ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
2 / 2024

APRILE - GIUGNO

Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici

Stefano Rossa

DOI: 10.13130/2723-9195/2024-2-29

Il contributo indaga la disciplina italiana degli appalti pubblici di cybersicurezza. Dopo essersi soffermato sulle norme in materia introdotte dal Codice appalti del 2023 e averne evidenziato la natura programmatica, l'articolo analizza la disciplina giuridica dettata per gli appalti pubblici nell'ambito della cybersecurity: sia quella applicabile alle Pubbliche Amministrazioni in generale (fra cui quelle ricomprese nel Perimetro di sicurezza nazionale cibernetica), sia quella speciale riservata alle procedure di gara bandite dall'Agenzia per la cybersicurezza nazionale, mettendo in evidenza il collegamento fra programmaticità della norma e necessità della promozione e diffusione della cultura della cybersicurezza svolta dai soggetti pubblici.

Public Procurement and Cybersecurity. The Italian Legal Framework

The paper investigates the Italian legal framework regarding cybersecurity public procurement. First, the rules introduced by the (Italian) 2023 Public Procurement Code are explored. Secondly, the residual legal framework is examined: both the general one applicable to all public administration (including within the [Italian] National Cybersecurity Perimeter), and the special one intended for tendering procedures launched by the (Italian) National Cybersecurity Agency. The necessary role of public actors in promoting and disseminating cybersecurity culture is highlighted.

il ruolo del legislatore nazionale.- 3. Le norme di natura programmatica introdotte dal Codice appalti del 2023.- 4. La disciplina (non programmatica) in materia di appalti di cybersicurezza, ovvero la sinergia fra Codice dell'amministrazione digitale e Codice appalti.- 4.1. La disciplina generale valevole per tutte le Pubbliche Amministrazioni.- 4.2. La disciplina generale valevole per le Pubbliche Amministrazioni ricomprese nel Perimetro di sicurezza nazionale cibernetica.- 4.3. La disciplina speciale dell'Agenzia per la cybersicurezza nazionale (cenni).- 5. Considerazioni conclusive: Programmaticità e cultura della cybersecurity.

1. Introduzione. La centralità degli appalti nell'ambito della cybersicurezza[1]

Negli ultimi anni le Istituzioni europee, e dunque quelle nazionali, sono intervenute con cadenza sempre più ravvicinata nel disciplinare sul piano giuridico la cybersicurezza[2]. Se fra i recenti interventi è possibile annoverare, ad esempio, il Regolamento (EU, Euratom) 2023/2841[3], la c.d. Direttiva NIS 2[4], la c.d. Direttiva CER (*Critical Entity Resilience*)[5] e il c.d. Regolamento DORA (*Digital Operational Resilience Act*)[6], bisogna sottolineare come uno degli atti normativi europei fondamentali in materia[7] risale al 2019 ed è rappresentato dal Regolamento (UE) 2019/881, il c.d. *Cybersecurity Act*[8].

Come noto, il *Cybersecurity Act* ha stabilito un quadro comune europeo per la certificazione della cybersecurity di prodotti, servizi e processi digitali[9]. Il legislatore europeo ha introdotto questa disciplina con un duplice intento: da un lato assicurare ai consumatori che i beni o i servizi che essi acquistano sul mercato della tecnologia abbiano un livello minimo e comune di sicurezza *cyber*, indipendentemente dal Paese membro in cui lo si acquista, rafforzando la fiducia dei consumatori sostenendone, dunque, la domanda[10]; dall'altro lato, omogenizzare il mercato europeo, impedendone la frammentazione[11], e quindi rafforzandolo innanzi alle minacce *cyber* (di natura transfrontaliera)[12] e altresì nei confronti degli altri mercati concorrenti (es. Cina).

Non volendo in questa sede addentrarsi nell'analisi della disciplina, complessa e intricata, della certificazione della cybersicurezza[13], dall'importanza del c.d.

Cybersecurity Act si desume un aspetto evidente: la centralità delle logiche di mercato anche – anzi: soprattutto – nell'ambito della cybersicurezza[14]. E dato che anche gli attori pubblici operano sul mercato al pari di quelli privati, ecco dunque come gli appalti pubblici di cybersicurezza assumano un ruolo primario: occorre infatti tenere in considerazione la consistente domanda di beni e servizi tecnologici delle Pubbliche Amministrazioni, le quali si vedono così chiamate all'aggiudicazione di procedure di acquisto di forniture, servizi e processi di natura *cyber*[15].

2. La disciplina normativa in materia di appalti di *cybersecurity* e il ruolo del legislatore nazionale

Come noto, le Direttive 2014/23-24-25/UE in materia di appalti e concessioni non contengono né una disciplina generale sugli appalti di *cybersecurity* né minime e particolari disposizioni[16]. Questo aspetto, che di primo acchito può essere giustificato con la riconduzione di questa materia all'ambito di stretto interesse nazionale "tradizionale" dei diversi Paesi membri[17] (nonostante vi sia una precisa disciplina europea in materia di appalti nel settore della difesa)[18], comporta che l'intervento in materia di appalti di *cybersecurity* sia demandato ai legislatori domestici.

3. Le norme di natura programmatica introdotte dal Codice appalti del 2023

Per quanto attiene al panorama italiano, il Codice appalti di recente approvazione, il d.lgs. n. 36/2023[19], ha introdotto due norme specifiche in materia di cybersicurezza: l'art. 19, co. 5, e l'art. 108, co. 4. Se questo fatto rappresenta una novità, dato che il d.lgs. n. 50/2016 ignorava totalmente il tema *cyber*, per le ragioni di seguito argomentate tali previsioni normative rappresentano una limitata innovazione operativa giuridico-amministrativa, costituendo un manifesto di politica di *cybersecurity*, soprattutto la prima delle due norme, a fronte della loro natura programmatica.

L'art. 19, co. 5, del d.lgs. n. 36/2023 impone alle stazioni appaltanti e agli operatori economici che prendono parte alle procedure di gara

(indipendentemente dal settore considerato) – le quali ora dovranno essere effettuate digitalmente, a seguito della digitalizzazione dell'intero ciclo dei contratti pubblici stabilita dal Codice[20] – l'obbligo dell'adozione di misure tecniche e organizzative finalizzate ad assicurare la sicurezza informatica[21] e la protezione dei dati personali[22].

L'art. 108, co. 4, del Codice, invece, al quarto periodo stabilisce che nelle procedure di approvvigionamento di forniture e servizi informatici per l'Amministrazione Pubblica le stazioni appaltanti, e le centrali di committenza, dovendo procedere con l'aggiudicazione sulla base del criterio dell'offerta economicamente vantaggiosa, sono tenute a considerare gli elementi di *cybersecurity* nella valutazione dell'elemento qualitativo-tecnico dell'offerta; e qualora tali procedure siano riferibili a contesti rilevanti per gli interessi nazionali strategici, le stazioni appaltanti devono limitare la ponderazione della valutazione della componente economica dell'offerta a dieci punti percentuali del punteggio complessivo, in tal modo aumentando notevolmente "il peso" della componente tecnica dell'offerta[23].

Dall'analisi di queste due introduzioni normative emerge un aspetto fondamentale: il legislatore è intervenuto per formalizzare, da un lato, l'obbligo in capo a chi partecipa a una procedura di aggiudicazione (dal lato dell'aggiudicazione e da quello del fornitore) di dotarsi di una struttura organizzativa sicura sul piano informatico; dall'altro, di attribuire un peso significativo all'elemento *cybersecurity* nella valutazione delle offerte di appalti di tecnologia. Ma proprio questo aspetto ne sottolinea la portata limitata: vengono formalizzati due aspetti che, nella realtà dei fatti, erano presenti già prima dell'intervento normativo del 2023 – soprattutto in relazione a quelle Amministrazioni aggiudicatrici da sempre deputate all'aggiudicazione di appalti di tecnologia.

Appare inesatto ritenere che, prima dell'entrata in vigore recente Codice appalti, le stazioni appaltanti non considerassero l'elemento della cybersicurezza nella valutazione della componente tecnica dell'offerta in gare relative a forniture, servizi e processi informatici. Ciò sia a fronte della discrezionalità affidata alle Amministrazioni aggiudicatrici relativa alla pianificazione, al disegno e alla gestione della procedura di gara, in vista del soddisfacimento "*taylor made*" degli specifici fabbisogni espressi nello specifico caso di specie[24]. E sia in conseguenza,

come si analizzerà in seguito, del fatto per cui le gare di tecnologia sono gestite in modo aggregato da centrali di committenza dotate di personale altamente specializzato e attento a tutti i profili della procedura, fra cui anche quello della cybersicurezza.

È necessario rilevare, tuttavia, la previsione del legislatore di imporre il limite del 10% alla componente economica dell'offerta e dunque, *ad contrarium*, di attribuire il peso del 90% alla componente tecnica della stessa, fra cui gli elementi di cybersicurezza, nell'ipotesi di appalti informatici impiegati in un contesto correlato alla tutela degli interessi nazionali strategici. Essa è una scelta chiara che dimostra, da un lato, la volontà ben precisa di limitare la discrezionalità delle stazioni appaltanti nei casi ritenuti più rilevanti per gli interessi del Paese, in un contesto, quale quello delineato dal Codice appalti del 2023, in cui è venuto meno il limite generale del peso del 30% della valutazione della componente economica dell'offerta, nell'ambito applicativo del criterio dell'offerta economicamente più vantaggiosa, stabilito invece dal precedente Codice appalti del 2016[25]. Dall'altro lato, invece, evidenzia sia la crescente centralità dei profili di *cybersecurity* per le scelte cardine dello Stato, sia il legame di questa materia con l'alveo della sicurezza pubblica e di quello dei servizi di informazione (e della difesa[26])[27].

Anche la norma introdotta dall'art. 19, co. 5, del Codice ha una chiara natura di "manifesto di politica di cybersicurezza". Sarebbe errato ritenere che prima del 2023 le stazioni appaltanti e gli operatori economici, specialmente quelli maggiormente strutturati, non dotassero di un'organizzazione interna volta a prevenire, limitare e contrastare rischi di *cyber* attacchi e di *cyber* incidenti[28]. Essendo la salute cibernetica cruciale per il funzionamento di ogni organizzazione, pubblica o privata, indipendentemente dalla partecipazione a procedure di gara, è intuitivo ritenere che ciò in realtà avvenisse già da tempo – anche considerando che il primo *worm*, creato da Robert Morris, risale al 1988[29]. Al contempo, tuttavia, è palese l'esigenza di una univoca direzione tracciata dal legislatore, soprattutto in conseguenza della digitalizzazione dell'intero ciclo di vita dei contratti pubblici: infatti, se con il d.lgs. n. 36/2023 la digitalizzazione diviene il mezzo principale con cui gestire il *public procurement*, risulta pertanto necessario che coloro i quali operano in questo ambito si dotino obbligatoriamente di adeguati profili organizzativi di sicurezza informatica (e di

trattamento dei dati personali). Ed è proprio questa la *ratio* dell'art. 19, co. 5, del Codice appalti, che ne evidenzia la natura programmatica, con una maggior rilevanza sul piano della politica di cybersicurezza anziché su quello strettamente giuridico-amministrativo. Aspetto, per altro, confermato dall'ultimo periodo della disposizione, secondo cui le Amministrazioni aggiudicatrici devono assicurare la formazione del personale addetto diffondendo, quindi, la cultura della cybersicurezza[30].

4. La disciplina (non programmatica) in materia di appalti di cybersicurezza, ovvero la sinergia fra Codice dell'amministrazione digitale e Codice appalti

Oltre alle due norme sopra analizzate, il recente Codice degli appalti non contiene norme ulteriori nella materia degli appalti di cybersicurezza. Se il d.lgs. n. 36/2023 racchiude norme di carattere programmatico, esse però devono essere necessariamente integrate da quelle contenute in altri testi normativi, di natura maggiormente operativa: su tutti il Codice dell'amministrazione digitale (c.d. CAD)[31].

Occorre innanzitutto premettere come vi siano due regimi normativi: uno generale e uno speciale[32]. Da un lato, quello generale è relativo agli appalti di forniture, servizi o lavori in materia di cybersicurezza applicabile a tutte le Amministrazioni intese in senso ampio. Unicamente in relazione a quelle Pubbliche Amministrazioni ricomprese all'interno del Perimetro nazionale di sicurezza cibernetica si applicheranno norme specifiche della disciplina generale. Dall'altro lato, invece, il regime speciale concerne le procedure di appalto di forniture, servizi e lavori aggiudicate dall'Agenzia per la Cybersicurezza Nazionale finalizzate alla tutela della sicurezza nazionale nel cyberspazio.

