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

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0197 • articolo sottoposto a peer review • pubblicato in anteprima il 19 dic. 2024

Lorenzo Nannipieri

Cybersicurezza e appalti. Interventi legislativi e prime criticità

Negli ultimi anni sta emergendo, nell'ordinamento italiano, la relazione tra contratti pubblici e cybersicurezza. Con una serie di interventi normativi succedutisi a breve distanza di tempo, il legislatore ha innestato con vigore la sicurezza informatica nell'ambito della disciplina degli appalti. Il presente contributo evidenzia i tratti salienti della normativa vigente, sottolineandone alcuni punti critici, in attesa che l'intero quadro regolatorio venga recepito dalle amministrazioni e interpretato dalla giurisprudenza.

Cybersicurezza – Appalti – Contratti pubblici

Cybersecurity and procurement. Legislative interventions and initial critical issues

Recently, the relationship between public contracts and cybersecurity has been emerging at a regulatory level. With a series of regulatory interventions that followed one another in a short space of time, the Italian legislator has vigorously included cybersecurity in the context of procurement regulations. This contribution highlights the salient features of the current legislation, highlighting some critical points, waiting for the entire regulatory framework to be implemented by the administrations and interpreted by administrative courts case-law.

Cybersecurity – Public procurement – Public contracts

L'Autore è ricercatore presso l'Istituto di Informatica Giuridica e Sistemi Giudiziari del CNR

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

1. Le norme applicabili

Negli ultimi anni, il tema della cybersicurezza ha acquisito un deciso "slancio" nella produzione normativa, disancorandosi da disamine proprie di ambiti extra-giuridici della conoscenza per approdare nel campo delle politiche pubbliche e, in definitiva, del diritto sostanziale, tanto da introdurre un nuovo tema di dibattito, legato all'esistenza di un "diritto alla cybersicurezza" di matrice individuale o collettiva[1].

La cybersicurezza è diventata un tema cruciale nel diritto contemporaneo, poiché il crescente utilizzo di tecnologie digitali espone individui, aziende e Stati a nuovi rischi e minacce informatiche. La protezione delle informazioni e dei sistemi digitali è ormai una necessità, non solo dal punto di vista tecnico, ma anche giuridico. In un contesto globalizzato, dove le normative nazionali sono spesso insufficienti a garantire una protezione adeguata, emergono nuove sfide legate alla governance della cybersicurezza e all'impatto non solo sui diritti dei cittadini ma anche sull'organizzazione amministrativa e sulla gestione dei servizi pubblici, finendo per intersecare in modo tangibile l'organizzazione delle Pubbliche Amministrazioni.

La P.A., come noto, è destinataria di stringenti obblighi derivanti, da ultimo, dall'attuazione della Direttiva NIS 2[2], come recepita dal d.lgs. 4 settembre 2024, n. 138[3].

Se, da un lato, la NIS 2 apporta una cospicua serie di obblighi alla generalità delle Pubbliche Amministrazioni, dall'altro, ulteriori fonti normative si sono susseguite e stratificate in merito ad ambiti *particolari* dell'attività amministrativa.

Tra questi rientra il settore in cui le Amministrazioni condensano i propri poteri di scelta dei contraenti per l'esecuzione di lavori, servizi e forniture, e cioè gli appalti pubblici[4].

Il tema è attualmente oggetto di alcune disposizioni normative, tutte di recentissima produzione e contenute, sostanzialmente, in tre fonti tra loro eterogenee: il codice dei contratti pubblici (d.lgs. n. 36/2023), la l.n. 90/2024 e il decreto di recepimento della Direttiva NIS 2 (d.lgs. n. 138/2024).

1. Cfr., senza pretesa di esaustività, Camisa-Simoncini 2024; Longo 2024; Moroni 2024; Di Corinto 2022; Simoncini 2021; De Vergottini 2019, p. 67 ss.
2. In conformità all'art. 7, comma 1, della Direttiva NIS 2, ciascuno Stato membro è tenuto a elaborare una strategia nazionale per la cybersicurezza, la quale deve definire non solo obiettivi strategici ma anche le risorse e gli strumenti normativi e operativi necessari per il loro perseguimento. Lo scopo è garantire e mantenere un livello elevato e costante di protezione contro le minacce cibernetiche, mediante l'adozione di misure strategiche e normative idonee a rispondere alle sfide in evoluzione. 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).
3. Cfr. Casarosa 2024; Pietrangelo 2024; Buffa 2023.
4. Cocchi 2024; Rossa 2024; sia altresì consentito rinviare a Nannipieri 2024.

