Corso Tozzi Martelli

La Cybersicurezza alla prova del Codice dei contratti pubblici (D.lgs. n. 36 del 2023): sfide e opportunità

Abstract: Il presente articolo, dedicato alla cybersecurity nell'ambito del nuovo Codice degli appalti pubblici (D.Lgs. n. 36/2023), intende sottolineare il ruolo cruciale dell'organizzazione amministrativa nella tutela dei diritti e degli interessi. Lo scritto esamina come le disposizioni del Codice, nonostante la loro natura programmatica, rappresentino un'opportunità significativa per rafforzare la protezione dei dati personali e la cybersecurity nel contesto degli appalti pubblici. Per garantire la loro piena efficacia, tuttavia, l'elaborato evidenzia la necessità di integrare queste disposizioni con regolamenti dettagliati e operativi. L'obiettivo è promuovere un approccio olistico alla digitalizzazione, che affronti non solo gli aspetti tecnologici ma anche quelli organizzativi, giuridici e culturali.

Keywords: Pubblica Amministrazione, Organizzazione amministrativa, Digitalizzazione, Cybersicurezza, Appalti pubblici, Codice dei contratti pubblici.

1. Premessa: l'aumento della minaccia *cyber* per l'Amministrazione digitale

In un mondo sempre più digitalizzato, siamo costantemente esposti a un numero crescente di attacchi informatici. Ogni giorno riceviamo numerosi messaggi, email e chiamate che nascondono tentativi di *phishing*, progettati per ingannarci e ottenere informazioni sensibili o accesso non autorizzato ai nostri sistemi informatici.

Quello che desta particolare preoccupazione è tuttavia che questi attacchi sono sempre più indirizzati verso soggetti pubblici[1].

1 V. il Rapporto Clusit 2024 sulla sicurezza ICT in Italia, reperibile al link: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2024_web.pdf, che indica: "Il settore pubblico è stato interessato da un importante aumento del numero degli attacchi fra il 2022 e il 2023.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760155

In tal senso, la Relazione annuale sulla politica dell'informazione per la sicurezza[2], presentata dal Sistema di Informazione per la Sicurezza della Repubblica al Parlamento nel febbraio 2024, evidenzia un "costante interesse degli attori della minaccia [cyber], crescente nei confronti delle infrastrutture digitali di soggetti pubblici, con particolare attenzione verso quelle riferibili alle Amministrazioni Centrali dello Stato e agli Istituti e Agenzie nazionali"[3].

Questa tendenza è ulteriormente confermata dal Rapporto Clusit 2024 dell'Associazione Italiana per la Sicurezza Informatica, che rivela come il 41% degli attacchi informatici "gravi" registrati nel 2023 abbia preso di mira le Pubbliche Amministrazioni[4].

Tale scenario dimostra chiaramente come, nell'attuale fase di trasformazione digitale della Pubblica Amministrazione[5], la cybersicurezza[6] – intesa come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[7] – diventi un requisito imprescindibile per garantire la tutela dei diritti e degli interessi, nonché per mantenere l'operatività dell'Amministrazione.

In effetti, come evidenziato in dottrina, "Una Pubblica Amministrazione che oggi ritenga di non poter essere soggetta ad attacchi di sicurezza, è un'organizzazione senza consapevolezza del livello di digitalizzazione della propria attività istituzionale"[8].

In tale prospettiva, il presente contributo si propone di indagare in che termini il Codice dei contratti pubblici disciplini il tema della cybersicurezza, evidenziando l'importanza dell'aspetto organizzativo delle Pubbliche Amministrazioni per affrontare efficacemente le sfide ad essa connesse.

Tra il 2019 e il 2023 il campione ha incluso 1.149 attacchi noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Globalmente la crescita è all'incirca lineare, con un forte incremento fra il 2022 e il 2023. Nell'arco dei cinque anni si è comunque passati dai 187 attacchi del 2019 ai 282 del 2023, con un incremento complessivo del 50%".

2 Relazione annuale 2023 sulla politica dell'informazione per la sicurezza, reperibile al link: https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true.

3 *Ivi*, p. 84.

4 V. il Rapporto Clusit 2024 sulla sicurezza ICT in Italia, pp. 98 e ss.

5 Sulla digitalizzazione della Pubblica Amministrazione, cfr. *ex multis*: Cavallo Perin e Galetta (a cura di) 2020; Cavallo Perin 2020; Cavallo Perin (a cura di) 2021; Galetta 2022; Galetta 2023; Galetta 2023; Auby, De Minico e G. Orsoni (a cura di) 2023; Torchia 2023.

