Cybersicurezza nazionale e disciplina dei contratti pubblici: l'attuale "stratificazione" normativa e il rapporto con il principio di trasparenza*

di Giovanni Botto

1. *Premessa: il complesso equilibrio fra trasparenza e sicurezza cibernetica nell'ambito della contrattualistica pubblica*

Nel corso delle pagine che seguono si tenterà di ricostruire, tramite l'impiego di una particolare lente di osservazione, quella della trasparenza nell'ambito dei contratti pubblici, la più recente disciplina in materia di sicurezza cibernetica nazionale.

In particolar modo, come emergerà da quanto scritto di seguito, si affronteranno vari profili, con l'obiettivo di calare la riflessione all'interno

* Questo lavoro è il risultato della ricerca condotta dall'autore nell'ambito del progetto di ricerca SERICS (Partenariato Esteso PE00000014 "SERICS SEcurity and RIghts in the CyberSpace", finanziato nell'ambito del Programma PNRR del MUR – Missione 4, Componente 2, Investimento 1.3 – Avviso Pubblico "Partenariati estesi a università, centri di ricerca, imprese per il finanziamento di progetti di ricerca di base" – Decreto n. 341 del 15 marzo 2022). Inoltre, il lavoro è anche il risultato di ulteriore ricerca condotta dall'Autore nell'ambito del progetto PRIN 2022 (scorrimento) "Ordine pubblico e sicurezza informatica" (Codice progetto: 022ZNBAFS – CUP D53C24004630006).

dei diversi e via via più profondi livelli della normativa in parola, al fine di ricostruire i principali obblighi cui i soggetti coinvolti soggiacciono, la loro *ratio* rispetto al quadro complessivo della disciplina e l'equilibrio raggiunto rispetto alle esigenze di trasparenza che dovrebbero informare l'attività contrattuale della pubblica amministrazione.

Ciò posto dal punto di vista degli obiettivi dello studio, si deve senz'altro prendere avvio da una delle caratteristiche principali della disciplina dei contratti pubblici, ossia – in controtendenza rispetto al suo caratteristico tecnicismo – la diretta aderenza ad una serie di principi generali del diritto amministrativo, che ne conformano l'operatività.

Ciò è oggi particolarmente evidente in ragione della sistematizzazione approntata dal d.lgs. n. 36/2023[1], che, come noto, dedica un'ampia sezione iniziale (Libro I, Parte I, Titolo I) proprio all'enucleazione dei principi generali che debbono informare l'attività delle stazioni appaltanti nell'ambito dei procedimenti di approvvigionamento: il principio del risultato, il principio della fiducia, il principio dell'accesso al mercato, i principi di buona fede e di tutela dell'affidamento, i principi di solidarietà e di sussidiarietà orizzontale, il principio di auto-organizzazione amministrativa, il principio di autonomia contrattuale, il principio di conservazione dell'equilibrio contrattuale, i principi di tassatività delle cause di esclusione e di massima partecipazione, il principio di applicazione dei contratti collettivi nazionali di settore[2].

Ai presenti fini, è interessante notare come dalla lettura delle disposizioni concernenti i menzionati principi generali del codice dei contratti pubblici – al cui testo, per ragioni di spazio ed economia della trattazione, si rinvia – emerga un elemento fondamentale che il legislatore accosta, di volta in volta, al risultato, alla fiducia, al buon andamento, all'imparzialità e via dicendo: ossia, la trasparenza delle procedure di gara[3].

---

[1] D.lgs. 31 marzo 2023, n. 36.

[2] Non rientra fra gli obiettivi del presente scritto l'analisi specifica e approfondita di tali principi, rispetto ai quali si rimanda, fra gli altri, a F. Saitta, *I principi generali del nuovo codice dei contratti pubblici*, in *www.giustiziainsieme.it*, 8 giugno 2023; G. Rovelli, *Introduzione al nuovo codice dei contratti pubblici. I princìpi nel nuovo codice degli appalti pubblici e la loro funzione regolatoria*, in *www.giustizia-amministrativa.it*, 2023; AA.VV., *Studi sui principi del Codice dei contratti pubblici*, Napoli, 2023; R. Ursi (a cura di), *Studi sui principi generali del Codice dei contratti pubblici*, Napoli, 2024; M. R. Spasiano, D*all'amministrazione di risultato al principio di risultato del Codice dei contratti pubblici: una storia da scrivere*, in *www.federalismi.it*, 2024, 9, 206 ss.

[3] Sul punto, fra gli altri, E. Midena, *Per una trasparenza semplificata nei contratti pubblici:*

In particolare, detto canone di trasparenza, nell'ambito del nuovo codice, seppure non autonomamente valorizzato all'interno del Titolo dedicato ai principi generali, costituisce un valore comune e funzionale alla concreta applicazione dei principi generali poc'anzi riportati e assurge a vero e proprio principio generale all'inizio della Parte II, del Libro I, del codice dei contratti, dedicata alla digitalizzazione del ciclo di vita dei contratti pubblici, il cui art. 19, c. 1, afferma che «le stazioni appaltanti e gli enti concedenti […] garantiscono l'esercizio dei diritti di cittadinanza digitale e operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica».

Ancora, il successivo articolo 20 (rubricato proprio "principi in materia di trasparenza"), statuisce che «fermi restando gli obblighi di pubblicità legale, a fini di trasparenza i dati, le informazioni e gli atti relativi ai contratti pubblici sono indicati nell'articolo 28 e sono pubblicati secondo quanto stabilito dal decreto legislativo 14 marzo 2013, n. 33», «le comunicazioni e l'interscambio di dati per le finalità di conoscenza e di trasparenza avvengono nel rispetto del principio di unicità del luogo di pubblicazione e dell'invio delle informazioni» e che «le regioni e le province autonome assicurano la trasparenza nel settore dei contratti pubblici».

Il principio in parola, come noto, è caratterizzato da una doppia, importante connotazione: sotto un primo punto di vista la trasparenza consiste nella piena accessibilità dell'attività amministrativa, permettendo una forma di controllo diffuso dell'attività della pubblica amministrazione; sotto un secondo punto di vista, nell'ambito delle procedure selettive, la trasparenza consiste anche nella comprensibilità dei requisiti da soddisfare, che si riverbera sulla trasparenza della motivazione degli atti di aggiudicazione. Richiamando autorevole dottrina sul tema, si può dire che la trasparenza, pertanto, consista nella «conoscibilità delle procedure di gara, nonché dell'uso di strumenti che consentano un accesso rapido e agevole alle informazioni relative alle procedure, è funzionale alla massima

il codice dei contratti e le iniziative dell'Anac, in *Studi e ricerche 37*, 2024, 41 ss., ove si afferma che «Il principio di trasparenza è richiamato più volte nell'ultimo codice dei contratti pubblici, il d.lgs. 36/2023. La trasparenza è presente nei principi generali – risultato, fiducia e accesso al mercato – costituendo sia un 'limite' da rispettare, sia un mezzo per garantire obiettivi previsti nel codice, sia uno dei connotati ontologici dell'attività delle pubbliche amministrazioni cui si lega il principio di fiducia».

semplicità e celerità nella corretta applicazione del codice e ne assicura la piena verificabilità»[4].

Ebbene, nell'ottica che qui interessa, deve sottolinearsi, sempre in via di introduzione, che le politiche e le misure volte a garantire un elevato livello di cybersicurezza delle pubbliche amministrazioni entrano sovente in tensione – rendendo necessario un complesso bilanciamento di interessi – con le esigenze di trasparenza di cui si è appena scritto, in ragione dell'attinenza delle prime ad esigenze di sicurezza nazionale e di ordine pubblico, con cui le seconde potrebbero, invece, entrare in conflitto.

In altri termini, l'effettività delle azioni poste a protezione della sicurezza cibernetica dipende, in maniera determinante, dalla segretezza delle misure di volta in volta adottate e il grado e l'intensità della tensione tra le esigenze di segretezza e quelle di trasparenza risulta strettamente legato al livello normativo (tra quelli che si individueranno a breve) di riferimento, con il risultato di un complesso sistema normativo a geometria variabile, dal quale possono trarsi interessanti considerazioni circa il rapporto tra autorità e collettività nell'era della digitalizzazione (e dei suoi rischi).

2. *Una (seconda) precisazione a carattere introduttivo: le due diverse dimensioni d'interesse del tema concernente il rapporto tra la disciplina della dei contratti pubblici e la normativa in materia di sicurezza cibernetica*

Il rapporto tra cybersicurezza e normativa sui contratti pubblici è divenuto, nel corso degli ultimi anni, un tema di crescente rilevanza, al quale il legislatore sta dedicando sempre maggiore attenzione, a partire dal presupposto per cui la protezione dei dati, delle informazioni e delle infrastrutture digitali è essenziale non solo per garantire l'efficienza e la trasparenza delle procedure amministrative, ma anche per preservare la fiducia dei cittadini e degli utenti nei confronti delle istituzioni e del loro corretto funzionamento.

In tale contesto, la disciplina sui contratti pubblici è stata sottoposta ad un notevole processo evolutivo teso ad includere specifiche considerazioni di cybersicurezza tra i requisiti fondamentali che caratterizzano la selezione dei fornitori, l'esecuzione dei contratti e la generale gestione delle gare d'appalto. Le autorità pubbliche, infatti, sono chiamate a garan-

[4] R. Dipace, *Manuale dei contratti pubblici*, II ed., Torino, 2025, 12.

tire che i contratti stipulati con i fornitori di beni e servizi tecnologici rispettino adeguati *standard* di sicurezza informatica, al fine di prevenire i rischi legati ai diversi tipi di attacchi informatici possibili.

In altri e più chiari termini, le ragioni per cui è possibile individuare un nesso fondamentale tra le politiche pubbliche in materia di sicurezza cibernetica e la disciplina della contrattualistica pubblica sono essenzialmente due, cui corrispondono, evidentemente, le due principali dimensioni d'interesse della tematica in parola (le quali, come si vedrà, emergono direttamente dal più recente intervento del legislatore italiano in materia di contrattualistica pubblica[5]): da un lato, in ragione del fondamentale ruolo che ricoprono, sussiste l'evidente esigenza di garantire la sicurezza cibernetica delle c.d. "stazioni appaltanti" (ossia dei soggetti pubblici cui è affidato lo svolgimento delle procedure); d'altro lato, invece, s'impone la necessità di garantire che le tecnologie e i servizi informatici acquisiti (e, di conseguenza, utilizzati) dalle pubbliche amministrazioni siano sicuri, resistenti e resilienti sotto il profilo cibernetico[6].

Sotto il primo profilo, pertanto, si pone chiaramente una questione attinente alla funzione di organizzazione (o "organizzatrice"[7]) di quel

[5] D.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici), modificato e integrato dal D.lgs. 31 dicembre 2024, n. 209 (Disposizioni integrative e correttive al codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36).

