Giuseppe Sferrazzo

La cybersecurity nel nuovo Codice dei contratti pubblici: l'art. 108 co. 4 e le criticità per le stazioni appaltanti

Abstract: Con l'entrata in vigore del nuovo Codice dei contratti pubblici, le amministrazioni sono tenute a considerare le caratteristiche di sicurezza dei prodotti e dei servizi da acquistare come un autonomo elemento di valutazione. Quanto previsto dalla norma rischia di entrare in conflitto con la normativa sulle infrastrutture critiche e con il concetto di perimetro nazionale di sicurezza cibernetica, complicando la gestione degli appalti, soprattutto quando il contesto di utilizzo è legato alla tutela di 'interessi strategici nazionali'. Si pongono a tal fine due problemi. Il primo è che l'amministrazione interessata dovrà giustificare il collegamento con gli interessi nazionali strategici. Il secondo, legato al prima, è se le amministrazioni, in modo discrezionale e autonomo, potranno definire i criteri per differenziare le ipotesi. Ne potrebbero derivare situazioni paradossali in cui lo stesso 'bene' verrebbe qualificato in modo diverso a seconda dell'amministrazione valutatrice, motivo per cui è necessario dotare le amministrazioni capofila di strumenti culturali e informativi adeguati.

Keywords: Cybersecurity; Codice dei contratti pubblici; Componenti di cybersicurezza; Interesse nazionale strategico; Amministrazione contraente.

1. Il concetto di cybersicurezza. Delimitazione del campo d'indagine

"In un mondo sempre più digitalizzato e connesso la cybersicurezza è diventata di fondamentale importanza"[1]. Il tema legato alla cybersicurezza sebbene sia concetto ampio, pieno di sfaccettature, si lega il più delle volte a concetti di difesa e prevenzione volte alla salvaguardia di strutture organizzative informatiche pubbliche e private. Invero, il concetto nella sua complessità, non può esser limitato a sin-

1 Frase di apertura del portale sulla strategia nazionale dell'Agenzia di cybersicurezza in https://acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760166

goli segmenti operativi, in quanto in uno "Stato digitale[2]", l'elemento *cyber* risulta correlato alla vita di tutti i giorni, compendiandosi in atti che sono centrali persino nella quotidianità del singolo cittadino, in un contesto tecnologico cangiante e destinato a innervare anche gli aspetti più impercettibili della società odierna.

In tale quadro, la sfera pubblica cade inevitabilmente al centro dell'attenzione. Lo stato dell'arte in 'salsa' digitale implica, in questa sede, un'analisi profonda del fenomeno cyber, in un contesto storico che ha evidenziato sempre più spesso l'incapacità delle amministrazioni pubbliche a dotarsi di metodi appropriati volti a creare un ambiente funzionale alle esigenze della collettività[3]. In un mondo sempre più tecnologico, solo infrastrutture digitali funzionanti ed evolute possono consentire alle amministrazioni nazionali di reggere il passo con la modernità e resistere agli attacchi cyber che imperversano sempre più tra le maglie difensive dei soggetti pubblici. A tal uopo, la difesa dei servizi e delle attività pubblicistiche vale non solo a preservare gli interessi delle singole amministrazioni al corretto raggiungimento dell'interesse pubblicistico ma deve essere strumentale, altresì, a garantire i diritti dei singoli cittadini[4]. Si tratta, in buona sostanza, di un compito cruciale che coinvolge, in via diretta, diverse istanze legate alla persona, agli interessi economici e, più in generale, ad obiettivi strategici nazionali[5].

Alla luce di quanto evidenziato, è opportuno tracciare i confini della materia.

L'elemento di resilienza cibernetica[6], in combinato disposto con quello di sicurezza cibernetica[7], si pongono fra le misure che consentono alla Repubblica italiana una difesa nazionale delle reti, dei sistemi informatici, dei servizi e delle infrastrutture tali da consentire la continuità dello svolgimento delle attività istituzionali del Paese avuto particolare riguardo ai servizi essenziali[8].

Tale presupposto non deve riguardare esclusivamente le alte sfere istituzionali del paese e i compiti più rilevanti e centrali dello Stato (inquadrabili in seno alle attività rientranti nel c.d. Perimetro di Sicurezza Nazionale Cibernetica[9]) dovendo interessare qualsiasi apparato amministrativo (perfino i più esigui) protagonisti principali ed erogatori delle prestazioni primarie presso le comunità di riferimen-

2 Torchia, 2023.

3 Piras, 2022: 426.

4 Carotti, 2020: 629.

5 Busia, 2020: 9.

6 Intendendosi con tale elemento alcuni aspetti tecnici specifici, quali la prevenzione e la risposta a minacce informatiche che possono danneggiare dati e infrastrutture informatiche.

7 Si fa riferimento ad una dimensione normativa e organizzativa di maggiore ampiezza attinente alla gestione e protezione di reti e infrastrutture, alla identificazione e rilevazione delle minacce, alla risposta e ripristino della funzionalità dei servizi e alla governance cibernetica a garanzia della efficacia e efficienza delle reti e infrastrutture.

8 Di Costanzo, 2022: 2.

9 Art. 1, co. 1, e art. 1, co. 2, lett. a), d.l. n. 105/2019, conv. l. n. 133/2019. Ci si riferisce a soggetti che svolgono un'attività essenziale per la Repubblica ovvero a soggetti, pubblici o privati, che forniscono 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 che possano comportare un pregiudizio per la sicurezza nazionale.

to. Sovente, soprattutto in tempi recenti, gli attacchi cibernetici hanno riguardato plessi amministrativi non di primo livello, bensì regionali o addirittura comunali[10], da cui si è definitivamente accertata la necessaria presenza, oltre che di figure centrali di riferimento quale l'Agenzia per la cybersicurezza nazionale (di seguito ACN), da un lato, di professionisti all'interno degli apparati dei vari enti statali e, dall'altro, di sistemi, beni e servizi capaci di proteggere gli enti locali o le amministrazioni anche meno conosciute ma che costituiscono parte centrale nella tutela e garanzia dei diritti dei cittadini[11].

Sebbene il tema presenti notevoli complessità, la precisazione si è resa necessaria per chiarire su quale profilo del più ampio tema sulla cybersicurezza si soffermerà il testo. In questa sede, si approfondiranno gli aspetti e gli strumenti di cybersicurezza delle pubbliche amministrazioni (di seguito P.A.) in particolar modo per ciò che concerne l'elemento della sicurezza e il rapporto sussistente con le regole del *public procurement*, in fase di acquisto di beni e servizi informatici.

Nel presente contributo particolare attenzione verrà data alla disciplina contenuta nel nuovo Codice dei contratti pubblici (D.lgs. n. 36/2023). Attualmente, differenziandosi dal recente passato, le complesse attività richieste alle stazioni appaltanti esigono molto più che una semplice elencazione del prodotto o del servizio da dover valutare, in realtà, contemplando l'obbligo di apprezzamenti complessi sia in via preliminare che, soprattutto, in una fase successiva, in cui la scelta è comprensiva della "costruzione" del bando di gara e della valutazione delle offerte pervenute. La selezione dell'operatore a cui affidare la gara dovrà includere tale valutazione, in un nuovo e immanente rapporto sicurezza/qualità del servizio offerto, non più svincolabile dalla attuale e moderna realtà informatica e digitalizzata.

Nella cornice generale ora delineata, si darà ampio spazio alle criticità presentate dall'attuale normativa codicistica. In effetti, nel vaglio dei documenti di gara e nella selezione dell'offerta che assicuri gli standard di sicurezza ricercati dal bene o dal servizio informatico oggetto della commessa pubblica, si richiedono ponderazioni altamente discrezionali che non poco incidono sul criterio di selezione e sulle modalità di scelta, differenziandosi a seconda che gli elementi debbano essere solo presi in considerazione ovvero debbano essere valutati autonomamente nel caso in cui la categoria dei beni e dei servizi sia collegata agli "interessi nazionali strategici", senza dimenticare la specificità della disciplina prevista per il Perimetro di Sicurezza Nazionale Cibernetica di cui se ne approfondirà il mancato coordinamento con quanto di nuovo elaborato.

10 Fra tutti, si fa riferimento all'attacco cyber subito dalla Regione Lazio, in data 5 agosto 2021, in cui si è accertata la mancanza di preparazione tra i dipendenti oltre che gli errori di progettazione circa la rete di sicurezza cyber, a fronte di un attacco di tipo "ransomware" che non ha nulla di particolarmente sofisticato e dovrebbe, al contrario, rientrare nelle capacità di gestione di un'infrastruttura critica come quella della Regione Lazio. Questo attacco e non solo, è stato uno dei casi emblematici che ha condotto, da lì a poco, alla creazione dell'Agenzia nazionale per la cybersicurezza.