L'art. 19 del codice dei contratti pubblici contiene quello che è stato definito in dottrina come il «manifesto di politica di cybersicurezza»[5], enunciando, rispettivamente, al comma 1, il principio secondo cui le stazioni appaltanti «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»; al comma 5, che gli stessi soggetti «adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali. Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento».

L'art. 14 del d.lgs. 28 giugno 2024, n. 90 (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici) rappresenta la disposizione centrale in materia di cybersicurezza e appalti. La disposizione, che si connota per una formulazione particolarmente articolata, prevede che:

> «1. 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 (…), 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) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. Ai fini del presente articolo, si intende per "elementi essenziali di cybersicurezza" 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.
> 2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:
> a) 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;
> b) 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;
> c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta;
> d) 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;
> e) 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 o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.
> 3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inseriti nell'elencazione di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

5. Rossa 2024, p. 342.

> 4. 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».

L'art. 108, comma 4, del codice dei contratti pubblici, poi, prevede che

> «nelle attività di approvvigionamento di beni e servizi informatici, 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».

Merita attenzione, *a latere*, l'art. 26 del codice che, nella formulazione attuale, prevede che

> «1. I requisiti tecnici delle piattaforme di approvvigionamento digitale, nonché la conformità di dette piattaforme a quanto disposto dall'articolo 22, comma 2, sono stabilite dall'AGID di intesa con l'ANAC e la Presidenza del Consiglio dei ministri, Dipartimento per la trasformazione digitale, entro sessanta giorni dalla data di entrata in vigore del codice.
> 2. Con il medesimo provvedimento di cui al comma 1 sono stabilite le modalità per la certificazione delle piattaforme di approvvigionamento digitale.
> 3. La certificazione delle piattaforme di approvvigionamento digitale, rilasciata dall'AGID, consente l'integrazione con i servizi della Banca dati nazionale dei contratti pubblici. L'ANAC cura e gestisce il registro delle piattaforme certificate».

Tale ultima disposizione è oggetto dell'intervento correttivo attualmente all'esame delle Camere[6], secondo cui l'AgID dovrebbe stabilire non i «requisiti tecnici delle piattaforme digitali di e-procurement», bensì «le modalità di certificazione dei medesimi requisiti tecnici delle citate piattaforme di approvvigionamento e la loro conformità all'ecosistema nazionale di approvvigionamento digitale».

Queste modalità di certificazione, peraltro, dovrebbero essere stabilite dall'AgID d'intesa non più solo con l'ANAC e la Presidenza del Consiglio dei ministri – Dipartimento per la trasformazione digitale, ma anche con l'Agenzia per la cybersicurezza nazionale, in ragione della sua specifica competenza.

Da ultimo, deve rilevarsi che il d.lgs. 4 settembre 2024, n. 138, nel recepire la Direttiva NIS 2, ha previsto, all'art. 24, comma 2, che le misure cui i c.d. "soggetti NIS" (essenziali e importanti) sono chiamati ad adottare, dovranno necessariamente contemplare misure finalizzate a garantire la «sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi».

2. Il ruolo centrale (e talvolta ripetitivo) dell'art. 14 della l. n. 90/2024

La disposizione centrale relativa all'impatto della cybersicurezza nelle procedure di appalto è costituita dall'art. 14 della l. 90/2024.

Preliminarmente, non può non evidenziarsi come la collocazione sistematica della disciplina desti qualche perplessità, in relazione all'esistenza di una fonte organica di regolamentazione della materia, e cioè il codice dei contratti pubblici.

L'art. 14 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».

Come precisato nella relazione tecnica allegata al disegno di legge, le norme introdotte dalla l. n. 90/2024 si prefiggono l'obiettivo primario di garantire un rafforzamento delle tutele connesse alle esigenze di cybersicurezza. Questo aspetto riveste particolare rilievo in tutte le ipotesi in cui le procedure di approvvigionamento delle Pubbliche Amministrazioni siano funzionalmente legate alla salvaguardia degli interessi strategici nazionali.

