Dati e sicurezza nel sistema digitale degli appalti

Lezione 4

Week 2 Procedure automatizzate e intelligenza artificiale nel ciclo di vita dei contratti pubblici

INTRODUZIONE AL SISTEMA DIGITALE DEGLI APPALTI

La transizione digitale nel settore pubblico

La digitalizzazione dei contratti pubblici rappresenta una rivoluzione sistemica che supera la mera sostituzione del cartaceo con il digitale. Si tratta di un processo che investe l'intero ciclo di vita delle commesse pubbliche, dalla programmazione all'esecuzione, richiedendo una trasformazione sostanziale dell'azione amministrativa.

Obiettivi strategici della digitalizzazione

Il processo di digitalizzazione persegue obiettivi multidimensionali che toccano aspetti operativi, economici e di governance del sistema pubblico.

GLI OBIETTIVI DELLA DIGITALIZZAZIONE

- **Efficienza operativa**: riduzione dei tempi procedurali e semplificazione delle procedure
- **Trasparenza**: maggiore visibilità e controllo sui processi decisionali
- **Parità di trattamento**: garanzia di condizioni uniformi per tutti gli operatori economici
- **Riduzione degli oneri**: diminuzione dei costi amministrativi e burocratici
- **Prevenzione della corruzione**: rafforzamento dei meccanismi di controllo e tracciabilità

IL QUADRO NORMATIVO DI RIFERIMENTO

La Parte II del nuovo Codice

Il D. Lgs. 36/2023 dedica l'intera Parte II alla "digitalizzazione del ciclo di vita dei contratti", evidenziando l'importanza strategica attribuita dal legislatore a questa trasformazione.

Principi fondamentali

Il nuovo Codice si basa su principi cardine che orientano l'intero processo di digitalizzazione, garantendo coerenza e uniformità nell'implementazione delle soluzioni tecnologiche.

I PRINCIPI CARDINE DELLA DIGITALIZZAZIONE

- **Neutralità tecnologica**: non imposizione di specifiche soluzioni tecnologiche
- **Interoperabilità**: capacità dei sistemi di comunicare tra loro
- **Trasparenza**: accessibilità e comprensibilità dei processi automatizzati
- **Sicurezza**: protezione dei dati e delle infrastrutture digitali
- **Accessibilità**: garanzia di fruibilità per tutti gli operatori

I DATI COME "MATERIA PRIMA" DELL'IA

Il concetto di dato nell'era digitale

Nell'ecosistema digitale dei contratti pubblici, i dati assumono un ruolo centrale, trasformandosi da semplici informazioni in risorse strategiche. La digitalizzazione genera volumi enormi di dati che costituiscono la base per l'implementazione di sistemi di intelligenza artificiale avanzati.

Caratteristiche dei Big Data nel procurement pubblico

I dati generati dalle procedure di affidamento presentano le caratteristiche tipiche dei Big Data, richiedendo approcci specifici per la loro gestione e valorizzazione.

LE "3 V" DEI BIG DATA NEGLI APPALTI

- **Volume**: quantità massicce di dati generati dalle procedure
- **Varietà**: diversi formati e tipologie di informazioni (documenti, dati strutturati, metadati)
- **Velocità**: necessità di trattamento in tempo reale per l'efficacia operativa
- **Veridicità**: qualità e affidabilità dei dati come requisito essenziale
- **Valore**: capacità di generare insights e miglioramenti processuali

L'INTELLIGENZA ARTIFICIALE NEI CONTRATTI PUBBLICI

Definizione e caratteristiche dell'IA

L'intelligenza artificiale, in particolare il machine learning, si distingue dal software tradizionale per la capacità di apprendimento automatico. Mentre il software convenzionale esegue istruzioni predefinite, l'IA sviluppa autonomamente strategie risolutive attraverso l'analisi dei dati.

Apprendimento automatico e predittivo

I sistemi di IA sono in grado di identificare pattern nei dati storici e utilizzarli per prevedere comportamenti futuri, ottimizzando i processi decisionali.

