



# costruire il futuro

ANCE | BRESCIA

4/2024

Rivista bimestrale di ANCE Brescia

# Appalti pubblici e cybersecurity

Aggiornamento normativo  
in materia di cybersicurezza  
e digitalizzazione

a cura dell'Avv. Chiara Micera  
© riproduzione riservata



Avvocata Chiara Micera  
Studio legale Micera

Il nuovo Codice Appalti, come ormai è noto, è un corpus normativo che esprime l'intento del legislatore di avviare un completo processo di transizione digitale della pubblica amministrazione

**I**l percorso individuato è complesso e necessita di essere attuato attraverso il coordinamento di diverse fonti normative interne ed europee, nonché dell'azione di autorità preposte.

Però non si può ragionevolmente affrontare il tema della digitalizzazione se non avendo ben chiara la centralità della sicurezza informatica, meglio nota come *cybersecurity*, espressione di una cultura di mitigazione e prevenzione dei rischi connessi all'utilizzo della tecnologia. Rischi che sono sensibilmente più alti ed impattanti quando attengono all'esercizio delle funzioni statali, o comunque al funzionamento della macchina amministrativa, che gestisce il consesso sociale.

Il decreto legislativo 36/2023, nel disciplinare gli appalti pubblici, ha introdotto due norme che si occupano segnatamente di sicurezza informatica: l'art. 19, co. 5, e l'art. 108, co. 4.

La prima norma è inserita nel Libro I, Parte II, con oggetto la digitalizzazione del ciclo di vita dei contratti, e richiamata preliminarmente la fonte normativa primaria del Codice dell'Amministrazione digitale, il decreto 82/2005, al comma 5, prevede che siano adottate misure tecniche e organizzative finalizzate ad assicurare la sicurezza informatica e la protezione dei dati personali, assicurando la formazione del personale addetto e il costante aggiornamento.

Il secondo articolo invece, è inserito nel Libro II, Parte V, relativo allo svolgimento delle procedure, e l'art. 108 in commento si occupa dei criteri di aggiudicazione degli appalti di lavori, servizi e forniture.

Al comma 4, il Codice stabilisce che le stazioni appaltanti e le centrali di committenza nell'attività di approvvigionamento di beni e servizi informatici, nel procedere all'aggiudicazione sulla base del criterio dell'offerta economicamente più vantaggiosa, ai fini della valutazione dell'elemento qualitativo in comparazione al prezzo *“..tengano sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto d'impiego è connesso alla tutela degli interessi nazionali strategici.”*

Inoltre, in tale ultimo caso, attesa la delicatezza degli interessi stessi, la stazione appaltante deve

## La normazione per una transizione digitale in sicurezza

Continuano gli approfondimenti dedicati alla digitalizzazione a cura dell'avvocata Chiara Micera, nel solco della collaborazione stretta con Ance Brescia per supportare le imprese edili in questa transizione. Approfondimenti che passano inevitabilmente da un'attenta analisi dell'apparato normativo che si sta via via costruendo in materia di sicurezza informatica e protezione dei dati. Un argomento di estrema attualità che nel presentare evidenti vantaggi per

l'efficientamento e l'evoluzione di processi e meccanismi di gestione aziendale, anche per il settore delle costruzioni, tocca temi quali l'etica e la privacy tanto dibattuti sui tavoli dei legislatori italiani ed europei. Ad interessare il comparto dell'edilizia è, in questo contesto, anche l'interconnessione tra la gestione in sicurezza dei dati e l'attività di approvvigionamento degli stessi da parte delle stazioni appaltanti e delle centrali di committenza durante le fasi di appalto. L'aggiornamento normativo è offerto alle imprese associate grazie alla partnership di Ance Brescia con lo Studio Legale Micera che continua e si consolida. L'avvocata nelle pagine che seguono passa così in rassegna le principali misure adottate per prevenire i rischi connessi all'utilizzo della tecnologia e i reati informatici, insieme alle linee guida e alle raccomandazioni indicate per le Pubbliche amministrazioni.

stabilire un tetto massimo per il punteggio economico entro il limite del dieci per cento, così valorizzando la valutazione tecnica nella corrispondente misura del novanta per cento.