[6] Da un punto di vista generale, deve notarsi sin d'ora, a prova della sua rilevanza, che l'argomento in questione è recentemente divenuto anche oggetto d'interesse dottrinale. Possono richiamarsi, ad esempio, i contributi di S. Rossa, *Cybersicurezza e pubblica amministrazione*, Napoli, 2023; Id., *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, in *Ceridap*, 2024, 2; 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*, 2024, 1, 177 ss.; L. Nannipieri, *Cybersicurezza e appalti. Interventi legislativi e prime criticità*, in *Rivista italiana di informatica e diritto*, 2024, 2, 71 ss.; S. Francario, *Appalti pubblici e cybersicurezza. La disciplina speciale dell'acquisto di beni e servizi informatici nei settori sensibili dopo il DPCM 30 aprile 2025*, in *www.giustiziainsieme.it*, 2025; M. Matassa, *La sicurezza cibernetica come funzione pubblica*, Milano, 2025; P. Heritier, S. Rossa (a cura di), *Cybersecurity e istituzioni democratiche*, Fasc. I e II, Milano, 2025.

[7] Con le parole, come noto, di M. Nigro, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano, 1966, il quale, nell'ambito del menzionato studio, poneva in evidenza il rapporto di diretta comunicanza che sussiste fra l'organizzazione di una pubblica amministrazione e la sua attitudine a svolgere le funzioni affidatele

particolare tipo di amministrazione che è costituito dalle stazioni appaltanti, ossia una problematica concernente gli strumenti, il personale e le procedure di cui dette amministrazioni dispongono e disporranno nello svolgimento delle attività che sono loro attribuite dalla legge.

Sotto il secondo profilo, invece, emergono questioni attinenti alla funzione di amministrazione attiva esercitata dalle stazioni di appaltanti, ossia, in linea di estrema sintesi, direttamente incidenti sulla costruzione dei bandi di gara e sul peso che le considerazioni relative al livello di adeguatezza e sicurezza degli strumenti da acquisire devono ricoprire in sede valutazione e comparazione delle offerte.

L'assoluta rilevanza di questo secondo, ulteriore profilo emerge chiaramente se si tiene conto, come efficacemente espresso in dottrina, della «centralità delle logiche di mercato anche […] nell'ambito della cybersicurezza», posta, infatti, «la consistente domanda di beni e servizi tecnologici delle Pubbliche Amministrazioni, le quali si vedono così chiamate all'aggiudicazione di procedure di acquisto di forniture, servizi e processi di natura *cyber*»[8], nonché, aggiungerei, a tenere in considerazione i criteri di sicurezza cibernetica in tutti gli acquisti tecnologici.

Come si avrà modo di vedere, nel corso della trattazione si farà riferimento principalmente alla normativa nazionale rilevante, ciò in quanto, come ricordato dalla dottrina poc'anzi menzionata, «le Direttive 2014/23-

dalle norme. Il tema in questione, proprio nell'ambito degli studi che osservano l'impatto delle nuove tecnologie sulle categorie dell'ordinamento, è vieppiù posto in risalto; a titolo esemplificativo, si possono richiamare i lavori di D.U. Galetta, *Il procedimento amministrativo come strumento di organizzazione e le conseguenze legate all'uso delle ICT*, in *Istituzioni del Federalismo*, 2023, 2; G. Carullo, *La nozione di servizi digitali: un nuovo paradigma per la pubblica amministrazione*, in *Istituzioni del Federalismo*, 2023, 2; Id, *Interoperabilità e riflessi organizzativi: il caso della conservazione digitale*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino 20/2021, Id, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2016. In tema, si rimanda anche agli altri interessanti contributi contenuti nel Fascicolo della Rivista *Istituzioni del Federalismo*, 2023, 2, intitolato "La digitalizzazione e l'organizzazione della pubblica amministrazione".

[8] S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit., 340, ove si precisa che «Questo aspetto, che di primo acchito può essere giustificato con la riconduzione di questa materia all'ambito di stretto interesse nazionale 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».

24-25/UE in materia di appalti e concessioni non contengono né una disciplina generale sugli appalti di *cybersecurity* né minime e particolari disposizioni»[9].

3. *La sicurezza cibernetica delle stazioni appaltanti: principali profili di rilievo*

Un primo ambito meritevole di approfondimento è senza dubbio quello della sicurezza cibernetica delle stazioni appaltanti: in primo luogo, in quanto, a seguito dell'approvazione del nuovo codice dei contratti pubblici del 2023, esse sono state oggetto di un ampio intervento di riforma (soprattutto con riferimento al problema della loro qualificazione); in secondo luogo, per via del processo di digitalizzazione del c.d. "ciclo di vita" dei contratti[10], posto che, come noto, l'attuale disciplina prevede una parte dedicata alla digitalizzazione delle procedure, la cui rilevanza è corroborata dalla scelta sistematica di raggruppare le disposizioni relative alla digitalizzazione negli articoli da 19 a 36, contenuti nella Parte II (intitolata "della digitalizzazione del ciclo di vita dei contratti") del Libro I del codice (intitolato "dei principi, della digitalizzazione, della programmazione, della progettazione").

In particolare, l'art. 19, c. 1, del d.lgs. n. 36/2023 stabilisce che le stazioni appaltanti e gli enti concedenti assicurano la digitalizzazione del ciclo di vita dei contratti e garantiscono l'esercizio dei diritti di cittadinanza digitale, operando secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica; ancora, il comma 3, del medesimo articolo, aggiunge che «le attività e i procedimenti amministrativi connessi al ciclo di vita dei contratti pubblici sono svolti digitalmente, secondo le previsioni del presente codice e del codice di cui al decreto legislativo n. 82 del 2005, mediante le piattaforme e i servizi digitali infrastrutturali delle stazioni appaltanti e degli enti concedenti», ragione per cui, ai sensi del successivo comma 5,

[9] *Ibidem*, cit.

[10] La promozione della digitalizzazione in questo settore è, infatti, tra gli obiettivi dettati dal PNRR che prevede, tra l'altro, la realizzazione di un Sistema Nazionale di e-Procurement, volto a raccogliere le spinte di efficienza che giungono dallo sviluppo tecnologico, che riguarda tutta la procedura, dalla fase della programmazione delle esigenze fino all'esecuzione del contratto; il tutto attraverso la realizzazione di una piena interconnessione e interoperabilità tra i sistemi telematici.

le stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti, adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali; le stazioni appaltanti e gli enti concedenti, inoltre, assicurano la formazione del personale addetto, garantendone il costante aggiornamento.

In altre parole, quello della "sicurezza informatica" diviene – in ragione della previsione codicistica, che risulta improntata ad una logica di integrazione generale dell'interesse in parola – un principio cardine che deve guidare l'attività delle stazioni appaltanti e degli enti concedenti, informandone per intero l'organizzazione[11].

Nell'ambito del particolare contesto degli acquisti di beni e servizi informatici, l'alto livello di sicurezza cibernetica delle stazioni appaltanti dovrebbe, peraltro, derivare dalla circostanza (prevista dalla "Legge di stabilità 2016") per cui le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione sono tenute ad acquisire beni e servizi informatici e di connettività esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip S.p.a. o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi[12].

In altri termini, si è già assistito ad un fenomeno di centralizzazione delle committenze e di accorpamento delle stazioni appaltanti – al fine di garantirne l'effettiva capacità di gestione delle gare – che oggi, con il codi-

[11] Come ricavabile dal dettato di cui all'art. 21, cc. 1 e 2, del nuovo codice dei contratti pubblici, ove si statuisce che «1. Il ciclo di vita digitale dei contratti pubblici, di norma, si articola in programmazione, progettazione, pubblicazione, affidamento ed esecuzione. 2. Le attività inerenti al ciclo di vita di cui al comma 1 sono gestite, nel rispetto delle disposizioni del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, attraverso piattaforme e servizi digitali fra loro interoperabili».

[12] Ai sensi dell'art. 1 commi 512-520 della l. 28 dicembre 2015, n. 208 ("Legge di stabilità 2016"). Inoltre, ai sensi del c. 516 della medesima legge, infatti, «le amministrazioni e le società di cui al comma 512 possono procedere ad approvvigionamenti al di fuori delle modalità di cui ai commi 512 e 514 [perciò, in deroga] esclusivamente a seguito di apposita autorizzazione motivata dell'organo di vertice amministrativo, qualora il bene o il servizio non sia disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione ovvero in casi di necessità ed urgenza comunque funzionali ad assicurare la continuità della gestione amministrativa. Gli approvvigionamenti effettuati ai sensi del presente comma sono comunicati all'Autorità nazionale anticorruzione e all'Agid».

ce del 2023, ha trovato più ampia formalizzazione[13]. Con una, importante, differenza: oggi, rispetto al momento di introduzione di dette regole, un ruolo estremamente rilevante è affidato all'Agenzia per la cybersicurezza nazionale (ACN), la quale, a tal proposito, ha sottoscritto apposito accordo d'intesa con l'Autorità nazionale anticorruzione (ANAC) e l'Agenzia per l'Italia digitale (AgID).

Deve, infatti, segnalarsi una rilevante novità introdotta dal c.d. "correttivo" al codice dei contratti pubblici, entrato (con alcune eccezioni) direttamente in vigore il 1° gennaio 2025[14]. Come ovvio, infatti – posto che ai sensi dell'art. 25 del codice dei contratti pubblici «le stazioni appaltanti e gli enti concedenti utilizzano le piattaforme di approvvigionamento digitale per svolgere le procedure di affidamento e di esecuzione dei contratti pubblici, secondo le regole tecniche di cui all'articolo 26» – un tema di estrema importanza, nell'ottica della sicurezza cibernetica delle stazioni appaltanti, è costituito dall'affidabilità delle menzionate piattaforme.

A tal proposito, perciò, il d.lgs. n. 209/2024 è intervenuto proprio sull'art. 26 del codice dei contratti, modificandone i commi 1 e 2 e aggiungendo, in tal modo, l'Agenzia per la cybersicurezza nazionale tra i soggetti cui spetta stabilire le modalità di certificazione dei requisiti tecnici delle piattaforme di approvvigionamento digitale, nonché individuare i requisiti e i titoli richiesti alle piattaforme di approvvigionamento digitale al fine di

[13] A tal proposito, infatti deve ricordarsi che Gli articoli 62 e ss. del nuovo codice riguardano le aggregazioni e la centralizzazione delle committenze (art. 62), la qualificazione delle stazioni appaltanti e delle centrali di committenza (art. 63) e gli appalti che coinvolgono stazioni appaltanti di altri Stati membri (art. 64). Con tali norme viene parzialmente innovata la disciplina del Codice del 2016. L'art. 1, comma 2, lett. c) della legge delega n. 78 del 2022 ha fissato l'obiettivo della riduzione del loro numero, anche mediante accorpamento, ma ha soprattutto puntato sull'obiettivo della loro riorganizzazione. Il nuovo Codice, dopo aver ribadito l'obiettivo di superare la frammentazione delle stazioni appaltanti e delle centrali di committenza, anche mediante accorpamento, ha privilegiato l'obiettivo della loro migliore organizzazione, anche curando la formazione dei funzionari, in modo da conseguire una maggiore efficacia ed efficienza nell'attuare gare in tempi più rapidi e con una maggiore accuratezza nella predisposizione di progetti e bandi, nonché in fase di gestione ed esecutiva. Tali obiettivi non erano alieni al Codice del 2016 ma sono stati solo in parte realizzati, anche perché non è stato emanato il Decreto attuativo del Presidente del Consiglio dei Ministri. Poiché, come è noto, il nuovo Codice è auto esecutivo, le misure previste non rischiano di restare lettera morta in attesa dell'atto attuativo ma entreranno immediatamente in vigore.