È utile ricordare, come già premesso, che il codice dei contratti pubblici impone alle stazioni appaltanti un obbligo generale di considerare gli *elementi* di cybersicurezza. Tale obbligo assume carattere più stringente – ancorché con contorni

6. A.G. n. 226, "Schema di decreto legislativo recante disposizioni integrative e correttive al codice dei contratti pubblici di cui al decreto legislativo 31 marzo 2023 n. 36"; si rinvia, sul punto, al parere favorevole espresso in sede consultiva da Cons. Stato, Comm. Spec., 2 dicembre 2024, n. 1463/2024.

applicativi non del tutto definiti – in tutti quei casi in cui l'appalto riguardi attività incidenti sugli interessi nazionali strategici.

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".

In tale ultimo ambito, peraltro, la disposizione intercetta la formulazione dell'art. 108, comma 4, d.lgs. 36/2023, già richiamato nelle premesse.

Problematica, però, è l'individuazione di un concetto positivo di "interesse nazionale strategico", ricorrente sia nell'articolo in esame che nel codice.

Sul punto, l'art. 14 della l. n. 90/2024 parrebbe operare un rimando implicito agli artt. 5 e 7 del d.l. 82/2021 che, nell'istituire l'ACN, le 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. 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[7].

Alcuni commentatori, sul punto, hanno rilevato che la nozione di "interessi nazionali strategici" di cui all'art. 14 della l. n. 90/2024 rappresenti una categoria più ampia rispetto ad altre simili, come quella di "sicurezza nazionale" di cui al d.l. 105/2019, nell'ambito della disciplina del Perimetro di sicurezza nazionale cibernetica[8].

Allo stato attuale, specialmente in considerazione della grande proliferazione di norme di rango primario e regolamentare, sembra esistere

7. Per una definizione di "funzione essenziale dello Stato", parzialmente affine a quella di "interesse nazionale strategico", si rinvia all'art. 2, comma 1, lett. a), d.P.C.M. 131/2020, 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».

8. Così Rossa 2024, p. 354, il quale evidenzia, sul punto, che tale interpretazione "estensiva" della categoria degli interessi nazionali strategici «pare essere confermata dall'art. 10 co. 1 e co. 3 del citato d.d.l. 16 febbraio 2024 A.C. 1717. Nell'elencare coloro i quali sono tenuti a rispettare gli elementi essenziali di cybersecurity nelle procedure di aggiudicazione di beni informatici, la norma menziona due distinte tipologie di soggetti: quelli indicati dall'art. 2, co. 2, d.lgs. n. 82/2005 (ovvero: Pubbliche Amministrazioni, gestori di servizi pubblici e società a controllo pubblico) e quelli privati previsti dall'art. 1, co. 2-*bis*, d.l. n. 105/2019 ma non ricompresi dal menzionato art. 2, co. 2, d.lgs. n. 82/2005 (vale a dire: soggetti privati ricompresi nel perimetro di sicurezza nazionale cibernetica (PSNC), aventi sede nel territorio nazionale, dai quali 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 o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale). Prevedendo anche soggetti ulteriori rispetto a quelli ricompresi nel perimetro di sicurezza nazionale cibernetica, il d.d.l. pare delineare un concetto di "interesse nazionale strategico" differente e maggiormente esteso rispetto a quello di "sicurezza nazionale" previsto dalla disciplina del PSNC».

effettivamente un problema tassonomico/definitorio[9], 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. 14 è quella di "elementi essenziali di cybersicurezza", dizione ricorrente, anch'essa, nel già citato art. 108, comma 4, del d.lgs. 36/2023[10].

È utile ricordare, come già premesso, che il codice dei contratti pubblici impone alle stazioni appaltanti un obbligo generale di considerare gli *elementi* di cybersicurezza. Tale obbligo assume carattere più stringente – ancorché con contorni applicativi non del tutto definiti – in tutti quei casi in cui l'appalto riguardi attività incidenti sugli interessi strategici nazionali.

Rispetto a quest'ultima disposizione, l'art. 14 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».