4.1. La disciplina generale valevole per tutte le Pubbliche Amministrazioni

Come è risaputo, il *corpus* normativo in tema di digitalizzazione della Pubblica Amministrazione, il CAD[33], ha indicato l'Agenzia per l'Italia Digitale (Agid) quale istituzione incaricata di conseguire gli obiettivi stabiliti dall'Agenda

Digitale Italiana e da quella Europea[34]. Fra i poteri attribuiti all'Agid, per quanto ivi di interesse emergono quelli di vigilanza, verifica, controllo e monitoraggio sul rispetto delle norme del CAD, delle proprie Linee guida e del Piano triennale per l'informatica nella Pubblica Amministrazione[35]. Quest'ultimo, nella sua versione attualmente in vigore (relativo agli anni 2024-2025-2026)[36], contiene le "Gare strategiche per la trasformazione digitale", vale a dire alcune precise procedure d'appalto in ambito tecnologico che permettono alla Pubblica Amministrazione di acquisire i servizi necessari per implementare le strategie per la trasformazione digitale del Paese[37]. Esse sono regolate dal combinato disposto della disciplina delineata dal d.lgs. n. 36/2023 e dal d.lgs. n. 82/2005, mentre sul piano gestionale sono realizzate sinergicamente da Consip[38], per il profilo dell'amministrazione della procedura di gara, e da Agid, in relazione alla definizione degli aspetti tecnico-informatici dell'oggetto della fornitura, servizio o lavoro.

La crescente centralità della *cybersecurity* nell'ambito pubblico, di cui si è avuto modo di evidenziare nelle pagine precedenti, è testimoniata altresì dalla presenza di procedure d'appalto di forniture, servizi e processi di cybersicurezza nel novero delle gare strategiche per la trasformazione digitale.

In questo contesto il ruolo di Consip è fondamentale, dato che essa è il soggetto a cui il legislatore ha affidato il ruolo di centrale di committenza nazionale in relazione, in particolare, alle reti telematiche delle Pubbliche Amministrazioni, al Sistema pubblico di connettività e alla rete internazionale delle Amministrazioni[39]. Tale circostanza, che si lega all'obbligo in capo alle Amministrazioni Pubbliche di ricorrere agli strumenti messi a disposizione da Consip nell'ipotesi di procedure di gara aventi a oggetto l'area merceologica "Informatica, elettronica, telecomunicazioni e macchine per l'ufficio"[40], comporta che la generalità degli appalti pubblici di cybersicurezza siano affidati a questa centrale di committenza, non potendo le singole Pubbliche Amministrazioni procedere con autonomia all'indizione e alla gestione di procedure di gara di *cybersecurity*[41].

Nel contesto delle gare strategiche per la trasformazione digitale, dunque, si applicano le norme generali del Codice appalti, in particolare quelle in tema di centralizzazione delle committenze[42], che impongono l'affidamento delle procedure di gara alle centrali di committenza, particolari stazioni appaltanti operanti per conto di altre Amministrazioni aggiudicatrici la cui azione

centralizzata comporta significativi vantaggi per l'intero ambito del *public procurement*[43]. Centralizzazione delle committenze che è legato a doppio filo al sistema di qualificazione delle stazioni appaltanti[44]. In particolare, il d.lgs. n. 36/2023 ha stabilito che nei casi di procedure con valore inferiore alle soglie europee previste per gli affidamenti diretti (140.000 € per servizi e forniture), e per l'affidamento di lavori d'importo pari o inferiore a 500.000 €, le stazioni appaltanti non qualificate possono procedere autonomamente alla procedura d'appalto, ma possono altresì effettuare in modo autonomo ordini a valere su strumenti di acquisto messi a disposizione dalle centrali di committenza qualificate e dai soggetti aggregatori[45]. Nell'ipotesi, invece, di procedure di valore superiore alle predette soglie, soltanto le stazioni appaltanti qualificate possono procedere autonomamente[46], mentre quelle non qualificate devono ricorrere alle centrali di committenza qualificate[47]: fra esse rientra proprio Consip[48], la quale risulta essere altresì un soggetto aggregatore[49].

Secondo il Codice appalti, nell'ipotesi in cui le Amministrazioni dovessero procedere all'aggiudicazione di procedure aventi un oggetto rientrante in una categoria merceologica fra quelle espressamente individuate[50], esse sono obbligate a ricorrere agli strumenti messi a disposizione da Consip[51]. Poiché le forniture, i servizi e i processi ricompresi nell'alveo delle gare strategiche per la trasformazione digitale del Piano triennale per l'informatica della Pubblica Amministrazione rientrano nell'area merceologica "Informatica, elettronica, telecomunicazioni e macchine per l'ufficio", in cui è compreso l'ambito della cybersicurezza, e in forza della citata normativa che ha conferito a Consip la natura di centrale di committenza nazionale per le reti telematiche delle Amministrazioni, al Sistema pubblico di connettività e alla rete internazionale delle Pubbliche Amministrazioni[52], allora risulta spettare proprio a Consip la predisposizione, l'indizione, la gestione e l'aggiudicazione degli appalti di cybersicurezza per l'Amministrazione Pubblica.

Tra i diversi strumenti di acquisto a sua disposizione[53], nell'ambito della cybersicurezza Consip ricorre in particolare all'accordo quadro[54].

L'accordo quadro[55] è uno strumento contrattuale di diritto pubblico, impiegato da specifiche Amministrazioni aggiudicatrici, a vantaggio di altre, mirato a definire le clausole degli appalti da aggiudicare, in un prestabilito arco temporale (quattro anni) in particolare in relazione al contenuto minimo della fornitura o

del servizio (ovvero: quantità[56] e prezzo), identificando uno o più operatori economici fornitori. L'accordo quadro è uno strumento contrattuale, e non una procedura di aggiudicazione, in quanto esso viene concretamente realizzato tramite le procedure di scelta del contraente previste esplicitamente dalla disciplina generale sul *public procurement*[57]. D'altronde, lo stesso Codice appalti 2023 sul piano strettamente sistematico disciplina l'accordo quadro in una norma (art. 59) distinta da quelle relative alla procedure di scelta del contraente (artt. 70-76); tale aspetto è confermato dallo stesso dato letterale espresso nella disciplina europea, per la quale l'accordo quadro non viene definito una "procedura" o un "appalto", bensì genericamente un «*accordo concluso tra una o più amministrazioni aggiudicatrici e uno o più operatori economici*»[58]; e altresì dal testo delle norme europea e nazionale, che distinguono i diversi istituti sul piano strumentale, affermando che «*[g]li appalti basati su un accordo quadro sono aggiudicati secondo le procedure previste [...]*»[59].

Nel caso ivi di interesse, l'accordo quadro è realizzato da Consip in favore di altre Pubbliche Amministrazioni, le quali dovranno darvi esecuzione tramite appalti specifici, che dovranno pertanto essere conformi a quanto definito dall'accordo quadro[60].

Ciò posto, l'accordo quadro può strutturarsi in diverse forme dipendenti da due variabili fra loro combinabili: il numero di operatori economici con cui l'accordo è aggiudicato e il livello di definizione delle condizioni contrattuali.

In relazione alla prima variabile, pertanto, vi potranno essere accordi quadro c.d. mono-fornitore in quanto stipulati soltanto con un operatore economico, oppure accordi quadro c.d. pluri-fornitore, conclusi cioè con due o più operatori[61]. In relazione alla seconda variabile, invece, vi potranno essere accordi quadro c.d. chiusi, nell'ipotesi in cui vengano già disciplinate tutte le condizioni che regoleranno l'esecuzione dei contratti specifici[62]; in questo caso, tutte le condizioni dei successivi appalti specifici sono già definite *in toto*, comportando che la scelta del fornitore (o dei fornitori, se l'accordo quadro è chiuso pluri-fornitore[63]) avviene già nella fase della definizione dell'accordo quadro. Ma potranno esservi altresì accordi quadro c.d. aperti, qualora non siano già stabilite tutte le clausole del contratto, occorrendo di una loro ulteriore precisazione nella fase di esecuzione degli appalti specifici, in quella fase che è nota come "riapertura del confronto competitivo"[64].

Dietro previa esplicita indicazione nella *lex specialis*, nella fase di riapertura è possibile avere sia un rilancio di natura economica – si pensi nell'ipotesi dell'aggiudicazione con il criterio del massimo ribasso – relative a un miglioramento della componente economica dell'offerta (*i.e.* riduzione del prezzo); al contempo è altresì possibile aver un rilancio di tipo tecnico – in particolare nel caso dell'aggiudicazione con il criterio dell'offerta economicamente più vantaggiosa – che avrà a oggetto una miglioria della componente tecnica dell'offerta. Le citate variabili "aperto o chiuso" e "mono-fornitore o pluri-fornitore" possono combinarsi fra loro dando vita, nello specifico, ad accordi quadro chiusi mono-fornitore, ad accordi quadro chiusi pluri-fornitore, ad accordi quadro aperti mono-fornitore e ad accordi quadro aperti pluri-fornitore[65].

Dal breve inquadramento teorico sopra ricostruito, emerge il carattere duttile e strategico insito nel ricorso all'accordo quadro. Esso è un istituto dotato di agilità[66], consentendo alle Amministrazioni aggiudicatrici di soddisfare i propri fabbisogni, definendo le prestazioni necessarie a tal fine e gli eventuali fornitori, senza però obbligarle a procedere in tal senso[67]. Parimenti è strategico poiché l'aggiudicazione dell'accordo quadro è affidata a una centrale di committenza, nella quale è elevato il livello di professionalità e di competenze tecniche: in tal modo non solo si riuscirà a ottenere prezzi più bassi, elevanti standard tecnici e omogenei per tutto il settore pubblico, ma si efficienta il processo di acquisto diminuendo gli eventuali errori nella fase della definizione della procedura e, dunque, diminuendo il possibile contenzioso[68].

Ciononostante, nella realtà delle cose è necessario – e possibile – ricorrere all'accordo quadro soltanto in presenza di forniture e servizi omogenei e standardizzati. E questo è esattamente ciò che accade, ad esempio, in relazione all'acquisto di beni e servizi di natura tecnologica, fra cui quelli di natura di cybersicurezza. Il ricorso al modello dell'accordo quadro per la fornitura di beni e servizi di *cybersecurity*, nell'ambito delle gare strategiche per la trasformazione digitale, gestite da Consip e predisposte sul piano tecnico da Agid, è testimoniato dalle più importanti gare aggiudicate in Italia in materia di sicurezza informatica[69].

4.2. La disciplina generale valevole per le Pubbliche Amministrazioni ricomprese nel Perimetro di sicurezza nazionale cibernetica

Se la disciplina generale relativa agli appalti in ambito di cybersicurezza si applica alla generalità delle Pubbliche Amministrazioni, occorre però precisare che talune di esse sono ricomprese nel Perimetro di sicurezza nazionale cibernetica (PSNC): a fronte di tale circostanza, per queste specifiche Amministrazioni si applicano alcune norme particolari della disciplina generale.

Senza voler soffermarsi in questa sede nell'analisi di questo istituto, in relazione a cui si rimanda alle riflessioni della dottrina[70], basti ivi ricordare come il PSNC, introdotto nel 2019[71], costituisce una cornice entro cui vengono applicate speciali norme in materia di *cybersecurity* in capo a taluni soggetti ritenuti particolarmente sensibili e la cui azione è esercitata (anche) con reti e infrastrutture digitali[72]. Da un lato, infatti, la disciplina del Perimetro si applica a quei soggetti che esercitano una funzione *essenziale* dello Stato. Dall'altro lato, esse valgono per quei soggetti, di natura pubblica o privata, che prestano un servizio *essenziale* per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, in relazione a cui un possibile malfunzionamento, interruzione o impiego improprio delle proprie infrastrutture informatiche si traduce in un pregiudizio alla sicurezza nazionale[73].

Sebbene sul piano regolamentare vengano specificati i settori di attività entro cui essi operano[74], per ragioni di sicurezza nazionale l'elenco preciso dei soggetti che sono ricompresi nel Perimetro non è pubblico (e non può essere oggetto di accesso): l'inserimento dello specifico soggetto nel PSNC è notificata, infatti, al destinatario con modalità riservate ed è comunicato ai servizi di informazione[75].