11 Rossa, 2023a: 25.

2. Il quadro normativo in materia di cybersecurity: le iniziative europee e i recepimenti nazionali

Il quadro giuridico di riferimento si presenta, come definito da autorevole dottrina, "alluvionale e multilivello"[12]. La comprensione dell'assetto normativo, difatti, non è semplice in quanto ai criteri guida indicati a livello sovranazionale, si sono succeduti gli adattamenti in ambito domestico, conseguendone una struttura legislativa che concorre a complicarne la comprensione concettuale[13].

L'esigenza europea di dotarsi di un'architettura cyber sorge dagli attentati terroristici occorsi nei primi anni 2000. Da quel momento, gli iniziali sforzi si concentrarono sulla costituzione di un'Agenzia che fosse capace di coadiuvare le istituzioni europee nell'elaborazione di strategie in grado di assicurare la sicurezza delle reti e di diffondere la cultura ICT all'interno degli Stati membri e tra operatori e cittadini. Da tale necessità, difatti, sorse l'Enisa[14]. Nonostante la presenza della nuova istituzione, la coscienza europea in tema di cybersicurezza era ancora lontana dal formarsi pienamente tanto da comportare un ruolo meramente marginale del settore e, conseguentemente, dell'Agenzia stessa.

Progressivamente, la volontà di creare una regolamentazione cyber si sedimentò in capo alle Istituzioni europee, portando, dapprima, sul piano normativo, ad un primo accenno alla cybersecurity nella direttiva 2008/114/CE in tema di protezione transfrontaliera di infrastrutture critiche, per poi giungere con la direttiva 2016/1146/UE c.d. 'direttiva NIS' (*Network and Information Systems*) ad una prima e accurata regolazione del settore[15]. All'interno di quest'ultima si segnala la costituzione di un gruppo di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Team* – il c.d. CSIRT, al fine di trattare le situazioni di crisi secondo procedure predefinite, mezzi di reazione proporzionati al tipo di evento e tempistiche il più possibile contenute[16].

12 Ursi, 2023: 18.

13 Da ultimo, l'integrazione nazionale sulla normativa CER per cui si veda Cerciello, 2024: 1.

14 Reg. Ce n. 460/200437, che istituì l'Agenzia europea per la sicurezza delle reti e dell'informazione (Enisa).

15 La volontà era quella di creare uno spazio cibernetico sicuro, adottando una serie di misure, tra cui l'istituzione di un Gruppo di Cooperazione tra gli Stati membri, centri di intervento per la sicurezza informatica negli Stati membri e un'apposita autorità di controllo e una strategia programmatica in materia. Sul punto, Matassa, 2022: 635; che ne sottolinea l'importanza per aver elaborato dei criteri di identificazione comuni degli operatori di servizi essenziali europei, affidando agli Stati membri l'onere di trasmettere e aggiornare con cadenza biennale l'elenco dei soggetti pubblici e privati ricavato sulla base dei parametri indicati dall'art. 5 della Direttiva28 e dei settori indicati dall'Allegato II.

16 I compiti del CSIRT sono definiti dal D.l. 18 maggio 2018, n. 65 e dal DPCM 8 agosto 2019 art. 4. Essi includono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT.

Sempre in ambito europeo, a seguito della prima Direttiva NIS, si è intervenuti nuovamente con il regolamento Ue n. 881/2019, il c.d. Cybersecurity Act. Il testo, suddiviso in due parti, ha, da un lato, riorganizzato le funzioni dell'Enisa rafforzando la posizione dell'Agenzia quale centro nevralgico per la sicurezza dello spazio cibernetico e attore principale atto a garantire la cooperazione tra le varie figure del settore e, dall'altro, ha creato un sistema europeo per la certificazione della sicurezza informatica[17].

Rientrando in ambito nazionale, l'Italia, anche se con ritardo, ha recepito gli obblighi sovranazionali, adottando una strategia volta a dar vita ad un impianto normativo capace di costruire un'infrastruttura nazionale di cybersicurezza, attuata attraverso una serie di interventi legislativi.

Sul punto, la direttiva NIS è stata recepita con il D.lgs. 18 maggio 2018, n. 65, che ne ha definito le regole e indicato le procedure per la strutturazione di una Strategia nazionale di sicurezza cibernetica, tra cui vi rientravano le misure necessarie per la sicurezza delle reti e dei sistemi informativi italiani rivolte agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD)[18]. Successivamente, il D.l. 21 settembre 2019, n. 105, convertito dalla L. 18 novembre 2019, n. 133, istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[19]

17 Sul tema e per maggiori approfondimenti Campara, 2020: 71 e ss.

18 Sica, 2022: 583.

19 Il Perimetro nazionale serve ad assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti (pubbliche amministrazioni, enti pubblici e privati) che esercitano "una funzione essenziale dello Stato" o che prestano "un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato", seppur non rientranti nell'ambito di applicazione della citata direttiva NIS. I soggetti sono individuati in un apposito elenco, adottato con DPCM, su proposta del Comitato interministeriale per la cybersicurezza, circostanza da cui ne discende che solo le amministrazioni e gli enti rientranti all'interno del suddetto Perimetro ricevono comunicazione dell'iscrizione (art. 1, comma 2-*bis*, d.l. n. 105/2019). Come evidenziato da Previti, 2022: 73; Tra i decreti che hanno contribuito a dare attuazione alle disposizioni del d.l. n. 105/2019, si segnalano: il DPCM 30 luglio 2020, n. 131, che definisce le modalità e i criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel Perimetro nazionale (art. 1, comma 2, lett. a), nonché i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi, dei servizi informatici da parte dei soggetti inclusi nel Perimetro (art. 1, comma 2, lett. b); il DPR 5 febbraio 2021, n. 54, che definisce le procedure e le modalità per le operazioni di valutazione spettanti al Centro di valutazione e certificazione nazionale (CVCN), attivo invero solo da luglio 2022, con riferimento alle forniture di beni e di servizi ICT richieste dai soggetti inclusi nel Perimetro (art. 1, comma 6, lett. a), b) e c); il DPCM 14 aprile 2021, n. 81, che definisce le procedure e le modalità per la notifica degli incidenti aventi impatto su reti, sistemi e servizi ICT al CSIRT Italia, nonché le misure di sicurezza relative alle reti, ai sistemi e ai servizi ICT adottate dai soggetti inclusi nel Perimetro (art 1, commi 2 e 3, lett. a) e b); il DPCM 15 giugno 2021, che individua le categorie di beni, sistemi e servizi ICT per la cui fornitura i soggetti inclusi nel Perimetro sono tenuti a seguire le procedure di valutazione spettanti al citato CVCN (art. 1, comma 6, lett. a); il DPCM 18 maggio 2022, n. 92, in vigore dal 30 luglio 2022, in materia di accreditamento degli istituendi laboratori accreditati di prova (LAP) e di raccordo tra i predetti laboratori, il suddetto CVCN e i Centri di valutazione (CV) del Ministero dell'Interno e del Ministero della Difesa (art. 1, comma 7, lett. b).

e, da ultimo, con il D.l. 14 giugno 2021, n. 82, convertito L. 4 agosto 2021, n. 109, con la quale si è istituita l'Agenzia per la cybersicurezza nazionale[20].

Nel contesto storico appena descritto, il Parlamento europeo è intervenuto nuovamente, approvando la Direttiva c.d. 'Nis2', (Dir. Ue 2022/2555, entrata in vigore il 17 gennaio 2023). Limitando l'analisi agli aspetti attinenti al presente contributo, è interessante sottolineare come la nuova direttiva prenda posizione sull'obbligo per gli Stati membri di dotarsi disponendo, tra le altre, misure strategiche riguardanti gli elementi di cybersicurezza nel settore degli appalti pubblici[21].

In ambito nazionale, la direttiva ha, dunque, imposto un cambiamento che non è tardato ad arrivare. Espressione di quanto ora evidenziato è il D.P.C.M., del 17 maggio 2022, adottato nel solco della più ampia Strategia nazionale di cybersicurezza e al fine di dotarsi di un Piano di implementazione adeguato alla protezione degli asset strategici nazionali, per il tramite di un approccio strategico orientato alla gestione del rischio di tutto il sistema Paese. In particolare, si mettono in evidenza gli aspetti concernenti la sicurezza degli approvvigionamenti e della supply chain, assumendo aspetto centrale la valorizzazione e inclusione degli elementi di sicurezza cibernetica nelle attività di procurement ICT della P.A. Il menzionato piano nel prevedere tre specifiche misure (le nn. 6,7 e 8)[22], anticipa, in grandi linee quanto effettivamente avvenuto con le innovative disposizioni contenute nel nuovo Codice dei contratti pubblici.

In altri termini, alla luce dell'importanza assunta dalla materia cyber, dimostrata anche dal susseguirsi di interventi normativi, la cybersicurezza diventa, nel quadro europeo, principio valido a regolare l'affidamento dei contratti pubblici aventi ad oggetto soluzioni tecnologiche per la P.A.[23].

20 Per un approfondimento sulla lunga scia normativa, Previti, 2022: 68 e ss.

21 In particolare, il secondo paragrafo dell'art. 7, nell'ambito della strategia nazionale per la cibersicurezza, "gli Stati membri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source".