[14] D.lgs. 31 dicembre 2024, n. 209.

dimostrare la conformità delle piattaforme stesse all'ecosistema nazionale di approvvigionamento digitale, nonché della sicurezza delle informazioni[15].

Dette regole tecniche – originariamente adottate da AgID nel 2023 – sono state aggiornate il 30 dicembre 2025, con la previsione di alcune, importanti novità.

Il processo di certificazione, infatti, si articola su quattro classi di conformità che coprono l'intero spettro operativo: dalla gestione degli accessi e della tracciabilità (Classe 1), alla redazione di atti nativi digitali e alla gestione del fascicolo di gara (Classe 2), fino alla piena interoperabilità con la Banca Dati Nazionale dei Contratti Pubblici (BDNCP) tramite la Piattaforma Digitale Nazionale Dati (Classe 3) e lo svolgimento di procedure end-to-end validate da organismi di valutazione della conformità (CAB) accreditati (Classe 4). La governance di questo sistema vede l'AgID responsabile della raccolta e verifica dei titoli, mentre l'ANAC gestisce il Registro delle Piattaforme Certificate (RPC), unico strumento che abilita le stazioni appaltanti all'utilizzo di strumenti conformi alla legge.

Le regole tecniche introducono, inoltre, precise disposizioni sull'uso dell'intelligenza artificiale, stabilendo che tali sistemi debbano operare secondo i principi di trasparenza, spiegabilità e non discriminazione, con l'obbligo inderogabile della supervisione umana per ogni decisione che comporti impatti giuridico-economici rilevanti, come l'aggiudicazione o l'esclusione di un operatore. La tracciabilità delle operazioni svolte dall'IA deve essere garantita per permettere al Responsabile Unico del Progetto (RUP) di validare i risultati e motivare le scelte amministrative.

In altri termini, pertanto, con riferimento alle stazioni appaltanti, la questione della trasparenza emerge, innanzitutto, sotto una duplice prospettiva: in primo luogo, le piattaforme di approvvigionamento digitale che esse utilizzano devono rispettare regole tecniche che permettano di farne un vero e proprio strumento di tracciabilità, comprensibilità e accessibilità delle attività che vi transitano; in secondo luogo, la trasparenza viene in rilievo ogni volta che dette piattaforme implementino sistemi di intelligenza artificiale.

Sin dai profili organizzativi, perciò, risulta evidente una doppia dimensione di problematicità, determinata dalla riflessività dei rischi tecnologici: lo strumento digitale, di per sé, è neutro, ma, a seconda delle sue

[15] D.lgs. n. 209/2024, cit., art. 10.

caratteristiche, può costituire sia un limite, sia un mezzo per la trasparenza dell'azione amministrativa. Da qui l'esigenza di regole tecniche come quelle che si sono brevemente menzionate.

Sempre sotto il profilo della trasparenza amministrativa delle stazioni appaltanti e dei loro mezzi informatici, dette regole tecniche contengono un ulteriore elemento di grande interesse: i gestori delle piattaforme (che possono essere le singole stazioni appaltanti) devono garantire che le infrastrutture cloud utilizzate rispettino i requisiti di cui al "Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione" adottato da ACN con il decreto direttoriale n. 21007 del 27 giugno 2024, che stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali e dei servizi cloud per le pubbliche amministrazioni italiane.

Al centro della normativa vi è l'obbligo per le amministrazioni di predisporre un elenco dei propri dati e servizi digitali, classificandoli in tre categorie distinte in base al potenziale pregiudizio derivante dalla loro compromissione: «ordinari», se non vi sono impatti significativi; «critici», se il pregiudizio riguarda funzioni sociali, salute, sicurezza pubblica o benessere economico; e «strategici», qualora la compromissione possa danneggiare la sicurezza nazionale. In particolare, tutti i dati e servizi soggetti al perimetro di sicurezza nazionale cibernetica sono automaticamente considerati strategici.

Il regolamento introduce un processo di qualificazione per i servizi cloud privati e di adeguamento per le infrastrutture e i servizi pubblici, articolato su quattro livelli di sicurezza crescente (livelli 1-4) che determinano quali asset possono ospitare specifiche classi di dati. Nello specifico, i dati strategici possono essere trattati esclusivamente da infrastrutture e servizi di livello 3 o 4, i quali devono garantire la localizzazione dei dati e dei metadati relativi all'amministrazione sul territorio dell'Unione Europea.

In particolare, il sistema di trasparenza delineato dal regolamento si impernia sul Catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, uno strumento pubblico volto a elencare i soggetti qualificati e le relative informazioni descrittive.

Tuttavia, la normativa prevede specifici limiti a tale visibilità pubblica a tutela della sicurezza: l'articolo 16 stabilisce, infatti, che gli operatori di infrastrutture e i fornitori di servizi possono presentare una motiva-

ta richiesta di non pubblicazione nel catalogo, soggetta alla valutazione dell'ACN, impedendo di fatto la diffusione di dettagli tecnici che potrebbero esporre l'amministrazione a rischi. Un altro elemento di riservatezza risiede nella gestione del personale, per il quale è previsto un addestramento specifico sui requisiti per la non divulgazione e sulla tutela della confidenzialità dei dati, sia in chiaro che cifrati.

Per quanto concerne i dati classificati come strategici, ovvero quelli la cui compromissione potrebbe danneggiare la sicurezza nazionale, il limite alla trasparenza e alla circolazione delle informazioni diventa ancora più stringente. In tali contesti, le misure tecniche di cifratura garantiscono che l'amministrazione mantenga l'accesso esclusivo ai dati in chiaro, specialmente attraverso modelli come l'*Hold Your Own Key* (HYOK, ossia un modello di sicurezza informatica in cui il proprietario dei dati mantiene il controllo esclusivo e fisico delle proprie chiavi di cifratura), che negano al fornitore stesso la possibilità di visualizzare il contenuto delle informazioni trattate.

Anche la gestione dei metadati segue logiche di segretezza: i metadati relativi all'amministrazione non devono permettere di estrarre i dati originali e, nel caso di infrastrutture di livello elevato, ogni richiesta di accesso da parte di entità extra-UE deve essere segnalata all'ACN e autorizzata esplicitamente dall'amministrazione interessata.

Infine, informazioni operative sensibili come le metodologie di verifica del personale (*vetting*) con accesso privilegiato e gli elenchi nominativi dei dipendenti autorizzati non sono accessibili pubblicamente, ma vengono resi disponibili esclusivamente all'amministrazione cliente, creando un perimetro di riservatezza che tutela l'integrità dei sistemi critici dello Stato.

In definitiva, pertanto, l'assetto normativo costituitosi, a seguito del correttivo 2024 al codice degli appalti, intorno alle piattaforme di approvvigionamento digitale utilizzate dalle stazioni appaltanti, che, come si è detto, voleva integrare nelle regole di certificazione delle stesse opportune considerazioni di cybersicurezza, mostrano fin da subito il complesso rapporto che sussiste fra la digitalizzazione dei contratti pubblici, la disciplina sulla cybersicurezza e il principio generale di trasparenza: d'un canto, il legislatore ha demandato alle autorità competenti l'adozione di regole tecniche volte a garantire la piena trasparenza delle piattaforme digitali; d'altro canto, tali regole risultano integrate da altre disposizioni, più precisamente concernenti la questione della sicurezza cibernetica, che,

pur garantendo il massimo grado di conoscibilità possibile delle caratteristiche tecniche delle piattaforme di approvvigionamento digitale (d'ora innanzi anche "PAD"), dispongono necessarie prescrizioni di riservatezza e opacità su quegli aspetti che, altrimenti, renderebbero le piattaforme certificate nuovamente vulnerabili.

In altri termini, l'attuale regolazione garantisce, tramite la certificazione, la fiducia nei confronti dei mezzi tecnologici con cui devono essere svolte le procedure do approvvigionamento; ciò avviene grazie a due condizioni: da un lato viene garantita la piena conoscibilità e interoperabilità delle operazioni svolte tramite PAD; d'altro lato, si accerta la corrispondenza di queste ultime a standard di sicurezza cibernetica adeguati, che sono a loro volta garantiti tramite la perimetrazione e la riservatezza degli aspetti infrastrutturali più rilevanti.

Si comprende bene, perciò, come nella moderna amministrazione digitale – di cui i contratti pubblici sono un fulgido esempio –, la quale è soggetta ai rischi della sua stessa riflessività, il rapporto fra trasparenza e segretezza non possa considerarsi secondo una prospettiva statica e binaria (quasi di mutua esclusione), ma, invece, debba necessariamente ricostruirsi secondo una visione dinamica e variabile (ossia di reciproca necessità e complementarità).

Se quanto scritto è vero per il semplice – si fa per dire – aspetto organizzativo, si vedrà a breve come valga altrettanto per la dimensione di amministrazione attiva, posto che gli strumenti normativi volti a garantire e integrare la sicurezza cibernetica nei processi di acquisizione di beni e servizi ICT pongono il problema di addivenire ad un costante bilanciamento fra le esigenze di trasparenza, che costituiscono un baluardo fondamentale della disciplina degli appalti, e quelle di segretezza, che si rendono necessarie al fine di non vanificare quel medesimo processo di messa in sicurezza per cui detti strumenti sono stati pensati e implementati.

4. *Gli elementi di sicurezza cibernetica nell'ambito del procurement di beni e servizi ICT: una progressiva stratificazione*

Premesso che la normativa direttamente riguardante i profili della cybersicurezza nazionale – quantomeno nelle forme, complesse, che oggi conosciamo – rappresenta il frutto di una consapevolezza alquanto recen-

te, è evidente che essa, nel corso degli ultimi anni, sia stata oggetto di un percorso evolutivo di notevole portata che, a partire da un quadro normativo piuttosto semplice (per quanto possibile in una materia di natura eminentemente tecnica come quella in oggetto) e lineare (costituito dalla previsioni della prima direttiva NIS (Network and Information Security) del 2016[16], successivamente recepita dal d.lgs. n. 65/2018[17]), ha condotto l'ordinamento a costruire un impianto affatto complesso e stratificato, in cui ad ogni livello corrispondono un maggiore grado di "delicatezza" delle funzioni svolte tramite gli strumenti informatici e, di conseguenza, una più ampia presenza di regole e procedure tecniche volte a garantire la sicurezza cibernetica delle infrastrutture più rilevanti.