In ogni caso, la disciplina del PSNC è volta a garantire un elevato livello di sicurezza delle reti e dei sistemi informativo-digitali da essi impiegati nel rispettivo esercizio di funzioni essenziali o nella prestazione di servizi pubblici essenziali. A tal fine essa si estrinseca in obblighi e misure di natura preventiva, volte a impedire *ex ante* un eventuale incidente o attacco informatico, e di carattere di notificazione (e risposta) mirate a informare le autorità competenti in relazione a un incidente o un attacco informatico e finalizzate all'adozione di ulteriori e

conseguenti misure tecniche di risposta. Fra gli obblighi di natura preventiva ve ne è uno che concerne proprio le procedure di aggiudicazione di beni e servizi ICT.

Per i soggetti ricompresi nel Perimetro, infatti, il legislatore ha imposto la comunicazione obbligatoria[76] al Centro di valutazione e certificazione nazionale (CVCN – istituito presso l'Agenzia per la Cybersicurezza Nazionale)[77] circa la volontà di procedere tramite centrali di committenza (ricorrendo dunque a Consip e ai suoi accordi quadro) all'acquisto specifico di forniture di beni, sistemi o servizi tecnologici da impiegare sulle proprie reti o nei propri sistemi digitali (tramite cui vengono esercitare le funzioni pubbliche e i servizi pubblici ricompresi nel PSNC)[78]. La *ratio* di questo obbligo è quella di garantire al CVCN lo svolgimento delle proprie funzioni istituzionali[79], anche avvalendosi dei Laboratori accreditati di prova (LAP)[80] con i quali effettuare test di sicurezza informatica su *hardware* e su *software*: *in primis* quella di controllo tecnico dei profili di *cybersecurity*, nella catena di approvvigionamento tecnologico, su quelle forniture, servizi e processi considerati sensibili per la sicurezza nazionale, verificandone l'assenza di vulnerabilità informatica e vagliandone le condizioni di sicurezza[81]. Considerata la delicatezza di questo tipo di controllo, il CVCN esercita la propria funzione in un lasso di tempo molto ristretto, ovvero entro quarantacinque giorni dalla comunicazione. Decorso tale termine senza l'intervento del CVCN, le amministrazioni che hanno inviato la comunicazione possono procedere con l'aggiudicazione. Nel caso contrario, invece, in cui il CVCN abbia espresso specifici rilievi (imponendo, ad esempio, test di sicurezza), la documentazione di gara della procedura d'appalto deve essere resa conforme a quanto imposto dal Centro[82].

Da quanto ricostruito emerge la centralità del ruolo rivestito dal CVCN, il quale, sulla base di un giudizio di discrezionalità tecnica, può condizionare – e in casi estremi impedire – l'aggiudicazione della fornitura o del servizio digitale. Ruolo centrale necessario proprio a fronte della rilevanza degli interessi in questione.

4.3. La disciplina speciale dell'Agenzia per la cybersicurezza nazionale (cenni)

A fianco alla disciplina generale valevole per la totalità delle Pubbliche

Amministrazioni si pone quella speciale dettata per gli appalti di forniture, servizi e lavori di natura tecnologica per le attività dell'Agenzia per la Cybersicurezza Nazionale (ACN)[83], volte alla tutela della sicurezza nazionale nello spazio cibernetico[84].

Tale disciplina speciale, la quale espressamente deroga a quella generale del Codice appalti[85], stabilisce che le procedure di gara di cui può avvalersi l'Agenzia devono essere realizzate in conformità al c.d. "Programma biennale degli acquisti di beni e servizi e del programma triennale dei lavori pubblici di ACN"[86]; esse devono, inoltre, essere contenute nella relazione che il Presidente del Consiglio dei Ministri presenta al Copasir[87].

In conseguenza alla natura riservata dell'attività cui le procedure di gara di ACN si riferiscono[88], gli operatori economici candidati fornitori sono chiamati sia a rispettare gli obblighi di riservatezza, di non divulgazione e di non impiego dei dati e delle informazioni di cui vengono a conoscenza[89]; sia a dar prova del possesso di particolari requisiti di partecipazione, di idoneità professionale, di capacità economico-finanziaria e (soprattutto) di capacità tecnico-professionale[90]: tutti questi requisiti devono essere posseduti per l'intera durata della procedura, durante la sua esecuzione e finché la prestazione contrattuale non sia correttamente eseguita[91].

Per poter procedere con l'aggiudicazione, la disciplina speciale impone all'ACN di impiegare una fra le cinque procedure di gara individuate sulla base del valore contrattuale[92]: l'affidamento diretto, la procedura negoziata con o senza previo esperimento di gara informale, l'accordo quadro[93], dialogo competitivo e partenariato pubblico-privato.

L'ACN può ricorrere all'affidamento diretto nel caso di forniture, servizi e prestazioni d'opera specialistica o intellettuale di importo inferiore a € 139.000 e per lavori di importo inferiore a € 150.000. Nel selezionare il fornitore l'Agenzia può non rispettare il principio di rotazione dei fornitori, ma sulla base dei principi di imparzialità e di buon andamento è tenuta acquisire almeno un preventivo[94].

È possibile, invece, ricorrere alla procedura negoziata, nell'ipotesi di appalti di forniture, di servizi e di lavori di importo pari o superiore alla soglia prevista per il ricorso all'affidamento diretto[95]. Come anticipato, essa può essere realizzata in presenza o in assenza di una previa gara informale[96]. Nel caso della gara informale

l'ACN deve invitare, inviando loro lettere di invito[97], almeno tre candidati fornitori, previamente individuati senza dover rispettare il principio di rotazione dei fornitori.
La disciplina regolamentare non specifica a quali condizioni l'Agenza possa ricorrere al dialogo competitivo e al partenariato pubblico-privato, rilievo dal quale si deduce applicazione delle norme generali del Codice appalti, a condizione della relativa conformità allo specifico fabbisogno espresso dell'ACN.
Per quanto invece attiene all'accordo quadro, che esplicitamente in questo caso non può avere durata superiore a nove anni, l'Agenzia può ricorrere a questo strumento contrattuale se l'oggetto dell'appalto non può essere quantificato con precisione e immediatezza[98]. Tuttavia, come analizzato, se nella disciplina generale applicabile a tutte le Amministrazioni aggiudicatrici la regola è il ricorso agli strumenti messi a disposizione di Consip, in particolare l'accordo quadro, in quella speciale il ricorso a tali strumenti è l'eccezione[99], essendo ciò consentito unicamente allorquando le condizioni e le modalità dell'appalto siano compatibili con le esigenze di tutela della sicurezza nazionale nel cyberspazio e permettano all'Agenzia un'azione tempestiva. All'infuori di quest'ultima ipotesi, tale circostanza si traduce nel fatto per cui sarà l'ACN a indire e gestire i "propri" accordi quadro.

5. Considerazioni conclusive: Programmaticità e cultura della *cybersecurity*

Dalla ricostruzione effettuata fino a qui è possibile formulare alcune riflessioni.
Pare innanzitutto necessario sottolineare una circostanza fattuale, ancor prima che giuridica. L'ordinamento, infatti, già da tempo, e dunque ancor prima dell'approvazione del d.lgs. n. 36/2023, ha dotato le Amministrazioni aggiudicatrici di una serie di meccanismi giuridico-amministrativi per consentir loro di acquistare determinati tipi di beni e servizi considerati "sensibili", fra cui forniture, servizi e processi tecnologici di natura *cyber*, ricorrendo, come ricostruito, a strumenti contrattuali al tempo stesso efficaci, efficienti e agili. E ciò anche in anni in cui la cybersicurezza era considerata marginale e, in qualche modo, nell'errato immaginario collettivo, un ambito appannaggio di *nerd* in *hoody*.

Tuttavia, se la disciplina degli appalti di cybersicurezza esisteva già prima dell'entrata in vigore del Codice appalti 2023, pur come risultante del combinato disposto di distinti *corpora* normativi, ci si potrebbe interrogare sull'opportunità dell'introduzione di specifiche norme in argomento da parte del d.lgs. n. 36/2023. Una risposta a tale quesito potrebbe derivare proprio dalla natura programmatica delle due norme introdotte e analizzate nella prima parte di questo contributo.

Come si è avuto modo di evidenziare, nella disciplina in materia di appalti di cybersicurezza valevole per tutte le Amministrazioni Pubbliche[100], di carattere più operativo che programmatico, la *cybersecurity* non assume rilievo in quanto tale, come elemento a sé, ma la sua centralità è strumentalmente collegata all'oggetto e al fine dell'appalto (vale a dire acquisire beni, servizi o processi di natura *cyber*). Nella disciplina programmatica introdotta dal Codice appalti 2023[101], invece, la cybersicurezza rileva in modo più ampio e indipendentemente dall'oggetto dello specifico appalto: essa assurge a valore, a elemento generale in grado di condizionare qualsiasi procedura di aggiudicazione, specialmente a seguito del processo di digitalizzazione del ciclo di vita degli appalti in cui tutto è trasformato in dati, e giocoforza diviene oggetto di possibili *cyber* attacchi e incidenti.

Tale aspetto risulta in particolare dalla formulazione dell'art. 19, co. 5, d.lgs. n. 36/2023[102], ma emerge con forza dalle previsioni in materia contenute nel disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" del 16 febbraio 2024 (A.C. 1717)[103], attualmente in corso d'esame alle Commissioni Affari Costituzionali e Giustizia della Camera dei Deputati.

Ciò si desume, nello specifico, dall'art. 10, co. 2, del citato d.d.l. Questa disposizione stabilisce che le stazioni appaltanti e le centrali di committenza, nel caso di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, possono decidere sia di non aggiudicare l'appalto all'operatore economico che ha presentato l'offerta economicamente più vantaggiosa se viene accertato che l'offerta non soddisfa gli elementi essenziali di cybersicurezza[104]; sia di non procedere all'aggiudicazione se nessuna offerta risulti idonea in relazione agli elementi essenziali di cybersicurezza[105]. La previsione della facoltà di non aggiudicare l'appalto sottolinea l'importanza che il legislatore attribuisce all'elemento "cybersicurezza",

in particolare se si considera come tale mancata aggiudicazione pare *ictu oculi* contrapporsi al principio del risultato, espressamente affermato dall'art. 1 del Codice appalti 2023[106]. In realtà, a ben guardare, non vi è affatto contrapposizione; al contrario, la facoltà di non aggiudicare l'appalto costituisce il corretto esercizio del potere discrezione nell'esatta applicazione del principio del risultato[107], posto che esso impone alle stazioni appaltanti e agli enti concedenti di perseguire «*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*»[108]. Se la manca la qualità – nel caso di specie corrispondente alla presenza di elementi essenziali di cybersicurezza – non è pertanto necessario aggiudicare "a ogni costo" la procedura, non dovendo l'Amministrazione farsi prendere da «*"l'ansia di provvedere"*[109] *purchessia, in vista del risultato rappresentato dalla più celere conclusione del procedimento*»[110].

La cybersicurezza, pertanto, assume forte centralità nella fase di aggiudicazione dell'appalto, sia che essa avvenga con il criterio dell'offerta economicamente più vantaggiosa sia con quello del minor prezzo[111], al punto da divenire fondamentale come elemento valoriale, emergendo e ponendo in secondo piano il suo legame strumentale con l'oggetto del contratto.

Rilevando la cybersicurezza *ex se*, è necessario che tutti coloro i quali intervengono nell'ambito dei contratti pubblici – che essi abbiano o meno a oggetto forniture, servizi o lavori di natura tecnologica – siano consapevoli dell'importanza di tale materia, dovendo giocoforza confrontarsi quotidianamente con essa. E per far ciò è essenziale agire sia a livello di organizzazione amministrativa[112], in considerazione dell'insegnamento della dottrina per cui la tutela dei diritti dei cittadini è garantita anche da un corretto disegno organizzativo[113]; ma occorre altresì agire sul piano delle competenze dei singoli individui[114].