6 Sulla cybersicurezza, cfr: Montessoro 2019; Bruno 2020; Brighi e Chiara 2021; Renzi 2021; Macrì 2021; Previti 2022; Serini 2022; Ursi 2023; Buoso 2023; Rossa 2023a; Rossa 2023b; Rossa 2024a; Moroni 2024.

7 Art. 2, (1), del Regolamento UE 2019/881 (c.d. *Cybersecurity Act*). Mentre, a livello nazionale, l'art. 1, comma 1, lett. *a*), del d.l. 14 giugno 2021, n. 82, convertito dalla l. n. 109/2021, definisce la "cybersicurezza" come "l'insieme delle attività (…) necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico".

8 V. Macrì 2021: 1196.

2. La protezione dei dati personali e la sicurezza informatica quali principi fondamentali della digitalizzazione degli appalti pubblici

Come noto, una delle principali novità introdotte dal decreto legislativo 31 marzo 2023, n. 36, c.d. Codice dei contratti pubblici[9] (d'ora in poi anche solo "Codice") riguarda la digitalizzazione e l'informatizzazione delle procedure di gara[10], cui è interamente dedicata la Parte II del Libro I (artt. 19-36)[11].

In particolare, il Codice prevede la piena digitalizzazione dell'intero "ciclo di vita" dei contratti pubblici, inteso come l'insieme di tutte le attività che si susseguono dalla programmazione alla definizione del fabbisogno, fino all'esecuzione del contratto[12]. Tuttavia, questa ambiziosa digitalizzazione (*end-to-end*) comporta l'esposizione di ogni fase del processo di approvvigionamento e di ogni dato trattato al rischio di *cyber* attacchi e/o incidenti informatici[13].

Per mitigare tale rischio, il legislatore ha deciso di introdurre specifiche disposizioni in materia di cybersicurezza. Si tratta di una novità 'assoluta', in quanto il precedente Codice (d.lgs. 18 aprile 2016, n. 50) ignorava, *tout court*, tale aspetto[14].

La cybersicurezza viene affrontata sotto un duplice profilo: da un lato, come requisito fondamentale che dovrà essere garantito durante l'intero processo di digitalizzazione delle procedure di gara, impattando l'organizzazione della Pubblica Amministrazione (art. 19, commi 1 e 5); dall'altro, quale elemento da tenere in considerazione nella valutazione della componente tecnica delle offerte nelle gare volte all'acquisto di beni e servizi informatici (art. 108, comma 4)[15], che a loro volta

9 Per alcuni commenti relativi alle norme del Codice dei contratti pubblici, cfr. *ex multis*: Cartei e Iaria 2023; Caringella 2023; Corradino 2023; Dall'Acqua, Meola e Purcaro 2023; Fanti 2023; Giovagnoli e Rovelli 2024; Botto e Castrovinci Zenna 2024; Villata e Ramajoli 2024; Ursi 2024; Tropea 2024.

10 Sul punto, è opportuno ricordare come la digitalizzazione del settore pubblico rappresenti uno degli obiettivi chiave del Piano Nazionale di Ripresa e Resilienza (PNNR), Missione 1, che, con riferimento alle procedure di gara, mira a "definire le modalità per digitalizzare le procedure per tutti gli appalti pubblici e concessioni e definire i requisiti di interoperabilità e interconnettività" (M1C1-70), nonché a realizzare un Sistema Nazionale di e-procurement "interoperabile con i sistemi gestionali delle pubbliche amministrazioni" (M1C1-75). V. link: https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/Dipartimenti/USG/Misure_attuazione_PNRR_20231231.pdf.

11 Sulla digitalizzazione dei contratti pubblici, cfr. *ex multis*: Cavallo Perin e Lipari, Racca (a cura di) 2022; Racca 2022; Guarnaccia 2022; Gambetta 2023; Corrado 2023; Galetta 2023; Carullo 2023; Forte e Pica 2023; Carlotti: 2023; Bruno 2024; Vesperini: 2024; Mancini Palamoni 2024.