Il tentativo in esame merita una valutazione positiva, in quanto si configura come un intervento idoneo a colmare una lacuna normativa derivante dalla formulazione, per certi aspetti carente, dell'art. 108, comma 4, del d.lgs. n. 36/2023. Tale disposizione, infatti, nel fare riferimento agli "elementi di cybersicurezza", non ha provveduto a fornire una delimitazione chiara e univoca del relativo ambito definitorio, lasciando margini di incertezza interpretativa che possono incidere negativamente sull'applicazione pratica della norma stessa.

La definizione introdotta dall'art. 14, pertanto, sembra rivolta a integrare tale mancanza mediante una precisazione normativa che contribuisca a determinare, con maggiore chiarezza, il perimetro concettuale e operativo degli elementi di cybersicurezza richiamati nella disposizione. In tal modo, si punta non solo a garantire un'applicazione più uniforme e coerente della disciplina, ma anche a soddisfare le esigenze di certezza del diritto richieste dagli operatori del settore, i quali necessitano di riferimenti normativi chiari per conformarsi alle previsioni legislative e regolamentari.

Rimane ferma, però, l'esigenza di distinguere gli "elementi *essenziali* di cybersicurezza" dagli "elementi di cybersicurezza" di cui all'art. 108, comma 4, del codice, atteso che il requisito dell'*essenzialità* (presente nell'art. 14 in commento ma non nell'art. 108, comma 4, del codice) appare, a propria volta, un concetto sfuggente e di difficile delimitazione[11].

Dal punto di vista soggettivo, l'art. 14 della l. 90/2024 richiama «i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 8» individuando, dunque, quali destinatari:

1. le 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,

9. Come evidenziato da Cocchi 2024, p. 196, il concetto di "interessi nazionali strategici" sconta «una non indifferente genericità, tanto che già dalle prime applicazioni la centrale di Committenza Consip ha escluso la rilevanza strategica di alcune procedure, onde escludere l'applicabilità del comma 4 dell'art. 108 del nuovo Codice».

10. Di "peccato originale delle regole sulla sicurezza nazionale" parla Monti 2023, secondo cui «una criticità che balza immediatamente all'occhio è il ricorso alla categoria "interessi nazionali strategici" come elemento discriminante per attivare l'obbligo di valutazione separata della componente "sicurezza" dell'offerta, invece di fare riferimento a categorie pur non esattamente definite ma già presenti nell'ordinamento come quelle che appartengono al perimetro nazionale di sicurezza cibernetica, alle infrastrutture critiche e al golden power. Questa criticità affligge sia la scrittura del bando, sia la definizione e la documentazione dei criteri di aggiudicazione».

11. Secondo Cocchi 2024, p. 200, la definizione normativa è «ancora insufficiente per fornire alle stazioni appaltanti indicazioni sufficientemente chiare», in attesa di un intervento chiarificatore che potrebbe giungere con il d.P.C.M. attuativo dell'art. 14 della l. 90/2024.

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 decreto legislativo 30 luglio 1999, n. 300;
2. le autorità di sistema portuale;
3. le autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
4. i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
5. le società a controllo pubblico, con esclusione delle società quotate.

Questo elenco di destinatari delle disposizioni in materia di appalti pubblici contenute nell'art. 14 appare decisamente ampio.

Come osservato in sede istruttoria, l'ambito di applicazione della disposizione avrebbe potuto essere meglio definito, in quanto il rinvio *per relationem* all'art. 2, comma 2, d.lgs. 82/2005 parrebbe condurre ad una generalizzata efficacia applicativa della disposizione stessa anche a soggetti che non svolgono attività di approvvigionamento di beni e servizi informatici legati alla tutela di interessi nazionali strategici[12].

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 dell'art. 14 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. 105/2019.

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» (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).

Il secondo comma dell'art. 14 in commento 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.

La disposizione sembra conferire alla cybersicurezza una rilevanza centrale nell'ambito dei contratti pubblici, indipendentemente al criterio di aggiudicazione previsto dalla stazione appaltante (offerta economicamente più vantaggiosa o prezzo più basso).

Tanto appare "forte" tale indirizzo normativo, che l'art. 14 contiene alcune disposizioni normative che parrebbero ridondanti rispetto alla (già vigente) disciplina del codice dei contratti pubblici.

In particolare, lo stesso comma 2 dell'art. 14, al punto b), 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».

