RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0149 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Lorenzo Nannipieri

Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio

L'Autore è ricercatore presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. L'art. 10 del DDL 1717 è finalizzato ad introdurre una «disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici».

Nello spirito dell'iniziativa legislativa, come risultante dalla relazione tecnica al DDL, le disposizioni proposte mirerebbero a promuovere maggiore garanzia delle esigenze di cybersicurezza nelle ipotesi in cui le attività di approvvigionamento delle PP.AA. siano connesse alla tutela degli interessi nazionali strategici.

Prima di esaminare il contenuto dell'articolo, occorre premettere che le disposizioni devono essere lette nel quadro normativo vigente in seguito all'entrata in vigore del nuovo codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36) e, segnatamente, delle novità introdotte dall'art. 108 del codice stesso.

Quest'ultima disposizione, nel regolamentare l'aggiudicazione di appalti, servizi e forniture sulla base del criterio dell'offerta economicamente più vantaggiosa, prevede (comma 4) che gli «elementi di cybersicurezza» debbano costituire un contenuto indefettibile dei documenti di gara nella scelta in ordine ai criteri di aggiudicazione dell'offerta ritenuti maggiormente pertinenti rispetto alla natura, all'oggetto e alle caratteristiche del contratto e al fine di individuare il miglior rapporto qualità prezzo per l'aggiudicazione.

L'esame della disposizione codicistica – pur problematica, sotto vari aspetti – esula dall'oggetto del presente contributo, ai fini del quale appare però necessario ricordare che il codice ha posto a carico delle stazioni appaltanti un generale obbligo di «considerazione» degli aspetti legati alla cybersicurezza, che subisce un aggravamento (invero piuttosto imprecisato) negli ambiti in cui l'attività appaltata intercetta gli interessi nazionali strategici.

Le misure adottate (o proposte) dal legislatore italiano si collocano nell'ambito della complessiva strategia nazionale per la cybersicurezza secondo cui «ogni Stato membro adotta una strategia nazionale per la cybersicurezza che prevede gli obiettivi strategici e le risorse necessarie per

conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza» (Direttiva NIS 2, art. 7, comma 1).

La citata direttiva pone in capo agli Stati membri l'obbligo di adottare misure strategiche riguardanti, tra l'altro, «l'inclusione e la definizione di requisiti concernenti la cybersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cybersicurezza, alla cifratura e l'utilizzo di prodotti di cybersicurezza open source» (art. 7, comma 2, lett. b).

2. Il primo comma dell'art. 10 prevede – oggi divenuto art. 13 nella versione attualmente in esame, comprensiva degli emendamenti approvati durante l'esame in commissione in sede referente nella sessione dell'8 maggio 2024 – che «con decreto del Presidente del Consiglio dei ministri, da adottare entro centoventi giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, 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, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO). Ai fini del presente articolo, per «elementi essenziali di cybersicurezza» si intende l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo».

Sul piano oggettivo, la disposizione 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 non riferibile agli appalti per l'approvvigionamento di beni e servizi informatici in «contesti» diversi da quelli connessi alla tutela, appunto, degli «interessi nazionali strategici».

In tale ultimo ambito, peraltro, la disposizione intercetta la formulazione del (già vigente) art. 108, co. 4, d.lgs. 36/2023, già richiamato nelle premesse.

Problematica, però, è l'individuazione di un concetto positivo di «interesse nazionale strategico», ricorrente sia nel DDL 1717 che nel codice.

Sul punto, il DDL 1717 parrebbe operare un rimando implicito agli artt. 5 e 7 del d.l. 82/2021 che, nell'istituire l'ACN, ne affida il ruolo di tutore degli «interessi nazionali nel campo della cybersicurezza», affidando all'Agenzia anche la funzione di promotrice delle azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche riguardo «a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore».

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. 15 marzo 2012, n. 21, recante «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. 5 dicembre 2022, n. 187, recante «misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici»).

Quello che parrebbe 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 (per una definizione di «funzione essenziale dello stato», parzialmente affine a quella di «interesse nazionale strategico», si rinvia all'art. 2, co. 1, lett. a), d.P.C.M. 30 luglio 2020, n. 131, secondo cui «un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la

sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti»).