Queste due norme esprimono una maturazione della sensibilità del legislatore, il quale nella precedente versione del Codice Appalti emanata nel 2016, pur prevedendo l'obbligatorietà dell'introduzione di alcuni processi digitalizzati, *in primis* la gestione informativa digitale delle costruzioni, gergalmente identificata con l'acronimo Bim che sta per *Building Information Modeling*, non aveva inserito alcuna norma che si riferisse segnatamente alla sicurezza informatica, sebbene vi fosse un quadro legislativo preesistente, in quel tempo vigente che, comunque, regolamentava la *cybersecurity*.

Infatti, l'emanazione del Codice dell'Amministrazione digitale sopracitata, noto con l'acronimo Cad, risale al 2005; da allora il quadro normativo è stato integrato da ulteriori fonti, espressioni altresì delle direttive europee.

Di queste ultime dobbiamo necessariamente citare il Regolamento Ue 2019/881 il cosiddetto *Cybersecurity Act*; questo documento immediatamente attuativo negli Stati dell'Unione prevede la certificazione delle infrastrutture "critiche", quali le reti energetiche, l'acqua e i siste-

mi bancari, oltre a prodotti, processi e servizi, e garantisce che soddisfino gli standard di sicurezza informatica. Il documento è espressione della "Strategia per la sicurezza cibernetica" e consente non solo di rafforzare la resilienza dell'Unione Europea agli attacchi informatici, ma anche di creare un mercato unico in termini di prodotti, servizi e processi. A tale documento si affianca la Direttiva Nis 2, entrata in vigore il 17 gennaio 2023, sulla sicurezza delle reti e delle informazioni, che integra e implementa il contenuto della Direttiva Nis, precedentemen-

**Il documento è espressione della "Strategia per la sicurezza cibernetica" e consente non solo di rafforzare la resilienza dell'Unione Europea agli attacchi informatici, ma anche di creare un mercato unico in termini di prodotti, servizi e processi**

te emanata nel 2019, pressoché contestualmente al Regolamento sopracitato. La stessa ovviamente si integra con altre normative e linee guida sulla protezione dei dati e della *privacy*, come il Gdpr (regolamento *privacy*), il Regolamento

Dora (*framework* Ue per la gestione del rischio in ambito finanziario che entrerà in vigore il 17 gennaio 2025) e il *Cyber Resilience Act* (per garantire la sicurezza informatica di prodotti *hardware* e *software*).

La Direttiva Nis 2 estende gli obblighi di *cybersecurity* a un numero maggiore di settori e servizi considerati "critici" per il funzionamento socioeconomico della Ue, e questi includono, oltre a quelli sopracitati, altresì piattaforme di *cloud computing*, *data center* e servizi sanitari. Tale norma europea è stata recepita in Italia

recentissimamente, lo scorso 19 giugno, mediante l'approvazione del Ddl titolato "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici". La legge consta di complessivi ventiquattro articoli, e appare di particolare

interesse per l'applicazione in tema di appalti pubblici. Essa infatti incide sulla regolamentazione esistente che prevede tre diverse fattispecie: una disciplina generale sulla sicurezza informatica che si applica a tutte Pubbliche amministrazioni,

una specifica della stessa che riguarda quelle rientranti nel “Perimetro nazionale di Sicurezza cibernetica”, che identifica quegli attori pubblici e privati che esercitano funzioni essenziali dello Stato o che assicurano un servizio essenziale alle attività fondamentali nell'interesse dello Stato, e da ultimo un regime speciale che

favorire il raggiungimento dell'autonomia tecnologica rispetto ai grandi produttori internazionali extraeuropei. Tra i suoi compiti principali c'è l'attuazione della “Strategia nazionale di Cybersicurezza” adottata dal Presidente del Consiglio che contiene gli obiettivi da perseguire entro