Tale stratificazione – la quale, peraltro, è il riflesso di un intricato sistema di fonti basato su alcune, importanti, normative di rango primario e su diverse fonti regolamentari di rango secondario, che attuano e specificano le prime – ha una ragione fondamentale: l'adeguamento dei vari soggetti dell'ordinamento, siano essi pubblici o privati, a nuovi e rigorosi *standard* di sicurezza cibernetica presuppone notevolissimi sforzi (e costi) in termini organizzativi (acquisizione di strumenti, formazione del personale, creazione di nuove strutture interne, rispetto di nuove misure di coordinamento con soggetti esterni, oneri informativi e comunicativi, integrazione dei procedimenti amministrativi con sub-procedimenti a carattere tecnico, oneri di segretezza, e via dicendo); senza contare la tensione che sovente si ingenera tra le esigenze di sicurezza e i principi generali che informano l'azione amministrativa (*in primis*, in questo contesto, quello di trasparenza). Pertanto, la logica del legislatore, improntata ad un canone di ragionevolezza, mira evidentemente a creare un ampio spettro di misure che debbono essere applicate progressivamente e proporzionatamente al crescere del rischio e che siano, perciò, adeguate e necessarie al singolo contesto di riferimento.

Ebbene, calando questa riflessione in una visione dinamica, si può notare come all'aumentare della rilevanza della questione inerente alla cybersicurezza nazionale – anche a seguito dei recenti risvolti geopolitici – sia corrisposta, del tutto naturalmente, la riduzione del grado di progressività della normativa (che pur rimane), a favore di un maggior rigore generalizzato. Basti pensare al tema concernente gli oneri in materia di

[16] Direttiva (UE) 2016/1148.

[17] D.lgs. 18 maggio 2018, n. 65.

notifica degli incidenti rilevanti, che a valle del recepimento nazionale della seconda direttiva NIS[18], avvenuto per il tramite del d.lgs. n. 138/2024[19], mostra un netto avvicinamento alle più rigorose prescrizioni applicabili all'interno del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), di cui al d.l. n. 105/2019[20].

Tale processo evolutivo è presente anche all'intersezione tra la disciplina della cybersicurezza e quella dei contratti pubblici, la quale, come si è anticipato, ricopre un ruolo di fondamentale importanza, incidendo alla fonte sugli acquisti tecnologici (ICT) delle amministrazioni e, pertanto, contribuendo in maniera determinante alla transizione verso un'amministrazione ciberneticamente sicura e resiliente, nonché, indirettamente, all'evoluzione del mercato e allo sviluppo di sistemi informatici adeguati alle esigenze moderne.

Se, infatti, sino ad alcuni anni fa, anche sotto la vigenza del d.lgs. n. 65/2018, non sussistevano disposizioni generali in materia di cybersicurezza nel c.d. "*public procurement*" di beni e servizi ICT – venendosi a costituire una generale distinzione, a seguito dell'adozione del d.l. n. 105/2019, tra la generalità delle procedure di acquisto e quelle riguardanti i soggetti ricompresi nell'ambito del PSNC (di cui si tratterà a breve) – a partire dal 2020 il quadro ha cominciato ad evolversi, dapprima tramite l'adozione delle Linee Guida sulla sicurezza nel procurement ICT[21], successivamente con l'adozione del nuovo codice dei contratti pubblici, nel 2023, e, infine, con l'approvazione della legge nazionale sulla cybersicurezza del 2024[22].

Il risultato di questo percorso di progressiva stratificazione è un quadro molto complesso che si potrebbe idealmente (per ragioni di utilità pratica) suddividere in cinque diversi livelli, cui corrispondono regole, procedure e adempimenti differenti e proporzionati al diverso grado di "delicatezza" del settore e della sua attinenza a preminenti interessi nazionali: un primo livello, che potremmo definire generale e residuale (da applicare a tutte le procedure di approvvigionamento di beni e servizi ICT che non rientrino in altri livelli); un secondo livello, che riguarda gli acquisti nell'ambito di "settori connessi alla tutela di interessi nazionali strate-

[18] Direttiva (UE) 2022/2555.

[19] D.lgs. 4 settembre 2024, n. 138.

[20] D.l. 21 settembre 2019, n. 105.

[21] Approvate ad aprile del 2020, le quali erano state precedute solamente, nel 2015, dal documento sulle "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

[22] L. 28 giugno 2024, n. 90.

gici" (di cui si dirà meglio nel prosieguo); un terzo livello, concernente i soggetti rientranti nel PSNC; un quarto livello (strettamente legato al precedente) riguardante la disciplina dei c.d. "*golden powers*"; infine, un quinto livello, che concerne gli acquisti di quel particolare Ente, istituito dal d.lgs. n. 82/2021, che è l'Agenzia per la cybersicurezza nazionale (ACN).

Nel corso dei paragrafi che seguono, si avrà modo di approfondire le discipline applicabili ai singoli livelli, analizzando, per ciascuno, il grado di tensione (e le soluzioni approntate dall'ordinamento) cui ciascuno di essi è sottoposto rispetto al tema della trasparenza. A tal proposito, è bene precisare che, per ragioni di chiarezza dell'esposizione, si è deciso di seguire un ordine per così dire "spaziale" (ossia dal livello più superficiale a quello più profondo), anziché "temporale" (ossia seguendo l'ordine di introduzione degli istituti da parte della legge)[23].

4.1. *I due primi (e più superficiali) livelli normativi e la trasparenza come "comprensibilità"*

I primi due livelli dell'attuale disciplina in materia di cybersicurezza e contrattualistica pubblica – i quali, si può anticipare, prevedono regole applicabili o in via generale o ad uno specifico contesto, ossia anche a soggetti dai quali non dipende direttamente un servizio essenziale legato alla sicurezza nazionale, ma il cui operare avviene in contesto strategico, che rende opportuno un maggior grado di precauzione, e che, pertanto, sono espressione di un vero e proprio principio di integrazione della sicurezza cibernetica – si possono desumere direttamente da un'interessante disposizione contenuta nell'attuale codice dei contratti pubblici: l'art. 108, c. 4, del d.lgs. n. 36/2023.

La menzionata disposizione – rubricata "criteri di aggiudicazione degli appalti di lavori, servizi e forniture" e che individua solo due possibili criteri di aggiudicazione delle gare, ossia quello dell'offerta economicamente più vantaggiosa e quello del minor prezzo – stabilisce che nelle attività di approvvigionamento di beni e servizi informatici per la pubblica amministrazione, le stazioni appaltanti, incluse le centrali di committenza,

[23] Peraltro, si tratta del medesimo criterio ritenuto opportuno anche da altra dottrina che si è occupata del tema: si veda, sul punto, S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit.

nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici; ancora, precisa che in questi ultimi casi, quando i beni e i servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del dieci per cento e che per i contratti ad alta intensità di manodopera, tale limite è deve assestarsi entro il trena per cento.

Il tenore letterale della disposizione in parola non lascia dubbi rispetto alla presenza di una scissione tra quella che si potrebbe definire la generalità delle procedure «di approvvigionamento di beni e servizi informatici per la pubblica amministrazione» (citando il primo periodo) e i casi in cui in cui «il contesto di impiego» dei beni o servizi oggetto dell'approvvigionamento sia «connesso alla tutela degli interessi nazionali strategici» (di cui al quarto periodo). Infatti, come chiaramente espresso dal prosieguo della disposizione, soltanto nel secondo caso «la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento»[24].

Evidentemente, non sarebbe peregrino chiedersi se detti acquisti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici costituisca concretamente una nuova categoria intermedia, oppure se, invece, il legislatore intendesse più semplicemente riferirsi ai soggetti compresi nel PSNC (ossia, come si è già detto, nel perimetro di sicurezza nazionale cibernetica).

La risposta a tale domanda parrebbe poter essere positiva (nel senso della prima ipotesi), in ragione di alcuni dati testuali e sistematici: innanzitutto, per i c.d. "soggetti perimetro" esiste già una normativa speciale volta a garantire l'adeguatezza, in termini di sicurezza cibernetica, degli

[24] Sul punto debbono certamente richiamarsi le interessanti riflessioni di L. Nannipieri, *Cybersicurezza e appalti. Interventi legislativi e prime criticità*, cit., 75, ove si afferma che «sul piano oggettivo, l'art. 14 rinvia a due nozioni di difficile delimitazione: quella degli "interessi nazionali strategici" e quella degli "elementi essenziali di cybersicurezza". La prima ("interessi nazionali strategici") costituisce altresì un requisito di applicabilità della disposizione, nel senso che la stessa, *a contrariis*, parrebbe inapplicabile agli appalti per l'approvvigionamento di beni e servizi informatici in "contesti" diversi da quelli connessi alla tutela, appunto, degli "interessi nazionali strategici"».

strumenti o dei servizi da acquistare; in seconda, ma connessa alla prima, istanza, l'art. 14 della recente legge nazionale sulla cybersicurezza (l. n. 90/2024, che, come si è detto, si riferisce esplicitamente ai "contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici") fa salva l'applicazione, ai soggetti contenuti nell'apposito elenco, delle regole di cui alla legge sul PSNC; in terza battuta, poi, l'espressione "connesso alla tutela degli interessi nazionali strategici" non coincide necessariamente con l'ambito di applicazione del d.l. n. 105/2019 (legge sul PSNC), che si riferisce alla sicurezza «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».

In altri termini, sebbene possano darsi casi di sovrapposizione, la seconda categoria cui si riferisce l'art. 108, c. 4, del codice dei contratti pubblici pare rimanere separata dai casi presi in considerazione dalla normativa sul PSNC.

Pertanto, nonostante si tratti di una disposizione dal valore fortemente programmatico[25], l'art. 108, c. 4, del d.lgs. n. 36/2023 presenta senz'altro alcuni profili di grande interesse operativo. In particolare: pone l'obiettivo di integrare le considerazioni concernenti la cybersicurezza in tutte le procedure di acquisto di beni e servizi ICT (in passato, invece, la disciplina dei contratti pubblici individuava nella cybersicurezza un particolare oggetto d'acquisto, per il quale erano già utilizzabili specifiche forme di *procurement*); introduce una disposizione operativa molto importante, stabilendo un limite al peso dell'offerta economica rispetto agli aspetti di cybersicurezza, nei casi in cui l'acquisto riguardi beni o servizi da utilizzare in contesti connessi alla tutela degli interessi nazionali strategici; ancora, individua una distinzione tra la generalità delle attività di approvvigionamento di beni e servizi informatici e quelle che riguardano, invece, beni servizi utilizzati in contesti connessi alla tutela degli interessi

[25] Come opportunamente affermato da S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit.

nazionali strategici (che si aggiunge all'ulteriore ripartizione concernente l'approvvigionamento dei c.d. "soggetti perimetro").

Tale impianto, inoltre, ha trovato conferma, come anticipato, nella l. n. 90/2024, il cui art. 14, c. 1, statuisce che con d.p.c.m., da adottare su proposta di ACN previo parere del CIC sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale[26], tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.

Ancora una volta, pertanto, viene rimarcata la distinzione tra gli «elementi di cybersicurezza» che le stazioni appaltanti debbono tenere in considerazione per tutti gli acquisti di beni e servizi informatici (probabilmente desumibili dalle menzionate Linee Guida sulla sicurezza nel procurement ICT di aprile 2020) e «gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici»[27].

