteri geopolitici e diplomatici, rimane comunque denso di implicazioni problematiche. Tale partecipazione, alla luce dell'art. 69 del d.lgs. 36/2023 e della normativa contenuta nel GPA, può essere infatti garantita a condizione che l'appalto rientri tra i c.d. "*covered procurements*". In difetto di tale copertura, la partecipazione di tali operatori economici non è preclusa a monte, ma rimarrà soggetta alla valutazione discrezionale delle stazioni appaltanti.

[i] Tra i primi commenti sul tema, riferiti al testo originario del DDL AC1717 e della legge 28 giugno 2024 n. 90 cui il DPCM 30 aprile 2025 dà attuazione, si vedano: L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giornale di diritto amministrativo*, I, 2025, pp. 60 e ss.; G. FIORINELLI e M. GIANNELLI (a cura di), *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS 2*, in *Rivista italiana di informatica e diritto*, I, 2024; L. NANNIPIERI, *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio*, in G. FIORINELLI e M. GIANNELLI (a cura di), *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS 2*, op. cit., pp. 19 e ss.

[ii] Sul più ampio tema della regolamentazione della sicurezza cibernetica dello Stato e delle sue articolazioni, nell'ambito di una vasta letteratura si vedano *ex multis*: M. MACCHIA e G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Diritto amministrativo*, I, 2025, pp. 109 e ss.; L. MORONI, *La Governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi*, 2024, pp. 179 e ss.; M. A. RIZZI e F. SERINI, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2024, pp. 115 e ss.; P.G. CHIARA, *DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2*, in *Rivista italiana di informatica e diritto*,

2024, pp. 31 e ss.; S. ROSSA, *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, Napoli, 2023; L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi*, 2022, pp. 65 e ss.; L. PREVITI, *La gestione del rischio informatico nella decisione amministrativa robotica*, in *Rivista italiana di informatica e diritto*, 2022, pp. 67 e ss.; F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi*, 2022, pp. 241 e ss.; B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Federalismi*, 2020, pp. 11 e ss.;

[iii] Come è noto lo sviluppo e la regolamentazione della cybersicurezza in Italia si colloca, a sua volta, all'interno di una più grande strategia comunitaria volta a rinforzare e soprattutto coordinare le difese cibernetiche dei Paesi europei e dell'Unione europea.

A livello europeo, le principali tappe relative alla creazione di un quadro giuridico comune in materia di cybersicurezza sono rappresentate da: l'istituzione della European Network and Information Security Agency -ENISA- (con regolamento UE/2004/460) che costituisce l'agenzia europea destinata ad operare in materia di cybersicurezza con importanti compiti in punto di cooperazione e coordinamento dell'attività dei singoli Stati membri; la direttiva UE 2016/1148, c.d. direttiva NIS I ("Network and Information System") la quale, oltre ad istituire il sistema di governance europea in materia, *inter alia*, prevede che alcuni soggetti, quali gli "operatori dei servizi essenziali" indicati dalla direttiva (OES) e i "fornitori di servizi digitali" (FSD) che offrono servizi all'interno dell'UE, debbano adottare misure tecniche e organizzative per rendere sicure le proprie reti e i sistemi informatici e più in generale debbano garantire il rispetto di alti standard di cybersicurezza; il regolamento UE 2019/881 (c.d. Cybersecurity Act) che implementa i compiti e le funzioni dell'ENISA; la direttiva UE 2022/2555, c.d. direttiva NIS II, che abroga e sostituisce la precedente NIS I, la quale potenzia e rafforza le misure già introdotte con la precedente NIS I e conferma, tra le altre cose, l'istituzione delle autorità nazionali in materia di cybersicurezza (c.d. autorità nazionali competenti NIS).

[iv] L'Agenzia per la Cybersicurezza Nazionale è stata istituita con d.l. 14 giugno 2021, n. 82, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" e costituisce l'autorità NIS di riferimento nell'ordinamento italiano.