Allo stato attuale, specialmente in considerazione della grande proliferazione di norme di rango primario e regolamentare, sembra esistere effettivamente un problema tassonomico/definitorio, la cui risoluzione appare urgente sia per garantire efficacia al diritto positivo che per ridurre al massimo i rischi di contenzioso amministrativo in un settore – quello degli appalti – già di per sé particolarmente critico, tanto da essere destinatario, ormai «storicamente», di specifiche misure normative deflattive.

La seconda nozione che delimita l'ambito oggettivo di applicazione dell'art. 10 è quella di «elementi essenziali di cybersicurezza», dizione ricorrente, anch'essa, nel già citato art. 108, co. 4, del d.lgs. 36/2023.

Rispetto a quest'ultima disposizione, l'art. 108 DDL 1717 ha il pregio di sperimentare un'*actio finium regundorum*, fornendo una definizione normativa di «elementi essenziali di cybersicurezza», da intendersi come «l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo».

Si tratta di un tentativo da apprezzare positivamente, atteso che l'intervento pare colmare una lacuna lasciata dalla formulazione piuttosto vaga dell'art. 108, comma 4, d.lgs. 36/2023 che, in effetti, nel riferirsi agli «elementi di cybersicurezza» non ne ha sufficientemente circoscritto l'ambito definitorio.

Rimane ferma, però, l'esigenza di distinguere gli «elementi essenziali di cybersicurezza» dagli «elementi di cybersicurezza» di cui all'art. 108 del codice, atteso che il requisito dell'essenzialità (presente nell'art. 10 in commento ma non nell'art. 108, comma 4, del codice) appare, a propria volta, un concetto sfuggente e di difficile delimitazione.

L'ambito soggettivo di applicazione dell'art. 10 del DDL si desume dal combinato disposto dell'art. 10, comma 1, del DDL 1717, da un lato e, dall'altro lato, gli artt. 2 d.lgs. 82/2005 (Codice dell'amministrazione digitale) e 1, comma 2, d.lgs. 30 marzo 2001, n. 165 (T.U.P.I.) individuando, quali destinatari, i seguenti soggetti:

1. Amministrazioni dello Stato, istituti e scuole di ogni ordine e grado, istituzioni educative, aziende ed amministrazioni dello Stato ad ordinamento autonomo, Regioni, Province, Comuni, Comunità montane e loro consorzi e associazioni, istituzioni universitarie, Istituti autonomi case popolari, Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, amministrazioni, aziende ed enti del Servizio sanitario nazionale, ARAN, altre Agenzie di cui al d.lgs. 30 luglio 1999, n. 300;
2. autorità di sistema portuale;
3. autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
4. gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
5. società a controllo pubblico, con esclusione delle società quotate.

Questo elenco di destinatari delle disposizioni in materia di appalti pubblici contenute nel DDL 1717 appare decisamente ampio.

Come osservato in sede istruttoria (cfr. audizione dell'ANCI), l'ambito di applicazione della disposizione dovrebbe essere meglio specificato, in quanto il rinvio *per relationem* all'art. 2, co. 2, d.lgs. 82/2005 condurrebbe ad una generalizzata efficacia applicativa della disposizione anche a soggetti che non svolgono attività di approvvigionamento di beni e servizi informatici legati alla tutela di interessi nazionali strategici.

Si pensi, ad esempio, alla generalità delle società a controllo pubblico, ovvero agli istituti di istruzione ovvero, ancora, alla generalità indiscriminata degli enti locali.

Il terzo comma allarga ulteriormente la portata applicativa della norma, ricomprendendo anche i soggetti privati inclusi nel perimetro di sicurezza nazionale cibernetica di cui all'art. 1 d.l. 21 settembre 2019, n. 105.

Si tratta degli operatori 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, è istituito il perimetro di sicurezza nazionale cibernetica» (art. 1, comma 1, d.l. 105/2019).

L'elencazione di tali soggetti è contenuta in un atto amministrativo della Presidenza del Consiglio dei Ministri su proposta del Comitato Interministeriale per la Cybersicurezza, sottratto al diritto di accesso e agli obblighi di pubblicazione (art. 1, comma 2-*bis*, d.l. 105/2019).