---

[26] Ossia, ai sensi della menzionata disposizione del d.lgs. 7 marzo 2005, n. 82, « […] le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione; […] gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; […] società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)».

[27] Ancora, il c. 2 della medesima disposizione precisa, sulla linea indicata dall'art. 108, c. 4, del codice dei contratti pubblici, che nei casi individuati ai sensi del c. 1, i soggetti appaltanti: possono applicare l'art. 107, c. 2 del nuovo codice dei contratti pubblici (ossia non aggiudicare a chi ha effettuato l'offerta economicamente più vantaggiosa) e l'art. 108, c. 10 del medesimo (ossia la possibilità di non aggiudicare se nessuna offerta risulti idonea o conveniente rispetto all'obiettivo del contratto) qualora non siano rispettati i requisiti di cyber previsti nel d.p.c.m.; tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione qualità/prezzo; nel caso in cui si applichi il criterio del minor prezzo, inseriscono i requisiti di cybersicurezza tra quelli minimi di aggiudicazione del contratto; applicano l'art. 108, c. 4 (tetto massimo per il punteggio economico entro il 10 %); prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi

A tal proposito, il 5 maggio 2025 è stato pubblicato in Gazzetta Ufficiale il D.P.C.M. 30 aprile 2025 contenente la "Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale" e che, appunto in applicazione dell'art. 14, c. 1, della legge 28 giugno 2024, n. 90, individua, fra l'altro: gli elementi essenziali di cybersicurezza che i menzionati soggetti tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici, appartenenti a specifiche categorie tecnologiche, impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e le specifiche categorie tecnologiche di beni e servizi informatici per i quali sono tenuti in considerazione gli elementi essenziali di cybersicurezza[28].

L'impianto normativo che si è venuto a costituire risulta, al contempo, particolarmente interessante per quanto concerne la prospettiva evolutiva della materia in oggetto ed evidentemente critica sotto il profilo definitorio e di individuazione dell'effettivo ambito di applicazione delle disposizioni in parola.

Sotto il primo profilo, infatti, non vi è dubbio che le regole individuate in materia di cybersicurezza (per la prima volta) dal codice dei contratti pubblici del 2023 rispondano alla volontà di passare dalla concezione della sicurezza cibernetica come semplice "oggetto" (uno dei tanti) di acquisto da parte delle pubbliche amministrazioni a quella che, invece, vi vede un vero e proprio interesse pubblico, il quale, in ragione delle sue caratteristiche, necessita di essere integrato (al pari di come, notoriamente, si agisce rispetto all'interesse ambientale, in applicazione del principio di

appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati con il decreto di cui al comma 1.

[28] D.P.C.M. 30 aprile 2025, art. 1. Come ben affermato da S. Francario, *Appalti pubblici e cybersicurezza. La disciplina speciale dell'acquisto di beni e servizi informatici nei settori sensibili dopo il DPCM 30 aprile 2025*, cit., «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; ii) in contesti connessi alla tutela della sicurezza nazionale».

integrazione) nell'ambito di tutti gli acquisti informatici delle amministrazioni. Si tratta, a ben vedere, di un approccio "di mercato" estremamente interessante. Se, d'un canto, infatti, l'obiettivo principale consiste nel fare in modo che ogni stazione appaltante sia tenuta a prendere in considerazione alcuni requisiti minimi di sicurezza cibernetica nell'acquisto di beni e servizi ICT, d'altro canto, l'inevitabile riflesso di tale circostanza non può che essere l'adattamento dei prodotti informatici offerti dal mercato, con un complessivo innalzamento del livello generale di cybersicurezza.

Sotto il secondo profilo, però, si pone evidentemente un problema di non poco rilievo, che riguarda principalmente la distinzione tra i due livelli che si sono enucleati nell'ambito del presente paragrafo. Se, infatti, ai livelli più profondi della normativa (di cui si tratterà a breve), l'ambito di applicazione delle prescrizioni normative di riferimento risulta chiarissimo, posto, ad esempio, che i soggetti ricondotti all'interno del perimetro di sicurezza nazionale cibernetica ne sono del tutto consapevoli, in quanto la registrazione all'interno dell'apposito elenco, non pubblico, è loro notificata; nei due livelli più superficiali non è del tutto evidente quali siano i confini tra le due categorie, ossia tra la generalità delle procedure di approvvigionamento di prodotti informatici e quelle connesse agli interessi nazionali strategici.

Infatti, tali incertezze interpretative non sono state interamente risolte dal D.P.C.M. 30 aprile 2025, che, sebbene precisando chiaramente gli elementi essenziali da valutare e le tecnologie interessate, non contiene, come ovvio, una definizione di "interesse nazionale strategico", la quale, perciò, rimane tuttora estremamente sfuggente, pur costituendo il nocciolo fondamentale della distinzione operata dal legislatore. Gli unici strumenti interpretativi a disposizione rimangono i riferimenti alle normative che, anche a scopi differenti, individuano settori per così dire strategici. Esemplificativamente, ci si potrebbe riferire a quanto stabilito dall'art. 32 del d.l. 9 agosto 2022, n. 115 – concernente l'individuazione delle "aree di interesse nazionale strategico"[29] – nonché alle stesse disposizioni della già

[29] La menzionata disposizione, infatti, afferma, al c. 1, che «Con decreto del Presidente del Consiglio dei ministri, anche su eventuale proposta del Ministero dello sviluppo economico, di altra amministrazione centrale o della regione o della provincia autonoma territorialmente competente e previa individuazione dell'area geografica, possono essere istituite aree di interesse strategico nazionale per la realizzazione di piani o programmi comunque denominati che prevedano investimenti pubblici o privati anche cumulativamente pari a un importo non inferiore ad euro 400.000.000,00 relativi ai

menzionata legge di stabilità del 2016, nell'ambito della quale è presente una nozione di "strategicità" proprio nell'ambito degli appalti di prodotti informatici[30].

Con particolare riguardo al tema della trasparenza, nei primi due, più superficiali, livelli normativi che si sono individuati, non è dato riscontrare particolari prescrizioni in termini di segretezza delle operazioni di gara (nel senso di prescrizioni che incidano direttamente sulla conoscibilità o

settori di rilevanza strategica. Ai predetti fini, sono di rilevanza strategica i settori relativi alle filiere della microelettronica e dei semiconduttori, delle batterie, del supercalcolo e calcolo ad alte prestazioni, della cibersicurezza, dell'internet delle cose (IoT), della manifattura a bassa emissione di CO2, dei veicoli connessi, autonomi e a basse emissioni, della sanità digitale e intelligente e dell'idrogeno, individuate dalla Commissione Europea come catene strategiche del valore».

[30] Ad esempio, è possibile fare riferimento al c. 513 – ove si stabilisce che «L'Agenzia per l'Italia digitale (Agid) predispone il Piano triennale per l'informatica nella pubblica amministrazione che è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato. Il Piano contiene, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica» – e al c. 514, ove si legge che «Consip SpA o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. Agid, Consip SpA e i soggetti aggregatori, sulla base di analisi delle informazioni in loro possesso relative ai contratti di acquisto di beni e servizi in materia informatica, propongono alle amministrazioni e alle società di cui al comma 512 iniziative e misure, anche organizzative e di processo, volte al contenimento della spesa. Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni». Sul punto, si rimanda anche a quanto ricostruito da L. Nannipieri, *Cybersicurezza e appalti. Interventi legislativi e prime criticità*, cit. 75, ove si ricorda che «L'ordinamento contiene effettivamente disposizioni riferibili, a vario titolo, al carattere "strategico" di determinate "attività" (si vedano, ad esempio, i diffusi richiami contenuti nel d.l. 21/2012, "norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni", nonché nel d.l. 187/2022, "misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici"). Quello che risulta tuttora mancante, però, è una nozione ordinamentale "organica" di "interesse nazionale strategico" che consenta di delimitare con sufficiente precisione l'ambito applicativo sia dell'articolo in commento che del già vigente art. 108 del codice dei contratti pubblici».

sull'ostensibilità di documenti e di informazioni attinenti alle procedure); pertanto il tema della trasparenza si pone principalmente con riguardo alla chiarezza e alla comprensibilità dei criteri di valutazione individuati, nonché con riferimento all'individuazione dei soggetti sottoposti alla disciplina. Con riguardo alla chiarezza dei criteri di valutazione degli elementi di cybersicurezza, si può distinguere tra la generalità (residuale) delle procedure di approvvigionamento di beni ICT, cui si applicano le Linee guida di cui *supra*, e le procedure per beni e servizi da utilizzare in contesti connessi alla tutela degli interessi nazionali strategici: in questo secondo caso, come detto, trova oggi applicazione d.p.c.m. 30 aprile 2025.

Come si diceva, invece, rimane tutt'oggi aperta la questione attinente alla poca chiarezza dell'ambito oggettivo di applicazione della disposizione in parola, il che incide inevitabilmente sulla trasparenza dell'attività amministrativa di approvvigionamento di strumenti digitali, quantomeno sul versante della sua piena comprensibilità e, conseguentemente, calcolabilità.

4.2. *La disciplina applicabile ai soggetti rientranti nell'ambito del perimetro di sicurezza nazionale cibernetica (PSNC): un'importante eccezione al diritto di accesso ai documenti amministrativi*

Più lineare, invece, è la questione concernente la disciplina applicabile ai soggetti rientranti nell'ambito del perimetro di sicurezza nazionale cibernetica.

Il già menzionato d.l. n.105/2019 (convertito in l. n. 133 /2019) ha introdotto, infatti, per la prima volta, regole specifiche che devono trovare applicazione nel caso di acquisizione di beni e servizi ICT da parte di soggetti ricompresi nel PSNC: ossia, di quelli «da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale […] dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale»[31].

[31] Art. 1 del d.l. n. 105/2019. Come ben espresso da S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit., «basti ivi ricordare come il PSNC, introdotto nel 2019, costituisce una cornice entro cui vengono applicate speciali norme in materia di cybersecurity in capo a taluni soggetti ritenuti particolarmente sensibili e la cui azione è esercitata (anche) con reti e infrastrutture digitali. Da un lato, infatti, la disciplina del Perimetro si

In particolare, come noto, l'art. 1, c. 6, del d.l. n. 105/2019, rimandava ad un apposito regolamento[32] la determinazione delle procedure, delle modalità e dei termini con cui i soggetti perimetro procedono all'affidamento di forniture di beni, sistemi e servizi ICT da utilizzare su *asset* strategici[33].

Ai sensi di tale normativa regolamentare di attuazione (art. 3, c. 1, del d.p.r. n. 54/2021), «i soggetti inclusi nel perimetro, prima dell'avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT […], anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza, ne danno comunicazione al CVCN», ossia al Centro di Valutazione e Certificazione Nazionale [34].

Come affermato in dottrina, «la *ratio* di questo obbligo [comunicativo] è quella di garantire al CVCN lo svolgimento delle proprie funzioni istituzionali, anche avvalendosi dei Laboratori accreditati di prova (LAP) con i quali effettuare test di sicurezza informatica su *hardware* e su *software*»[35].