Sull'Agenzia per la Cybersicurezza Nazionale si vedano, *ex multis*: L. MORONI, *La Governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, op. cit.; G.G. CUSENZA, *I*

poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico , in R. URSI (a cura di), *La sicurezza nel cyberspazio*, Franco Angeli, Milano, 2023, pp. 123 e ss.; L. PARONA, *L'istituzione dell'Agenzia per la Cybersicurezza Nazionale*, in *Giornale di diritto amministrativo*, 2021, pp. 709 e ss.

[v] Ci si riferisce al documento, di carattere programmatico e di indirizzo generale, adottato dall'Agenzia per la Cybersicurezza Nazionale, che illustra le principali sfide da affrontare in tema di cybersicurezza nel quadriennio di riferimento, gli obiettivi da raggiungere e le strategie da impiegare. In particolare, la citata Strategia nazionale di cybersicurezza persegue tre obiettivi fondamentali: i. Obiettivo protezione (ovverosia "*la protezione degli asset strategici nazionali, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese. Di particolare importanza è lo sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e supply-chain a impatto nazionale*"); ii. Obiettivo risposta (ovverosia "*la risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale*"); iii. Obiettivo sviluppo (ovverosia "*lo sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze di mercato. La costellazione di centri di eccellenza e imprese che compongono, assieme all'accademia, il tessuto della ricerca e dello sviluppo è infatti un patrimonio essenziale per il nostro Paese con importanti potenzialità di espansione*"). Ai fini del presente articolo giova sottolineare che anche all'interno della Strategia nazionale di cybersicurezza, nell'ambito dell'obiettivo protezione, viene ribadito che costituisce un aspetto di particolare importanza il rafforzamento delle misure di cybersicurezza all'interno delle "*infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e supply-chain a impatto nazionale*", una formulazione molto ampia, e che data proprio la sua ampiezza sembra ricomprendere appieno la fornitura e l'approvvigionamento di beni e servizi informatici (o comunque infrastrutture ICT in genere) anche da parte di soggetti pubblici.

[vi] Il perimetro di sicurezza nazionale cibernetica è stato istituito con d.l. 21 settembre 2019, n. 105, il cui fine, a mente dell'art. 1, co. 1, del medesimo d.l., è quello di "*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, 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 dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale […].” I soggetti ricompresi nel PSNC sono individuati con separato DPCM non soggetto a pubblicazione o istanze di accesso, con la conseguenza che solo i soggetti ivi ricompresi riceveranno comunicazione della relativa iscrizione all’interno del PSNC.

In generale sul PSNC si veda, fra tutti, S. MELE, *Il Perimento di sicurezza nazionale cibernetica e il nuovo “golden power”*, in G. CASSANO e S. PREVITI (a cura di), *Il diritto di internet nell’era digitale*, Giuffrè, Milano, 2020, pp. 186 e ss.

[vii] Come evidenziato dalla dottrina, il concetto di cybersicurezza tenderebbe ormai a distinguersi e ad assumere una propria autonomia rispetto al concetto di sicurezza nazionale, pur rimanendo a questo strettamente connesso. Cfr. in ptc. M. MACCHIA e G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, op. cit., pp. 115 e ss.

Sotto questo profilo la dottrina giunge anche ad affermare che la cybersicurezza potrebbe essere qualificata come vero e proprio bene pubblico. *Ex multis* si veda R. BRIGHI e P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell’Unione Europea*, in *Federalismi*, 2021, pp. 18 e ss.

[viii] Come è stato notato da S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, II/2024, p. 340, con specifico riferimento alla mancata regolamentazione della materia da parte del legislatore comunitario, “ *le Direttive 2014/23-24-25/UE in materia di appalti e concessioni non contengono né una disciplina generale sugli appalti di cybersecurity né minime e particolari disposizioni. Questo aspetto, che di primo acchitto può essere giustificato con la riconduzione di questa materia all’ambito di stretto interesse nazionale “tradizionale” dei diversi Paesi membri (nonostante vi sia una precisa disciplina europea in materia di appalti nel settore della difesa), comporta che l’intervento in materia di appalti di cybersecurity sia demandato ai legislatori domestici*”.