É, infatti, necessario che coloro i quali sono chiamati a operare nel contesto degli appalti pubblici, in particolar modo i dipendenti e i funzionari pubblici, siano messi nelle reali condizioni di conoscere questa tematica attraverso un'azione pubblica di diffusione e di promozione della cultura della *cybersecurity*, come del resto espressamente previsto dall'ultimo periodo dell'art. 19, co. 5, d.lgs. n. 36/2023, secondo cui «*[l]e stazioni appaltanti e gli enti concedenti assicurano la*

formazione del personale addetto, garantendone il costante aggiornamento».
La programmaticità di queste norme è da plaudere proprio in funzione della loro promozione della cultura della cybersicurezza, di cui l'intero Paese ha estremo bisogno in conseguenza della cruciale e crescente rilevanza che la *cybersecurity* ha assunto per il fisiologico funzionamento delle Istituzioni democratiche e per gli interessi nazionali strategici – categoria che pare essere distinta e più estesa rispetto ad altre categorie simili, quale quella della "sicurezza nazionale" cui fa riferimento la disciplina del Perimetro di sicurezza nazionale cibernetica (d.l. n. 105/2019, conv. l. n. 133/2019)[115]. Aspetto imprescindibile, d'altronde, per poter far sì che l'Amministrazione possa valutare effettivamente nel merito l'elemento di *cybersecurity* della componente tecnica dell'offerta nell'ipotesi di approvvigionamento di forniture e servizi informatici, così come ora espressamente sancito dall'art. 108, co. 4, d.lgs. n. 36/2023, siano essi riferiti o meno alla tutela degli interessi nazionali strategici.
Sotto questo punto di vista, pare dunque che il legislatore abbia colto la possibilità di piantare nella disciplina normativa dei contratti pubblici due piccoli semi, nell'intento di far germogliare una (più ampia) cultura della *cybersecurity* nella Pubblica Amministrazione – e di riflesso anche negli operatori economici. Tali norme, infatti, possono costituire un pungolo alla lotta all'analfabetismo digitale italiano[116], presente anche all'interno della Pubblica Amministrazione[117], ponendosi in continuità con i più strutturati piani strategici che sono stati istituiti proprio a tal fine[118], oltre a coincidere con il raggiungimento degli obiettivi stabiliti dalla Missione 1 del PNRR in tema di rilancio della competitività e della produttività del Paese[119]. Ciononostante, rappresentando una sorta di "manifesto di politica di cybersicurezza", bisogna essere consci che viene in tal modo posto un obiettivo a lungo termine, tanto importante e ambizioso quanto di ardua realizzazione. Pur essendo consapevoli di ciò, occorre però non dimenticare l'insegnamento della celebre favola di Jean-Pierre Claris de Florian, *La Guenon, le Singe et la Noix*. Essa narra di un giovane cercopiteco che gettò via una noce con cui si era ferito nel tentativo di mangiarla senza, prima, averla aperta, sostenendo che la madre avesse mentito nel dirgli che le noci facessero bene. Avendo assistito alla scena, una scimmia più anziana prese la noce scarta dal giovane cercopiteco, la aprì e iniziò a mangiarla, rivolgendosi così all'altro animale: «*[l]e noci sono buone, ma bisogna aprirle. Ricordati che*

nella vita senza fatica non vi è piacere»[120].

1. La pubblicazione è stata realizzata da ricercatore con contratto di ricerca finanziato dall'Unione Europea – FSE REACT-EU, PON Ricerca e Innovazione 2014-2020 – CUP C65F21001410001. Le pagine web riportate in nota o nel testo si intendono consultate in data 30.04.2024.
2. O *cybersecurity*, per impiegare il termine anglosassone. La cybersicurezza non è stata al centro dell'interesse tradizionale della dottrina, perlomeno quella amministrativa italiana, per evidenti ragioni legate alla recente evoluzione di tale fenomeno. Ciononostante, i recentissimi studi dedicati a questo argomento sottolineano il crescente interesse della letteratura giuridica verso questo tema. È possibile dunque rimandare a E. Buoso, *Potere amministrativo e sicurezza nazionale cibernetica*, Giappichelli, Torino, 2023; R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Franco Angeli, Milano, 2023, nonché ai contenuti ivi presenti, fra cui quello di M. Matassa, *La regolazione della cybersecurity in Italia*, pp. 21 ss.; L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *federalismi.it*, 25, 2022, pp. 65 ss.; F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *federalismi.it*, 12, 2022, pp. 241 ss.; A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. dir. amm.*, 4, 2021, pp. 538 ss.; P.L. Montessoro, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Istituzioni del Federalismo*, 3, 2019, pp. 783 ss. Siano inoltre consentiti i rimandi a S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, Napoli, 2023, nonché a S. Rossa, *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, 2023, pp. 161 ss. Per gli studi relativi all'Agenzia per la Cybersicurezza Nazionale italiana, istituita nel 2021, si rimanda a G.G. Cusenza, *I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, *cit.*, pp. 123 ss.; a M. Fernandes dos Santos, A. Contaldo, *L'agenzia per la cybersicurezza nazionale: istituzione e problematiche in campo*, in *Riv. amm. Repub. Ita.*, 5-6, 2022, pp. 343 ss.; a I. Forgione, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzione, fra regolazione europea e interna*, in *Dir. amm.*, 4, 2022, pp. 113 ss.; e a L. Parona, *L'istituzione dell'Agenzia per la Cybersicurezza Nazionale*, in *Giorn. dir. amm.*, 6, 2021, pp. 709 ss. In relazione alla cybersicurezza, ma con profili variegati, R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *federalismi.it*, 21, 2021, p.. 18 ss., contente riflessioni di natura maggiormente filosofica; per profili di informatica giuridica G. Ziccardi, *La cybersecurity nel quadro tecnologico (e politico) attuale*, in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, vol. III, Giuffrè, Milano, 2019, pp. 210 ss.; per un'attenta analisi delle principali normative, invece, A. Contaldo, D. Mula (a cura di), *Cybersecurity Law.*

Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche, Pacini, Pisa, 2020; in senso ampio – e critico – sul contesto digitale europeo B. Carotti, *La politica europea sul digitale: ancora molto rumore*, in *Riv. trim. dir. pubbl.*, 4, 2022, pp. 997 ss. Per profili comparati con il diritto europeo si rimanda ad E. Longo, *La disciplina della cybersecurity nell'Unione europea e in Italia*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, pp. 203 ss.; E.C. Raffiotta, *Cybersecurity regulation in the European Union and the issues of Constitutional Law*, in *Rivista AIC*, 4, 2022, pp. 1 ss.; nonché a S. Rossa, *Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy*, in *Italian Journal of Public Law*, Vol. 14, 2, 2022, pp. 426 ss. La dottrina straniera si è invece occupata di questo tema da maggior tempo: a titolo non esaustivo, si vedano M.F. Grady, F. Parisi (a cura di), *Law and Economics of Cybersecurity*, Cambridge University Press, Cambridge, 2005; D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, in F.D. Kramer, S.H. Starr, L.K. Wentz (a cura di), *Cyberpower and national security*, National Defence University Press, Lincoln 2009; O. Hathaway et. al., *The law of Cyber-Attack*, in *California Law Review*, Vol. 100, 4, 2012, pp. 817 ss.; N.A. Sales, *Regulating cyber-security*, in *Northwestern University Law Review*, 4, 2013, pp. 1503 ss.

3. Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (in https://s.uniupo.it/dj5rf).
4. Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (in https://s.uniupo.it/wfh8t).
5. Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (in https://s.uniupo.it/posui).
6. Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (in https://s.uniupo.it/ugva0).
7. In argomento si rimanda alla ricostruzione effettuata da S.A. Salvaggio, N. González, *The European framework for cybersecurity: strong assets, intricate history*, in *Int. Cybersecur. Law Rev.*, 4, 2023, pp. 137 ss.
8. Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (in https://s.uniupo.it/p9zra). Si consideri, in ogni caso, che lo stesso *Cybersecurity Act* è al centro di un percorso istituzionale di modifica: cfr. in tal senso la Proposta di

Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti (COM/2023/208 final) (in https://s.uniupo.it/njhwy).

9. Oltre ad aver inciso sulla struttura e sulle funzioni istituzionali dell'ENISA, l'Agenzia europea per la *cybersecurity* (acronimo di *European Network and Information Security Agency*). Il Regolamento (UE) 2019/881 deve essere letto unitamente alla proposta del c.d. *EU Cyber Resilience Act*, vale a dire la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM/2022/454 final) (in https://s.uniupo.it/s6ky8).
10. *Ex multis* si vedano i considerando 7), 10) e 65) Regolamento (UE) 2019/881.
11. Si consideri, infatti, che in precedenza vi erano numerosi sistemi di certificazione di cybersicurezza nazionali, i quali però non prevedevano un automatico riconoscimento reciproco.
12. Vedasi i considerando 5) e 6) Regolamento (UE) 2019/881.
13. Per approfondimenti si vedano A. Mitrakas, *The emerging EU framework on cybersecurity certification*, in *Datenschutz und Datensicherheit*, 7, 2018, pp. 411 ss. e F. Campara, *Il Cybersecurity Act*, in A. Contaldo, D. Mula (a cura di), *Cybersecurity Law*, cit., pp. 57 ss.; sia inoltre consentito rimandare a S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 122 ss.
14. Legame sottolineato altresì da M. Bassini, *Cybersecurity*, in M.T. Paracampo (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Torino, pp. 319 ss. e da B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *federalismi.it*, 14, 2020, pp. 11 ss. In questo secondo studio viene altresì affrontato il tema del *golden power*, argomento in relaziona a cui si vedano L. Belviso, *Golden Power. Profili di diritto amministrativo*, Giappichelli, Torino, 2023, nonché, per profili più specifici, S. De Nitto, *Il "golden power" nei settori rilevanti della difesa e della sicurezza nazionale: alla ricerca di un delicato equilibrio*, in *Dir. amm.*, 2, 2022, pp. 553 ss.; A. Sandulli, *Lo "Stato digitale". Pubblico e privato nelle infrastrutture digitali nazionali strategiche*, in *Riv. trim. dir. pubbl.*, 2, 2021, pp. 513 ss.; mentre, con particolari riferimenti alla cybersicurezza, S. Mele, *Il Perimetro di Sicurezza Nazionale Cibernetica e il nuovo "Golden Power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020.
15. Questo argomento non è stato ancora studiato approfonditamente dalla letteratura. Ciononostante, si rimanda ad AREL (Agenzia di Ricerche e Legislazione), *Appalti pubblici e sicurezza informatica*, in *Oss. Reti*, 3, 2018, nonché J. Ruohonen, *An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union*, in *Eur. J. for Sec. Res.*, 5, 2020, pp. 349 ss. Per alcuni riferimenti più ampi al tema si vedano altresì le riflessioni di A. Sanchez-Graells, *Digital Technologies and Public Procurement.*

Gatekeeping and experimentation in digital public governance, Oxford University Press, Oxford, 2024.