22 Piano di implementazione Strategia nazionale di cybersicurezza 2022-2026: Misura n. 6: Introdurre norme giuridiche che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione, fornendo indicazioni sia a quest'ultima che agli operatori di mercato per garantire che i beni e i servizi informatici, acquistati dai soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro, rispondano ad adeguati livelli di cybersicurezza. Ciò, compatibilmente con la celere definizione delle relative procedure di aggiudicazione. Misura n. 7: Promuovere la realizzazione, a livello nazionale ed europeo, di un sistema di gare pubbliche impostato su criteri che garantiscano soluzioni di qualità sotto il profilo della cybersicurezza. Misura n. 8: Introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.

23 Cocchi, 2024: 189.

Sebbene un primo tentativo di regolazione della materia sia stato abbozzato[24], è solo con il nuovo art. 108, co. 4, D.lgs. n. 36/2023 che si pone una definitiva rivoluzione nel settore in esame, per cui l'adeguata progettazione e selezione di prodotti e servizi di sicurezza informatica deve necessariamente passare dalla procedura di evidenza pubblica. In definitiva, la crescente centralità assunta dalla sicurezza delle infrastrutture digitali nel contesto attuale impone alle amministrazioni di dotarsi di mezzi cibernetici adatti a perseguire, un approccio integrato per ottimizzare la sicurezza delle infrastrutture critiche, combinando protezione fisica e cybersecurity, in modo da rispondere efficacemente alle nuove minacce[25].

3. La valutazione della nuova componente "sicurezza" e i concetti di "elementi di cybersicurezza" e "interessi nazionali strategici"

Le previsioni in materia di cybersicurezza adottate dal nuovo Codice dei contratti pubblici si pongono in controtendenza con quanto contenuto dalla previgente disciplina di cui al D.lgs. n. 50/2016.

In tale contesto, come noto, il legislatore è nuovamente intervenuto, innovando la materia, con il nuovo Codice dei contratti pubblici (D.lgs. n. 36/2023), introducendo due norme specifiche in materia di cybersicurezza da rinvenire negli artt. 19 co. 5 e 108 co. 4.

24 Sul punto, in attuazione dell'art. 29, co. 3, D.l. 21 marzo 2022, n. 21, l'ACN con circolare pubblicata il 21 aprile 2022, n. 4336, ha stabilito delle prime regole in materia che, anche in via indiretta, hanno coinvolto i fornitori privati di tecnologia, tenuti al rispetto di quanto previsto. La lett. c) individuava una disciplina applicativa e operativa, per cui tutte le stazioni appaltanti si dovevano adeguare a quanto descritto in un'ottica di generalizzata diffusione di 'best practice' nella strutturazione dei bandi di gara. Diversi fattori sono stati messi in risalto, su tutti l'istallazione e la successiva configurazione dei sistemi, oltre che l'impatto rivestito dai nuovi strumenti in un'ottica di continuità, compatibilità operativa con le varie infrastrutture presenti. Nella gestione del bando di gara rispetto all'installazione dei sistemi, la circolare poneva in capo alle stazioni appaltanti una necessaria valutazione di elementi attinenti a tutte le fasi della gestione del rischio. In altri termini, si suggeriva alle P.A., di optare per servizi e prodotti che fossero testati in una fase preliminare in modo da valutarne la loro operatività e considerarli in virtù di scelte tecnologiche che ne migliorassero le risposte in uno scenario di rischio cyber elevato, senza dimenticare i processi di controllo e manutenzione volti ad eliminare le eventuali criticità sorte. Sebbene le rilevanti novità portate dalla circolare fossero a tutti gli effetti applicabili alle stazioni appaltanti, la natura giuridica della circolare, non comportando alcun obbligo attuativo per le P.A., è stata fortemente disattesa. Nonostante ciò, permane l'utilità della stessa nell'aver creato in ambito nazionale pubblica un nuovo modo di pensare alla cybersicurezza nel settore della contrattualistica pubblica.

25 Approccio combinato che continua ancora oggi con Il recepimento delle Direttive NIS 2 e CER rappresenta un passo significativo nello sviluppo del quadro normativo nazionale in materia di cybersecurity, che porta avanti l'obiettivo dell'Unione Europea di rafforzare i livelli di sicurezza informatica degli Stati membri e garantire la resilienza dei soggetti critici e dei servizi essenziali; come evidenziato da Cerciello, 2024: 1.

Innanzitutto, è presente il nuovo art. 19 co. 5 D.lgs. n. 36/2023[26]. In un'ottica di rivoluzione del settore in commento, il legislatore ha imposto la digitalizzazione dell'intero ciclo di vita dei contratti pubblici, prescrivendo una necessaria preparazione del personale e richiedendo adeguati profili organizzativi di sicurezza. Se dal punto di vista complessivo tale soluzione brilli per innovatività, le scelte attuate sono la risultante di quanto già invero avvenuto nella prassi. Difatti, nonostante la mancanza normativa, non vi è dubbio alcuno che i soggetti operanti nel settore contrattualistico (stazioni appaltanti ed operatori economici) si fossero già dotati di una struttura interna volta ad evitare il proliferarsi di attacchi o pericoli cyber[27].

Prescindendo dall'art. 19, oggetto centrale del presente contributo è l'art. 108 co. 4 D.lgs. n. 36/2023[28], su cui è opportuno soffermarsi. La norma, assente nella prima bozza del Codice e poi successivamente introdotta[29], stabilisce che nel

26 Art. 19, co. 5, D.lgs. n. 36/2023: Le stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti di cui al comma 3, 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.

27 Rossa, 2023b, d'altra parte l'Autore in Rossa, 2024: 341 ne rileva la natura di "manifesto di politica di cybersicurezza", dato che il legislatore ha recepito quanto già messo in pratica da tempo da parte dalle pubbliche amministrazioni. Infatti, l'elemento di cybersicurezza essendo ormai divenuto cruciale per il funzionamento di ogni organizzazione, pubblica o privata, indipendentemente dalla partecipazione a procedure di gara, aveva necessariamente condotto le pubbliche amministrazioni alla ricezione delle basilari esigenze cyber in tempo di gran lunga antecedente anche rispetto a quanto contenuto dalla circolare dell'ACN.

28 Art. 108, co. 4, D.lgs. n. 36/2023: I documenti di gara stabiliscono i criteri di aggiudicazione dell'offerta, pertinenti alla natura, all'oggetto e alle caratteristiche del contratto. In particolare, l'offerta economicamente più vantaggiosa, individuata sulla base del miglior rapporto qualità/prezzo, è valutata sulla base di criteri oggettivi, quali gli aspetti qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto. La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. 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. Nei casi di cui al quarto periodo, 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. Per i contratti ad alta intensità di manodopera, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.

29 Il riferimento agli elementi cyber si ritiene possa esser stato aggiunto anche in virtù delle indicazioni fornite dall'ACN in audizione parlamentare (documento disponibile al seguente link: lhttps://documenti.camera.it/leg19/documentiAcquisiti/COM08/Audizioni/leg19.com08.Audizioni.Memoria.PUBBLICO.ide-Ges.7977.15-06-2023-15-03-25.709.pdf) in cui si evidenziava che "si potrebbe, altresì, ragionare sul criterio di aggiudicazione degli appalti quando si utilizza quello dell'offerta economicamente più vantaggiosa. (…) appare di tutta importanza, quindi, che la stazione appaltante attribuisca un opportuno peso ai profili tecnico qualitativi di sicurezza cibernetica rispetto ai profili economici, non potendo rischiare che l'elemento prezzo

procedere all'aggiudicazione della commessa pubblica su attività di approvvigionamento di beni e servizi informatici, nell'utilizzare il criterio dell'offerta economicamente più vantaggiosa, le amministrazioni (stazioni appaltanti o centrali di committenza) contemplino adeguatamente gli elementi di cybersicurezza inseriti nel contesto tecnico qualitativo dell'offerta. Eccezion fatta nel caso in cui siano accertati i c.d. "interessi nazionali strategici", circostanza dalla quale discende una forte preponderanza in favore della valutazione della componente tecnica dell'offerta, a discapito della componente economica che sarà da valutare nei limiti dei dieci punti percentuali del punteggio complessivo. In altri termini, secondo quanto predisposto dalla nuova disciplina, nel caso in cui non si sia in presenza di interessi nazionali strategici, la P.A., dovrà solo valutare la presenza di tali elementi ma sarà libera, in ogni caso, di scegliere l'offerta economicamente più vantaggiosa anche se quest'ultima non presenti i migliori livelli di sicurezza dal punto di vista qualitativo-tecnico. Nel caso in cui siano presenti gli interessi nazionali strategici, invece, la maggiore qualità della componente sicurezza giustificherebbe la scelta del partecipante malgrado possa presentare un'offerta meno vantaggiosa dal punto di vista economico, in tal modo valorizzando a valle la scelta discrezionale dalla P.A.