Sebbene non sia presente nelle direttive europee in materia di appalti pubblici, la disciplina generale della cybersicurezza in ambito europeo si rinviene in altre fonti normative e, in particolare, nel c.d. Cybersecurity Act contenuto nel Regolamento 2019/881 e nelle altre fonti indicate *supra sub* nota 3.

[ix] In generale, sulla disciplina recata dal codice dei contratti pubblici in materia di cybersicurezza si veda T. COCCHI, *La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*, in *Munus*, I, 2024, pp. 177 e ss.

[x] Per un'analisi dettagliata della norma in esame si rinvia a G. VESPERINI, *Commento all'articolo 19*, in A. BOTTO e S. CASTROVINCI ZENNA (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino, Giappichelli, 2024, pp. 200 e ss.

[xi] Cfr. G. VESPERINI, *Commento all'articolo 19*, op. cit., p. 211, ove si sottolinea che "*La relazione del Consiglio di Stato giustifica così la norma: 'in attesa che le iniziative di regolazione dell'utilizzazione di strumenti e tecnologie digitali, anche per quanto concerne i profili di sicurezza, vengano portate a compimento e, soprattutto, concretamente attuate', le norme in esame 'sono funzionali anche a favorire la diffusione di misure, da parte delle amministrazioni, utili alla qualificazione e alla sicurezza, stimolando anche per tale via una uniformità di standard e una crescita complessiva della cultura della sicurezza informatica nella pubblica amministrazione e tra gli operatori economici'*".

[xii] Non deve essere sottovalutata l'importanza della norma sotto il profilo della formazione e del costante aggiornamento del personale amministrativo. La materia della cybersicurezza, soprattutto nel settore delle gare pubbliche, si presenta particolarmente tecnica e -soprattutto, come avviene di consueto in ambito tecnologico- è una materia caratterizzata da una rapidissima evoluzione, il che implica che la formazione e l'aggiornamento del personale delle stazioni appaltanti costituisce un presupposto fondamentale per garantire la resilienza cibernetica della p.a.

Cfr. G. VESPERINI, *Commento all'articolo 19*, op. cit., p. 212.

[xiii] Cfr. G. MACDONALD, *Commento all'articolo 108*, in A. BOTTO e S. CASTROVINCI ZENNA (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino, Giappichelli, 2024, pp. 977 e ss.

[xiv] Cfr. S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, op. cit., p. 341.

[xv] Cfr. S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, op. cit., p. 341 ove l'A. in particolare specifica che "*L'art. 108, co. 4, del Codice, invece, al quarto periodo stabilisce che nelle*

procedure di approvvigionamento di forniture e servizi informatici per l'Amministrazione Pubblica le stazioni appaltanti, e le centrali di committenza, dovendo procedere con l'aggiudicazione sulla base del criterio dell'offerta economicamente vantaggiosa, sono tenute a considerare gli elementi di cybersecurity nella valutazione dell'elemento qualitativo-tecnico dell'offerta; e qualora tali procedure siano riferibili a contesti rilevanti per gli interessi nazionali strategici, le stazioni appaltanti devono limitare la ponderazione della valutazione della componente economica dell'offerta a dieci punti percentuali del punteggio complessivo, in tal modo aumentando notevolmente "il peso" della componente tecnica dell'offerta."

[xvi] Parte della dottrina ha comunque evidenziato che l'introduzione di tali due nuove disposizioni nel d.lgs. 36/2023, sebbene abbia risvolti positivi poiché ha il merito di codificare importanti principi, d'altro lato ha comunque una "*portata limitata: vengono formalizzati due aspetti che, nella realtà dei fatti, erano presenti già prima dell'intervento normativo del 2023 – soprattutto in relazione a quelle Amministrazioni aggiudicatrici da sempre deputate agli appalti di tecnologia. Appare inesatto ritenere che, prima dell'entrata in vigore del recente Codice appalti, le stazioni appaltanti non considerassero l'elemento della cybersicurezza nella valutazione della componente tecnica dell'offerta in gare relative a forniture, servizi e processi informatici*", cfr. S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, op. cit., p. 341.