**Tra i compiti dell'Agenzia per la Cybersicurezza nazionale, meglio nota come Acn c'è l'attuazione della “Strategia nazionale di Cybersicurezza” adottata dal Presidente del Consiglio che contiene gli obiettivi da perseguire entro il 2026**

concerne le procedure di appalto di forniture, servizi e lavori aggiudicate dall'Agenzia per la Cybersicurezza nazionale, meglio nota come Acn. Questa è l'Autorità nazionale istituita nel 2021 per ridefinire l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della sicurezza nazionale nello spazio cibernetico. Si occupa di prevenire e mitigare il mag-

gior numero di attacchi e di favorire il raggiungimento dell'autonomia tecnologica rispetto ai grandi produttori internazionali extraeuropei. Tra i suoi compiti principali c'è l'attuazione della “Strategia nazionale di Cybersicurezza” adottata dal Presidente del Consiglio che contiene gli obiettivi da perseguire entro il 2026. Il provvedimento legislativo testé emanato valorizza ulteriormente il ruolo dell'Autorità nazionale, e agli art. nn.8-10, prevede l'adozione di misure di rafforzamento della resilienza delle Pubbliche amministrazioni e l'istituzione di un referente per la cybersicurezza in ciascuna di esse “... nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente...”. Questa figura, si sottolinea, obbligatoria, dovrà realizzare le iniziative necessarie per una *security by design*, cioè ap-

prontando un sistema di prevenzione del rischio a seguito di un'analisi preventiva di rilevamento; dovrà altresì redigere un documento che definisca i ruoli e l'organizzazione del sistema, ed alla pianificazione ed attuazione delle misure dei linee guida per la cybersicurezza emanate dall'Acn, la quale avrà la facoltà di coordinare i citati referenti delle varie Amministrazioni “per facilitare la resilienza” delle stesse. I referenti dovranno altresì verificare che i programmi e le applicazioni informatiche e di comunicazioni elettroniche in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia, nonché quelle sulla conservazione delle password adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali. A conferma della necessità di sviluppare algoritmi per proteggere le informazioni, l'Autorità viene incaricata di istituire il Centro nazionale della Crittografia, anche a vantaggio della blockchain come strumento di sicurezza informatica. Verrà poi emesso entro novanta giorni dall'entrata in vigore della legge, non ancora pubblicata, un regolamento avente ad oggetto il procedimento sanzionatorio amministrativo per l'irrogazione delle sanzioni a carico della Pubblica amministrazione, nell'ipotesi di violazioni delle prescrizioni.

All'art.14 poi si prevede che l'approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, debbano essere previsti criteri di premialità per l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione Europea o di Paesi aderenti all'Alleanza Atlantica (Nato) o che abbiano accordi di collaborazione con ciascuna di esse, che prevedano “elementi es-

senziali di cybersicurezza”, che possano garantire “...confidenzialità, l'integrità e la disponibilità dei dati...”. Il comma 2 dello stesso articolo, in merito all'aggiudicazione dell'appalto, richiama espressamente l'art. 108 del Codice dei Contratti sopracitato, ulteriormente valorizzando l'elemento della sicurezza informatica nell'offerta formulata dall'operatore economico. Quindi, la breve disamina ci conduce a due considerazioni: la prima è che di palmare evidenza l'intento del legislatore europeo prima ed italiano poi, di condurre la Pubblica amministrazione verso un percorso sempre più rapido della completa digitalizzazione dei processi e dei prodotti. Tale dato dovrebbe far riflettere gli attori privati sulla corrispondente necessità di strutturare le proprie organizzazioni secondo le medesime Linee guida e raccomandazioni indicate per le Pubbliche amministrazioni, anche in considerazione che, al di là della partecipazione agli appalti per la fornitura dei servizi tecnologici, anche la sola digitalizzazione del ciclo di vita dei contratti, ha come presupposto la maturità digitale dell'operatore economico. La seconda è la riflessione del giurista sul superamento delle categorie tradizionali del diritto, idonee a disciplinare fattispecie pensate su una realtà analogica, in corso di progressivo abbandono. Secondo il parere della scrivente, la sfida di disegnare nuove categorie giuridiche, di abbracciare inediti paradigmi, di ibridare le competenze con altre discipline, e di utilizzare tutte le potenzialità che la tecnologia può offrire per migliorare l'offerta di servizi professionali, è un privilegio conseguente al vivere questo tempo di tali proporzioni da doverlo meritare, investendo le nostre energie intellettuali per essere protagonisti del cambiamento. E poter dire poi: “io c'ero”.