La soluzione appena descritta si pone in linea di continuità con la scelta di eliminare il tetto massimo per il punteggio economico entro il limite del 30%[30](secondo la nota regola del c.d. 70/30[31]) alla luce della valorizzazione degli elementi qualitativi dell'offerta. In tale ottica, prevale la volontà di rimettere alle stazioni appaltanti la scelta circa l'incidenza dell'aspetto tecnico ed economico in modo da adeguare le due componenti alle effettive caratteristiche dell'appalto da assegnare[32]. In simili situazioni, si evidenzia la chiara esigenza affinché la stazione appaltante assegni opportunamente il giusto peso ai profili tecnici afferenti alla sicurezza cibernetica anche in sfavore della parte economica, in modo da valorizzare gli elementi della singola gara ed evitando, al contempo, che il prezzo diventi un fattore decisivo nella scelta, con chiara elusione di tutto l'impianto di sicurezza cibernetico[33].

sia decisivo, anche attraverso meccanismi di gara che riconoscano la necessaria attenzione che le stazioni appaltanti debbono avere per questi aspetti".

30 Art. 95, co. 10-bis, D.lgs. n. 50/2016: La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. A tal fine la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.

31 Secondo quanto appreso dalla relazione illustrativa, la scelta è dipesa dall'analisi economica fatta dall'Autorità Garante della Concorrenza e del Mercato (AGCM) nel 2021, in cui se ne sono evidenziati gli elementi critici, in larga parte distorsivi delle regole presenti nel mercato (documento disponibile al seguente link: https://www.agcm.it/dotcmsdoc/relazioni-annuali/relazioneannuale2021/Relazione_annuale_2022.pdf).

32 Catarisano, 2023: 811.

33 Unica eccezione è fondata sul periodo conclusivo del quarto comma, che reintroduce nel campo dei contratti ad alta intensità di manodopera il tetto massimo del 30% al punteggio relativo all'offerta economica, derogando in via generale la nuova disciplina complessiva che non prevede alcun tetto massimo per l'offerta economica ed in particolar modo, lo stesso comma che stabilisce nel limite del 10% la valutazione in presenza di interessi strategici.

Sebbene il nuovo art. 108 co. 4 D.lgs. n. 36/2023, premi in modo convinto la componente della sicurezza, privilegiandola nel rispetto degli *asset* definiti sia dall'ordinamento italiano che dai nuovi formanti europei, il contenuto precettivo desta non poche criticità in ordine alle regole da applicare, delle definizioni da rispettare e circa l'ampia discrezionalità lasciata alle stazioni appaltanti in sede di scelta. Gli interrogativi sorgono in merito alle nozioni di "beni e servizi informatici" o di "elementi di cybersicurezza" ma soprattutto riguardo alla nuova e apparentemente contrastante definizione di "interessi nazionali strategici", che rischia di collidere con la regolamentazione di infrastrutture critiche e con il Perimetro di Sicurezza Cibernetica, rendendo ulteriormente complessa la gestione degli appalti in un settore che, come quello in esame, nasconde innumerevoli insidie.

Il riferimento è senza dubbio problematico ma nasconde solo parte delle questioni sottese alla norma in commento, laddove già non poche difficoltà sorgono, preliminarmente, in merito alla definizione di beni e servizi informatici e, in particolar modo, sul concetto di elementi di cybersicurezza.

Rispetto alla prima, si critica il campo di applicazione, incerto e quantomai ampio. Invero, è possibile reperire dalle precedenti produzioni normative delle linee guida da seguire in ordine alla perimetrazione del campo di applicazione, segnatamente dai vari Piani triennali per l'informatica nella Pubblica amministrazione. Se indubbiamente sono da considerare le strutture immateriali (da intendere come comprensivi dei dati delle P.A., insieme ai meccanismi e alle piattaforme create per offrire servizi ai cittadini) l'attenzione va focalizzata su quelle materiali. In effetti, i beni e i servizi informatici, connessi anche ai beni di connettività, sono considerati una categoria merceologica speciale[34]. All'interno di questa lista sono sicuramente da ricomprendere beni quali gli hardware, i software e soluzioni, le macchine per gli uffici amministrativi, i prodotti di networking, gli apparati di telefonia e di trasmissione dati, così come gli strumenti di elettronica, fotografia, ottica e audio/video. In altre parole, tutto ciò che attiene all'ambito informatico, seppur anche mediatamente, dovrebbe rientrare nel campo di applicazione dell'art. 108 co. 4 D.lgs. n. 36/2023.

Nonostante sussista una certa sicurezza sul punto non poche incertezze residuano nel caso in cui i beni e i servizi non siano attinenti all'ambito di applicazione ma quantunque presentino segmenti informatici o anche di connettività. In definitiva, se determinati beni dovessero appartenere ad un campo di applicazione differente (come quello stradale, ferroviario o anche sanitario) la loro esclusione comporterebbe non pochi stravolgimenti, a maggior ragione, nel caso in cui ci fosse la connessione con gli interessi nazionali strategici, discendendone un'elusione diretta della disciplina codicistica.

A dispetto di quanto appena analizzato per la categoria merceologica dei beni e servizi informatici, più incertezze sussistono in merito al concetto di elementi di cybersicurezza.

34 Di cui la legge ne impone il ricorso per l'acquisto tramite le convenzioni CONSIP o al Mercato elettronico, senza alcuna distinzione di valore e dunque anche per importi pari a 1 o 2 euro.

Se per cybersecurity ci si riferisce all'insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici, in un'ottica di riconduzione al sistema, per tecnologia di cybersicurezza si dovrebbero intendere le attività o i controlli, finanche le misure di sicurezza da disporre per proteggere l'entità interessata. Parte centrale dell'assetto di cybersicurezza sono gli elementi che, a parere di chi scrive, andrebbero ricondotti nei concetti di: reti, sistemi, dati, applicazioni e dispositivi IT (Information Technology). In sostanza, la stazione appaltante nel configurare gli elementi di cybersicurezza di un bene o servizio informatico dovrebbe includere le tecnologie, le policy e, più in generale, tutti i processi necessari per proteggere le parti più importanti dell'ecosistema IT[35].

Da ultimo, vi è il concetto di interesse nazionale strategico. La "connessione" con tale particolare interesse innesta una serie di valutazioni complesse di cui la stazione appaltante è prima protagonista affinché il "motore" cibernetico si attivi. Questa deve *in primis* effettuare una valutazione preventiva sull'oggetto della gara. Nel caso in cui il bando rientrasse nell'ambito di tutela degli interessi nazionali strategici di cui all'art. 108 co. 4 D.lgs. n. 36/2023, allora sarà necessario strutturare il capitolato individuando esattamente le parti riguardanti gli elementi di cybersicurezza[36].

Se l'opzione legislativa è volta a limitare la discrezionalità amministrativa in un settore critico come quello in oggetto (potendosi valutare il "solo" 10% del lato economico dell'offerta) la *ratio* sottesa all'intervento evidenzia la centralità assunta dal settore cyber per lo Stato[37].

La scelta è connaturata all'ampio potere discrezionale rimesso nelle mani della stazione appaltante e tale presupposto, in un contesto applicativo e definitorio quantomai indecifrabile e lacunoso, può comportare differenze in termini di scrittura del bando e determinazione dei criteri di aggiudicazione.

Tralasciando la discrezionalità nell'individuazione della connessione rimessa alla stazione appaltante, confusione e difficoltà di coordinamento sono rilevabili anche con riferimento alla creazione della nuova categoria degli interessi nazionali

35 In tali attività si ritiene siano presenti: a) Sicurezza della rete o sicurezza delle informazioni per difendersi dagli attacchi mirati a vulnerabilità e sistemi operativi, architettura di rete, server, host, punti di accesso wireless e protocolli di rete; b) sicurezza nel cloud per proteggere i dati, le applicazioni e l'infrastruttura che risiedono in cloud pubblici, privati o ibridi; c) sicurezza dell'IoT (Internet of Things) in ordine alla protezione di una moltitudine di dispositivi facenti parte di una rete IoT; d) sicurezza delle applicazioni per impedire agli aggressori di sfruttare le vulnerabilità nel software; e) gestione di identità e accessi per controllare le autorizzazioni concesse agli individui per accedere a sistemi, applicazioni e dati; f) sicurezza degli endpoint per proteggere i dispositivi connessi a Internet come laptop, server e telefoni cellulari; g) soluzioni per la sicurezza dei dati sensibili e delle risorse informative in transito o inattivi tramite metodi come crittografia e backup dei dati.

36 Monti, 2023; 2.

37 Ricotta, 2023: 102; l'autore sottolinea che "la sicurezza nel dominio cibernetico è una delle espressioni del moderno concetto di sicurezza nazionale, con il quale individuiamo quel novero di valori indispensabili sui quali si basa la stessa sopravvivenza della Repubblica come comunità di istituzioni e di cittadini e quelle indefettibili necessità ultra-individuali legate al mantenimento delle condizioni essenziali per tenere una nazione unita e proteggerne lo sviluppo".

strategici, paragonata alle altre tipologie di cui al perimetro nazionale di sicurezza cibernetica, alle infrastrutture critiche e al golden power.