12 V. l'art. 21 del d.lgs. n. 36/2023; nonché l'art. 3, co. 1, lett. p), dell'Allegato I.1 del Codice.

13 V. Rossa 2024a: par. 5.

14 Del resto, anche le Direttive 2014/23-24-25/UE in materia di appalti e concessioni non prevedono né una disciplina generale sugli appalti di *cybersecurity* né disposizioni generali o particolari in merito, rimettendo quindi la relativa previsione alla discrezionalità dei legislatori nazionali. Reperibili al link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L:2014:094:FULL.

15 L'articolo 108, comma 4, del Codice stabilisce che "(…) Nelle attività di approvvigionamento di beni e servizi informatici per la pubblica amministrazione, le stazioni appaltanti,

potranno essere utilizzati per digitalizzare (ulteriormente) l'Amministrazione e la sua attività[16].

Volendo concentrare l'attenzione al profilo organizzativo, l'analisi che segue si focalizza sull'articolo 19 del Codice dei contratti pubblici. In particolare, tale articolo, al comma 1, prevede che:

> Le stazioni appaltanti e gli enti concedenti assicurano la digitalizzazione del ciclo di vita dei contratti nel rispetto dei principi e delle disposizioni del Codice dell'Amministrazione Digitale […], garantiscono l'esercizio dei diritti di cittadinanza digitale e operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica.

Al riguardo, si può rilevare come il legislatore, consapevole delle complessità e delle criticità del processo di digitalizzazione, abbia voluto tracciare la direzione degli sviluppi futuri. Infatti, con la norma in commento, non si è limitato a fissare l'obiettivo della "digitalizzazione dell'intero ciclo di vita dei contratti", ma ha stabilito anche quei principi fondamentali che dovranno guidare ed essere garantiti in tale processo[17].

Tra questi principi, spiccano – per quanto qui interessa – quelli di protezione dei dati personali e di sicurezza informatica. Il collegamento tra questi due principi suggerisce un'interpretazione del concetto di "sicurezza informatica" nella sua accezione di "cybersicurezza"[18], ovverosia un sistema di sicurezza in grado di garan-

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".

16 Si pensi, in particolare, alle "gare strategiche per la trasformazione digitale", che, secondo quanto indicato nelle Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026 di AGID (reperibile al link: https://www.agid.gov.it/sites/agid/files/2024-05/piano_triennale_per_linformatica_nella_pa_2024-2026_0.pdf), sono "strumenti che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione digitale della Pubblica Amministrazione" (pp. 38 ss.). Sul punto, si veda anche il Portale informatico Consip Gare Strategiche, al link: https://www.consip.it/attivit/gare-strategiche.

17 Oltre ai principi elencati già al primo comma dell'art. 19, occorre fare riferimento anche ai principi: del "*once only*" (art. 19, comma 2); del "digital by default" (art. 19, comma 3); della "interoperability by default" (art. 19, comma 4); del riuso delle informazioni e di accessibilità e fruibilità dei dati in formato aperto (art. 19, comma 4); di accessibilità e di conoscibilità (art. 19, commi 6 e 7).

18 Si osserva infatti in dottrina come i due termini, di regola, non siano coincidenti o sovrapponibili. Sul punto v. Rossa 2024a, nota n. 21, afferma che "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

tire non solo la protezione dei sistemi informativi e delle infrastrutture, ma anche un'adeguata tutela dei dati personali[19].

In proposito, è bene sottolineare – come evidenziato dal Consiglio di Stato nella Relazione sullo Schema definitivo di Codice dei contratti pubblici – che "tutte le iniziative dovrebbero andare oltre il semplice rispetto del quadro giuridico in materia di protezione dei dati personali e privacy e sicurezza informatica, integrando tali elementi nella fase di progettazione" [20] (o, in inglese, *by design*).

In effetti, la digitalizzazione – come sottolineato nella Relazione –, pur accrescendo l'efficacia e l'efficienza dei processi, "non può implicare un arretramento delle garanzie [di sicurezza informatica] e dei diritti [di protezione dei dati personali e privacy] degli operatori economici né dei doveri che gravano sulle amministrazioni"[21].

3. Il ruolo dell'organizzazione e la formazione continua del personale nel prevenire e gestire gli attacchi *cyber*

Nella prospettiva sopra delineata, il comma 5 dell'articolo 19 assume particolare rilevanza, poiché impone alle stazioni appaltanti, agli enti concedenti e agli operatori economici che partecipano alle attività e ai procedimenti connessi al ciclo vita dei contratti, indipendentemente dal loro settore di attività, l'obbligo di adottare misure tecniche e *organizzative* volte a garantire la sicurezza informatica e la protezione dei dati personali.