16. Sul punto, a titolo non esaustivo, R. Caranta, A. Sanchez-Graells (a cura di), *European Public Procurement: Commentary on Directive 2014/24/EU*, Elgar, Cheltenaham, 2021; F. Lichère, R. Caranta, S. Treumer (a cura di), *Modernising Public Procurement. The New Directive*, Djøf, Copenaghen, 2014. Per un approccio ulteriore, anche D.C. Dragos, K.M. Halonen, B. Neamtu, S. Treumer (a cura di), *Contract Changes. The Dark Side of EU Procurement Law*, Elgar, Cheltenaham, 2023. Per un Quadro precedente all'approvazione delle Direttive appalti del 2014, si veda M. Trybus, R. Caranta, G. Edelstam (a cura di), *EU Public Contract Law: Public Procurement and Beyond*, Bruylant, Bruxelles, 2013.
17. In argomento si rimanda a B. Carotti, *Sicurezza cibernetica e Stato-Nazione*, in *Giorn. dir. amm.*, 5, 2020, pp. 629 ss. Sul punto anche N. De Felice, *Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali*, in U. Gori, L.S. Germani (a cura di), *Information warfare. La sfida della cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Franco Angeli, Milano, 2012, pp. 69 ss.
18. Vale a dire la Direttiva 2009/81/CE del Parlamento europeo e del Consiglio del 13 luglio 2009 relativa al coordinamento delle procedure per l'aggiudicazione di taluni appalti di lavori, di forniture e di servizi nei settori della difesa e della sicurezza da parte delle amministrazioni aggiudicatrici/degli enti aggiudicatori, e recante modifica delle direttive 2004/17/CE e 2004/18/CE (in https://s.uniupo.it/wejd2). Su di essa il presente contributo non si sofferma. In ogni caso si rimanda *ex multis* a C. Kennedy-Loest, N. Pourbaix, *The new EU defence procurement directive*, in *ERA Forum*, 11(3), 2010, pp. 399 ss.; nonché, in lingua italiana, a N. Di Lenna, *La direttiva europea sul procurement della difesa*, in *Quaderni dell'Istituto Affari Internazionali*, Roma, 2009.
19. A riguardo si veda, per alcuni commenti alle norme, G.F. Cartei, D. Iaria (a cura di), *Commentario al nuovo Codice dei contratti pubblici*, Editoriale Scientifica, Napoli, 2023; F. Caringella (diretto da), *Nuovo codice dei contratti pubblici*, Giuffrè, Milano, 2023; M. Corradino (a cura di), *La riforma dei contratti pubblici. Commento al d.lgs. 31 marzo 2023, n. 36*, Giuffrè, Milano, 2023. Si veda V. Fanti (a cura di), *Corso sui contratti pubblici riformati dal d.lgs. 31 marzo 2023, n. 36*, Edizioni Scientifiche Italiane, Napoli, 2023, nonché i contributi di G. Napolitano, P. Clarizia, M. Nunziata, A. Cancrini, F. Vagnucci, E. Lionetti, V. Bontempi, E. Giardino, A. Vitale, L. Zanghi Buffi, e R. Fragale pubblicati in *Giorn. dir. amm.*, 3, 2023.
20. E ciò sulla base di quanto previsto dalla parte II del libro I del Codice appalti (artt. 19-36), che racchiude norme basate sull'assunto secondo cui la digitalizzazione apporterebbe ingenti benefici sul piano dell'efficienza, dell'efficacia, dell'economicità e della trasparenza dell'azione amministrativa. In argomento si vedano, fra i numerosi contributi: G.M. Racca, *Trasformazioni e innovazioni digitali nella riforma dei contratti pubblici*, in *Dir. amm.*, 4, 2023, pp. 723 ss.; G. Carullo, *Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici*, in *federalismi.it*, 19, 2023, pp. 110 ss.; P. Clarizia, *La digitalizzazione*, in *Giorn. dir. amm.*, 3, 2023, pp. 302 ss.; L. Iannotta, *Decisioni*

algoritmiche e valutazione dell'offerta: la digitalizzazione nel settore dei contratti pubblici, tra strumenti digitali e contributo umano, in *federalismi.it*, 5, 2024, pp. 33 ss.; G.M. Racca, *La digitalizzazione dei contratti pubblici: adeguatezza delle pubbliche amministrazioni e qualificazione delle imprese*, in R. Cavallo Perin, M. Lipari, G.M. Racca (a cura di), *Contratti pubblici e innovazioni. Per l'attuazione della legge delega*, Jovene, Napoli, 2022, pp. 9 ss.; in senso ampio anche P. Chirulli, *Contratti pubblici e amministrazione del futuro*, in *CERIDAP*, 3, 2023, pp. 24 ss.; in ogni caso, ancora prima dell'approvazione del Codice, G.M. Racca, *La modellazione digitale per l'integrità l'efficienza e l'innovazione nei contratti pubblici*, in *Ist. del fed.*, 3, 2019, pp. 739 ss. In relazione al legame fra digitalizzazione e trasparenza si veda F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2, 2015, pp. 227 ss. e sia consentito il rimando a S. Rossa, *Trasparenza e accesso all'epoca dell'amministrazione digitale*, in R. Cavallo, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, Torino, 2020, pp. 247 ss.

21. Come si evince dalla voce *Sicurezza Informatica*, in *Enciclopedia online Treccani* (in https://s.uniupo.it/iqgic), con il termine "sicurezza informatica" concerne quel ramo dell'informatica che studia come tutelare le reti informative. Sotto questo punto di vista, pertanto, non vi è completa identità con il concetto di cybersicurezza, posto che con esso si intende un sistema organizzativo finalizzato a proteggere le infrastrutture digitali di organizzazioni complesse, grazie alla predisposizione di misure tecniche idonee a tutelare diritti e libertà fondamentali. Sul punto, per una definizione giuridica di cybersicurezza, in particolare in relazione al significato del termine originario anglosassone *cybersecurity*, sia permesso il rimando a S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 9 ss.
22. Art. 19 co. 5 d.lgs. n. 36/2023: «*[l]e stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti di cui al comma 3* [vale a dire alle procedure di gara effettuate digitalmente]*, 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*».
23. 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 per la pubblica amministrazione, 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».

24. Il riferimento è all'art. 77 del precedente Codice appalti, il d.lgs. n. 50/2016. In argomento G.M. Racca, S. Ponzio, *La scelta del contraente come funzione pubblica: i modelli organizzativi per l'aggregazione dei contratti pubblici*, in *Dir. amm.*, 1, 2019, pp. 33 ss.
25. Cfr. art. 95, co. 10-*bis*, d.lgs. n. 50/2016, secondo cui «*[l]a 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*».
26. Sul rapporto fra servizi di *intelligence* e difesa T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, in *Dir. cost.*, 1, 2022, pp. 21 ss.
27. Legame che si evince, *inter alia*, nella relazione che intercorre fra l'Agenzia per la Cybersicurezza Nazionale e il Presidente del Consiglio dei Ministri, al quale spetta in «*via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza*» (*ex* Art. 2, co. 1, lett. *a*), d.l. n. 82/2021, conv. l. n. 109/2021), ma a cui è attribuita in via esclusiva «*l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento*» (*ex* art. 1, co. 1, lett. *a*), l. n. 124/2007), come si è avuto già modo di sottolineare in S. Rossa, *Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy*, cit., pp. 440 ss. Sul punto M. Ridolfi, *Servizi di informazione e cybersicurezza*, in *Giorn. dir. amm.*, 2, 2023, pp. 207 ss. In relazione ai servizi di informazione italiani, M. Savino, *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, in *Giorn. dir. amm.*, 2, 2008, pp. 121 ss.; N. Gallo, T.F. Giupponi (a cura di), *L'ordinamento della sicurezza. Soggetti e funzioni*, Franco Angeli, Milano, 2014; G. De Lutiis, *I servizi segreti in Italia. Dal fascismo all'intelligence del XXI secolo*, Sperling & Kupfer, Milano, 2010.
28. In argomento sia consentito il riferimento alle riflessioni riportare in S. Rossa, *Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario*, cit., pp. 162 ss. In generale, per riflessioni fondamentali sull'organizzazione amministrava si veda *ex multis* R. Marrama, *I principi regolatori della funzione di organizzazione pubblica*, in AA.VV., *Diritto amministrativo*, Monduzzi, Bologna, 1998, pp. 397 ss.
29. Sul punto M. Colajanni, *Trent'anni di (in)sicurezza digitale (1988-2018): che ci riserva il prossimo decennio?*, in *Agenda Digitale*, 8 gennaio 2019. Per un approfondimento sul funzionamento del *worm* di Morris si rimanda alla lettura di D. De Angelis, *Come il Morris Worm ha cambiato per sempre la storia di internet*, in *Vice*, 24 ottobre 2017.

30. Sul punto si rimanda a quanto esposto *infra* nel paragrafo conclusivo.
31. D.lgs. n. 82/2005. Sul tema, molto ampio, della digitalizzazione della Pubblica Amministrazione, fra i numerosi contributi, oltre al già citato R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'Amministrazione Pubblica digitale*, cit., si vedano L. Torchia, *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2023; A. Lalli (a cura di), *L'amministrazione pubblica nell'era digitale*, Giappichelli, Torino, 2022; D.U. Galetta, *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal Piano Nazionale di Ripresa e Resilienza e problemi ancora da affrontare*, in *federalismi.it*, 7, 2022, pp. 103 ss.; R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Rubettino, Torino, 2021; Id., *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2, 2020, pp. 305 ss.; A.G. Orofino, *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico*, Cacucci, Bari, 2020; Id., *La semplificazione digitale*, in *Dir. econ.*, 3, 2019, pp. 87 ss.; E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Dir. pubbl.*, 2, 2019, pp. 363 ss.; B. Carotti, *L'amministrazione digitale: le sfide culturali e politiche del nuovo codice*, in *Giorn. dir. amm.*, 1, 2017, pp. 7 ss.; F. Martines, *La digitalizzazione della pubblica amministrazione*, in *Media Laws*, 2, 2018, pp. 1 ss.; Si consenta il rimando a S. Rossa, *Contributo allo studio delle funzioni amministrative digitali*, CEDAM-Wolters Kluwer, Milano, 2021, nonché a Id., *Open data e amministrazioni regionali e locali. Riflessioni sul processo di digitalizzazione partendo dall'esperienza della Regione Piemonte*, in *Dir. inf.*, 4-5, 2019, pp. 1121 ss. Per un commento invece C. Boccia, C. Contessa, E. De Giovanni (a cura di), *Codice dell'amministrazione digitale (D.lgs. 7 marzo 2005, n. 82 commentato e annotato per articolo. Aggiornato al D.lgs. 13 dicembre 2017, n. 217)*, La Tribuna, Piacenza, 2018; S. Calzolaio, *"Digital (and privacy) by default". L'identità costituzionale della amministrazione digitale*, in *Giorn. st. cost.*, 31, 2016, pp. 185 ss.; F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2, 2015, pp. 227 ss.; E. D'Orlando, *Profili costituzionali dell'amministrazione digitale*, in *Dir. inf.*, 2, 2011, pp. 213 ss.
32. Nel testo si recuperano le categorie già impiegate in S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 132 ss., a cui le riflessioni successive si richiamano e che tentano di approfondire e ampliare.
33. Cfr. art. 14-*bis*, co. 1, d.lgs. n. 82/2005.
34. Comunicazione della Commissione europea del 19 maggio 2010 (COM(2010)245 def), rubricata "Un'agenda digitale europea" (in https://s.uniupo.it/nyzk4). In argomento F.M. Lazzaro, *L'Agenda digitale per l'Italia. L'amministrazione pubblica e le nuove sfide digitali*, Wolters Kluwer, Milano, 2013; M. Iaselli (a cura di), *La nuova pubblica amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014; F. Gaspari, *L'agenda digitale europea e il riutilizzo dell'informazione del settore pubblico*, Giappichelli, Torino, 2016.

35. Questo ai sensi dell'art. 18-*bis*, co. 1 primo periodo, d.lgs. n. 82/2005.
36. Agid, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026*, Roma, 2023 (in https://s.uniupo.it/4ymzw).
37. Agid, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026*, cit., pp. 38 ss. L'elenco delle gare strategiche per la trasformazione digitale è consultabile sul sito istituzionale di Consip all'indirizzo https://s.uniupo.it/w1q9m.
38. Consip (acronimo di Concessionaria Servizi Informativi Pubblici) è una società pubblica controllata dal Ministero dell'Economia e delle Finanze che mette a disposizione delle Pubbliche Amministrazioni strumenti volti all'acquisto aggregato (*recte*: come riportato sul sito istituzionale di Consip «*strumenti e soluzioni di e-procurement per la digitalizzazione degli acquisti di amministrazioni e imprese*» - cfr. https://s.uniupo.it/w9772). Istituita inizialmente nel 1997 come soggetto incaricato di gestire i servizi telematici di quello che, allora, era il Ministero del Tesoro (cfr. d.lgs. n. 414/1997 e decreti del Ministero del Tesoro del 22 dicembre 1997 e del 17 giugno 1998), Consip ha visto con gli anni incrementare le proprie competenze e il proprio ambito di azione, indirizzando progressivamente la propria azione a favore di tutte le Pubbliche Amministrazioni, a partire, nello specifico, dalla legge n. 488/1999 (legge finanziaria per l'anno 2000) e dal Decreto ministeriale del 24 febbraio 2000 del Ministero dell'Economia e delle Finanze. La disciplina che regola l'attività di Consip è frastagliata e disorganica: per una sua esaustiva ricostruzione si rimanda alla pagina del sito istituzionale dedicata https://s.uniupo.it/5ryiw. Anticipando quando sarà ricostruito nel testo, Consip è attualmente la più grande e più importante centrale di committenza italiana ed è qualificata *ex lege* come soggetto aggregatore, vale a dire è una fra quelle centrali di committenza qualificate per procedere all'acquisizione aggregata di forniture e servizi per conto di altre Pubbliche Amministrazioni in relazione a specifiche categorie merceologiche. Per un inquadramento, in particolare riferito ai primi anni di funzionamento di questo organismo, si vedano F.M. Nicosia, *"Modello Consip" tra Stato e mercato (lineamenti e prospettive evolutive)*, in *Riv. it. dir. pubbl. comunit.*, 4, 2022, pp. 711 ss.; E. D'Alterio, *Acquisti delle pubbliche amministrazioni e Consip SPA: luci e ombre*, in *Astrid Rassegna*, 14, 2010.
39. Conformemente a quanto previsto dall'art. 4, co. 3-*quater*, d.l. n. 95/2012 conv. l. n. 135/2012.
40. Sul punto si rimanda al sito istituzionale di Acquisti in rete alla pagina https://s.uniupo.it/bd2h7. È necessario sottolineare che le aree merceologiche raggruppano al loro interno numerose categorie merceologiche, le quali sono periodicamente modificate e integrate. Si consideri, ad esempio, che fino al 2019 la categoria merceologica ivi di interesse erano nominata "Beni e servizi informatici e di connettività".
41. In relazione ai beni e servizi informatici e di connettività si consulti lo schema elaborato da Consip e dal MEF *Strumenti del Programma per la razionalizzazione degli acquisti nella P.A*, agg. Al 07.03.2024, 4, in https://s.uniupo.it/62vni.