APPLICAZIONI DELL'IA NEL PROCUREMENT PUBBLICO

- **Analisi predittiva**: identificazione di anomalie e irregolarità nelle procedure
- **Ottimizzazione delle procedure**: miglioramento dell'efficienza operativa
- **Supporto decisionale**: assistenza nella valutazione delle offerte
- **Controllo automatico**: verifica della conformità dei documenti
- **Prevenzione della corruzione**: individuazione di comportamenti sospetti

LE AUTORIZZAZIONI NORMATIVE PER L'IA

Previsioni del nuovo Codice

Il legislatore ha previsto la possibilità di ricorrere a procedure automatizzate, anche con IA e tecnologie di registri distribuiti (DLT), per migliorare l'efficienza delle stazioni appaltanti.

Articolo 30 del D.Lgs. 36/2023

L'articolo 30 rappresenta la prima previsione normativa nazionale specifica sull'uso di procedure automatizzate negli appalti pubblici, stabilendo un quadro giuridico per l'implementazione di sistemi di IA.

PROBLEMATICHE DELLA QUALITÀ DEI DATI

Criticità rilevate nei dati pubblici

L'analisi dei dati pubblici sui contratti ha evidenziato diverse problematiche strutturali che ostacolano l'efficace implementazione di sistemi di IA.

- **Assenza di dati significativi**: mancanza di informazioni cruciali come il numero dei partecipanti
- **Errori sistematici**: inesattezze nelle date di pubblicazione e aggiudicazione
- **Incompletezza**: carenza di informazioni sulla fase di aggiudicazione
- **Frammentazione territoriale**: banche dati non integrate
- **Documenti non strutturati**: prevalenza di formati non elaborabili automaticamente

IL PRINCIPIO "GARBAGE IN, GARBAGE OUT"

Importanza cruciale della qualità dei dati

Per i sistemi di intelligenza artificiale, la qualità dei dati rappresenta un requisito inderogabile. Il principio "garbage in, garbage out" sottolinea come dati inaccurati o obsoleti conducano inevitabilmente a valutazioni fuorvianti e decisioni errate.

Misure per garantire la qualità

Le pubbliche amministrazioni devono adottare misure tecniche e organizzative specifiche per garantire l'affidabilità dei dati utilizzati dai sistemi automatizzati.

MISURE PER MIGLIORARE LA QUALITÀ DEI DATI

- **Rettifica dei fattori di inesattezza**: identificazione e correzione sistematica degli errori
- **Minimizzazione del rischio**: implementazione di controlli preventivi
- **Prevenzione degli effetti discriminatori**: verifica dell'equità dei risultati
- **Standardizzazione dei formati**: adozione di formati strutturati e interoperabili
- **Validazione automatica**: controlli di coerenza e completezza
- **Aggiornamento continuo**: mantenimento dell'attualità delle informazioni

LA "GELOSIA DEL DATO" NELLE PA

Caratteristiche del fenomeno

Il concetto di "gelosia del dato" descrive la tendenza delle amministrazioni pubbliche a gestire i propri dati in modo proprietario, limitando la condivisione e l'integrazione con altri sistemi.

Conseguenze negative

Questo approccio ostacola la realizzazione di un ecosistema digitale integrato e limita le potenzialità dei sistemi di intelligenza artificiale, che necessitano di dataset ampi e diversificati.

SUPERARE LA FRAMMENTAZIONE DEI DATI

- **Cultura della condivisione**: promozione di un approccio collaborativo
- **Standardizzazione**: adozione di formati e protocolli comuni
- **Interoperabilità**: sviluppo di sistemi comunicanti
- **Governance condivisa**: definizione di regole comuni per la gestione dei dati
- **Incentivi alla cooperazione**: meccanismi premiali per la condivisione

L'INTEROPERABILITÀ COME PARADIGMA

Definizione e obiettivi

L'interoperabilità rappresenta la capacità dei sistemi informatici di comunicare, scambiare dati e utilizzare le informazioni condivise in modo efficiente e sicuro. Nel contesto degli appalti pubblici, l'interoperabilità è fondamentale per superare la logica dei "silos informativi".

