Digeat N.3 - 19 Settembre 2024

# Fiducia negli strumenti e servizi digitali 2027

*Di Andrea Piccoli*

Rubrica: Gestione documentale 2027

## Abstract

Il terzo articolo di questa Rubrica accoglie alcune riflessioni sulla fiducia negli strumenti e servizi digitali, sia lato lavoratori, che lato fruitori dei servizi pubblici, ossia della pubblica amministrazione. Quale impatto hanno le nuove piattaforme ed evoluzioni delle soluzioni di gestione documentale per chi opera nei procedimenti e attività amministrative all'interno delle pubbliche amministrazioni? Quale impatto hanno i servizi digitali per garantire la fiducia dei cittadini?

## Indice



Quando un funzionario della pubblica amministrazione utilizza una piattaforma digitale ha in primo luogo l'esigenza di sentirsi accompagnato nell'eseguire attività e procedimenti in **modo lecito**. Anche se può sembrare scontata come affermazione, data la complessità e sedimentazione della norma, **non è sempre così ovvio che le azioni amministrative compiute "automaticamente" per mezzo dell'utilizzo di servizi digitali risultino corrette da un punto di vista della norma e dei loro effetti giuridici**.

> La soluzione informatica, o piattaforma online, deve essere in grado di supportare l'operatore nel compiere tutti i passaggi previsti dalla norma nella corretta sequenza e nei tempi previsti.

## La fiducia negli strumenti digitali lato PA

Per esemplificare si pensi alla gestione di un **affidamento di servizi** con il corrispondente procedimento amministrativo, realizzata mediante la negoziazione pubblica su una centrale di committenza (MEPA) e conseguente stesura, adozione e pubblicazione dell'atto di affidamento. **I documenti sono completi e corretti, efficaci, tutti correttamente archiviati e conservati nell'archivio digitale**? L'affidamento ha tenuto conto di tutti i requisiti cogenti normativi?

> Molto spesso la mancanza di fiducia da parte del funzionario negli strumenti e servizi informatici lo porta ad instaurare una sorta di “burocrazia difensiva” atta a raccogliere e richiedere molteplici evidenze documentali, la cui efficacia informativa e amministrativa è spesso garantita già dalle piattaforme digitali in uso. Oppure, semplicemente, porta ad un allungamento dei tempi amministrativi per effettuare una serie di controlli atti a recuperare la propria certezza amministrativa.

La **trasparenza dell’azione amministrativa** è tra i requisiti primari dell’esercizio della funzione pubblica. Siamo davvero sicuri che le piattaforme e servizi digitali possano sempre garantire un adeguato livello di integrazione con i requisiti sulla trasparenza amministrativa?

**Purtroppo, la mia personale sensazione è che vi siano delle lacune**. Già prendendo in esame le diverse **soluzioni di gestione documentale** sono poche quelle che integrano i passaggi in trasparenza all’interno dei flussi digitali relativi alla raccolta delle evidenze amministrative, dati e documenti, nei fascicoli delle corrispondenti attività e procedimenti amministrativi.

## La (scarsa) fiducia nelle soluzioni di gestione documentale

Da diverso tempo le soluzioni di gestione documentale e protocollo informatico adottano tecnologie di gestione dei flussi di lavoro (workflow) e di automazione di processo (RPA, *robot process automation*) in grado di assistere gli operatori nello svolgimento dei procedimenti e attività amministrative.

> Spesso per i limiti di tali soluzioni, talvolta troppo rigide o approssimative, i funzionari non dimostrano molta fiducia nel loro utilizzo, ripiegando sull’uso di strumenti di condivisione documentale alternativi e alimentando la piattaforma “ufficiale” solo al termine del procedimento. In risposta alla rigidità dell’approccio dell’automazione dei flussi di lavoro si è iniziato da tempo a **sperimentare e inserire modelli di intelligenza artificiale** che valutano e suggeriscono in tempo reale sulla base del contesto amministrativo i prossimi passi del procedimento ed eventuali dati da inserire.

Un esempio interessante è il **progetto in riuso e sviluppato con l’Università di Pisa** relativo all’applicazione di **modelli di intelligenza artificiale a supporto della classificazione secondo titolario dell’ente di una registrazione di protocollo**.