In particolare, infatti, il CVCN (ai sensi dell'art. 4) è tenuto a espri-

---

applica a quei soggetti che esercitano una funzione essenziale dello Stato. Dall'altro lato, esse valgono per quei soggetti, di natura pubblica o privata, che prestano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, in relazione a cui un possibile malfunzionamento, interruzione o impiego improprio delle proprie infrastrutture informatiche si traduce in un pregiudizio alla sicurezza nazionale».

[32] D.p.r. 5 febbraio 2021, n. 54.

[33] Concretamente individuati con d.p.c.m. del 15 giugno 2021.

[34] Accanto al CVCN, peraltro, sono istituiti anche i CV, ossia i Centri di Valutazione relativi alla materia, rispettivamente del Ministero Difesa e del Ministero degli Affari Interni, da non confondere con i Ce.Va. anch'essi centri di valutazione per le certificazioni di sicurezza cibernetica di prodotto in ambito *common criteria* per i prodotti che operano su dati classificati.

[35] S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit., 349. Sul punto, inoltre, si richiama T. Cocchi, *La cybersicurezza nel prisma del diritto dei contratti pubblici*, cit., 202: «Tale previsione come lucidamente osservato in dottria, stride con i fondamentali principi europei e nazionali del favor partecipationis, trasparenza e par condicio, in forza dei quali difficilmente potrebbe ammettersi un'eterointegrazione della lex specialis in corso di gara, specie se rimessa a valutazioni amministrative svolte ex post. Emblematico in tal senso sarebbe il caso in cui il Cvcn ritenesse necessario il possesso di alcuni requisiti tecnici non previsti dalla lex specialis di gara e in base alla quale gli operatori economici si erano vincolati a presentare offerta».

mersi entro quarantacinque giorni da detta comunicazione (salvo possibile proroga, per una sola volta, di quindici giorni): decorso tale termine senza che il CVCN si sia espresso i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento; qualora, invece, «il CVCN abbia espresso specifici rilievi (imponendo, ad esempio, test di sicurezza), la documentazione di gara della procedura d'appalto deve essere resa conforme a quanto imposto dal Centro»[36].

In altri termini, a differenza che nei livelli, per così dire, più superficiali della disciplina in parola, in cui l'integrazione dell'interesse alla sicurezza cibernetica avviene tramite l'indirizzamento, più o meno stringente, della discrezionalità[37] delle stazioni appaltanti, in questo caso il legislatore stabilisce forme di rigorosa integrazione tecnica del procedimento, prevedendo un vero e proprio subprocedimento affidato ad un soggetto specializzato, la cui valutazione incide in maniera determinate sulla procedura.

Per quanto concerne il rapporto con il principio di trasparenza, dalla disciplina applicabile, così come poc'anzi brevemente richiamata, risulta evidente che – siccome l'esito dei test condiziona in maniera determinate la possibilità per il soggetto perimetro di utilizzare un certo bene o servizio ICT e per il fornitore di aggiudicarsi la relativa gara – in caso di esito negativo delle procedure di valutazione *software* e *hardware* i fornitori avrebbero senz'altro interesse ad effettuare accesso alla documentazione di gara e, in particolare, alle metodologie e alle procedure di test utilizzate dal CVCN o dai LAP. Il che, come ovvio, pone numerosi problemi circa l'effettività delle medesime, in ragione del fatto che la diffusione di

[36] *Ibidem*, cit., ove si precisa ulteriormente che «Da quanto ricostruito emerge la centralità del ruolo rivestito dal CVCN, il quale, sulla base di un giudizio di discrezionalità tecnica, può condizionare – e in casi estremi impedire – l'aggiudicazione della fornitura o del servizio digitale. Ruolo centrale necessario proprio a fronte della rilevanza degli interessi in questione».

[37] Sul punto, si può richiamare anche T. Cocchi, *La cybersicurezza nel prisma del diritto dei contratti pubblici*, cit., 197, ove si afferma che «i suddetti margini di discrezionalità appaiono particolarmente marcati nella disposizione in commento, ove si conferisce alle stazioni appaltanti la potestà di attribuire, nella valutazione degli elementi qualitativi delle offerte attinenti all'approvvigionamento di beni e servizi informatici – «specifico e peculiare rilievo» nella valorizzazione degli «elementi di cybersicurezza». La ratio della norma è evidentemente quella di premiare le imprese che siano compliance con le esigenze di cybersicurezza richieste nell'approvvigionamento delle soluzioni tecnologiche per la pubblica amministrazione e senza dubbio dev'essere vista con favore, estrinsecando una nuova sensibilità del legislatore su questi temi».

informazioni concernenti le modalità di valutazione potrebbe inficiarne la concreta capacità di garanzia della sicurezza cibernetica dei sistemi informatici che ad esse soggiacciono.

Il Ministero dello sviluppo economico, perciò, ha significativamente ritenuto necessario integrare l'elenco dei casi di sottrazione al diritto di accesso in relazione all'esigenza di salvaguardare la sicurezza e la difesa nazionali, di cui all'art. 24, c. 6, lett. a), della l. n. 241/1990, che demanda al Governo la possibilità di estendere con regolamento i casi di esclusione del diritto di accesso.

Il regolamento di attuazione del menzionato articolo 24 è il decreto del Ministro delle Poste e delle telecomunicazioni 10 aprile 1996, n. 296, al cui art. 1, c. 1, è stata aggiunta (con decreto 16 ottobre 2020, n. 194) la lett. i-*bis*, che sottrae al diritto di accesso anche i documenti relativi alle procedure e alle metodologie di test di *hardware* e *software* definiti, disposti, imposti o comunque impiegati, direttamente o indirettamente, dal Centro di valutazione e certificazione nazionale.

Il decreto 16 ottobre 2020, n. 194 ha ricevuto sia l'avvallo della Commissione per l'accesso agli atti amministrativi istituita presso la Presidenza del Consiglio dei Ministri[38], sia – allorquando era in bozza – il parere positivo del Consiglio di Stato[39].

In particolare, è interessante mettere in rilievo alcune modifiche che il Consiglio di Stato ha ritenuto necessario suggerire rispetto alla bozza di decreto che gli è stata sottoposta: inizialmente, infatti, essa faceva riferimento soltanto alle procedure e alle metodologie *utilizzate* dal CVCN, mentre nel decreto finale si fa menzione, come suggerito, ai test *definiti*, *disposti*, *imposti* o *comunque impiegati*, *direttamente* o *indirettamente*, dal Centro di valutazione e certificazione nazionale.

[38] La quale con atto in data 10 luglio 2020 ha rilevato che «l'integrazione del decreto del Ministero delle poste e telecomunicazioni n. 296/1996, con l'inserimento tra i casi esclusione dei 'documenti relativi alle procedure ed alle metodologie di test di hardware e software utilizzati dal Centro di valutazione e certificazione nazionale, di cui all'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni nella legge 18 novembre 2019 n. 133' – alla lettera 'i- bis' all'art. 1 comma 1 – rientra pienamente nella previsione dell'art. 24 della Legge 241/'90 'Esclusione dal diritto di accesso', che demanda alle amministrazioni la individuazione delle ipotesi di esclusione dall'accesso dei documenti dalle stesse detenuti, per la salvaguardia dei prevalenti interessi menzionati nello stesso».

[39] Cons. Stato, Sezione Consultiva per gli Atti Normativi, Adunanza di Sezione del 3 settembre 2020.

In secondo luogo, il Consiglio di Stato riteneva opportuno, come è stato fatto, precisare che la normativa fa riferimento ai documenti relativi alle sole procedure e metodologie di test di *hardware* e *software* strumentali a valutare la sicurezza delle «*forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici*» ai sensi e per le finalità di cui all'articolo 1 del decreto-legge n. 105 del 2016.

In altri termini, nella lettura di queste disposizioni è molto importante comprenderne precisamente, posta la natura derogatoria rispetto al principio di trasparenza, l'ambito di applicazione: l'esclusione dell'accesso si applica soltanto alle procedure e metodologie di test di *hardware* e *software* strumentali a valutare la sicurezza delle forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, ma quando ci si trova in questo contesto, affinché la deroga sia adeguata all'obiettivo perseguito, è necessario che si applichi non solo alle procedure genericamente utilizzate dal CVCN, bensì, più precisamente, ai test *definiti*, *disposti*, *imposti* o *comunque impiegati*, *direttamente* o *indirettamente*, dal Centro di valutazione e certificazione nazionale.

Si può dire, perciò, che nella sua formulazione iniziale, il decreto in parola fosse, d'un canto, eccessivamente restrittivo, nella parte in cui fa riferimento ai soli test e metodologie "*utilizzati*" dal Centro di valutazione e certificazione nazionale, e, d'altro canto, troppo ampio, in quella in cui individuava precisamente il "perimetro" procedimentale cui si applica l'esclusione.

Infine, sempre con riferimento alla disciplina dei soggetti rientranti nel PSNC, l'esigenza di segretezza alla base delle procedure, che ne determina l'intrinseca ed inevitabile "opacità", è confermata anche dall'art. 4, c. 9, del medesimo d.p.r. n. 54/2021, ove si afferma, in via generale, che «gli atti del procedimento di verifica e valutazione sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'articolo 1, comma 1, del decreto-legge».

4.3. *Il caso dei c.d. "golden powers" e alcune recenti innovazioni in materia di rete 5G*

Un'altra normativa rilevante in tema di contratti pubblici è quella concernente i c.d. «*golden powers*» del governo, di cui all'art. 1-*bis* del d.l. n. 21/2012, come, da ultimo, modificato dall'art. 28 del d.l. n. 21/2022, che

ha ridefinito i poteri speciali[40] in materia di strumenti di comunicazione elettronica a banda larga basati sulla tecnologia di quinta generazione (5G) e cloud.

La disposizione in parola, infatti, qualifica i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G quali attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, ai fini dell'esercizio dei poteri speciali.

Per rafforzare ulteriormente le difese cibernetiche, il governo può, infatti, individuare altri servizi, beni, rapporti, attività e tecnologie cruciali per la sicurezza cibernetica nazionale. Tali designazioni saranno effettuate tramite uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro delle imprese e del made in Italy, il Ministro dell'interno, il Ministro della difesa, il Ministro degli affari esteri e della cooperazione internazionale e gli altri Ministri competenti per settore; verrà sentita l'Agenzia per la cybersicurezza nazionale e sarà acquisito il parere delle Commissioni parlamentari competenti prima dell'approvazione finale.

In particolare, limitandoci, per quanto qui d'interesse, alle disposizioni, del nuovo art. 1-*bis* del d.l. n. 21/2012, che pertengono alla tematica della contrattualistica pubblica: il secondo comma della disposizione modifica l'oggetto dell'obbligo di notifica funzionale all'esercizio dei poteri speciali, che fa riferimento al piano annuale degli acquisti da parte delle imprese invece che al singolo contratto. Il comma 2 dell'articolo 1-*bis* impone un obbligo informativo alle imprese che, anche attraverso contratti o accordi, intendano acquisire, a qualsiasi titolo, beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero componenti ad alta intensità tecnologica funzionali alla già menzionata realizzazione o gestione.