[xvii] Cfr. S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, op. cit., pp. 341-342.

[xviii] Il DPCM in esame, tuttavia, non contiene una definizione positiva della nozione di "interessi nazionali strategici." Ciò, come già evidenziato dalla dottrina, l'assenza di un'esatta perimetrazione dell'ampio concetto di "interessi nazionali strategici" costituisce una prima (e notevole) criticità del DPCM ora in esame che ne potrebbe ostacolare la corretta applicazione e generare un notevole contenzioso in una materia già di per sé altamente tecnica e relativa a interessi o contesti -comunque denominati- sensibili.

Cfr. L. NANNIPIERI, *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio*, op cit., pp. 20-21.

[xix] L'art. 1, co. 1, lett. a), del DPCM 30 aprile 2025, nel delimitare l'ambito di applicazione soggettivo della normativa, fa riferimento ai soggetti di cui all'art. 2, co. 2, del codice dell'amministrazione digitale, di cui al d.lgs. 7 marzo 2005, n. 82, il quale a sua volta rimanda all'art. 1, co. 2, del d.lgs. 30 marzo 2001, n. 165. In buona sostanza, tramite i rinvii operati dal

DPCM 30 aprile 2025, si arriva a coprire pressoché l'intera platea dei soggetti pubblici il che, tenuto conto delle finalità del DPCM in esame, potrebbe risultare sovrabbondante. Come sottolineato da L. NANNIPIERI, *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio*, op cit., p. 21, (ove l'A. si riferisce segnatamente all'art. 10 del DDL 1717 ma la cui formulazione, sul punto, è rimasta pressoché inalterata nell'attuale art. 1, co. 1, lett. a) del DPCM 30 aprile 2025) l'elenco dei destinatari della norma "*appare decisamente ampio*" e "*Come osservato in sede istruttoria (cfr. audizione dell'ANCI), l'ambito di applicazione della disposizione dovrebbe essere meglio specificato, in quanto il rinvio* per relationem *all'art. 2, co. 2, d.lgs. 82/2005 condurrebbe ad una generalizzata efficacia applicativa della disposizione anche a soggetti che non svolgono attività di approvvigionamento di beni e servizi informatici legati alla tutela di interessi nazionali strategici. Si pensi, ad esempio, alla generalità delle società a controllo pubblico, ovvero agli istituti di istruzione ovvero, ancora, alla generalità indiscriminata degli enti locali.*"

[xx] DPCM 30 aprile 2025, art. 3, il quale rinvia all'allegato 2.

[xxi] DPCM 30 aprile 2025, art. 2, il quale rinvia all'allegato 1.

[xxii] L'art. 4, co. 1, del DPCM 30 aprile 2025, si riferisce infatti ai soggetti di cui all'art. 1, co. 2bis, del d.l. 105/2019, il quale, rinviando all'art. 1, co. 2, lett. a), fa riferimento a tutti i soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel Perimetro di sicurezza nazionale cibernetica.

[xxiii] L'art. 4, co. 1, del DPCM 30 aprile 2025, rimanda alle "reti, sistemi informativi e servizi informatici" di cui all'art. 1, co. 2, lett. b) del d.l. 105/2019, il quale a sua volta rimanda all'art. 1, co. 1, del medesimo d.l. 105/2019 sopra riportato.

[xxiv] L'allegato 3 del DPCM 30 aprile 2025, fa riferimento ai Paesi terzi che sono parte di accordi di collaborazione sia con l'Unione europea sia con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. Nello specifico, tali Paesi sono: Australia, Corea del Sud, Giappone, Israele, Nuova Zelanda e Svizzera.

[xxv] DPCM 30 aprile 2025, art. 1, co. 1, lett. c).

[xxvi] Nel vigente codice dei contratti pubblici di cui al d.lgs. 36/2023 la norma di riferimento è contenuta nell'art. 13 del codice che prevede che "*le disposizioni del codice non si applicano ai contratti esclusi*".