3. Il secondo comma dell'art. 10 del DDL 1717 prevede che «nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza (…) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1».

In buona sostanza, nelle ipotesi in cui la stazione appaltante ritenga non rispettati i requisiti previsti dall'emanando d.P.C.M. in tema di «elementi essenziali di cybersicurezza» nella predisposizione dell'offerta, diverrebbe possibile procedere con la non aggiudicazione dell'appalto stesso all'offerente che abbia presentato l'offerta economicamente più vantaggiosa.

Dal punto di vista sistematico, la disposizione avrebbe trovato una migliore collocazione nell'art. 108 del codice e non in un testo normativo ad esso estraneo.

Il rinvio all'art. 107, comma 2, d.lgs. 36/2023, appare frutto di una tecnica normativa di dubbia apprezzabilità, atteso che la citata disposizione codicistica è riferita a vizi dell'offerta attinenti a fattori del tutto distinti dalla cybersicurezza (obblighi in materia ambientale, sociale e del lavoro), circostanza che renderebbe opportuna, semmai, una revisione dello stesso art. 107, comma 2, del codice ovvero del successivo art. 108, piuttosto che l'inserimento in un distinto provvedimento normativo di una disposizione che, di fatto, ne allarghi l'ambito applicativo.

Inoltre, per quanto l'intera disposizione avrebbe trovato una miglior collocazione sistematica altrove, il «gancio» normativo con le facoltà di cui all'art. 108, comma 10, del codice (non aggiudicazione dell'appalto in caso di inidoneità di tutte le offerte rispetto all'oggetto del contratto) appare congruo in quanto il rinvio è riferito, in questo caso, ad una disposizione codicistica formulata in termini generali.

Al punto b), il comma 2 dispone che le Stazioni Appaltanti «tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione».

La disposizione appare ridondante rispetto a quanto già previsto dall'art. 108 del codice, nella parte in cui si prevede che «le stazioni appaltanti, incluse le centrali di committenza, 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 e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici».

Stesso dicasi per la lettera d), secondo cui le Stazioni Appaltanti, «nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento». La disposizione sembra ricalcare pedissequamente quanto già previsto dall'art. 108, comma 4, penultimo periodo, del codice, nella parte in cui è specificato che «quando i beni e 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 10 per cento».

In sede di esame in commissione, è stato approvato un emendamento con cui si è proposto di aggiungere una lettera d-bis), secondo cui le Stazioni Appaltanti «prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza».

Innovativa, invece, appare la previsione della lettera c), che introduce l'obbligo di inserimento

degli elementi di cybersicurezza tra i requisiti minimi dell'offerta, anche nel caso di utilizzo del criterio del minor prezzo, di cui all'art. 108, comma 3, del codice.

In buona sostanza, ll DDL 1717 parrebbe determinare un effetto estensivo delle prescrizioni dell'art. 108, quarto comma (riferite agli appalti affidati con il criterio dell'offerta economicamente più vantaggiosa) anche ai casi di utilizzo del criterio del minor prezzo.

Anche in questo caso, però, l'intervento legislativo avrebbe trovato una migliore collocazione sistematica direttamente nel codice.

Inoltre, l'implementazione – *de facto* – della portata prescrittiva dell'art. 108 del codice parrebbe foriera del rischio di apportare un deciso aggravio in termini di contenzioso amministrativo, specialmente per il carattere non sufficientemente delineato della nozione di «interessi nazionali strategici», dei diversi adempimenti che gli operatori sarebbero chiamati a rispettare in punto di cybersicurezza (elementi «essenziali» o meno di cybersicurezza, a seconda dei casi) e della latitudine della discrezionalità riservata alle Stazioni appaltanti per la valutazione delle offerte in punto di adempimenti cyber.

Ancor più critica, sul piano sistematico, è la previsione di cui al comma 4, nella versione riformulata con una proposta emendativa approvata durante l'esame in commissione in sede referente, secondo cui «resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di *information and communication technology* destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo 1».

Al di là del merito della questione, risulta piuttosto sfuggente la logica di introdurre una disposizione normativa di rango primario finalizzata a «mantenere ferma» un'altra norma di pari rango, mai abrogata.