Vantaggi dell'ecosistema interoperabile

Un sistema interoperabile permette lo scambio automatico di informazioni tra piattaforme diverse, riducendo la duplicazione degli sforzi e migliorando l'efficienza complessiva.

VANTAGGI DELL'INTEROPERABILITÀ

- **Efficienza operativa**: riduzione dei tempi di elaborazione
- **Semplificazione procedurale**: eliminazione di passaggi ridondanti
- **Riduzione degli errori**: minimizzazione dell'intervento umano
- **Economie di scala**: condivisione di costi e risorse
- **Miglioramento della qualità**: standardizzazione dei processi
- **Trasparenza**: maggiore visibilità delle attività

SFIDE DELL'INTEROPERABILITÀ

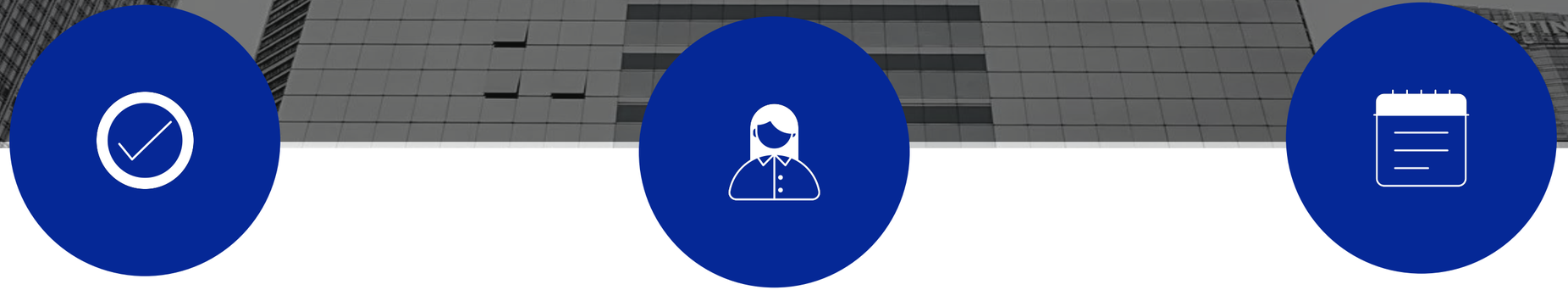
Rischi della comunicazione machine-to-machine

L'ambiente interoperabile, caratterizzato dall'acquisizione diretta e automatica di dati tra sistemi diversi, presenta rischi specifici legati all'assenza di filtri umani nel processo di elaborazione.

Propagazione degli errori

In un sistema interconnesso, un dato impreciso può compromettere l'affidabilità dell'intero ecosistema, riproducendo e amplificando gli errori attraverso le diverse piattaforme.

RISCHI DELL'INTEROPERABILITÀ AUTOMATIZZATA



- **Amplificazione degli errori**: propagazione di dati inesatti
- **Perdita di controllo umano**: riduzione della supervisione diretta
- **Complessità sistemica**: difficoltà nell'identificazione delle cause di errore
- **Dipendenza tecnologica**: vulnerabilità in caso di malfunzionamenti
- **Standardizzazione forzata**: perdita di specificità locali

GOVERNANCE DELL'INTEROPERABILITÀ

Ruolo di AGID e ANAC

Il Codice dei Contratti Pubblici e le normative correlate attribuiscono ad AGID e ANAC un ruolo nella definizione delle regole tecniche e degli standard di sicurezza per le piattaforme e i servizi digitali.

Standard di conformità

Le piattaforme devono rispettare standard specifici che garantiscano non solo l'interoperabilità tecnica, ma anche la protezione e la riservatezza dei dati trattati.