Dubbi che finanche il nuovo DDL (AC1717) finalizzato ad introdurre una nuova disciplina in tema di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, è riuscito a dissipare.

4. Nuovi spunti positivi: Il nuovo DDL "cybersicurezza" e le novità legislative

Il DDL "cybersicurezza" (AC1717)[38] recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" è stato recentemente approvato anche al Senato della repubblica e, dunque, definitivamente approvato.

L'articolo 10[39] (attualmente a seguito degli emendamenti articolo 14) introduce (*rectius* aggiunge) nuovi criteri di cybersicurezza nella esaminata disciplina presente nel Codice dei contratti pubblici. In tal senso, si consente alle P.A., le società pubbliche e i soggetti privati compresi nel Perimetro di Sicurezza Cibernetica, in presenza di approvvigionamento di beni e servizi informatici, di tenere in considerazione gli elementi essenziali di cybersicurezza individuati da un DPCM da emanarsi entro 120 giorni, da parte del Presidente del Consiglio dei ministri su proposta dell'ACN.

Passando brevemente in rassegna le principali novità contenute nel testo, è necessario previamente individuare l'ambito di applicazione soggettivo per poi considerare *se* e *come* le nuove previsioni possano modificare quanto contenuto all'interno del nuovo Codice dei contratti e, in particolar modo, dell'art. 108 co. 4 D.lgs. n. 36/2023.

Per quel che concerne l'ambito di applicazione soggettivo, i soggetti individuati sono quelli indicati nell'articolo 2, comma 2, del codice dell'amministrazione digi-

38 Il testo del D.D.L 16 febbraio 2024 A.C. 1717, così come approvato dalla Camera dei deputati è consultabile su https://www.senato.it/service/PDF/PDFServer/BGT/01418571.pdf.

39 Art. 14, co. 1, D.D.L. Senato n. 1143: Con decreto del Presidente del Consiglio dei ministri, da adottare entro cento venti 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 del l'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 collabo razione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

tale (D.Lgs. 82/2005) che saranno tenuti a rispettare gli elementi essenziali in fase di acquisto di beni ICT[40].

Critica per collocazione sistematica ma opportuna per quanto previsto, risulta il secondo comma dell'attuale art. 14, in cui si compendiano una serie di obblighi e facoltà in capo alle stazioni appaltanti rispetto agli elementi essenziali di cybersicurezza individuati dal comma precedente. In particolare, si consente l'esercizio di facoltà di cui agli articoli 107, comma 2, e 108, comma 10, D.Lgs. 36/2023, nell'accertarsi dell'assenza degli elementi essenziali di cybersicurezza. Trattasi segnatamente del potere dato in capo alla P.A., circa la "riserva di non aggiudicazione"[41], precisandosi che di tale facoltà la stazione appaltante può avvalersi non oltre il termine di 30 giorni dalla conclusione della valutazione delle offerte. In altri termini, la stazione appaltante nel caso in cui non rinvenga gli elementi cyber connessi all'oggetto della gara, potrà procedere alla non assegnazione all'offerente, malgrado quest'ultimo abbia presentato l'offerta economicamente più vantaggiosa.

In effetti, è chiaro il collegamento effettuato dal DDL, laddove l'art. 107 co. 2, D.Lgs. 36/2023, nel richiamare le sole materie afferenti all'ambiente, il sociale e l'ambito giuslavoristico, preclude la possibilità di applicare la disposizione nel caso in cui si vertesse in materia di cybersicurezza. Sebbene l'accenno sia apprezzabile dal punto di vista garantistico del sistema cyber, risulta poco conciliabile il quadro giuridico delineato, in cui una disposizione fuori contesto richiami una disciplina settoriale facente riferimento a determinate materie, mancando, principalmente, di logicità sul piano programmatico codicistico. Senz'altro più attinente appare il richiamo all'art. 108, co. 10, D.Lgs. 36/2023, in quanto la generale applicabilità della fattispecie ad una serie indefinita di casi (inidoneità di tutte le offerte rispetto all'oggetto del contratto) consente, senza alcuna difficoltà, l'applicazione al caso in esame[42].

Da ultimo, per quel che ci interessa, prescindendo dai richiami ridondanti fatti al testo di cui all'art. 108, co. 4 D.Lgs. 36/2023, è opportuno evidenziare l'introduzione di cui alla lett. c) dell'attuale art. 14 DDL, in cui si obbliga l'inserimento degli elementi di cybersicurezza tra i requisiti minimi dell'offerta, nel caso in cui sia utilizzato il criterio del minor prezzo[43]. L'intenzione del legislatore per tal via è quella di sottolineare l'indefettibilità delle prestazioni o del bene previste dalla *lex specialis* di gara, affermando, di pari passo, il concetto per cui a prescindere dalle modalità di selezione dell'operatore economico, ciò che non può mai manca-

40 Come indicato dal terzo comma dell'art. 14 DDL (AC1717) facendosi riferimento alle pubbliche amministrazioni, comprese le autorità di sistema portuale e le autorità amministrative indipendenti di garanzia, vigilanza e regolazione; i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; le società a controllo pubblico, escluse le società quotate a meno che non gestiscano servizi di pubblico interesse.

41 Cancrini, Vagnucci 2023: 329.

42 Nannipieri, 2024: 4.

43 Art. 108, co. 3, D.lgs. n. 36/2023: Può essere utilizzato il criterio del minor prezzo per i servizi e le forniture con caratteristiche standardizzate o le cui condizioni sono definite dal mercato, fatta eccezione per i servizi ad alta intensità di manodopera di cui alla definizione dell'articolo 2, comma 1, lettera e), dell'allegato I.1.

re sono le suindicate condizioni di partecipazione alla procedura selettiva, come, d'altronde, evidenziato dalla stessa giurisprudenza amministrativa[44]. Il rispetto dei requisiti minimi dell'offerta, dunque, costituisce una condizione per poter partecipare alla procedura selettiva e l'eventuale non conformità ai requisiti individuati successivamente dal DPCM comporterà l'impossibilità di prendere parte alla gara con conseguente esclusione dalla stessa.

In definitiva, se da un lato, le novità legislative rafforzano, completando, la disciplina codicistica, dall'altro lato, appare senz'altro discutibile la scelta di farlo con un altro strumento legislativo correlato, appartenente ad altro settore di riferimento. Più opportunamente, si sarebbe (forse) dovuta riconoscere la parziale fallibilità della disciplina, contemplando la possibilità di un'integrazione in via diretta sulla norma del nuovo Codice[45]. In tal modo, si sarebbe consentita una migliore collocazione sistematica delle previsioni, oltre ad un supporto agli operatori del settore che, da sempre, navigano in un mare quantomai sovraffollato di regole da rispettare[46].

Non vi è dubbio, tuttavia, che l'attenzione va riposta rispetto alle definizioni circa gli elementi essenziali di cybersicurezza e gli interessi nazionali strategici, su cui è opportuno indagare con sguardo critico.

Nel nuovo assetto individuato dal DDL "cybersicurezza", non si fa più riferimento ai soli elementi di cybersicurezza ma la definizione viene contornata dal criterio dell'essenzialità. Se da un lato, tale elemento crea delle difficoltà circa l'armoniosa convivenza con quanto previsto dal Codice, dall'altro lato, l'intervento appare risolutivo rispetto al vuoto definitorio lasciato dall'art. 108, co. 4, D.lgs. n. 36/2023. In effetti, gli elementi essenziali di cybersicurezza sono definiti 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". Tale ricostruzione, valorizza quanto sostenuto nel precedente paragrafo, chiarendo, nell'attesa che venga emanato il futuro DPCM, uno degli aspetti più controversi della norma[47].

Il DPCM, sebbene risolva il dubbio classificatorio, apre ad un'ulteriore questione circa il requisito dell'essenzialità degli elementi apparso per la prima volta nel DDL e alla sua eventuale distinzione rispetto a quanto contenuto nell'art. 108 co. 4 D.lgs. n. 36/2023, in cui si fa riferimento ai soli "elementi di cybersicurezza". In attesa di chiarimenti, si possono dedurre una serie di considerazioni.

Gli elementi evidenziati dal Codice rispetto a quelli essenziali presenti nel DDL potrebbero definirsi come "ordinari" o quantomeno non essenziali. Il dubbio per-

44 Cons. Stato, sez. V, 27 ottobre 2022, n. 9249; Cons. Stato sez. V, 1° dicembre 2022, n. 10577; Cons. Stato sez. V, 12 gennaio 2023, n. 423.

45 Alla luce anche del nuovo ed imminente correttivo al nuovo Codice dei contratti pubblici, in fase di pubblicazione in Gazzetta ufficiale.