Per quanto riguarda l'individuazione delle singole categorie di contratti esclusi, l'art. 56 individua i contratti esclusi nei settori ordinari, mentre gli artt. 141-152 recano l'elenco dei

contratti esclusi nei settori speciali.

Per un'analisi approfondita dell'art. 13 del d.lgs. 36/2023, si veda S. TOSCHEI, *Commento all'articolo 13*, in A. BOTTO e S. CASTROVINCI ZENNA (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino, Giappichelli, 2024, pp. 132 e ss.

[xxvii] In generale sul tema della partecipazione degli operatori economici extracomunitari alle procedure di evidenza pubblica bandite in Italia, seppur con riferimento alla normativa recata dal previgente codice dei contratti pubblici di cui al d.lgs. 50/2016, sia consentito il rinvio a S. FRANCARIO, *La partecipazione alle gare d'appalto pubblico degli operatori economici extracomunitari*, in *Amministrativamente*, 2022, pp. 145 e ss.

[xxviii] Cfr. D.lgs. 36/2023, art. 65.

[xxix] L'art. 69 del d.lgs. 36/2023 riprende in maniera pressoché identica l'art. 49 del previgente d.lgs. 50/2016.

Sull'inquadramento generale e sulla disciplina recata dall'art. 49 del d.lgs. 50/2016 si rinvia a F. FRACCHIA, *Fonti internazionali*, in M.A. SANDULLI e R. DE NICTOLIS (diretto da), *Trattato sui Contratti Pubblici*, Milano, 2019, II, pp. 84 e ss.

Sulla disciplina recata dall'art. 69 del d.lgs. 36/2023 si rinvia a M. MARTINELLI, *Commento all'articolo 69*, in A. BOTTO e S. CASTROVINCI ZENNA (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino, Giappichelli, 2024, p. 706.

[xxx] Nell'ambito di una vastissima letteratura, sul GPA si rinvia per tutti a S. ARROWSMITH e R.D. ANDERSON (edito da), *The WTO Regime on Government Procurement: Challenge and Reform*, Cambridge University Press, Cambridge, 2011, e ivi ulteriori riferimenti bibliografici.

[xxxi] Sulla struttura e sul funzionamento generale della WTO si vedano, *ex multis*: VAN DE BOSSCHE e D. PRÉVOST, *Essentials of WTO Law*, Cambridge, Cambridge University Press, 2016; B.M. HOEKAMN e P.C. MAVROIDIS, *World Trade Organization – Law, Economics and politics*, New York, Routledge, 2016.

[xxxii] L'Unione europea e i suoi Stati membri contano come un'unica parte in quanto il GPA è stato sottoscritto direttamente dalla prima.

[xxxiii] Segnatamente, nell'Allegato 1 vengono indicate le amministrazioni centrali e le relative soglie di rilevanza per l'acquisto di beni e servizi; nell'Allegato 2 vengono indicate le amministrazioni sub-centrali e le relative soglie di rilevanza per l'acquisto di beni e servizi;

nell'Allegato 3 vengono indicate tutte le altre amministrazioni e le relative soglie di rilevanza per l'acquisto di beni e servizi.

[xxxiv] Nell'Allegato 4 e nell'Allegato 5 vengono specificati, rispettivamente, i beni e i servizi rientranti nell'ambito di applicazione del GPA.

[xxxv] Nello specifico, l'art. 4, co. 1, del GPA prevede che "*With respect to any measure regarding covered procurement, each Party, including its procuring entities, shall accord immediately and unconditionally to the goods and services of any other Party and to the suppliers of any other Party offering the goods or services of any Party, treatment no less favourable than the treatment the Party, including its procuring entities, accords to: a) domestic goods, services and suppliers; and b) goods, services and suppliers of any other Party*."

Mentre l'art. 4, co. 2, del GPA stabilisce che "*With respect to any measure regarding covered procurement, a Party, including its procuring entities, shall not: a) treat a locally established supplier less favourably than another locally established supplier on the basis of the degree of foreign affiliation or ownership; or b) discriminate against a locally established supplier on the basis that the goods or services offered by that supplier for a particular procurement are goods or services of any other Party*."