Prima di procedere all'acquisto, infatti, le imprese sono quindi tenute

[40] Per poteri speciali (*golden power*) si intendono, tra gli altri, la facoltà di dettare specifiche condizioni all'acquisito di partecipazioni, di porre il veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni. L'obiettivo del decreto-legge n. 21 è; stato quello rendere compatibile con il diritto europeo la disciplina nazionale dei poteri speciali del Governo, che si ricollega agli istituti della *golden share* e dell'*action spécifique* – previsti rispettivamente nell'ordinamento inglese e francese – e che in precedenza era già stata oggetto di censure sollevate dalla Commissione europea e di una pronuncia di condanna da parte della Corte di giustizia UE.

a notificare un piano nel quale sono contenute dettagliate informazioni inerenti, fra l'altro: il settore interessato dalla notifica; i dati identificativi del soggetto notificante; il programma di acquisti; i dati dei fornitori; la descrizione dei beni, dei servizi e delle componenti ad alta intensità tecnologica funzionali alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività rilevanti; un'informativa completa sui contratti in corso e sulle prospettive di sviluppo della rete 5G, ovvero degli ulteriori sistemi e attivi rilevanti; ogni ulteriore informazione funzionale a fornire un dettagliato quadro delle modalità di sviluppo dei sistemi di digitalizzazione del notificante, nonché dell'esatto adempimento alle condizioni e alle prescrizioni imposte a seguito di precedenti notifiche; un'informativa completa relativa alle eventuali comunicazioni effettuate ai fini dello svolgimento delle verifiche di sicurezza da parte del Centro di valutazione e certificazione nazionale (CVCN), inclusiva dell'esito della valutazione, ove disponibile, e delle relative prescrizioni, qualora imposte.

La norma fa salvi gli obblighi previsti dal citato decreto-legge n. 105 del 2019, che ha istituito il perimetro di sicurezza nazionale cibernetica.

Ancora, il quarto comma della disposizione esplicita i criteri e gli elementi di valutazione in base ai quali sono esercitati i poteri speciali in relazione ai piani annuali trasmessi, mentre il comma 5 disciplina il regime sanzionatorio applicabile alla violazione di obblighi imposti ai sensi dei precedenti commi e le ulteriori misure per garantire la piena attuazione della relativa disciplina.

Nel caso della normativa in parola, pertanto, l'interesse alla sicurezza cibernetica viene perseguito imponendo ai soggetti che operano all'interno del suo ambito di applicazione di pianificare gli acquisti di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero componenti ad alta intensità tecnologica funzionali alla già menzionata realizzazione o gestione, sottoponendo tale atto pianificatorio al controllo del CVCN, dalla cui valutazione può dipendere in maniera determinante l'esercizio dei poteri di veto o conformativi in capo al Governo.

Anche in questo caso, perciò, si evidenzia un netto approccio precauzionale al problema (messo ulteriormente in luce dal focus sulla programmazione degli acquisti più delicati) e una decisa integrazione tecnica dell'eventuale procedimento di applicazione dei poteri governativi.

Per quanto riguarda, anche in questo caso, il rapporto tra le istanze di trasparenza e la disciplina dei poteri speciali governativi, deve ricordarsi che l'art. 12 del d.p.r. n. 54/2021, in attuazione del d.l. n. 109/2015, afferma che «ai sensi dell'articolo 3, comma 2, del decreto-legge, la valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, strumentale ai fini dell'esercizio dei poteri speciali di cui all'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, è effettuata secondo le procedure, le modalità e i termini di cui all'articolo 1, comma 6, del decreto-legge, e di cui al presente decreto», ossia, in altri termini, le medesime procedure previste per i soggetti PSNC, cosicché anche quella che potremmo definire la "valutazione preliminare" all'esercizio dei poteri speciali del Governo sarà caratterizzata dalla medesima opacità, nei limiti che si sono visti, che caratterizza le procedure e le metodologie di test previste per gli acquisti nell'ambito del PSNC.

Sotto questo punto di vista, però, deve essere svolta una precisazione, opportunamente posta in evidenza anche dal Consiglio di Stato, sempre in sede consultiva: «non è, infatti, la valutazione preventiva per l'esercizio dei poteri speciali di cui all'articolo 1-*bis* del decreto-legge n. 21 del 2012 (potere di veto o di imposizione di specifiche prescrizioni o condizioni) che deve essere effettuata secondo le procedure, le modalità e i termini di cui all'articolo 1, comma 6, del d.l. n. 109/2015, ma solo la verifica tecnica istruttoria propedeutica alle valutazioni dell'autorità di governo preposta alla scelta tecnico-discrezionale o discrezionale-amministrativa in ordine all'esercizio (o al non esercizio) dei suddetti poteri speciali»[41].

Pertanto, pare di potersi ritenere che, anche in questo caso, le importanti deroghe al principio di trasparenza di cui si è detto debbano limitarsi a questa porzione di procedimento.

4.4. *I contratti pubblici dell'Agenzia per la Cybersicurezza Nazionale (ACN): l'assenza del principio di trasparenza e l'istituzionalizzazione della "fiducia"*

Come ricordato in dottrina, infine, «a fianco alla disciplina generale valevole per la totalità delle Pubbliche Amministrazioni si pone quel-

[41] Cons. Stato, Sezione Consultiva per gli Atti Normativi, Adunanza di Sezione del 20 ottobre 2020.

la speciale dettata per gli appalti di forniture, servizi e lavori di natura tecnologica per le attività dell'Agenzia per la Cybersicurezza Nazionale (ACN), volte alla tutela della sicurezza nazionale nello spazio cibernetico […] la quale espressamente deroga a quella generale del Codice appalti, stabilisce che le procedure di gara di cui può avvalersi l'Agenzia devono essere realizzate in conformità al c.d. "Programma biennale degli acquisti di beni e servizi e del programma triennale dei lavori pubblici di ACN"[42]; esse devono, inoltre, essere contenute nella relazione che il Presidente del Consiglio dei Ministri presenta al Copasir»[43].

In particolare, il D.P.C.M. 1° settembre 2022, n. 166 (ossia il "Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico") – posto che «le procedure di cui all'articolo 2 sono espletate in coerenza con i principi di economicità, efficacia, tempestività, proporzionalità, correttezza e non discriminazione e comunque con modalità idonee ad assicurare la tutela della sicurezza nazionale nello spazio cibernetico» – stabilisce alcune regole specifiche concernenti, innanzitutto, gli operatori economici ammessi a contrattare con ACN e, in secondo luogo, le modalità di affidamento dei contratti.

Per quanto concerne il primo aspetto, i contratti di lavori, forniture e servizi sono affidati ad operatori economici che, oltre a possedere i requisiti di cui all'articolo 8[44], rispondono anche a criteri di affidabilità

[42] Salvo nei seguenti casi: a) per sopravvenute e indifferibili esigenze di acquisizione di lavori, beni e servizi necessari allo svolgimento delle attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico; b) quando ricorre la necessità di eliminare, mitigare o prevenire vulnerabilità, eventi di natura cibernetica, ovvero situazioni di rischio delle reti, dei sistemi informativi e dei servizi informatici, ovvero delle comunicazioni elettroniche, da cui possa derivare un pregiudizio, per la sicurezza nazionale nello spazio cibernetico, anche al fine di assicurarne la resilienza.

[43] S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit., 350.

[44] Ossia, «a) l'assenza dei motivi di esclusione di cui all'articolo 80 del Codice; b) il possesso dei requisiti di idoneità professionale, la capacità economico-finanziaria e quella tecnico-professionale proporzionati all'oggetto dell'appalto; c) il possesso dei requisiti di sicurezza laddove connessi alla natura e peculiarità dell'appalto». Peraltro, ai sensi del successivo art. 9, «I requisiti di cui all'articolo 8 devono essere posseduti per l'intera durata della procedura di affidamento di lavori, servizi e forniture e fino alla completa esecuzione contrattuale senza soluzione di continuità, pena il recesso immediato

eventualmente individuati nella determina a contrarre, in relazione alla natura, all'oggetto e alla finalità dell'appalto; inoltre, gli operatori economici hanno l'obbligo di mantenere riservati i dati e le informazioni dei quali vengano comunque a conoscenza, di non divulgarli in alcun modo e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente connessi alla procedura di affidamento (art. 7).

In particolare, la valutazione della capacità economica degli operatori è effettuata in relazione agli elementi di natura finanziaria e patrimoniale desumibili dai bilanci, dalle dichiarazioni di affidabilità rese da istituti bancari o intermediari autorizzati e dalle dichiarazioni concernenti il fatturato o le forniture nel settore realizzate nell'ultimo triennio, mentre la valutazione delle capacità tecnico-organizzative e professionali è effettuata in relazione all'organizzazione e all'organico degli operatori economici, alle attrezzature e ai macchinari, alle certificazioni o abilitazioni possedute, alle qualificazioni professionali del personale dipendente e ad ogni altro elemento utile, ivi compreso il ricorso all'avvalimento di imprese ausiliarie (art. 10).

Infine, sempre sotto il profilo della parte contraente, è molto rilevante l'art. 12 del D.P.C.M. n. 166/2022, concernente il subappalto: a tal proposito, infatti, la disposizione stabilisce che ACN può escludere il subappalto laddove le prestazioni devono essere eseguite direttamente dall'aggiudicatario in ragione delle specifiche caratteristiche dell'appalto, ma che quando è previsto dagli atti della procedura di affidamento di lavori, servizi e forniture, gli operatori economici possono chiedere l'autorizzazione al subappalto in sede di presentazione dell'offerta, precisando la percentuale e la tipologia della prestazione che intendono subappaltare. L'autorizzazione al subappalto da parte dell'Agenzia è subordinata alla verifica dei requisiti di cui all'articolo 8, del menzionato decreto, in capo ai subappaltatori e, ferma la responsabilità dell'appaltatore per l'esatto adempimento delle obbligazioni del contratto principale stipulato con l'Agenzia, lo stesso appaltatore e il subappaltatore sono responsabili in

dell'Agenzia dal rapporto negoziale mediante semplice comunicazione, in caso di perdita dei requisiti dopo la stipula del contratto […] In caso di recesso dell'Agenzia, fatto sempre salvo il diritto di quest'ultima al risarcimento del danno, il contraente ha diritto al solo pagamento del valore dei lavori già eseguiti, dei beni ceduti o dei servizi regolarmente prestati e al rimborso delle spese sostenute per l'esecuzione della restante parte, nei limiti delle utilità conseguite».

solido nei confronti dell'Agenzia, in relazione alle prestazioni oggetto del contratto di subappalto.

