LA DIGITALIZZAZIONE DEL NUOVO CODICE DEI CONTRATTI PUBBLICI E LA RILEVANZA DEI PROFILI DI *CYBERSECURITY* NEL *PROCUREMENT* PUBBLICO

Come noto, lo schema di decreto legislativo sul nuovo **Codice dei contratti pubblici** all'esame del Parlamento prevede una parte dedicata alla **digitalizzazione delle procedure**, la cui rilevanza è corroborata dalla scelta sistematica di raggruppare le disposizioni relative alla digitalizzazione all'inizio dell'articolato, negli articoli da 19 a 36.

La promozione della digitalizzazione in questo settore è, infatti, tra gli **obiettivi** dettati dal **PNRR** che prevede, tra l'altro, la realizzazione di un **Sistema Nazionale di *e-Procurement***, volto a raccogliere le spinte di efficienza che giungono dallo sviluppo tecnologico, che riguarda tutta la procedura, dalla fase della **programmazione delle esigenze** fino all'esecuzione del **contratto**; il tutto attraverso la realizzazione di una piena interconnessione e interoperabilità tra i sistemi telematici.

Alcune disposizioni del provvedimento in esame appaiono, in termini di cybersicurezza, particolarmente degne di attenzione:

- l'**articolo 19** afferma **i principi e i diritti digitali**. Prevede che "*le stazioni appaltanti e gli enti concedenti 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***", rispetto ai quali l'Agenzia, quale Autorità nazionale di cybersicurezza, è naturalmente disponibile ad offrire ogni contributo utile e necessario ai fini di garantire i più alti livelli di cybersicurezza e resilienza nello spazio cibernetico. Principi che consentiranno di dare attuazione *in primis* al diritto di cittadinanza digitale. Viene, inoltre, a mio giudizio opportunamente affermato il principio dell'unicità dell'invio (*once only*), per cui **i dati sono forniti una sola volta** a **un solo sistema informativo** e non possono essere richiesti da altri sistemi o banche dati, ma sono **resi disponibili** dal sistema informativo ricevente. Altre

disposizioni dell'articolo ribadiscono principi e concetti che sono già noti e che meritano una rinnovata attenzione per i profili di cybersicurezza. Mi riferisco, in particolare, ai seguenti: **le attività e i procedimenti amministrativi sono svolti digitalmente** mediante le piattaforme e i servizi digitali infrastrutturali delle stazioni appaltanti (comma 3); dati e informazioni sono gestiti e resi fruibili in **formato aperto** (comma 3); deve essere resa effettiva l'interoperabilità automatica tra banche dati (comma 4); vanno adottate **misure tecniche e organizzative a presidio della sicurezza informatica** e della protezione dei dati personali (comma 5);

- l'**articolo 22** prevede la creazione di un **ecosistema nazionale di approvvigionamento digitale**, costituito dalle **piattaforme** e dai **servizi digitali infrastrutturali** abilitanti per la gestione del ciclo di vita dei contratti pubblici e dalle piattaforme di approvvigionamento digitale utilizzate dalle stazioni appaltanti;
- l'**articolo 23** è dedicato alla **Banca dati nazionale dei contratti pubblici**, istituita presso l'**ANAC**, che diventa l'infrastruttura tecnologica portante dell'ecosistema nazionale di *e-procurement*. Su questo punto mi soffermo tra poco per alcuni elementi di dettaglio;
- l'**articolo 24** disciplina il **Fascicolo virtuale** dell'operatore economico, istituito presso la Banca dati nazionale dei contratti pubblici di ANAC;
- l'**articolo 25** disciplina le **piattaforme di approvvigionamento digitale**, che le stazioni appaltanti devono utilizzare per svolgere le procedure di affidamento ed esecuzione dei contratti pubblici, secondo le **regole tecniche** di cui al successivo articolo 26;
- l'**articolo 26** stabilisce che i requisiti tecnici delle piattaforme digitali di *e-procurement* e la conformità di dette piattaforme siano stabilite dall'**AgID** (di intesa con ANAC e il Dipartimento per la trasformazione digitale presso la Presidenza del Consiglio dei ministri), che fisserà anche le modalità per la **certificazione** delle

piattaforme digitali di *e-procurement* erogate da **soggetti privati** al fine della loro compatibilità con l'ecosistema nazionale di *e-procurement*. **Naturalmente ritengo che anche tali piattaforme dovranno assicurare adeguati livelli di cybersicurezza**.