42. Cui agli artt. 62 e ss. del d.lgs. n. 36/2023. In argomento, fra i numerosi studi, *ex multis* si rimanda a M.R. Spasiano, *Riflessioni in tema di centralizzazione della committenza negli appalti pubblici*, in *CERIDAP*, 1, 2023, pp. 127 ss.; G.M. Racca, *La Corte di giustizia e le scelte nazionali per una efficiente e trasparente aggregazione dei contratti pubblici: una sfida per l'evoluzione digitale della "funzione appalti" nazionale, regionale e locale*, in *Riv. it. dir. pubbl. comunit.*, 2, 2021, pp. 185 ss.; M. Immordino, A. Zito, *Aggregazione e centralizzazione della domanda pubblica di beni: stato dell'arte e proposte di migliorie al sistema vigente*, in *Nuove autonomie*, 2, 2018, pp. 223 ss.; M.E. Comba, *Aggregazioni di committenza e centrali di committenza: la disciplina europea e il modello italiano*, in *Urb. App.*, 2016, pp. 1053 ss.; B.G. Mattarella, *La centralizzazione delle committenze*, in *Giorn. dir. amm.*, 2016, pp. 613 ss.; G.M. Racca, *Le centrali di committenza nelle nuove strategie di aggregazione dei contratti pubblici*, in *Italiadecide, Rapporto 2015, Semplificare è possibile: come le pubbliche amministrazioni potrebbero fare pace con le imprese*, Bologna, 2015, pp. 489 ss.; W. Gasparri, *L'evoluzione della disciplina per la concentrazione della domanda di beni e servizi nell'amministrazione pubblica*, in D. Sorace (a cura di), *Amministrazione pubblica dei contratti*, Editoriale Scientifica, Napoli, 2013; G.M. Racca, *La professionalità nei contratti pubblici della sanità: centrali di committenza e accordi quadro*, in *Foro amm. CDS*, 7-8, 2010, pp. 1727 ss.; R. Caranta, *Le centrali di committenza*, in M.A. Sandulli, R. De Nictolis, R. Garofoli (a cura di), *Trattato sui contratti pubblici*, Giuffrè, Milano, 2008, pp. 607 ss.; in relazione al tema specifico delle opere pubbliche, invece, S. D'Ancona, *L'accentramento delle funzioni e dei poteri amministrativi: il caso della progettazione delle opere pubbliche*, in *Dir. econ.*, 1, 2020, pp. 1123 ss. Circa la tutela dei lavorati, invece, E. Caruso, *Equo trattamento dei lavoratori nel nuovo Codice dei contratti pubblici tra sostenibilità e risultato amministrativo*, in *Dir. amm.*, 4, 2023, pp. 863 ss. Per uno studio comparato e molto approfondito sulle centrali di committenza, si veda C. Risvig Hamer, M. Socha, K.M. Halonen (Editors), *Public procurement. Centralisation and new trends*, Djøf Publishing, Copenhagen, 2024; C. Risvig Hamer, M.E. Comba (Editors), *Centralising Public Procurement. The Approach of Eu Member States*, Elgar, Cheltenham, 2021, in cui il capitolo relativo al caso italiano è scritto da G.M. Racca, *Central Purchasing Bodies in Italy: Reluctance and Challenges*, pp. 220 ss. Per riflessioni di natura prettamente della scienza economica e di analisi economica del diritto invece si vedano G.L. Albano, M. Sparro, *Flexible Strategies for Centralized Public Procurement*, in *Review of Economics and Institution*, 2010, pp. 1 ss. e G.L. Albano, C. Nicholas, *The Law and Economics of Framework Agreements. Designing Flexible Solutions for Public Procurement*, Cambridge University Press, Cambridge, 2016.
43. Vantaggi fra cui è possibile menzionale l'aumento di competitività dei prezzi a parità di oggetto contrattuale; l'incremento dell'omogeneità delle caratteristiche tecniche dell'oggetto contrattuale; l'innalzamento del livello di professionalità delle stazioni appaltanti, in attuazione del principio di buon andamento amministrativo; nonché la facilitazione dell'attività di controllo sulle procedure di gara e di contrasto alla corruzione. Sulla relazione tra organizzazione e funzionalità M.R. Spasiano, *Il principio di buon*

andamento, in M. Renna e F. Saitta (a cura di), *Studi sui principi del diritto amministrativo*, Giuffrè, Milano 2012, pp. 117 ss.

44. Il sistema di qualificazione delle stazioni appaltanti e delle centrali di committenza, disciplinato dal combinato disposto degli artt. 62 e 63 d.lgs. n. 36/2023, attuati dall'Allegato II.4, assume un ruolo cruciale nel Codice appalti del 2023, in quanto esso risulta essere strumentale alla centralizzazione delle committenze, alla digitalizzazione del ciclo di vita dei contratti pubblici, nonché all'incremento della professionalizzazione del personale che opera nell'ambito degli appalti, come messo in luce da R. Morzenti Pellegrini, *La formazione nel sistema di qualificazione delle stazioni appaltanti: la strategia professionalizzante e il nuovo codice dei contratti pubblici*, in *ambientediritto.it*, 3, 2023, pp. 1 ss. Il sistema di qualificazione, ai sensi dell'art. 63, co. 5, d.lgs. n. 36/2023, ha a oggetto le attività inerenti al processo di acquisizione di forniture, servizi o lavori, e in particolare quelle attinenti alla capacità di progettazione tecnico-amministrativa delle procedure; alla capacità di affidamento e controllo dell'intiera procedura; nonché alla capacità di verifica sull'esecuzione contrattuale, ivi incluso il collaudo e la messa in opera. Il sistema di qualificazione ruota attorno al criterio del valore della procedura da aggiudicare, parametrato alle soglie europee stabilite per l'affidamento diretto di forniture e servizi (pari a 140.000 €) e per l'affidamento di lavori d'importo pari o inferiore a 500.000 €. Al di sotto di queste soglie, tutte le stazioni appaltanti possono procedere in modo diretto e autonomo all'acquisizione di forniture, servizi e lavori. Al di sopra di queste soglie soltanto le stazioni appaltanti qualificate possono procedere con l'acquisizione diretta e autonoma; le stazioni appaltanti non qualificate, invece, sono obbligate a ricorrere agli strumenti di acquisto messi a disposizione dalle stazioni appaltanti qualificate e dalle centrali di committenza qualificate. Il criterio del valore della procedura da aggiudicare permette di distinguere tre livelli differenti di qualificazione: ai sensi dell'art. 63, co. 2, d.lgs. n. 36/2023, vi sono un primo livello (qualificazione base) per servizi e forniture fino alla soglia di 750.000 € e per lavori fino a 1 milione €; un secondo livello (qualificazione intermedia) per servizi e forniture fino a 5 milioni € e per lavori fino alla soglia di rilevanza europea stabilita all'art. 14 del Codice appalti del 2023; infine un terzo livello (qualificazione avanzata) senza limiti di importo. A fronte della rilevanza del tema, l'elenco delle stazioni appaltanti qualificate e delle centrali di committenza qualificate, istituito presso l'ANAC, è pubblico ed è consultabile all'indirizzo https://s.uniupo.it/kkjd8. Ai sensi dell'art. 63, co. 4, d.lgs. n. 36/2023, alcune soggetti espressamente elencati (il Ministero delle infrastrutture e dei trasporti, i Provveditorati interregionali per le opere pubbliche, Consip, Invitalia, Difesa servizi, l'Agenzia del demanio, i soggetti aggregatori, Sport e salute) sono iscritti di diritto in tale elenco. Secondo i dati raccolti da ANAC, a marzo 2024 il numero di stazioni appaltanti che hanno richiesto e ottenuto la qualificazione si è attestato a 4.282: cfr. ANAC, *I dati sulla qualificazione delle stazioni appaltanti e delle centrali di committenza*, report aggiornato al 31.03.2024 (in https://s.uniupo.it/eskov). In argomento M. Nunziata, *Le stazioni appaltanti e il RUP*, in *Giorn. dir. amm.*, 3, 2023, pp. 311 ss.; C. Pinelli, *La qualificazione delle stazioni*

appaltanti nel nuovo codice dei contratti pubblici, in *Riv. trim. appalti*, 3, 2023, pp. 837 ss. In relazione al contesto normativo precedente, invece, P. Lombardi, *La qualificazione delle stazioni appaltanti: spunti di riflessione sul ruolo di ANAC in materia di contratti pubblici*, in *CERIDAP*, 4, 2022, pp. 40 ss.; P. Chirulli, *Qualificazione delle stazioni appaltanti e centralizzazione delle committenze*, in Banca d'Italia – Eurosistema, *Quaderni di Ricerca Giuridica della Consulenza Legale, Qualità ed efficienza nel nuovo codice dei contratti pubblici. Prospettive e questioni aperte*, 83, 2018, pp. 21 ss.

45. Cfr. art. 62, co. 1 e co. 6, d.lgs. n. 36/2023.
46. Cfr. art. 62, co. 2 e co. 5, d.lgs. n. 36/2023.
47. Cfr. art. 62, co. 1 e co. 7, d.lgs. n. 36/2023. Sul punto M.R. Spasiano, *Riflessioni in tema di centralizzazione della committenza negli appalti pubblici*, cit., p. 139. Esse aggiudicano e stipulano accordi quadro e convenzioni favore delle stazioni appaltanti non qualificate, a cui queste ultime possono aderire per aggiudicare i propri contratti specifici.
48. Cfr. art. 63, co. 4, d.lgs. n. 36/2023.
49. Cfr. art. 9, co. 1, d.l. n. 66/2014, conv. l. n. 89/2014. I soggetti aggregatori sono soggetti qualificati per procedere all'acquisizione aggregata di forniture e servizi per conto di altre Pubbliche Amministrazioni in relazione a particolari tipologie di beni rientranti in aree e categorie merceologiche. Per la consultazione delle aree e delle categorie merceologiche si rimanda al sito di Acquisti in rete all'indirizzo https://s.uniupo.it/7rner. Essi sono individuati esplicitamente della Delibera ANAC n. 643 del 22 settembre 2021, secondo la quale i soggetti aggregatori sono: Consip, le diciannove centrali d'acquisto di società regionali, le due centrali per ciascuna delle Province autonome di Trento e Bolzano, le due centrali istituite nella provincia di Vicenza e Brescia e le otto centrali acquisti delle città metropolitane. Per l'elenco completo e dettagliato si rimanda a FARE, Federazione delle Associazioni Regionali degli Economi e Provveditori della Sanità, *Soggetti Aggregatori: arriva il nuovo elenco*, 23 ottobre 2021. *Centrale di committenza* e *soggetti aggregatore* sono dunque due concetti distinti ma fra loro collegati.
50. Si veda la nota 40.
51. Cfr. art. 9 d.l. n. 66/2014, conv. l. n. 89/2014. I contratti pubblici stipulati in violazione di tale norma sono nulli e sono fonte di responsabilità erariale.
52. Si rimanda alla nota 39.
53. Consip pone in essere le proprie attività di centralizzazione impiegando alcuni strumenti di acquisto, le convenzioni e gli accordi quadro, e ricorrendo a strumenti di negoziazione, quali il MEPA (Mercato elettronico della Pubblica Amministrazione, il SDAPA (Sistema dinamico di acquisto della Pubblica Amministrazione) e le gare in ASP (*Application Service Provider*). Basti ivi sottolineare come le convezioni sono una categoria particolare di accordi quadro che Consip stipula per conto del Ministero dell'Economia e delle Finanze ai sensi di quanto già disciplinato dall'art. 26 della legge n. 488/1999. Nelle convenzioni gli operatori economici accettano le condizioni stabilite nel caso di specie in relazione allo specifico bene o servizio (es. oggetto, prezzo, durata), in relazione a cui le amministrazioni aggiudicatrici emettono i propri ordinativi di fornitura. In argomento L. Soccorso, *Il*