12. Come evidenziato dall'ANCI in sede di istruttoria parlamentare, «se da un lato il riferimento all'art. 2 comma 2 del CAD lascia intendere che si applichi a tutti i Comuni e loro società controllate, dall'altro si parla di approvvigionamento di beni e servizi informatici legati alla tutela degli interessi nazionali strategici. Nel caso di interesse, i Comuni, in base alla classificazione operata dalla stessa ACN, sono gestori di informazioni e dati ordinari, ad eccezione di Roma Capitale e Milano». Cfr. il contributo scritto dell'ANCI.

Tale disposizione non sembra molto dissimile (apparendo, anzi, 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».

Ancora, secondo la successiva lettera d), 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». Senonché l'art. 108, comma 4, del codice, già specifica 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».

Alla lettera c) del secondo comma dell'art. 14, invece, il legislatore ha introdotto 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, l'art. 14 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, la concreta applicazione della disposizione normativa contenuta nell'art. 108 del codice, nella sua portata prescrittiva ed esecutiva, appare suscettibile di generare un significativo incremento del contenzioso dinanzi alla giustizia amministrativa. Tale rischio risulta amplificato dalla natura non adeguatamente circoscritta della nozione di "interessi nazionali strategici", che si configura come un concetto giuridico indeterminato, suscettibile di interpretazioni divergenti anche in sede giurisdizionale.

Ulteriore fonte di criticità è rappresentata dalla complessità degli obblighi cui gli operatori economici sarebbero tenuti ad adempiere in materia di cybersicurezza, con particolare riferimento alla distinzione tra elementi "essenziali" e "non essenziali" di sicurezza cibernetica, il cui confine normativo risulta ancora incerto. A ciò si aggiunga che l'ampiezza della discrezionalità riconosciuta alle Stazioni appaltanti nella valutazione delle offerte per quanto attiene al rispetto degli adempimenti prescritti in ambito cyber potrebbe determinare difformità applicative.

3. Una (parziale) conclusione

Il tema della cybersicurezza nell'ambito degli appalti è in fase di "emersione".

Allo stato attuale, è possibile, però, raggiungere una conclusione solo parziale, dovendosi prendere atto di quanto appaia decisa la spinta del legislatore verso l'implementazione delle misure di sicurezza cibernetica nell'ambito dei contratti pubblici. Tanto che la produzione normativa in materia, per quanto non sempre ordinata, non nasconde – ed anzi esplicita – la volontà di raccordare la sicurezza informatica con altri principi cardine dell'azione amministrativa in materia di *procurement*, quali i principi di neutralità tecnologica, trasparenza e protezione dei dati personali.

Non è possibile, ad oggi, valutare l'effettiva portata applicativa di questo nuovo quadro regolatorio, risultante dalla "triangolazione" tra il codice dei contratti pubblici, il decreto attuativo della Direttiva NIS 2 e la l. n. 90/2024, in assenza di specifiche prassi amministrative e, soprattutto, senza la possibilità (ad ora) di capire *se* e *quando* la giurisprudenza amministrativa avrà la possibilità di intervenire a fronte di aggiudicazioni di contratti pubblici in cui la valutazione degli aspetti connessi alla cybersicurezza possa avere avuto una rilevanza decisiva o preponderante.

Riferimenti bibliografici

M. Buffa (2023), *La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in "Democrazia e Diritti Sociali", 2023, n. 1

F. Camisa, A. Simoncini (2024), *Il fattore umano e la regolazione della cybersecurity*, in "Mondo Digitale", 2024, n. 103

F. Casarosa (2024), *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, in "Rivista italiana di informatica e diritto", 2024, n. 1

T. Cocchi (2024), *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, n. 1

G. De Vergottini (2019), *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in "Rivista AIC", 2019, n. 4

A. Di Corinto (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1

E. Longo (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna Parlamentare", 2024, n. 2

A. Monti (2023), *L'impatto del nuovo Codice degli appalti sulla cybersecurity della Pa*, in "Formiche.net", 13 aprile 2023

L. Moroni (2024), *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in "federalismi.it", 2024, n. 14

L. Nannipieri (2024), *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio*, in "Rivista italiana di informatica e diritto", 2024, n. 1

M. Pietrangelo (2024), *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in "Rivista italiana di informatica e diritto", 2024, n. 1

S. Rossa (2024), *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, in "CERIDAP", 2024, n. 2

A. Simoncini (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", 2021, n. 2