RESPONSABILITÀ DI AGID E ANAC

AGID (Agenzia per l'Italia Digitale)

- Definizione delle regole tecniche per l'interoperabilità
- Standard per la sicurezza informatica
- Coordinamento delle piattaforme digitali pubbliche

ANAC (Autorità Nazionale Anticorruzione)

- Supervisione della trasparenza nelle procedure automatizzate
- Definizione dei requisiti di sicurezza per le piattaforme
- Controllo della conformità normativa

TECNOLOGIE DLT E BLOCKCHAIN NEGLI APPALTI

Definizione e caratteristiche

Le tecnologie DLT (Distributed Ledger Technology) e blockchain rappresentano soluzioni innovative per garantire la sicurezza e la tracciabilità nelle procedure di approvvigionamento pubblico.

Applicazioni pratiche

Un esempio concreto di applicazione delle DLT è rappresentato dalle garanzie fideiussorie digitali, che utilizzano la blockchain per garantire la certezza dell'emissione e la verificabilità telematica dei documenti.

VANTAGGI DELLE TECNOLOGIE DLT

- **Immutabilità**: impossibilità di alterare i dati registrati
- **Trasparenza**: tracciabilità completa delle transazioni
- **Decentralizzazione**: riduzione dei punti di fallimento
- **Sicurezza**: crittografia avanzata per la protezione dei dati
- **Efficienza**: riduzione dei tempi di verifica e validazione
- **Riduzione delle frodi**: meccanismi di controllo automatico

IL PATRIMONIO INFORMATIVO PUBBLICO

Gestione integrata dei dati

L'interoperabilità deve estendersi alla gestione del "patrimonio informativo" pubblico nel suo complesso, superando le barriere settoriali e territoriali.

Ostacoli alla integrazione

La difficoltà nell'integrare basi di dati diverse è spesso causata da interpretazioni restrittive delle norme sulla protezione dei dati personali, che rallentano la realizzazione di un ecosistema coeso.

REQUISITI PER DATASET EFFICACI

- **Coesione**: struttura uniforme e standardizzata
- **Aggiornamento tempestivo**: mantenimento dell'attualità
- **Controllo interno**: capacità di rilevare anomalie
- **Completezza**: copertura esaustiva delle informazioni necessarie
- **Qualità**: accuratezza e affidabilità dei dati
- **Accessibilità**: fruibilità per gli operatori autorizzati

LA CYBERSICUREZZA COME PILASTRO STRATEGICO

Evoluzione del concetto di sicurezza

Il D.Lgs. n. 36/2023 rappresenta un punto di svolta nella concezione della cybersicurezza, elevandola da mera questione tecnica a pilastro strategico dell'azione amministrativa.

Contesto delle minacce

La Pubblica Amministrazione si confronta quotidianamente con attacchi informatici di varia natura, dal phishing al ransomware, che minacciano la continuità operativa e la tutela dei diritti dei cittadini.

TIPOLOGIE DI MINACCE INFORMATICHE

- **Phishing**: sottrazione di credenziali tramite inganno
- **Ransomware**: crittografia dei dati per estorcere denaro
- **Malware**: software dannoso per compromettere i sistemi
- **Attacchi DDoS**: sovraccaricare i servizi per renderli inutilizzabili
- **Intrusioni**: accesso non autorizzato ai sistemi
- **Social engineering**: manipolazione psicologica per ottenere informazioni

IL QUADRO NORMATIVO EUROPEO E NAZIONALE

Direttiva NIS2

La Direttiva NIS2 (Network and Information Security) costituisce il riferimento europeo principale, ampliando significativamente il campo di applicazione della normativa sulla cybersicurezza.

Perimetro di Sicurezza Nazionale Cibernetica

Istituito con il D.L. n. 105/2019, definisce il quadro strategico per la protezione dei beni ICT di rilevanza nazionale, attribuendo un ruolo centrale all'Agenzia per la Cybersicurezza Nazionale (ACN).