regime di adesione alle convezioni-quadro di Consip tra obblighi e facoltà, nell'ambito di un quadro normativo complesso, in *I Contratti dello Stato e degli Enti pubblici*, 2, 2023, pp. 31 ss.; F. Della Marta, *Convenzioni Consip: cosa sono, come funzionano e quando convengono*, in *Agenda Digitale*, 16 luglio 2018. Per approfondimenti mirati, in relazione agli strumenti di negoziazione si vedano A. Contaldo, *La contrattazione telematica e la P.A.*, in *Riv. amm. Rep. Ita.*, 3-4, 2022, pp. 137 ss.; P. Piselli, *Public procurement 4.0: i nuovi strumenti digital al servizio della contrattualistica pubblica*, in *Riv. trim. app.*, 3, 2019, pp. 861 ss.; S. Cresta, *Procedure elettroniche e strumenti di acquisto telematici nel nuovo Codice dei contratti pubblici*, in *Urb. app.*, 8-9, 2016, pp. 981 ss. Con specifico riferimento al MEPA, invece, G. Sorrentino, *Il sistema degli acquisti sul Mepa nella "release" 2022: guida operativa sulle nuove modalità di negoziazione*, in *App. e contr.*, 6, 2022, pp. 57 ss.; A. Massari, G. Sorrentino, *Gli acquisti nei comuni non capoluogo e il ricorso al MEPA*, Maggioli, Santarcangelo di Romagna, 2015; G.L. Albano, *Il Public Procurement come stimolo alle PMI: Il caso del Mercato Elettronico della Pubblica Amministrazione Italiana*, in *Riv. pol. econ.*, VII-IX, 2014.

54. In argomento, a titolo non esaustivo, si vedano G.M. Racca, *La professionalità nei contratti pubblici della sanità: centrali di committenza e accordi quadro*, cit.; R. Caranta, *I contratti pubblici*, Giappichelli, Torino, 2012, pp. 155 ss.; A. Massari, M. Montalti, A.P. Oliveri, *L'accordo quadro negli appalti pubblici*, Maggioli, Santarcangelo di Romagna, 2013; G. Giovannini, V. Lopilato, A. Cianflone (a cura di), *L'appalto di opere pubbliche*, Giuffrè, Milano, 2018, pp. 1196 ss.; S. Vinti, *Gli accordi quadro e i sistemi dinamici di acquisizione*, in A. Cancrini, C. Franchini, S. Vinti (a cura di), *Codice degli appalti pubblici*, Giappichelli, Torino 2014, pp. 370 ss.; F.S. Cantella, *Accordo quadro*, M.A. Sandulli, R. De Nictolis (diretto da), *Trattato sui contratti pubblici*, Vol. III, Giuffrè, Milano, 2019, pp. 147 ss.; E. Morlino, *Centralizzazione degli acquisti pubblici ed enti locali: la prospettiva europea nel caso Asmel*, in *Riv. it. dir. pubbl. comunit.*, 2, 2021, pp. 315 ss.; S. Biancardi, *L'accordo quadro per appalti di servizi e fornitura*, Maggioli, Santarcangelo di Romagna, 2020.
55. Cfr. artt. 33 e 51 Direttiva 2014/24/UE e art. 59 d.lgs. n. 36/2023.
56. La giurisprudenza della Corte di Giustizia dell'Unione Europea ha precisato che negli accordi quadro è necessario identificare le Amministrazioni potenziali beneficiarie dell'accordo quadro (cfr. Corte giust., sentenza 19 dicembre 2018, C–216/17, *Antitrust e Coopservice*, ECLI:EU:C:2018:1034, nonché stabilire la quantità massima stimata della prestazione (in tal senso Corte giust., sentenza 17 giugno 2021, C-23/20, *Simonsen & Weel A/S,* ECLI:EU:C:2021:490.
57. Cfr. art. 59, co. 2, d.lgs. n. 36/2023. Tale interpretazione è confermata altresì dall'ANAC nelle FAQ (*Frequently Asked Questions*) dedicate sull'accordo quadro (in particolare la D4), reperibile sul sito istituzionale dell'Autorità all'indirizzo https://s.uniupo.it/oqpta.
58. Art. 33, co. 1, Direttiva 2014/24/UE.
59. In tal senso sia l'art. 33, co. 2, Direttiva 2024/24/UE sia l'art. 59, co. 2, d.lgs. n. 36/2023.
60. L'accordo quadro ha, pertanto, natura normativa. Sul punto S. Maiorca, voce *Normativo*

(contratto), in *Dig. civ.*, 1995, vol. XII, pp. 169 ss.; G. Gitti, *Contratti regolamentari e normativi*, CEDAM, Padova, 1994, pp. 5 ss.; G. Guglielmetti, voce *Contratto normativo*, in *Enc. giur. Treccani*, 1988, IX, pp. 1 ss.; F. Messineo, voce *Contratto normativo*, in *Enc. dir.*, X, 1962, pp. 121 ss.; L. Barassi, *La teoria generale delle obbligazioni*, II, Giuffrè, Milano, 1948, pp. 134 ss.

61. È necessario sottolineare un aspetto peculiare che caratterizza l'accordo quadro, ribadito in più occasioni dalla giurisprudenza amministrativa. Innanzitutto, in capo alle singole Amministrazioni chiamate a dare esecuzione agli appalti specifici l'obbligo di aderire all'accordo quadro sorge unicamente a fronte della necessità concreta e attuale di soddisfare il particolare fabbisogno (riferito all'oggetto dell'accordo quadro). *Ad contrarium*, in assenza di tale necessità l'obbligo di adesione degrada a facoltà. In tal senso Cons. St., sez. III, sent. n. 1329/2019; T.A.R. Lazio, Roma, sez. I, sent. n. 2864/2021; T.A.R. Campania, Napoli, sez. I, sent. n. 4264/2016. D'altronde, A. Morbidelli, *commento* sub *art. 54*, in F.G. Ferrari, G. Morbidelli (a cura di), *Codice dei contatti pubblici. Il D.L.vo 18 aprile 2016, n. 50 commentato articolo per articolo*, La Tribuna, Piacenza, 2017, p. 344 in relazione all'accordo quadro (disciplinato dal precedente Codice appalti del 2016) ne sottolineò nella pratica la sua caratteristica di "contratto-chiamata".
62. In questa specifica ipotesi i contratti specifici coincideranno con meri ordini di acquisto inviati dalle Amministrazioni aderenti all'accordo quadro.
63. Nell'accordo quadro si è *ridotta la complessità* selezionando alcuni operatori economici ma non si è stabilito a chi affidare gli appalti specifici: in tal caso è necessario selezionare con precisione l'operatore economico tramite un rilancio migliorativo delle condizioni base stabilite nell'accordo quadro: si badi, infatti, che non sono consentite modifiche sostanziali ma unicamente modifiche migliorative.
64. Cfr. art. 59, co. 4, d.lgs. n. 36/2023.
65. Come è stato messo in evidenza dalla dottrina, vi sono *pro* e *contra* in ogni ipotesi: nello specifico, G.M. Racca, S. Ponzio, *La scelta del contraente come funzione pubblica: i modelli organizzativi per l'aggregazione dei contratti pubblici*, cit., p. 63 sottolineano che «*[l]'aggiudicazione di un accordo quadro (chiuso) ad un solo operatore economico assicura prezzi competitivi, riduzione dei costi transattivi, facilità di utilizzo del modello e certezza giuridica. Tuttavia [...] potrebbe evidenziare una scarsa rispondenza ai bisogni delle singole amministrazioni aggiudicatrici o limitare la partecipazione delle piccole medie imprese allorché non si provveda ad una adeguata strutturazione in lotti. Ove tale accordo quadro sia aggiudicato a più operatori, pur in assenza di previsioni normative relative alle modalità di affidamento dei contratti specifici, la disciplina europea richiede la definizione di criteri oggettivi, trasparenti e non discriminatori per l'individuazione della migliore offerta, al fine di evitare violazioni o elusioni dei principi posti a presidio del corretto espletamento delle gare pubbliche nella fase di esecuzione dell'accordo quadro*».
66. Oppure, secondo dottrina, di "flessibilità": cfr. G.L. Albano, M. Sparro, *Flexible Strategies for Centralized Public Procurement*, in *Review of Economics and Institution*, cit.
67. Sul punto si rimanda alla nota 61.

68. Aspetti che comportano altresì vantaggi per la concorrenza del mercato, come sottolineato dalla dottrina internazionale, fra cui A. Sanchez Graells, I. Herrera Anchustegui, *Impact of Public Procurement Aggregation on Competition: Risks, Rational and Justification to the Rules in Directive 2014/24*, in R. Fernandez, P. Valcarcel (a cura di), *Centralización de compras públicas*, Civitas-Thomson Reuters, 2016; C. Risvig Hamer, *Regular purchases and aggregated procurement: the changes in the new Public Procurement Directive regarding framework agreements, dynamic purchasing systems and central purchasing bodies*, in *Public Procurement Law Review*, 2014, pp. 201 ss.
69. Cfr. ad esempio la "Gara a procedura aperta per l'affidamento di un accordo quadro in un unico lotto per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le pubbliche amministrazioni" (c.d. "Gara Sicurezza On Premises"); oppure la "Gara a procedura aperta per la conclusione di un accordo quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni" (c.d. "Gara Servizi Sicurezza da Remoto"). La prima delle due gare recepisce e attua le norme del d.l. n. 77/2021, conv. l. n. 108/2021, finalizzate a permettere alle pubbliche amministrazioni di acquisire beni, servizi e sistemi di cybersicurezza necessari per attuare il Piano nazionale di ripresa e resilienza. La documentazione della prima gara è consultabile sul sito istituzionale di Consip alla pagina https://s.uniupo.it/0rfg6, mentre quella della seconda all'indirizzo https://s.uniupo.it/1anhl. In ogni caso, per un'analisi approfondita di entrambe queste gare, sia consentito il rimando a S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 149 ss.
70. In argomento, oltre a E. Buoso, *Potere amministrativo e sicurezza nazionale cibernetica*, cit., e a S. Mele, *Il Perimetro di sicurezza nazionale cibernetica e il nuovo "golden power"*, in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, cit., si vedano S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in *MediaLaws*, 2, 2023, pp. 398 ss.; F. Serini, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in *Riv. it. inform. e dir.*, 2, 2023, pp. 41 ss.; L. Calandriello, *Il perimetro di sicurezza nazionale cibernetica*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, cit., pp. 139 ss.; F. Carchidi, *Perimetro di sicurezza nazionale cibernetica, dal d.l. 105/2019 ai d.p.c.m. n. 131/2020 e n. 81/2021: la sublimazione delle cc.dd.* information and communication technologies, in *ambientediritto.it*, 3, 2021, pp. 295 ss.; L. Fiorentino, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea, L. Fiorentino (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Editoriale Scientifica, Napoli, 2020, pp. 39 ss.
71. Precisamente con d.l. n. 105/2019 n. 105, conv. l. n. 133/2019.
72. Sul punto, per approfondimenti, C. Chiari, A. Mazzetti, *Cybersicurezza, le norme in vigore e in arrivo per i soggetti inclusi nel perimetro di sicurezza nazionale*, in *Agenda digitale*, 1°

marzo 2023.