46 Sul punto, Carbone, 2023: 9 e ss; che nell'analizzare il lavoro che ha portato all'introduzione del nuovo Codice dei contratti, ha definito punto focale del lavoro il lavoro di semplificazione attuato, comportante, tra le altre misure, la riduzione delle regole da rispettare da parte delle amministrazioni interessate.

47 Per un ulteriore approfondimento si v. nota 35.

mane nel caso in cui, la disciplina indicata dallo strumento legislativo in attesa di approvazione, possa essere suscettibile di applicazione se non si sia in presenza di elementi essenziali[48]. È più probabile, a parere di chi scrive, che si sia trattato di una svista dal punto di vista letterale, per cui nei casi in cui si presentino degli elementi cibernetici (anche non essenziali) connessi ad interessi nazionali strategici, dovrebbe trovare applicazione la disciplina di cui all'art. 14 del DDL cybersicurezza.

Ma se, in questo caso, il legislatore ci verrà in soccorso chiarendo nel prossimo futuro quali di questi componenti siano da inglobare nel concetto di elementi essenziali di cybersicurezza, altrettanto non avviene per il concetto di interessi nazionali strategici, su cui non pochi dilemmi sorgono.

4.1. Le evidenti criticità: I vuoti da colmare e il mancato coordinamento con le amministrazioni operanti nel Perimetro Nazionale di Sicurezza Cibernetica

In virtù di quanto delineato nei precedenti paragrafi si possono trarre alcuni spunti di riflessione.

Innanzitutto, dati i molteplici campi attuativi e la contestuale presenza di varie definizioni che ne differenziano, circoscrivendo, il campo di applicazione sui settori e le attività essenziali per lo Stato, sarebbe auspicabile una revisione, o quantomeno come fatto con gli elementi di cybersicurezza, una specifica in ordine al corretto perimetro della definizione di interessi nazionali strategici.

Invero, se il bando dovesse riguardare prodotti o servizi "connessi" alla tutela di interessi nazionali strategici, diventerebbe necessario strutturare la gara in modo da definire la sezione afferente alla cybersecurity. L'art. 108 co. 4 D.lgs. n. 36/2023, nell'affiancare gli interessi nazionali strategici ad altre categorie già presenti all'interno del nostro ordinamento quali quelle di sicurezza nazionale[49], interesse nazionale nei settori produttivi strategici[50] e attività di rilevanza strategica[51], tuttavia difetta di una nozione organica che ne delimiti il campo di applicazione.

Sebbene manchi un concetto identificativo apparentemente, come rilevato da parte della dottrina, altra nozione può venire in soccorso, ponendosi per affinità e contiguità attuativa in posizioni simili rispetto agli interessi nazionali strategici, che è quella di "funzione essenziale dello stato[52]". In particolare, si fa riferimento

48 Come sottolineato nel paragrafo 3, la disciplina cambia e non poco se si rinvengano tali elementi, connessi con gli interessi nazionali strategici, prevedendo una ponderazione tecnica in sede di valutazione dell'offerta con valutazione del solo 10% dell'offerta economica.

49 D.l. 82/2021, agli artt. 5 e 7 si fa riferimento agli "interessi nazionali nel campo della cybersicurezza", affidando all'ACN 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".

50 D.l. 5 dicembre 2022, n. 187, recante "misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici".

51 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".

52 Decreto del presidente del Consiglio dei ministri 30 luglio 2020, n. 131 Regolamento

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 … 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".

Inoltre, chiaro indice di conformità con gli interessi nazionali strategici, è l'art. 2 co. 1, lett. b), che nel delineare i servizi essenziali, contemplando attività (quali quelle necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica o di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia) rimarca il concetto per cui anche in altri settori di riferimento, se si presentino aspetti di "rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale della competitività e dello sviluppo del sistema economico nazionale", debbano essere inquadrati in un'ottica di rilevanza strategica, non distante da quanto presumibilmente prospettato dalla nuova definizione.

L'incertezza sulla comprensione concettuale degli interessi nazionali strategici desta notevoli implicazioni anche rispetto all'eventuale accesso alle gare da parte degli operatori economici. Le scelte discrezionali delle stazioni appaltanti sul *se* e *quando* ritenere sussistenti gli interessi nazionali strategici, può pregiudicare non solo la vulnerabilità complessiva dell'infrastruttura tecnologica della P.A. italiana ma anche la concorrenza nel mercato, dato che, in alcuni casi, il rispetto degli elementi cyber potrebbe configurare un requisito per accedere ai bandi di gara. In tal senso, risulta decisiva una ponderazione degli interessi in gioco, in modo da non limitare la libertà di iniziativa economica dei soggetti operanti nel comparto di riferimento, non diminuendo, al contempo, la sicurezza delle infrastrutture tecnologiche delle amministrazioni[53]. Si auspica, dunque, un chiarimento sul punto in modo che i principi del *favor partecipationis*, della trasparenza e della *par condicio*[54], vengano rispettati e conseguentemente non si complichi la buona riuscita della novella.

Sotto altro punto di vista, tale aspetto è immanentemente collegato alle pubbliche amministrazioni rientranti nel Perimetro Nazionale di Sicurezza Cibernetica (di seguito PSNC), per cui il coordinamento con la disciplina in esame risulta ancora più complicato.

in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. Così, Nannipieri, 2024; 4.

53 Cocchi, 2024: 204; il quale auspica un ruolo operativo dell'ACN, che dovrà vigilare sull'applicazione della normativa e, nel caso, applicare le sanzioni in presenza di violazioni oltre che partecipare all'implementazione del contesto regolatorio di concerto con la presidenza del Consiglio dei ministri.

54 Sul punto è la stessa direttiva 2014/24/Ue sugli appalti pubblici che all'art. 42, par. 2, della direttiva dispone che "le specifiche tecniche consentono pari accesso degli operatori economici alla procedura di aggiudicazione e non comportano la creazione di ostacoli ingiustificati all'apertura degli appalti pubblici alla concorrenza".

Il PSNC inserito nel 2019, crea un ambito entro cui impiegare norme caratterizzate da alta specializzazione in materia di cybersicurezza nei confronti di alcuni soggetti ritenuti particolarmente sensibili e la cui azione è esercitata (anche) con reti e infrastrutture digitali[55].

La disciplina delineata coinvolge tutte le pubbliche amministrazioni presenti all'interno dell'ordinamento nazionale; potendo, quindi, interessare entità pubbliche che rientrino all'interno del PSNC o, in alternativa, determinati beni, servizi e sistemi ICT destinati ad essere impiegati sulle loro reti, ricompresi dalla disciplina normativa e regolamentare di dettaglio[56].

Per quanto riguarda la disciplina del Perimetro, essa trova applicazione sotto un duplice punto di vista. In primo luogo, essa si riferisce ai soggetti esercitanti una funzione essenziale dello Stato. In secondo luogo, esse valgono per quei soggetti, di natura pubblica o privata[57], 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.

Senza onere di esaustività, in questa sede preme ricordare gli obblighi, per i soggetti rientranti nel Perimetro, di ricorrere alle procedure di aggiudicazione di beni e servizi ICT, di cui all'articolo 1 del D.L. 105/2019[58]. In tale ambito, il ruolo del

55 Si veda Chiari, Mazzetti, 2023; Cassano, Iaselli, Spangher,2023; Giupponi, 2024; Rossa, 2024 ed in particolar modo Buoso, 2023: 98 e ss.

56 Rossa, 2023a: 153.

57 Sul punto il DDL cybersicurezza porta con sé una grossa novità contemplando la presenza anche dei soggetti privati, non compresi tra quelli risultanti 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.), ma rientranti nel PSNC, di cui all'articolo 1, comma 2-bis, del D.L. 105/2019. Come specificato dalla relazione tecnica, trattasi dei soggetti aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione di cui all'art. 1, co. 1, e art. 1, co. 2, lett. a), D.l. n. 105/2019. In altre parole, soggetti in settori quali quello governativo, l'interno, la difesa, lo spazio e l'aerospazio, l'energia, le telecomunicazioni, l'economia e la finanza, i trasporti, i servizi digitali e le tecnologie critiche; a cui si impongono compiti di natura preventiva per ovviare ad attacchi cyber e di carattere comunicativo nei confronti delle Autorità competenti in modo da migliorare le capacità di risposta.