Questa disposizione, che si rivolge a tutti i soggetti coinvolti nelle procedure di aggiudicazione, evidenzia il ruolo cruciale dell'organizzazione nella prevenzione e gestione delle minacce informatiche.

È fondamentale, dunque, che tale obbligo non sia inteso come un mero adempimento burocratico, ma piuttosto come un elemento chiave per la costruzione di un sistema di sicurezza di cybersicurezza resiliente, capace di adattarsi alle sfide poste dall'evoluzione delle minacce digitali.

Una gestione efficace dei processi (organizzativi) consente, infatti, di identificare tempestivamente le criticità, implementare soluzioni in via preventiva e reagire prontamente agli incidenti. In altri termini, l'obbligo di adottare "misure tecniche e organizzative" non rappresenta tanto un obbligo formale, quanto un requisito

digitali di organizzazioni complesse, grazie alla predisposizione di misure tecniche idonee a tutelare diritti e libertà fondamentali".

19 In effetti, sebbene la sicurezza informatica e la protezione dei dati personali non siano concetti coincidenti, essi risultano strettamente connessi, come avviene quando una violazione di sicurezza comporta anche una violazione dei dati personali (c.d. "*data breach*").

20 Consiglio di Stato, *Schema definitivo di Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante "Delega al Governo in materia di contratti pubblici". III – Relazione agli articoli e agli allegati*, Roma, 7 dicembre 2022, reperibile al link: https://www.giustizia-amministrativa.it/documents/20142/17550825/3_CODICE+CONTRATTI+RELAZIONE.pdf/d3223534-d548-1fdc-4be4-e9632c641eb8?t=1670936691000.

21 *Ivi*, 40.

sostanziale per proteggere l'integrità dei dati e la continuità operativa delle Pubbliche Amministrazioni.

Un aspetto centrale per una gestione efficace della sicurezza informatica è poi la formazione continua del personale, come espressamente previsto dal comma 5 dell'articolo in esame[22].

Considerando che il panorama delle minacce *cyber* evolve rapidamente, con attacchi sempre più sofisticati, è infatti necessario che il personale sia costantemente aggiornato. Affidarsi esclusivamente a soluzioni tecniche, senza investire nel capitale umano, non può che limitare significativamente l'efficacia delle misure di sicurezza.

Del resto, la formazione e l'aggiornamento costante sono fondamentali per sviluppare una consapevolezza in materia di sicurezza informatica (cosiddetta *cybersecurity awareness*). È infatti da tale consapevolezza che possono derivare le azioni organizzative necessarie a mitigare i rischi relativi alla sicurezza informatica[23].

Investire nella formazione, pertanto, non significa solo elevare il livello delle competenze digitali dei singoli individui, ma anche rafforzare l'intero sistema di difesa contro le minacce informatiche, rendendo ciascun membro di un'organizzazione complessa un attore attivo nella protezione delle risorse informative[24].

L'articolo 19, comma 5, del Codice dei contratti pubblici evidenzia, in sintesi, come la cybersicurezza sia intrinsecamente legata all'organizzazione amministrativa[25] e come l'adozione di misure organizzative adeguate, tra cui la formazione continua del personale addetto, rappresenti un pilastro fondamentale per la sicurezza informatica.

4. Sfide normative: l'articolo 19 del Codice dei contratti pubblici come "norma manifesto" e la necessità di integrazione

Dall'analisi svolta emerge che le disposizioni in materia di cybersicurezza presenti nel Codice dei contratti pubblici rappresentano un significativo passo in avanti nella regolazione della sicurezza informatica all'interno del settore pubblico.

22 A tal fine, l'art. 19, comma 5, precisa che "Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento".

23 Cfr. il Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022, in https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/capitolo_6_sicurezza_informatica.html.

24 Per altro verso, come evidenziato da Rossa 2023a: 219 ss.: "Lo sviluppo delle competenze richieste dalla cybersicurezza pubblica appare necessario, soprattutto all'interno della Pubblica Amministrazione, in particolare nell'ambito degli appalti di tecnologia – come del resto espressamente previsto dal nuovo Codice appalti. E questo per una ragione chiara. Essendovi l'esigenza di instaurare una relazione collaborativa fra i soggetti pubblici e quelli privati, che riequilibri la situazione di disparità che normalmente avvantaggia gli operatori economici e che perciò sia funzionale sul piano concreto, è imprescindibile che i soggetti pubblici siano realmente in grado di possedere le medesime conoscenze dei privati".