73. Cfr. art. 1, co. 1, e art. 1, co. 2, lett. a), d.l. n. 105/2019, conv. l. n. 133/2019.
74. Si veda il DPCM n. 131/2020. Fra tali settori rientrano, ad esempio, 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.
75. Cfr. art. 1, co. 2-*ter*, d.l. n. 105/2019, conv. l. n. 133/2019.
76. Cfr. art. 1, co. 6, lett. a), d.l. n. 105/2019, conv. l. n. 133/2019.
77. O in specifiche ipotesi al Centro di valutazione del Ministero dell'interno e di quello del Ministero della difesa. Il CVCN svolge la funzione di valutazione della sicurezza di forniture, sistemi e servizi tecnologici destinati a essere impiegati nel Perimetro, conformemente alla disciplina regolamentare. In argomento si veda V. Balocco, *Cybersicurezza, operativo il Centro di valutazione e certificazione*, in *corrierecomunicazioni.it*, 1° luglio 2022.
78. Tale comunicazione deve essere affiancata dalla valutazione del rischio associato al particolare oggetto della fornitura.
79. Cfr. art. 1, co. 7, d.l. n. 105/2019, conv. l. n. 133/2019.
80. In argomento si veda il DPCM 18 maggio 2022, n. 92.
81. Potendo il CVCN eseguire verifiche tecniche preliminari, test su *hardware* e su *software*, oltre a imporre specifiche condizioni di impiego al committente.
82. Si badi che il CVCN può imporre, nella documentazione di gara, l'inserimento di clausole che condizionano sospensivamente o risolutamente il contratto pubblico alla conformità delle prescrizioni del CVCN nonché all'esito positivo dei testi di sicurezza informatica su *hardware* e *software*. Cfr. art. 1, co. 6, lett. a) quinto periodo d.l. n. 105/2019, conv. l. n. 133/2019.
83. Agenzia che, ai sensi dell'art. 5, co. 2, d.l. n. 82/2021, conv. l. n. 109/2021, gode di autonomia regolamentare, amministrativa, organizzativa, patrimoniale, finanziaria e contabile.
84. Disciplina prevista dall'art. 11, co. 4, d.l. n. 82/2021, conv. l. n. 109/2021 e demandata, a livello regolamentare, al DPCM del 1° settembre 2022, n. 166 rubricato "Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico". In argomento si veda il documento *Cybersicurezza: disciplinate le procedure per la stipula di contratti di appalti di lavori, servizi e forniture*, cura della Redazione Ipsoa, in *Ipsoa*, 4 novembre 2022.
85. Cfr. artt. 2, co. 1, e 23, co. 4, DPCM n. 166/2022. La disciplina speciale in questione è altresì distinta da quella dettata in relazione ai contratti secretati cui all'art. 139 d.lgs. n. 36/2023.
86. Cfr. art. 3, co. 2, DPCM n. 166/2022.
87. Cfr. art. 21, co. 2, DPCM n. 166/2022.
88. Circostanza che consente sia l'esecuzione delle prestazioni in via d'urgenza, sia la modifica dei contratti d'appalto durante il fisiologico periodo di efficacia: cfr. artt. 17 e 19 DPCM

n. 166/2022.

89. Cfr. art. 7, co. 2, DPCM n. 166/2022.
90. Cfr. art. 8 DPCM n. 166/2022. Si noti come tali requisiti vengono verificati autonomamente dall'Agenzia per la Cybersicurezza Nazionale.
91. Cfr. art. 9 DPCM n. 166/2022, riservandosi l'Agenzia il diritto di recesso di azione di risarcimento. Ai sensi del capoverso di questa norma, ACN ha, tuttavia, facoltà di non recedere dal contratto: «*a) quando, valutate le circostanze del caso, dal venir meno della prestazione possa comunque derivare un grave pregiudizio per la sicurezza nazionale cibernetica; b) quando la perdita dei requisiti attiene ai dipendenti, o comunque a coloro che per conto dell'operatore economico eseguono la prestazione, e gli stessi sono tempestivamente sostituiti senza pregiudizio per l'esecuzione dell'appalto*».
92. Cfr. art. 13 DPCM n. 166/2022. La disciplina ammette, a determinate condizioni, il raggruppamento temporaneo di imprese e il subappalto.
93. L'accordo quadro è ricompreso fra le procedure di scelta del contraente di ACN pur essendo, come già si è avuto modo di argomentare, uno strumento contrattuale e non una procedura di aggiudicazione.
94. Cfr. art. 14 DPCM n. 166/2022.
95. Cfr. art. 15 DPCM n. 166/2022.
96. La procedura negoziata senza previa gara informale è prevista unicamente in casi tassativi.
97. Cfr. art. 16 DPCM n. 166/2022.
98. Cfr. art. 13, co. 1, lett. c), DPCM n. 166/2022.
99. Cfr. art. 13, co. 2, DPCM n. 166/2022.
100. Analizzata nel paragrafo 4 del presente scritto.
101. Programmaticità che D. Gambetta, *Digitalizzazione (artt. 19-36)*, in V. Fanti, *Corso sui contratti pubblici riformati da d.lgs. 31 marzo 2023, n. 36*, cit., p. 104 sottolinea in relazione all'attribuzione della perifrasi di "norma manifesto" all'art. 19 del Codice appalti in riferimento alla digitalizzazione del ciclo di vita dei contratti pubblici.
102. Programmaticità che emerge altresì dalla circostanza per cui tale norma impone alle Amministrazioni aggiudicatrici e agli operatori economici di adottare misure tecniche e organizzative a presidio della sicurezza informatica senza, però, prescrivere in cosa si sostanzino tali misure sul piano tecnico.
103. Il testo del d.d.l. 16 febbraio 2024 A.C. 1717 è consultabile sul sito istituzionale della Camera dei Deputati in https://s.uniupo.it/2vlsz. In argomento si veda E. Longo, *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in *Riv. it. inform. e dir.*, 1, 2024, pp. 1 ss.
104. Ai sensi dell'art. 10, co. 1, d.d.l. 16 febbraio 2024 A.C. 1717, con tale perifrasi si deve intendere «*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* [degli interessi nazionali strategici]».

105. Il d.d.l. 10 febbraio 2014 A.C. 1717 stabilisce che entro 120 dall'entrata in vigore del provvedimento che tradurrà in legge il d.d.l. *de quo* dovrà essere adottato un DCPM (su proposta di ACN e previo parere del Comitato interministeriale per la cybersicurezza) contenente l'individuazione degli elementi essenziali di cybersicurezza che dovranno essere tenuti in considerazione in relazione alle attività di approvvigionamento di forniture e servizi ICT impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.
106. In argomento *ex multis* S. Perongini, *Il principio del risultato e il principio di concorrenza nello schema definitivo del codice dei contratti pubblici*, in G. Corso, M. Immordino (a cura di), *Scritti in onore di Filippo Salvia*, Editoriale Scientifica, Napoli, 2023, pp. 517 ss.; M.R. Spasiano, *Codificazione di principi e rilevanza del risultato*, in C. Contessa, P. Del Vecchio (a cura di), *Codice dei contratti pubblici*, Editoriale Scientifica, Napoli, 2023, pp. 49 ss.; F. Cintioli, *Il principio del risultato nel nuovo codice dei contratti pubblici*, in *giustiziaamministrativa.it*, 2023; A.M. Chiariello, *Una nuova cornice dei principi per i contratti pubblici*, in *Dir. econ.* 1, 2023; D. Capotorto, *I rischi di derive autoritarie nell'interpretazione del principio del risultato e l'indissolubilità del matrimonio tra buon andamento e imparzialità dell'amministrazione*, in *federalismi.it*, 14, 2023, pp. 47 ss. Invece, in relazione all'amministrazione di risultato, si veda M.R. Spasiano, *Nuove riflessioni in tema di amministrazione di risultato*, in AA.VV., *Studi per Franco Gaetano Scoca*, V, Editoriale Scientifica, Napoli, 2020, pp. 4845 ss.; L. Torchia, *L'efficienza della pubblica amministrazione fra ipertrofia legislativa e atrofia dei risultati*, Varenna 20 -22 settembre 2018, in *www.osservatorioar.it*, 2019; A. Romano Tassone, *Amministrazione di risultato e provvedimento amministrativo*, in M. Immordino, A. Police (a cura di), *Principio di legalità e amministrazione di risultati. Atti del Convegno Palermo, 27-28 febbraio 2003*, Giappichelli, Torino 2004; L. Iannotta, *La considerazione del risultato nel giudizio amministrativo: dall'interesse legittimo al buon diritto*, in *Dir. proc. amm.*, 2, 1998, pp. 299 ss.;
107. Sulla relazione fra discrezionalità e principio di risultato si veda M.R. Spasiano, *Dall'amministrazione di risultato al principio di risultato del Codice dei contratti pubblici: una storia da scrivere*, in *federalismi.it*, 9, 2024, pp. 222 ss.
108. Art. 1, co. 1, d.lgs. n. 36/2023 (enfasi aggiunta).
109. Secondo la nota espressione di E. Casetta, *La difficoltà di "semplificare"*, in *Dir. amm.*, 3-4, 1998, p. 344.
110. R. Ferrara, *Il procedimento amministrativo visto dal terzo*, in *Dir. proc. amm.*, 4, 2003, p. 1055.
111. Si consideri, infatti, che ai sensi dell'art. 10, co. 2, d.d.l. 16 febbraio 2024 A.C. 1717, gli elementi essenziali di cybersicurezza sono tenuti in considerazione nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione sulla base dell'applicazione del criterio dell'offerta economicamente più vantaggiosa. Di pari, però, gli elementi essenziali di cybersicurezza divengono requisiti minimi dell'offerta nell'ipotesi di valutazione dell'offerta sulla base del criterio minor prezzo.

112. Come del resto espressamente previsto dall'art. 19, co. 5, d.lgs. n. 36/2023.
113. Cfr. V. Bachelet, *Profili giuridici della organizzazione amministrativa. Strutture tradizionali e tendenze nuove*, Giuffrè, Milano, 1965, p. 3, il quale sottolinea come «*la disciplina giuridica dell'organizzazione della pubblica amministrazione, oltre a stabilirne la struttura con criteri di funzionalità, vuole anche costituire un sistema di garanzia della legittimità e opportunità obiettiva dell'azione e dei procedimenti dell'amministrazione pubblica*».
114. In relazione alla necessità della formazione dei dipendenti pubblici già S. Cassese, *A che serve la formazione dei dipendenti pubblici?*, in *Pol. dir.*, 1989, pp. 432 ss.
115. Interpretazione che 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. Criticità simili, del resto, erano già state evidenziate da A. Monti, *L'impatto del nuovo Codice degli appalti sulla cybersecurity della Pa*, in *formiche.net*, 13 aprile 2023.
116. Per approfondimenti si rimanda al report di ISTAT, *Società: Cittadini e competenze digitali*, 22 giugno 2023, pp. 3 ss., in https://s.uniupo.it/v30m0. Sul punto sia consentito il rimando a S. Rossa, *Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario*, cit., pp. 172 ss.
117. Cfr. in argomento M. Iaselli, *Competenze digitali nella PA: i problemi da risolvere per avere servizi di qualità*, in *Agenda digitale*, 14 marzo 2022.
118. Cfr. il *Digital Education Action Plan 2021-2027* elaborato dalla Commissione europea; ma anche, a livello nazionale la *Strategia Nazionale per le Competenze Digitali – Piano operativo 2023-2026* elaborato dal Dipartimento per la trasformazione digitale e da Repubblica Digitale, 2023, in https://s.uniupo.it/7bojw, nonché la *Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025* elaborato dal Ministero per l'Innovazione Tecnologica e la Digitalizzazione nel 2021.
119. Cfr. LXVII Governo Italiano, *Piano Nazionale di Ripresa e Resilienza*, Roma, 2021, in https://s.uniupo.it/5yl85. In argomento E. Cavasino, *Il Piano Nazionale di Ripresa e*

Resilienza e le sue fonti, Editoriale Scientifica, Napoli, 2022.

120. Traduzione di chi scrive. Cfr. Jean-Pierre Claris de Florian, *Fables de Florian*, in *Œuvres de Florian*, Briand, Parigi, 1811, Livre IV, Fable XII, p. 137: «*Une jeune guenon cueillit / Une noix dans sa coque verte; / Elle y porte la dent, fait la grimace... ah ! Certe, / Dit-elle, ma mère mentit / Quand elle m'assura que les noix étaient bonnes. / Puis, croyez aux discours de ces vieilles personnes / Qui trompent la jeunesse! / Au diable soit le fruit! / Elle jette la noix. Un singe la ramasse, / Vite entre deux cailloux la casse, / L'épluche, la mange, et lui dit: / Votre mère eut raison, ma mie, / Les noix ont fort bon goût, mais il faut les ouvrir. / Souvenez-vous que, dans la vie, / Sans un peu de travail on n'a point de plaisir*».