58 Nel sistema di approvvigionamento dei beni ICT dei soggetti inclusi nel PSNC un ruolo centrale è svolto dal Centro di valutazione e certificazione nazionale (CVCN), organismo operante presso l'Agenzia per la cybersicurezza nazionale, disciplinato dall'articolo 1 del D.L. 105/2019. Il CVCN ha il compito di valutare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del PSNC e appartenenti alle categorie individuate dal DPCM 15 giugno 2021. I soggetti rientranti nel PSNC che intendono procedere, anche tramite le centrali di committenza (su tutti Consip e i suoi accordi quadro), all'affidamento di beni ICT sono obbligati a comunicare al CVCN per le opportune verifiche, le quali possono prevedere anche specifici test software e hardware. I fornitori di beni ICT a loro volta sono tenuti ad assicurare al CVCN la collaborazione per l'effettuazione di test. Il CVCN, inoltre, contribuisce all'elaborazione delle misure di sicurezza, definisce le metodologie di verifica e test ed elabora gli schemi di certificazione cibernetica. Il Ministero dell'interno e quello della difesa utilizzano propri centri

Centro di Valutazione e Certificazione Nazionale (da qui in poi CVCN) è di primaria importanza[59]. L'ente, nell'effettuare test di sicurezza informatica e nel controllare la solidità dei profili di cybersecurity, garantisce la stabilità delle forniture, dei servizi e dei processi considerati sensibili per la sicurezza nazionale, accertandone le capacità tecniche alla prevenzione e, eventuale, risoluzione dei problemi ad essi connessi. La disciplina si presenta in modo differente rispetto a quanto disposto dall'art. 108 co. 4 D.lgs. n. 36/2023, richiedendo, data la sensibilità degli interessi in gioco, un controllo continuo da parte del CVCN, il quale esercita le proprie competenze nel termine di quarantacinque giorni dalla comunicazione delle amministrazioni per l'affidamento di beni ICT. Il parere positivo o negativo del CVCN è dirimente sul punto, in quanto le specifiche indicazioni date dall'ente devono essere recepite nella documentazione di gara della procedura, potendosi prevedere segnalazioni piuttosto significative, tra cui l'inserimento di clausole che condizionano sospensivamente o risolutamente il contratto pubblico[60].

Proprio su questo punto si riflette il mancato coordinamento con la nuova disciplina definita dal Codice dei contratti pubblici, segnatamente se si fa riferimento ad appalti che siano connessi alla tutela di interessi nazionali strategici. Il disallineamento provoca non pochi problemi, principalmente nel caso in cui l'applicazione della disciplina di cui all'articolo 1 del D.L. 105/2019, comporti il rispetto degli *standards* di cybersicurezza da criterio di aggiudicazione a requisito di partecipazione, circostanza non prevista nella disciplina codicistica. Pertanto, in un contesto in cui l'aggiudicazione dei contratti relativi al Perimetro concerne servizi quasi esclusivamente certificati, il rispetto delle norme di cybersicurezza non è semplicemente un aspetto da "premiare", ma rappresenta una condizione necessaria per partecipare alla procedura, circostanza questa apparentemente trascurata dal nuovo Codice dei contratti[61].

In definitiva, la ricostruzione ora effettuata, fa trasparire un quadro normativo in cui a risaltare è la difficoltà definitoria riguardante gli interessi nazionali strategici e il mancato coordinamento tra l'articolo 108 e la normativa nazionale riguardante il PNSC. Tali aspetti, inevitabilmente, oltre a generare dubbi e incertezze in sede applicativa per i soggetti partecipanti nel settore di riferimento, ostacola

di valutazione in luogo del centro nazionale. Per ulteriori approfondimenti sul punto si veda Rossa, 2023a e 2024.

59 Per un approfondimento sull'ente e sui compiti svolti nel processo di acquisizione delle amministrazioni, Bruno, 2020.

60 Come rilevato da Rossa, 2024: 349.

61 Cocchi, 2024: 197 e 198; l'autore valorizza la disciplina indicata dal secondo paragrafo dell'art. 7 della direttiva Nis II, per evidenziare il disallineamento tra le due discipline, la direttiva, infatti, nel prevedere l'ambito di applicazione della strategia nazionale per la cibersicurezza, dispone che "gli Stati membri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source".

il buon andamento delle amministrazioni, aumentando il rischio del contenzioso, in un settore che è sempre stato critico e al centro di annosi dibattiti politici, con buona pace del principio del risultato, da intendere quale vera e propria stella polare posta alla base della rivoluzione copernicana intervenuta all'interno della commessa pubblica[62].

5. Cenni conclusivi

A seguito di quanto ricostruito è opportuno soppesare i *pro* e i *contro* della riforma.

Indubbiamente, nel nuovo assetto delineato dal Codice del 2023, la materia cyber assurge a nuovo ruolo, configurandosi quale vero e proprio fattore di rilevante importanza. Tale elemento non va più considerato in correlazione all'oggetto dell'appalto ma deve essere riletto con nuova centralità, tale da poter comportare anche un cambio delle normali regole applicabili.

In effetti, l'apprezzamento dell'elemento cyber diviene essenziale, circostanza da cui scaturisce l'anteporsi di tale valutazione rispetto all'oggetto globale del contratto, in un'inversione di priorità logica e interferenziale che denota l'emersione della centralità della cybersicurezza in una realtà odierna fortemente incentrata sul *dataset.*

Rispetto ai tratti essenziali della disciplina, è chiaro che prescindendo dagli interessi nazionali strategici o meno, la stazione appaltante dovrà valutare attentamente l'oggetto della gara, tenendo comunque "in debita considerazione" la materia cyber. Tutto ciò non può che essere accolto favorevolmente, laddove l'intenzione legislativa mira a creare un "nuovo" assetto di interessi in cui risulta imprescindibile l'apporto fornito dagli appartenenti alla P.A., imponendo un onere generale per ogni stazione appaltante di conoscere e fronteggiare gli elementi di cybersecurity.

In questo aspetto risiede la prima criticità. Le amministrazioni sono capaci di valutare l'oggetto cyber insito nella gara e, eventualmente, motivare il collegamento con gli interessi nazionali strategici? Tale considerazione non è scevra di conseguenze, anche centrali, nell'applicazione del dato normativo. Senza dubbio, la più significativa permane il pericolo che ciascuna stazione appaltante decida in autonomia i criteri da seguire per mettere in risalto le gare cyber, giungendo al pa-

62 Sul punto, si richiamano le annotazioni di Nannipieri, 2024; 5; in cui si critica: "sul piano sistematico, 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".

radossale risultato in cui lo stesso bene sia qualificato in modo differente a seconda dell'amministrazione valutatrice.

In tale aspetto vi è intimamente correlata la seconda criticità della materia, l'ampia discrezionalità lasciata in capo alle P.A. In un'ottica di sistema, il nuovo Codice rilancia verso nuove modalità di cura dell'interesse pubblico incoraggiando le stazioni appaltanti ad utilizzare lo spazio discrezionale a loro riservato, in particolar modo nello sviluppo di un modo di agire che interessi il potere di tipo "tecnico"[63]. In questo senso, sembrano assumere rilievo nuovi interessi di tipo economico, sociale ma anche commerciale che, già perseguiti dall'ordinamento, si realizzano compiutamente all'interno del nuovo Codice, anche per il tramite dei principi generali, attraverso cui si riconosce nuovo e ampio spazio decisionale in capo alle autorità pubbliche[64].

Sennonché, la discrezionalità implica delle scelte, scelte che, a loro volta, richiedono un'ampia preparazione e conoscenza della materia. La P.A. deve essere in grado di motivare le valutazioni effettuate, dovendosi spingere persino a definire quando il bando debba essere connesso con gli interessi nazionali strategici. Lampante ne è la conseguenza: servono delle competenze scientifiche atte a padroneggiare il settore della cybersecurity, in un momento storico in cui non è certo che i profili professionali postulati siano disponibili in numero adeguato a tutte le stazioni appaltanti[65].

Se dal punto di vista organizzativo il legislatore si è messo in moto attraverso lo "slogan" contenuto nell'art. 19 D.lgs. n. 36/2023, d'altra parte serve agire su di un piano "individuale", in modo che i funzionari amministrativi "siano messi nelle reali condizioni di conoscere questa tematica attraverso un'azione pubblica di diffusione e di promozione della cultura della cybersecurity"[66].

Da ultimo, tali assunti sono da coordinare con il principio del risultato di cui all'articolo 1 D.lgs. n. 36/2023[67]. La logica del risultato amministrativo persegue

63 Ramajoli, 2023: 47.

64 Macchia, 2024: 31.

65 Già sostenuto in tempi non sospetti da Giannini, 1979; in cui si dedicava ampio risalto al personale ed in particolar modo alla sua formazione e addestramento; per un approfondimento in tempi più recenti a seguito delle problematiche odierne, in un'ottica sistemica rispetto a quanto dettato nel PNRR, Angeletti, 2021/ 4.

66 Rossa, 2024: 353.

67 Art.1 D.lgs. n. 36/2023: 1. Le stazioni appaltanti e gli enti concedenti perseguono il risultato dell'affidamento del contratto e della sua esecuzione con la massima tempestività e il migliore rapporto possibile tra qualità e prezzo, nel rispetto dei principi di legalità, trasparenza e concorrenza. 2. La concorrenza tra gli operatori economici è funzionale a conseguire il miglior risultato possibile nell'affidare ed eseguire i contratti. La trasparenza è funzionale alla massima semplicità e celerità nella corretta applicazione delle regole del presente decreto, di seguito denominato "codice" e ne assicura la piena verificabilità. 3. Il principio del risultato costituisce attuazione, nel settore dei contratti pubblici, del principio del buon andamento e dei correlati principi di efficienza, efficacia ed economicità. Esso è perseguito nell'interesse della comunità e per il raggiungimento degli obiettivi dell'Unione europea. 4. Il principio del risultato costituisce criterio prioritario per l'esercizio del potere discrezionale e per l'individuazione della regola del caso concreto.

l'obiettivo principale della valutazione dell'interesse sotteso all'*agere pubblicistico*, nel rispetto dei termini che ne scandiscono l'efficienza e la funzionalità. Al contempo, con tale principio si concede ampia autonomia alla P.A., nel raggiungimento di esigenze che nascono anche da obiettivi posti a livello europeo e che nella prassi si soppesano all'interno degli acquisti di beni e servizi, tra cui vi rientra, oggi, la cybersicurezza[68].