SOGGETTI COINVOLTI NELLA CYBERSICUREZZA

ACN (Agenzia per la Cybersicurezza Nazionale)

- Coordinamento della sicurezza cibernetica nazionale
- Definizione delle politiche di cybersicurezza
- Gestione delle emergenze informatiche

Settore pubblico e privato

- Protezione delle infrastrutture critiche
- Implementazione delle misure di sicurezza
- Collaborazione nella prevenzione delle minacce

LA CYBERSICUREZZA COME CRITERIO DI AGGIUDICAZIONE

Innovazione dell'articolo 108

L'articolo 108 del D.Lgs. n. 36/2023 supera la concezione tradizionale che vedeva la sicurezza informatica come un requisito tecnico accessorio, trasformandola in un elemento di valutazione paritetico.

Parità con altri criteri

La cybersicurezza diventa un criterio autonomo di valutazione, equiparato al prezzo e alla qualità tecnica dell'offerta, segnando un cambio di paradigma nella valutazione delle proposte.

CRITERI DI VALUTAZIONE DELLA CYBERSICUREZZA

- **Requisiti di partecipazione**: capacità minime in materia di sicurezza
- **Criteri di aggiudicazione**: elementi di valutazione dell'offerta
- **Misure tecniche**: soluzioni per la protezione dei dati
- **Misure organizzative**: procedure e processi di sicurezza
- **Certificazioni**: riconoscimenti di conformità agli standard
- **Competenze specialistiche**: qualificazione del personale

INVESTIMENTI IN CYBERSICUREZZA

Allocazione delle risorse

Il Codice prevede la possibilità di destinare risorse economiche specifiche per la cybersicurezza fino al 10% del valore del contratto, percentuale che può salire al 30% per i contratti stipulati tra amministrazioni pubbliche.

Riconoscimento del valore economico

Questa previsione rappresenta un riconoscimento esplicito del valore economico della sicurezza informatica e della necessità di investimenti adeguati per garantire la protezione dei sistemi.

PRINCIPI "BY DESIGN"

Security by Design

Il principio del security by design richiede che la sicurezza informatica sia considerata sin dalle prime fasi di progettazione dei sistemi, integrandola nell'architettura piuttosto che aggiungerla successivamente.

Digital by Design

Il principio del digital by design promuove la digitalizzazione nativa dei procedimenti amministrativi, evitando approcci ibridi che spesso introducono vulnerabilità e inefficienze.

IMPLEMENTAZIONE DEI PRINCIPI "BY DESIGN"

Security by Design

- Progettazione sicura dall'origine
- Valutazione preventiva dei rischi
- Integrazione delle misure di protezione
- Test di sicurezza durante lo sviluppo

Digital by Design

- Digitalizzazione nativa dei processi
- Eliminazione dei supporti cartacei
- Ottimizzazione dei flussi informativi
- Riduzione delle vulnerabilità ibride

LE TRE SFIDE INTERCONNESSE

Sfide per il successo della digitalizzazione

Il successo di questa evoluzione dipende dalla capacità delle amministrazioni di affrontare tre sfide interconnesse: garantire la qualità dei dati come prerequisito per l'intelligenza artificiale, implementare robuste misure di cybersicurezza con capacità di resilienza, e mantenere un'efficace supervisione umana sui processi automatizzati.

Approccio sistemico

Le tre sfide sono strettamente interconnesse e richiedono un approccio integrato per garantire l'efficacia complessiva del sistema.

INVESTIMENTI NECESSARI

- **Tecnologie**: infrastrutture e software avanzati
- **Competenze**: formazione del personale
- **Standard**: protocolli di interoperabilità
- **Sicurezza**: sistemi di protezione robusti

Cambiamento culturale

È necessario un profondo cambiamento culturale nelle pubbliche amministrazioni, supportato da formazione continua del personale.

Elementi del cambiamento • Mentalità orientata all'innovazione • Collaborazione inter-istituzionale • Condivisione delle conoscenze • Approccio data-driven alle decisioni

Grazie!