25 Sul punto, cfr. Rossa 2023b: 162, afferma che "l'attività organizzativa si pone come fondamento logico del concetto stesso di cybersicurezza".

Tuttavia, tali norme presentano una natura programmatica, configurandosi più come 'norme manifesto'[26] piuttosto che come 'istruzioni operative-pratiche' per la gestione concreta della cybersicurezza da parte delle Pubbliche Amministrazioni[27].

Per esempio, l'articolo 19 sancisce l'obbligo di formare e aggiornare costantemente il personale, ma non ne stabilisce né le modalità né i contenuti minimi, lasciando alle singole amministrazioni l'onere di definire i propri percorsi formativi, in base al principio di auto-organizzazione.

Questo approccio, sebbene flessibile, comporta il rischio di creare livelli di sicurezza disomogenei e talvolta inadeguati, con possibili conseguenze negative sull'efficacia complessiva della protezione cibernetica a livello nazionale.

Infatti, pur stabilendo importanti obiettivi e principi, le disposizioni contenute nel Codice non forniscono indicazioni sufficientemente dettagliate per consentire alle Amministrazioni di tradurre in azioni concrete i principi fissati.

L'assenza di regole chiare e di istruzioni precise può portare a strategie di sicurezza informatica frammentate e non coordinate, compromettendo così la capacità di risposta del settore pubblico alle minacce informatiche.

Di conseguenza, per superare tali criticità e rendere le disposizioni del Codice realmente efficaci, diventa necessario integrarle con normative che offrano un approccio più operativo, come, ad esempio, il Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) ovvero la legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"[28].

In proposito, l'articolo 8 della l. n. 90/2024 prevede che le amministrazioni di maggiori dimensioni – come Regioni, Province autonome di Trento e Bolzano, città metropolitane, comuni con più di 100.000 abitanti (inclusi i capoluoghi di regione), società di trasporto pubblico urbano con bacini d'utenza superiori a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nelle città metropolitane e aziende sanitarie locali – devono individuare una struttura, anche tra quelle già esistenti, dedicata alla cybersicurezza. Questa struttura avrà il compito di sviluppare politiche e procedure di sicurezza, implementare sistemi di analisi e gestione del rischio informatico, definire ruoli e organizzazione per la sicurezza, redigere un piano programmatico per la protezione di dati e infrastrutture, potenziare la capacità di gestione del rischio, adottare le misure previste dalle linee guida dell'Agenzia per la cybersicurezza nazionale, e monitorare costantemente le minacce e le vulnerabilità per mantenere aggiornati i sistemi di sicurezza.

All'interno di tale struttura, è inoltre prevista l'istituzione di un referente per la cybersicurezza, selezionato in base a specifiche e comprovate professionalità e competenze nel settore[29].

26 V. Gambetta 2023: 104.

27 Cfr. Rossa 2024a: parr. 3 e 5.

28 Per un commento al Disegno di Legge n. 1717 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") si rinvia a Rossa 2024b.

29 V. art. 8, comma 2, della legge n. 90/2024.

Tuttavia, un limite significativo all'attuazione delle misure di sicurezza informatica è rappresentato dall'obbligo di utilizzare esclusivamente le risorse umane, strumentali e finanziarie disponibili a legislazione vigente[30]. Questo vincolo rischia di compromettere la capacità delle Amministrazioni di implementare efficacemente tali misure, specialmente laddove le risorse siano scarse.

Alla luce di ciò, appare chiaro che un cambiamento culturale orientato alla promozione della *cybersecurity awareness* diventa ancor più imprescindibile. In un contesto caratterizzato da risorse limitate, investire nella sensibilizzazione e nella formazione del personale può rappresentare una soluzione 'sostenibile' per innalzare il livello di sicurezza informatica delle Amministrazioni. La consapevolezza dei rischi e delle *best practice*, infatti, deve diventare parte integrante dell'operatività quotidiana.

Inoltre, la natura programmatica dell'articolo 19 del Codice, unitamente alla necessità di promuovere una cultura della cybersicurezza, evidenzia l'importanza di un impegno concreto nella formazione e nella diffusione di conoscenze specifiche. Senza tale impegno, le disposizioni rischiano di rimanere inapplicate, impedendo così il raggiungimento degli obiettivi prefissati.