Il principio del risultato diviene espressione di un comando espresso volto a condizionare l'azione amministrativa verso l'elaborazione di parametri operativi ai quali adattare i casi concreti e le scelte discrezionali in essi operate[69]. In buona sostanza, l'art. 1 del nuovo Codice si fa portavoce del principio di imparzialità e buon andamento di cui all'art. 97 della Costituzione che oggi fornisce parametro concreto di sindacato dell'azione amministrativa[70]. Attraverso tale dogma, perno centrale attorno a cui ruotano gli altri principi[71], s'intende tutelare la certezza del rapporto contrattuale e il legittimo affidamento della parte privata nella stabilità del rapporto, facendo si che la solidità del primo porti ad una compattezza complessiva del mercato[72], ed in questo caso dei valori della cybersecurity e della sicurezza di tutte le amministrazioni.

In questo nuovo assetto di interessi, è necessario partire dalle certezze date dalla nuova disciplina in tema di cybersicurezza valorizzando il nuovo dato normativo e accrescendo il patrimonio culturale di tutta la P.A., credendo e investendo fortemente nella crescita individuale dei singoli funzionari formanti il "cuore" della mano pubblica. Dall'altro lato, in un contesto in cui si vuole neutralizzare la c.d. "paura di amministrare" e aumentare la *performance* dell'azione amministrativa, su un piano di nuova fiducia tra il settore pubblico e quello privato, i dubbi recati dalla nuova normativa, in particolar modo per quel che concerne i concetti, le definizioni date e il mancato coordinamento con la disciplina riguardante il PNSC, comporta un fattore di incertezza sul risultato finale della gara, in contrasto con quanto si fa portavoce il nuovo Codice.

Incoraggiare le stazioni appaltanti è fondamentale e riconoscergli il più ampio potere discrezionale consente di passare da una amministrazione riflessiva ad una amministrazione che opera nel "caso concreto". Ma ciò deve essere fatto con criterio logico, in virtù di una normativa che non lascia spazio a dubbi interpretativi che solo criticità possono comportare rispetto a quanto di buono prospettato. L'attuale disciplina in combinato con i nuovi principi del Codice consentono un'opera di bilanciamento che deve ispirare costantemente gli operatori del settore dato che solo in virtù di quest'ultimi la P.A. può assurgere a ruolo di "architetto delle scelte" tale

68 Sul risultato e sull'impiego delle risorse finanziarie, in un sistema di valutazione del rendimento attraverso indicatori di efficienza, Ursi, 2016: 229.

69 Per una visione completa sul principio del risultato, si veda Cintioli, 2023.

70 Spasiano, 2023a.

71 Segnatamente, il principio della fiducia (art. 2 D.lgs. n. 36/2023); il principio dell'accesso al mercato (art. 3 D.lgs. n. 36/2023); principi di buona fede e tutela dell'affidamento (art. 5 D.lgs. n. 36/2023).

72 Spasiano, 2023b.

da incentivarne l'indipendenza, aumentandone l'attitudine in sede decisionale[73], anche in un settore delicato come quello della cybersecurity.

Bibliografia

Angeletti S., 2021, "'Capacity training'. Formazione e capacità amministrativa delle PA nel Piano Nazionale di Ripresa e Resilienza", in *Rivista italiana di Public management*, vol. 4, n. 2.

Buoso E., 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli: 98 e ss.

Busia G. 2020, "Cybersecurity: una sfida per tutti", in Contaldo A.-Mula D. (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: IX e ss.

Bruno B., 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *federalismi*, 14.

Campara F., 2020, "Il Cybersecurity Act", in Contaldo A., Mula D. (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 70 e ss.

Cancrini A. e Vagnucci F., 2023 "Le procedure di scelta del contraente e la selezione delle offerte", in *Giorn. Dir. amm.*, 3: 329.

Carbone L., 2023, "La scommessa del 'codice dei contratti pubblici' e il suo futuro", in *Giustiziamministrativa.it:* 9 e ss.

Carotti B., 2020, "Sicurezza cibernetica e Stato nazione", in *giornale di diritto amministrativo*, 5: 629.

Cassano G., Iaselli M., Spangher G., 2022, "Cybersecurity: contesto normativo di riferimento a livello nazione ed europeo", in *Diritto di Internet, Digital Copyright e Data Protection*, 4.

Catarisano C., 2023, "Articolo 108 D.lgs. n. 36/2023", in L. Perfetti (a cura di) *Codice dei contratti pubblici commentato*, Milano: Wolters Kluwer-Ipsoa: 811.

Cerciello F., 2024, "Tra NIS 2 e CER: un filo comune per la cybersecurity e la sicurezza nazionale", in *Il Quotidiano Giuridico,* 1.

Cintioli F., 2023, "Il principio del risultato nel nuovo codice dei contratti pubblici", in *Giustiziamministrativa.it.*

Chiari C., Mazzetti A., 2023, "Cybersicurezza, le norme in vigore e in arrivo per i soggetti inclusi nel perimetro di sicurezza nazionale", in *Agenda digitale*.

Cocchi T., 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 – Rivista giuridica dei servizi pubblici*, 1: 179 – 200.

Di Costanzo C., 2022, "La resilienza cibernetica a partire da alcuni recenti documenti", in *Osservatorio sulle fonti*, 2: 1-3.

Giannini M. S., 1979, *Rapporto sui principali problemi della amministrazione dello Stato*, trasmesso alle Camere il 16 novembre.

73 Macchia, 2024: 30.

Giupponi T. F., 2024, "Il governo nazionale della cybersicurezza"*,* in *Quaderni Costituzionali,* 2.
Macchia M., 2024, "Il ruolo dei principi nel Codice dei contratti", in Macchia M. (a cura di) *Costruire e acquistare, Lezioni sul nuovo Codice dei contratti pubblici*, Torino: Giappichelli: 7 – 31.
Matassa M., 2023, "Una strategia nazionale a difesa del cyberspazio"*,* in *Pa persona e amministrazione Ricerche Giuridiche sull'Amministrazione e l'Economia*: 11/2: 635.
Monti A., 2023, "L'impatto del nuovo Codice degli appalti sulla cybersecurity della Pa", in *Formiche.net.*
Nannipieri L., 2024, "Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio", in *Rivista italiana di informatica e diritto*, 1: 1 – 5.
Piras P., 2022, "L'amministrazione digitale tra divari e doveri. 'Non camminare davanti a me, ma al mio fianco'", in *Pa persona e amministrazione Ricerche Giuridiche sull'Amministrazione e l'Economia,* 11/2: 426.
Previti L., 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi*: 25: 68 e ss.
Ramajoli M., 2023, "I principi generali", in Contessa C. e Del Vecchio P., (a cura di) *Codice dei contratti pubblici*, Vol. I, Napoli: Editoriale scientifica: 47.
Ricotta F. N., 2023, "Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria" in *Diritto Penale Contemporaneo*: 1: 102.
Rossa S., 2023 (a), Cybersicurezza e pubblica amministrazione, Napoli: Editoriale Scientifica.
Rossa S., 2023 (b), "Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario", in *Vergentis. Revista de Investigación de la Cátedra Internacional conjunta Inocencio* III, 17: 161 – 175.
Rossa S., 2024, "Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici", in *Ceridap*, 3: 1 – 15.
Sica T., 2022, "Cybersecurity e governo del rischio (Cybersecurity and risk management)", in *Corporate Governance*: 4: 583.
Spasiano M. R., 2023 (a), "Codificazione di principi e rilevanza del risultato", in C. Contessa e P. Del Vecchio, (a cura di) *Codice dei contratti pubblici*, Vol. I, Napoli: Editoriale scientifica: 49-78.
Spasiano M. R., 2023 (b), "Principi e discrezionalità nel nuovo codice dei contratti pubblici: i primi tentativi di perimetrazione del sindacato", in *Federalismi.it*, 24: 222-239.
Torchia L., 2023, *Lo Stato digitale. Una Introduzione,* Bologna: Il Mulino.
Ursi R., 2016, *Le stagioni dell'efficienza. I paradigmi giuridici della buona amministrazione,* Santarcangelo di Romagna: 229.
Ursi R., 2023, "La sicurezza cibernetica come funzione pubblica", in *La sicurezza nel cyberspazio*, a cura di Ursi R., Milano: Franco Angeli.