Per quanto riguarda, invece, i metodi di affidamento, l'art. 13 prevede che l'acquisizione di lavori, servizi e forniture può essere effettuata attraverso le seguenti procedure: «a) affidamento diretto di cui all'articolo 14, per lavori di importo inferiore a 150.000 euro e per servizi e forniture di importo inferiore a 139.000 euro; b) procedura negoziata previo o senza previo esperimento di gara informale di cui all'articolo 15, per affidamenti di lavori di importo pari o superiore a 150.000 euro e di servizi e forniture di importo pari o superiore a 139.000 euro; c) accordo quadro di lavori, servizi e forniture, di durata massima di nove anni, quando non è possibile l'immediata ed esatta quantificazione dei lavori da eseguire, dei beni da fornire e dei servizi da prestare, ferma restando la predeterminazione della spesa massima complessiva e la facoltà di recesso dell'Agenzia senza che alcun compenso, a nessun titolo, sia dovuto al contraente per le prestazioni non eseguite; d) dialogo competitivo per l'affidamento di lavori, servizi e forniture; e) partenariato pubblico-privato per l'affidamento di lavori, servizi e forniture»[45].

Ciò posto in termini generali, possono svolgersi anche in questo caso alcune considerazioni aventi riguardo il rapporto con il principio di trasparenza.

Come si è scritto, per gli acquisti dell'Agenzia per la Cybersicurezza Nazionale (ACN), la normativa di riferimento è il d.p.c.m. 1° settembre 2022, n. 166, che riguarda esclusivamente, ai sensi dell'art. 2, c. 1, le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, rispetto alle quali – è bene rimarcarlo – l'art. 2, c. 2, stabilisce che si debba «dare espressa e adeguata motivazione nella determina a contrarre».

Ai sensi dell'art. 3 del medesimo decreto (rubricato "principi generali"), le procedure di cui all'articolo 2 sono espletate in coerenza con i principi di economicità, efficacia, tempestività, proporzionalità, correttez-

[45] Il c. 2 della medesima disposizione precisa, inoltre, «l'utilizzo degli strumenti di acquisto messi a disposizione dalla società CONSIP S.p.a. è ammesso soltanto quando le condizioni e le modalità dell'appalto risultino compatibili con le esigenze di tutela della sicurezza nazionale nello spazio cibernetico e di tempestività dell'Agenzia».

za e non discriminazione e comunque con modalità idonee ad assicurare la tutela della sicurezza nazionale nello spazio cibernetico.

Non si può non notare, nell'ambito di una formulazione che richiama evidentemente – e, forse, pleonasticamente – i principi di cui al codice dei contratti pubblici, l'assenza espressa del principio di trasparenza, che pare immediatamente bilanciata dal legislatore con l'indicazione espressa dell'esigenza di adottare modalità idonee ad assicurare la tutela della sicurezza nazionale nello spazio cibernetico.

La mancata enunciazione del principio di trasparenza, evidentemente, risulta del tutto giustificata dal particolare contesto (e dalle finalità) di utilizzo degli acquisti in parola; si tratta, fra quelli che si sono enucleati, del livello più profondo della normativa in materia di cybersicurezza ed è inevitabile che alle procedure "ordinarie" si sostituiscano percorsi "speciali", in cui le esigenze di accessibilità e comprensibilità dell'azione amministrativa vengono sacrificate o, comunque, poste sullo sfondo.

Ad ogni modo, anche in questo caso, è bene tenere a mente l'importante precisazione contenuta nell'art. 2 del decreto in parola: il regime speciale non si applica a tutti i contratti di ACN, ma solo ed esclusivamente ai contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, e solo previa e specifica motivazione.

Infine, deve ricordarsi che, ai sensi dell'art. 21 del decreto, «degli affidamenti di lavori, servizi e forniture disposti ai sensi dell'articolo 3, comma 2, lettere a) e b), è data dall'Agenzia comunicazione al COPASIR tempestivamente e, comunque, non oltre trenta giorni dalla conclusione delle procedure di affidamento»; inoltre, «degli affidamenti di cui al comma 1 è data altresì un'organica illustrazione nella relazione del Presidente del Consiglio dei ministri al COPASIR di cui all'articolo 14, comma 2, del decreto-legge».

In altri termini, al livello più profondo della normativa in discussione, dove, per ragioni di sicurezza nazionale, la segretezza tende a prevalere sulla trasparenza, determinando la possibile opacità di ampie porzioni procedimentali, il meccanismo fiduciario viene, in un certo qual modo, recuperato, tramite una sua istituzionalizzazione o una sua "internalizzazione".

5. *Considerazioni a carattere conclusivo*

Sulla base di quanto sin qui scritto, è possibile svolgere alcune considerazioni a carattere conclusivo con riguardo al rapporto fra cybersicurezza, contratti pubblici e trasparenza amministrativa.

Da un punto di vista generale, deve segnalarsi come, in ragione delle innovazioni normative introdotte con il codice dei contratti del 2023, prima, e con la legge nazionale sulla cybersicurezza del 2024, poi, un primo grande mutamento riguardi la natura giuridica della sicurezza informatica, che passa da semplice "oggetto" di acquisto (un servizio o un *software* da comprare), a interesse pubblico primario da integrare in tutti gli acquisti tecnologici.

Ancora, sempre in chiave ricostruttiva, l'approccio del legislatore italiano, specialmente con il codice del 2023, mira evidentemente ad utilizzare il *procurement* pubblico come uno strumento di politica industriale: imponendo standard elevati e criteri di valutazione che premiano soluzioni sicure e resilienti sotto il profilo della cybersicurezza, si obbliga di fatto il mercato a innalzare la qualità dei prodotti offerti, determinando un circolo virtuoso, in base al quale l'amministrazione si protegge e, contemporaneamente, fa propendere l'intero ecosistema ICT nazionale verso livelli di resilienza più elevati.

Per quanto concerne, invece, il rapporto con il principio di trasparenza, si potrebbe a tutti gli effetti trattare di una trasparenza a geometria variabile.

Per quanto concerne il piano dell'organizzazione (ossia dei mezzi digitali utilizzati dalle stazioni appaltanti), si è visto come la dinamicità del rapporto sussistente fra trasparenza e riservatezza sia derivabile dal complesso delle disposizioni tecniche che trovano applicazione alle piattaforme di approvvigionamento digitale, la fiducia nelle quali è garantita tramite la certificazione, al contempo, della loro trasparenza e della loro sicurezza cibernetica, la quale, a sua volta è determinata anche dalla predisposizione di alcune aree di opacità (circa gli aspetti più delicati delle piattaforme stesse).

Sul piano, invece, dell'amministrazione attiva, la dinamica del menzionato rapporto segue il declinarsi, su diversi piani, della normativa da applicare, la cui stratificazione dipende essenzialmente dall'aumentare del

rischio cibernetico al modificarsi del contesto di utilizzo degli strumenti digitali in discussione. Si possono perciò svolgere alcune distinzioni.

In primo luogo, nei casi riconducibili alla disciplina generale e a quella legata agli acquisti il cui contesto di utilizzo sia connesso alla tutela degli interessi nazionali strategici, la cybersicurezza è evidentemente perseguita attraverso il "direzionamento" della discrezionalità tecnica delle stazioni appaltanti e il problema della trasparenza si pone essenzialmente rispetto all'accessibilità e alla comprensibilità dei parametri stessi.

Negli altri casi, invece, il procedimento di approvvigionamento di ACN e delle amministrazioni che operano nel PSNC risulta fortemente integrato da sub procedimenti affidati a soggetti tecnici specializzati che influenzano in maniera determinante, con le loro valutazioni, la procedura di acquisizione: in questi casi l'ordinamento pone veri e propri limiti all'accessibilità di alcuni documenti o di alcuni procedimenti *tout court*.

In altre parole, se ai livelli più superficiali e meno delicati della disciplina la trasparenza amministrativa continua a ricoprire un ruolo di fondamentale importanza, sostenendo il rapporto di fiducia che deve intercorrere fra le parti in gioco, nonché fra l'amministrazione e la collettività, rendendo possibili forme più o meno incisive di controllo sull'attività della prima, quando si scende verso il livelli più profondi e critici della normativa sulla sicurezza cibernetica nazionale, le esigenze di trasparenza cedono necessariamente il passo a quelle di segretezza: in questi casi, è evidente che a garantire la fiducia fra le parti sia la netta integrazione tecnica dei procedimenti e la sussistenza di obblighi informativi nei confronti degli organi apicali dell'infrastruttura nazionale di cybersicurezza.

In definitiva, però, ciò che emerge dall'analisi normativa che si è svolta è che, sebbene nel particolare contesto qui d'interesse il principio di trasparenza (che soprattutto a seguito dell'imponente fenomeno di digitalizzazione, avvenuto con la più recente codificazione, rappresenta una sorta di super principio della materia dei contratti pubblici) debba venire a patti con la segretezza che tipicamente determina l'efficacia della materia della sicurezza informatica (e, più in generale, della sicurezza nazionale), l'intenzione del legislatore sia chiaramente quella di limitare al minimo indispensabile il sacrificio delle garanzie di comprensibilità e conoscibilità che devono informare le attività di *procurement* pubblico: di qui tutte le precisazioni che si sono messe in luce circa il concreto ambito di operatività delle deroghe al regime ordinario[46].

[46] In chiusura, tuttavia, vale la pena di segnalare come, a fronte di un quadro così

Abstract

Il presente lavoro analizza l'articolata relazione tra la disciplina della sicurezza cibernetica nazionale e la normativa sui contratti pubblici, utilizzando come lente d'osservazione privilegiata il principio di trasparenza. In un contesto caratterizzato da una crescente "stratificazione" normativa, lo studio esamina come le esigenze di protezione delle infrastrutture digitali dello Stato entrino in tensione con i canoni di accessibilità e conoscibilità che informano il *procurement* pubblico.

l'analisi evidenzia come il rapporto fra trasparenza e segretezza non possa essere interpretato in termini binari di mutua esclusione, bensì come una relazione dinamica e necessaria. Sebbene le esigenze di sicurezza nazionale impongano deroghe al regime ordinario di accesso, l'intenzione del legislatore appare orientata a limitare tali sacrifici al minimo indispensabile, istituzionalizzando, ove necessario, la fiducia attraverso procedimenti integrati e obblighi informativi verso gli organi apicali del sistema di *governance* della sicurezza cibernetica nazionale.

National cybersecurity and public procurement regulation: the current regulatory "stratification" and the relationship with the principle of transparency

This paper analyzes the complex relationship between national cybersecurity regulations and public procurement law, using the principle of transparency as a primary lens of observation. In a context characterized by increasing regulatory "stratification" the study examines how the requirements for protecting the State's digital infrastructure clash with the standards of accessibility and disclosure that inform public procurement.

The analysis highlights that the relationship between transparency and secrecy cannot be interpreted in binary terms of mutual exclusion, but rather as a dynamic and necessary relationship. Although national security needs impose derogations from the ordinary access regime, the legislator's intent appears oriented toward limiting such sacrifices to the

complesso, sarebbe opportuno che le norme in esame presentassero – in assenza di una vera e propria ricomprensione nel codice dei contratti pubblici – precisi rinvii ai corpi normativi di riferimento, al fine di rendere più agevole il lavoro degli interpreti.

minimum necessary, institutionalizing trust, where required, through integrated procedures and information obligations toward the top-level bodies of the national cybersecurity governance system