Pertanto, investire nella cultura della sicurezza informatica, prevedendo specifici ruoli e responsabilità all'interno delle Amministrazioni, non solo supporta l'attuazione pratica delle disposizioni esaminate, ma contribuisce a creare un ambiente più resiliente alle minacce cibernetiche, stimolando al contempo la domanda di soluzioni innovative e di competenze digitali e aprendo così nuove prospettive di crescita per l'intero comparto della cybersicurezza.

5. Riflessioni conclusive: la digitalizzazione dell'organizzazione amministrativa quale presupposto per una buona amministrazione digitale

In conclusione, si può affermare che le disposizioni in materia di cybersicurezza previste dal Codice dei contratti pubblici, in particolare dall'articolo 19, offrono l'opportunità di riflettere sull'impatto della digitalizzazione sulla Pubblica Amministrazione e, in particolare, sulla sua organizzazione.

La crescente digitalizzazione delle attività della Pubblica Amministrazione richiede, infatti, un adattamento della struttura organizzativa per supportare efficacemente le nuove modalità attraverso cui si svolge il potere pubblico.

Nel contesto degli appalti pubblici, se l'intero ciclo di vita dei contratti deve essere svolto digitalmente, allora anche la struttura amministrativa che supporta le procedure di affidamento e gestione dei contratti deve essere adeguatamente organizzata per affrontare i rischi associati alla digitalizzazione.

Di conseguenza, la necessità di garantire una struttura amministrativa impermeabile alle minacce informatiche potrebbe essere considerata una declinazione specifica del principio di buon andamento, sancito dall'articolo 97, comma 2, della

30 V. artt. 8 e 24 della legge n. 90/2024.

Costituzione. In altre parole, la cybersicurezza si configurerebbe come un "corollario" di tale principio, influenzando direttamente l'efficienza, l'efficacia e la sicurezza dell'azione amministrativa.

Pertanto, una Pubblica Amministrazione che intenda conformarsi a un modello costituzionale di "buona amministrazione"[31] deve necessariamente considerare i rischi cibernetici derivanti dalla trasformazione digitale della propria struttura organizzativa. Non può esistere una "buona amministrazione" in senso digitale in assenza di un adeguato livello sicurezza informatica, tanto sul piano materiale quanto su quello organizzativo.

In definitiva, è importante riconoscere che le norme sulla cybersicurezza analizzate hanno il pregio di mettere in luce la necessità di affrontare la trasformazione digitale della Pubblica Amministrazione non solo dalla prospettiva della digitalizzazione dell'azione amministrativa, ma anche da quella dell'organizzazione.

Bibliografia

Auby J.B., De Minico G. e Orsoni G. (a cura di) 2023, *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte*, Napoli: Editoriale scientifica.

Botto A, Castrovinci Zenna S. (a cura di), 2024, *Commentario alla normativa sui contratti pubblici*, Torino: Giappichelli.

Brighi R. e Chiara p. G. 2021, "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, n. 21: 18 ss.

Bruno B. 2020, "'Cybersecurity' tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, n. 14: 11 ss.

Bruno B. (2024), "*Art. 19 Principi e diritti digitali*, in R. Giovagnoli e G. Rovelli (a cura di), *Codice dei contratti pubblici*, Milano, Giuffrè: 212 ss.

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

Caringella F. (diretto da) 2023, *Nuovo codice dei contratti pubblici*, Milano: Giuffrè.

Carloni E. 2020, "Diritti by design. Considerazioni su organizzazione, autonomia organizzatoria e protezione degli interessi", in *p. A. Persona e Amministrazione*, n. 1: 51 ss.

Cartei G.F. e Iaria D. (a cura di) 2023, *Commentario al nuovo Codice dei contratti pubblici*, Napoli: Editoriale Scientifica.

Carullo G. 2023, "Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici", in *Federalismi.it*, n. 19: 110 ss.

Cavallo Perin R. (a cura di) 2021, *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino: Rubettino.

Cavallo Perin R. 2020, "Ragionando come se la digitalizzazione fosse data", in *Dir. amm.*, n. 2: 305 ss.

Cavallo Perin R., Galetta D.U. (a cura di) 2020, *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli.

Cavallo Perin R., Lipari M. e Racca G.M. (a cura di) 2022, *Contratti pubblici e innovazioni. Per l'attuazione della legge delega*, Napoli: Jovene.