Ritornando, come vi ho anticipato, alla **Banca dati nazionale dei contratti pubblici**, evidenzio che lo scorso 7 novembre è stato stipulato un **Protocollo d'intesa** tra ACN e **ANAC** che prevede una collaborazione tra le Parti in materia di contratti pubblici. Tale collaborazione istituzionale riguarda, tra l'altro, la definizione di strategie condivise di **valorizzazione e protezione del patrimonio informativo gestito da ANAC** e, in particolare, della richiamata Banca dati nazionale dei contratti pubblici, al fine di adottare **misure di prevenzione e mitigazione** degli incidenti di sicurezza, anche attraverso l'attivazione di un rapporto di collaborazione continuativo con il **CSIRT Italia**. L'ACN, infatti, **supporterà l'ANAC** al fine di agevolare un migliore orientamento della propria strategia di trasformazione digitale, segnalando le opportune tecniche di intervento idonee a preservare le informazioni raccolte nella Banca dati nazionale dei contratti pubblici.

La riflessione sul nuovo Codice dei contratti pubblici potrebbe, tuttavia, costituire anche un'occasione unica per interrogarsi sulle modalità attraverso cui **valorizzare gli aspetti legati alla cybersicurezza di prodotti e servizi acquisiti dalle pubbliche amministrazioni**, anche al fine di contribuire a garantire che la transizione digitale del Paese sia sicura.

Sul punto, la **Strategia nazionale** di cybersicurezza e il relativo **Piano di implementazione**, adottati con DPCM del 17 maggio 2022, prevedono, tra i vari obiettivi, quello della **protezione degli *asset* strategici nazionali** attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possano abilitare una

transizione digitale resiliente del Paese. In particolare, si evidenziano gli aspetti relativi alla **sicurezza degli approvvigionamenti** e della *supply chain*.

Al riguardo, assume un fondamentale rilievo **perseguire la valorizzazione dell'inclusione di elementi di sicurezza cibernetica nelle attività di *procurement* ICT della PA**. A tale fine, il menzionalo **Piano di implementazione** della richiamata Strategia prevede **3 specifiche misure** (le n. 6, n. 7 e n. 8) volte a:

- (n. 6) introdurre disposizioni che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della PA, fornendo indicazioni sia alla stessa PA che agli operatori di mercato per garantire che i beni e i servizi informatici, acquistati da soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro – compatibilmente con la celere definizione delle procedure di aggiudicazione – rispondano a adeguati livelli di cybersicurezza;
- (n. 7) promuovere la realizzazione di un sistema di gare pubbliche impostato su criteri che garantiscano soluzioni di qualità sotto il profilo della cybersicurezza;
- (n. 8) introdurre disposizioni volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.

In considerazione della complessità dell'ambito della cybersicurezza e del digitale più in generale, si potrebbe, altresì, **ragionare sul criterio di aggiudicazione degli appalti** quando si utilizza quello dell'offerta economicamente più vantaggiosa. Si registra, infatti, la **soppressione della disposizione** della norma che, allo scopo di valorizzare gli elementi **qualitativi** dell'offerta, disponeva che **la stazione appaltante stabilisse un tetto massimo** per il punteggio economico entro il limite del **30 per cento** (c.d. **regola del 70/30**). Si è appreso dalla relazione illustrativa come la scelta dell'eliminazione di tale regola è dipesa dall'analisi economica che ha dimostrato che la stessa contiene degli elementi critici, distorsivi del mercato, secondo quanto

rilevato anche dall'Autorità Garante della Concorrenza e del Mercato (AGCM) nel 2021.

È prevalsa, pertanto, la volontà di **rimettere alle stazioni appaltanti la scelta di quanto incidano l'aspetto tecnico e quello economico**, con l'obiettivo di consentire la migliore fruizione del criterio dell'offerta economicamente più vantaggiosa, adeguando il peso delle due componenti (prezzo e qualità) alle effettive caratteristiche dello specifico appalto. In questi casi **appare di tutta importanza**, quindi, che **la stazione appaltante attribuisca un opportuno peso ai profili tecnico-qualitativi di sicurezza cibernetica rispetto ai profili economici**, non potendo rischiare che l'elemento prezzo sia decisivo, anche attraverso meccanismi di gara che riconoscano la necessaria attenzione che le stazioni appaltanti debbono avere per questi aspetti.