Come noto, la classificazione di un documento soggetto a registrazione di protocollo, demandata spesso in una prima fase al funzionario, individua il contesto amministrativo del documento indirizzandone la successiva fascicolazione. **Un’accurata individuazione della classificazione è quindi alla base di una corretta fascicolazione del documento e sedimentazione del procedimento amministrativo**. Per classificare correttamente si devono prendere in considerazione diversi aspetti del contesto amministrativo del documento soggetto a registrazione, come il mittente e destinatario, l’oggetto, la modalità di trasmissione, eventuali riferimenti ad altri documenti e soprattutto il contenuto informativo del documento stesso. Ecco che un modello sviluppato a partire dalle registrazioni già effettuate e che impara direttamente dalle scelte compiute, a fronte delle possibili classificazioni suggerite, può in tempo reale elaborare il contesto amministrativo e fornire le possibili classificazioni suggerite.

Sul tema, per una soluzione di questo tipo influiscono due fattori fondamentali per la fiducia lato utente/utilizzatore: **la trasparenza**, ovvero il funzionario deve conoscere capacità e limiti della tecnologia e **l’affidabilità**, ovvero la misura in cui riesce effettivamente ad incidere sull’ efficacia ed efficienza dell’attività o procedimento amministrativo.

Un richiamo, doveroso, riguarda i **presupposti di adozione di soluzioni basate su modelli d'intelligenza artificiale nella Pubblica Amministrazione**, dati dall'applicazione dell'IA Act e della Strategia Italiana per l'Intelligenza Artificiale 2024-2026 su cui altri scrivono in modo dettagliato su questo numero.

## La fiducia nei servizi digitali lato cittadino

Dal punto di vista dei cittadini la fiducia verso l'utilizzo delle piattaforme digitali nazionali passa da diversi aspetti.

Il primo è **l'efficacia della comunicazione** sia durante l'uso di un servizio digitale, che nei suoi esiti. Il cittadino si aspetta di essere accompagnato nell'inserimento di informazioni e documenti necessari attraverso una comunicazione chiara e una fruizione semplice dei diversi passaggi, **senza che siano richiesti particolari sforzi o competenze informatiche**.

> Il linguaggio è un elemento cruciale dell'esperienza utente di un sito o servizio digitale e le linee guida di Design Italia offrono numerose indicazioni realizzative. Tale aspetto di comunicazione deve anche essere esteso ai canali di supporto agli utenti di tali servizi digitali in modo da accompagnare nell'utilizzo quanti si trovino in difficoltà. È importante avere immediata conferma delle azioni fatte usando i servizi digitali e comunicazione dei tempi e modi del procedimento.

I servizi digitali devono essere resi semplici e indipendenti dai limiti o presupposti tecnologici sottostanti. Ad esempio, se viene richiesto di inserire una **copia della carta d'identità** il servizio deve permettere di caricarla in diversi formati comuni, sia che fronte e retro siano in un singolo file, che separati; non devono esserci particolari limiti alle dimensioni del file e l'acquisizione dovrebbe essere consentita utilizzando la fotocamera o webcam del dispositivo, effettuando automaticamente le operazioni di OCR valide per precompilare i dati richiesti (Comune di emissione, data scadenza, …) e al contempo validarne quindi la leggibilità.

Le Linee guida sul punto di accesso telematico ai servizi della Pubblica  Amministrazione di AgID costituiscono un buon punto di riferimento per curare una realizzazione efficace dei servizi digitali, così come gli strumenti di Designers Italia ed in particolare quelli dedicati alla progettazione dei servizi digitali sono strumenti essenziali per un approccio efficace ai servizi digitali mirando anche a rendere uniforme l'esperienza utente.

Nel numero precedente, avevamo avuto modo di riflettere anche sull'approccio ai servizi digitali da parte dei soggetti digitali deboli e di come si stia prefigurando un ruolo di un *caregiver digitale* della centralità dell'introduzione delle deleghe nell'uso delle identità digitali e dei servizi digitali. **Sicuramente i soggetti digitali deboli sono quelli a mostrare meno fiducia nei servizi digitali stessi**.

> Un ultimo aspetto che incide sulla fiducia dei cittadini è la trasparenza nell'utilizzo dei propri dati durante l'uso dei servizi digitali. Ci si chiede "Può la mia assicurazione accedere al mio fascicolo sanitario per fare una valutazione sul rischio e quindi adeguare o meno la mia polizza? Può l'Agenzia delle Entrate valutare il mio profilo economico sulla base delle transazioni bancarie e pagamenti online? Può il mio Comune accedere al fascicolo previdenziale per fare una valutazione sulla graduatoria di particolari benefici e servizi sociali?" Molto spesso le informative dei servizi digitali sono in un linguaggio legale, più finalizzate all'assolvimento degli obblighi normativi da parte dell'erogatore del servizio digitale che per una reale trasparenza verso il cittadino.

Insomma, è chiaro che l'assenza di comunicazione e di trasparenza nelle finalità ed utilizzo dei dati può alimentare la diffidenza e fantasie sul loro utilizzo.