31 Sulla digitalizzazione e la buona amministrazione, cfr. su tutti Galetta 2020: 85 ss.

Corradino M. (a cura di) 2023, *La riforma dei contratti pubblici. Commento al d.lgs. 31 marzo 2023, n. 36*, Milano: Giuffrè.
Corrado A. 2023, "I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro", in *Federalismi.it*, n. 19: 128 ss.
Corrado A. 2023, "La digitalizzazione dei contratti pubblici", in Dall'Acqua F., Meola A. e Purcaro A.S. (a cura di), *La nuova disciplina degli appalti pubblici*, Pisa: Pacini giuridica: 119 ss.
Dall'Acqua F., Meola A. e Purcaro A.S. (a cura di) 2023, *La nuova disciplina degli appalti pubblici*, Pisa: Pacini giuridica.
Fanti V. (a cura di) 2023, *Corso sui contratti pubblici riformati dal d.lgs. 31 marzo 2023, n. 36*, Napoli: Edizioni Scientifiche Italiane.
Forte p. e Pica N. 2023, "Principi per la digitalizzazione e l'automazione nel ciclo di vita dei contratti pubblici", in AA.VV., *Studi sui principi del Codice dei contratti pubblici*, Napoli: Editoriale Scientifica: 303 ss.
Galetta D.U. 2020, "Digitalizzazione e diritto ad una buona amministrazione (il procedimento amministrativo, fra diritto UE e tecnologie ICT)", in Cavallo Perin R. e Galetta D.U. (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli.
Galetta D.U. 2022, "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*, n. 7: 118 ss.
Galetta D.U. 2023, "Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono", in *Federalismi.it*, n. 12: iv ss.
Galetta D.U. 2023, "Il procedimento amministrativo come strumento di organizzazione e le conseguenze legate all'uso delle ICT", in *Istit. del Federalismo*, n. 2: 289 ss.
Gambetta D. 2023, "Digitalizzazione (artt. 19-36)", in Fanti V. (a cura di) 2023, *Corso sui contratti pubblici riformati dal d.lgs. 31 marzo 2023, n. 36*, Napoli: Edizioni Scientifiche Italiane: 93 ss.
Guarnaccia E. 2022, "Il processo di digitalizzazione delle gare d'appalto: dal DM n. 148/2021 al Codice dei Contratti Pubblici 2023", in *CERIDAP*, n. 4: 134 ss.
Macrì I. 2021, "Cybersicurezza per la Pubblica Amministrazione", in *Azienditalia*, n. 12: 1196 ss.
Mancini Palamoni G. 2024, "Il paradigma digitale dell'evidenza pubblica", in *CERIDAP*, n. 2.
Montessoro p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Ist. del Federalismo*, n. 3: 783 ss.
Moroni L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179 ss.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, n. 25: 65 ss.
Racca G.M. 2020, "La digitalizzazione dei contratti pubblici: adeguatezza delle pubbliche amministrazioni e qualificazione delle imprese", in R. Cavallo Perin e D.U. Galetta (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli: 321 ss.
Racca G.M. 2022, "Le innovazioni necessarie per la trasformazione digitale e sostenibile dei contratti pubblici", in *Federalismi.it*, n. 15: 191 ss.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giorn. dir. amm.*, n. 4: 538 ss.
Rossa S. 2023a, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.

Rossa S. 2023b, "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*: 161 ss.
Rossa S. 2024a, "Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici", in *CERIDAP*, n. 2.
Rossa S. 2024b, "L'istituzione della figura del "referente per la cybersicurezza" nel d.d.l. 16 febbraio 2024", in *IRPA, Osservatorio sullo Stato digitale – www.irpa.eu*, 8 maggio 2024.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, n. 12: 241 ss.
Tropea G. (a cura di) 2024, *Lineamenti di diritto dei contratti pubblici*, Napoli: Editoriale Scientifica.
Ursi R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: Franco Angeli.
Ursi R. (a cura di) 2024, *Studi sui principi generali del Codice dei contratti pubblici*, Napoli: Editoriale Scientifica.
Vesperini G. 2024, "Art. 19. Della digitalizzazione del ciclo vita dei contratti", in Botto A e Castrovinci Zenna S. (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino: Giappichelli: 200 ss.
Villata R. e Ramajoli M. (a cura di) 2024, *Commentario al codice dei contratti pubblici*, Pisa: Pacini giuridica.