## Sicurezza e fiducia

I miei dati sono al sicuro? Da un certo punto di vista **il cittadino si aspetta, e basa la propria fiducia sul fatto i propri dati siano al sicuro**, dall'altro la continua crescita di attacchi cibernetici espone le piattaforme digitali ad elevati standard di sicurezza e protezione dei dati personali.

> Se qualche lettore ha infelicemente sperimentato la ricezione di comunicazioni relative al coinvolgimento dei propri dati in un data breach, avrà magari notato la scarsa trasparenza di tali comunicazioni e provato il senso di disagio nel pensare ai possibili scenari negativi dovuti alla divulgazione e all'uso che i criminali ne faranno, timore accompagnato dall'impotenza.

L'azione dell'ACN, dall'Agenzia per la Cybersicurezza Nazionale, che svolge funzioni volte a tutelare la sicurezza nazionale nello spazio cibernetico e che – ai sensi del decreto-legge n. 82/2021, rappresenta l'interlocutore unico in materia, è incessante. La **definizione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC)** con l'obiettivo di tutelare la sicurezza dello Stato e garantire un elevato livello di sicurezza cibernetica delle reti, dei sistemi informativi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato è da ricondursi al decreto-legge n. 105/2019, convertito con modificazioni dalla legge n. 133/2019, pubblicato in Gazzetta Ufficiale n. 272 del 20 novembre 2019.
L'attenzione alla sicurezza delle soluzioni e infrastrutture in uso nelle Pubbliche Amministrazioni si è consolidata con il con **Decreto Direttoriale n. 21007/24 di ACN** del 27 giugno 2024 e applicabile dal 1° agosto 2024, che **aggiorna i livelli minimi e le caratteristiche al mutato scenario di rischio e i termini legati al procedimento di rilascio delle qualifiche**.
Il Regolamento norma anche l'utilizzo delle infrastrutture di housing e i servizi di prossimità, sempre più diffusi in ragione dell'esigenza di ridurre i tempi di latenza per gli utenti finali dei servizi digitali.
Rispetto all'applicazione del Regolamento si sottolinea che **la classificazione dei dati e servizi è una responsabilità della singola amministrazione** che basandosi sui template predisposti da ACN deve valutare il livello di criticità dei dati trattati.

> Quello della corretta classificazione dei dati trattati è un passaggio fondamentale che deve essere posto in relazione con la valutazione del rischio di trattamento operata in ambito di applicazione del GDPR. In modo coerente con tale classificazione devono essere poi scelte le infrastrutture e i servizi cloud qualificati da ACN.

Si noti che il Regolamento copre in primo luogo i requisiti di sicurezza e protezione dei dati personali per le soluzioni qualificate, ma anche indirizza gli aspetti di continuità di servizio e scalabilità delle risorse.

La recente adozione della direttiva NIS 2 a livello europeo dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024. A livello nazionale la legge di delegazione europea 2023, pubblicata nella Gazzetta Ufficiale n. 46 del 24 febbraio 2024, contiene all'art. 3, **i principi e i criteri direttivi per l'implementazione della nuova disciplina**, **attribuendo elevati requisiti operativi alle pubbliche** amministrazioni ed erogatori di servizi pubblici essenziali.

In particolare, a seguito dell'approvazione della citata legge, il Governo dovrà esercitare la delega al recepimento della NIS2, mediante l'adozione di un apposito atto normativo, che andrà a sostituire il d.lgs. n. 65/2018, recante l'implementazione della prima direttiva NIS.

La normativa NIS 2 in primo luogo **elimina la distinzione tra gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (DSP), introducendo nuove categorie di operatori basate sull'importanza del servizio offerto**. Inoltre, estende gli obblighi di cybersecurity a un numero maggiore di settori e servizi considerati critici per il funzionamento socioeconomico dell'UE. Questi includono, oltre ai settori già coperti, **piattaforme di cloud computing, data center e servizi sanitari** . La direttiva stabilisce anche un quadro più dettagliato per le misure di sicurezza, richiedendo un approccio multirischio e la segnalazione tempestiva di incidenti significativi alle autorità competenti.

## Conclusioni

In questa breve raccolta di spunti di riflessione e approfondimento abbiamo visto come la fiducia nell'utilizzo dei servizi digitali tocchi una molteplicità di temi, ciascuno ampio e complesso. Altresì la fiducia nei servizi e nelle soluzioni digitali è un prerequisito fondamentale per la trasformazione e l'inserimento di nuove tecnologie a supporto dell'efficienza ed efficacia dell'azione amministrativa.