PAdvisor: un assistente intelligente per la protezione delle informazioni nella pubblica amministrazione

Alessandra De Paola[1], Salvatore Gaglio[1], Andrea Giammanco[1], Giuseppe Lo Re[1], Marco Morana[1], Claudio Ruocco[1], and Margherita Federico[2]

[1]Università degli Studi di Palermo, Dip.to di Ingegneria, *{nome.cognome}@unipa.it*
[2]IBM Italia S.p.A, Ricca IT Srl, *mfederico@it.ibm.com*

Abstract

Nel percorso verso una completa digitalizzazione dei processi legati alla Pubblica Amministrazione, l'intelligenza artificiale può svolgere un ruolo cruciale, fornendo un supporto automatico per l'analisi e l'individuazione di criticità nei processi di gestione dei dati e delle informazioni. In questo contesto, il laboratorio di Intelligenza Artificiale e Sistemi Distribuiti dell'Università degli Studi di Palermo ha avviato un progetto di ricerca che mira alla realizzazione di un assistente intelligente che, tramite le più innovative tecniche di intelligenza artificiale, supporti gli operatori umani della Pubblica Amministrazione nella valutazione dei rischi per la privacy derivante da una errata protezione delle informazioni.

1 Introduzione

Al giorno d'oggi, la Pubblica Amministrazione (PA) sta subendo una profonda trasformazione che ha come obiettivo la digitalizzazione dei suoi processi e delle informazioni trattate. La Regione Siciliana mira ad incentivare questa trasformazione grazie all'individuazione di specifiche aree di intervento nella Strategia Regionale di Innovazione per la Specializzazione, che tra i domini di interesse individua la *Smart Governance*, direttamente riconducibile all'obiettivo "Amministrazione Digitale".

Nel contesto della digitalizzazione della PA, è necessario mettere in atto opportune procedure di controllo per garantire che vengano mantenuti elevati standard di sicurezza a garanzia delle istituzioni e dei cittadini coinvolti. A questo scopo, il legislatore, tramite il regolamento 2016/679 sulla General Data Protection Regulation (GDPR), ha definito le linee guida per la gestione e protezione dei dati, individuando nel rispetto della privacy uno dei principali obiettivi da raggiungere. In questo senso, sono state individuate alcune figure nominate dalle PA (es. Data Protection Officer - DPO) il cui compito non è solo quello di controllare il rispetto dei requisiti, ma anche di fornire un supporto strategico alle decisioni per l'individuazione delle più adeguate misure attuative. Nelle PA, le procedure di salvaguardia e protezione delle informazioni rivestono un ruolo di particolare rilievo poichè devono garantire alcune imprescindibili proprietà dei dati manipolati all'interno dei diversi processi amministrativi. Inoltre, gli stessi processi e le risorse su cui agiscono devono essere protetti affinchè sia garantita la loro corretta esecuzione e la legittimità degli accessi alle risorse, nel rispetto del principio del privilegio minimo

Obiettivo di alcune delle attività in corso presso il laboratorio di Intelligenza Artificiale e Sistemi Distribuiti dell'Università degli Studi di Palermo è la progettazione e realizzazione di un assistente intelligente (PAdvisor) a supporto degli operatori umani. PAdvisor sfrutterà le più recenti ed innovative tecniche di intelligenza artificiale per valutare i rischi derivanti da una errata protezione delle informazioni e suggerire l'adozione delle più adeguate misure di contrasto. Il raggiungimento di tale obiettivo consentirà di portare una rilevante innovazione tecnologica nell'ambito della *Smart Governance*, abilitando una sicura e affidabile transizione verso la piena digitalizzazione dei processi della pubblica amministrazione.

Per la realizzazione di tale strumento, saranno progettati opportuni modelli che consentano una rappresentazione dei processi aziendali, delle tecniche adottate per la protezione delle informazioni e dei rischi conosciuti. La conoscenza così rappresentata costituirà la *Knowledge Base* del sistema intelligente, congiuntamente ad altre informazioni non strutturate, come ad esempio quelle insite nella normativa vigente e nei documenti di *best practices*.

L'applicazione di tecniche cognitive proprie dell'intelligenza artificiale a questo vasto insieme di informazioni consentirà di individuare le diverse criticità rispetto alla protezione delle informazioni e dei processi e di suggerire le migliori contromisure. L'interazione dell'assistente intelligente con l'utente finale sfrutterà avanzate tecniche di elaborazione del linguaggio naturale, con l'obiettivo di ridurre il gap causato dal *digital divide* e di consentire l'uso del sistema anche ad utenti non esperti nell'uso delle tecnologie ICT. Inoltre, tramite l'adozione di algoritmi di *machine learning*, il sistema sarà in grado di apprendere ad ogni interazione e migliorare i propri processi cognitivi in modo proattivo.

L'assistente intelligente sarà fruibile in modalità Cloud, attraverso dispositivi eterogenei (anche mobili), consentendo alla PA di ridurre i costi necessari alla realizzazione e al mantenimento dell'infrastruttura ICT. Saranno in particolare utilizzate le tecnologie ICT messe a disposizione dalla piattaforma IBM Watson.

2 Stato dell'arte

L'analisi di dati strutturati e non provenienti da diverse fonti, la digitalizzazione dei processi amministrativi, la ricerca e catalogazione di eventi di sicurezza, ed il *cognitive computing* per la creazione di una *knowledge base* da interrogare attraverso il linguaggio naturale, rappresentano alcune delle più interessanti frontiere dei sistemi ICT di *Data Analytics*. Questo tipo di sistemi, che ha trovato impiego in diversi scenari applicativi, non è mai stato applicato nel settore della *Smart Governance* per il supporto alle decisioni e la gestione del rischio. L'approccio tecnologico che si intende adottare è stato prelimarmente validato nella letteratura scientifica, che fornisce una chiara *proof-of-concept* dell'utilizzo delle tecnologie cognitive per l'individuazione delle vulnerabilità (si vedano ad esempio i lavori descritti in [Rao *et al.*, 2016; Chung *et al.*, 2014; Lourdes *et al.*, 2015]). In particolare, il progetto qui descritto mira ad utilizzare i servizi cognitivi messi a disposizione dalla piattaforma cloud di IBM Watson, che ha mostrato la sua piena maturità in altri ambiti, ma non è mai stata applicata per il raggiungimento degli scopi di questo progetto.

3 Rappresentazione della conoscenza

L'assistente intelligente dovrà sfruttare un'adeguata rappresentazione della conoscenza del dominio in cui si troverà ad agire. In particolare, per raggiungere gli scopi del progetto qui descritto sarà necessario modellare in maniera accurata i processi della PA relativi all'acquisizione, alla memorizzazione e al trattamento delle informazioni. Sarà necessario progettare dei modelli di rappresentazione dei processi che consentano di distinguere le singole attività che costituiscono il processo, e i vincoli logici e le relazioni esistenti tra queste attività. Poichè uno degli scopi principali del sistema è la verifica della correttezza di tutti gli attori coinvolti nella gestione dei dati, sarà necessario supportare la modellazione dei diversi attori e il loro grado di coinvolgimento nelle attività. Infine, con lo scopo di abilitare la possibilità di svolgere un ruolo attivo di supporto alle decisioni, sarà necessario prevedere delle modalità di rappresentazione dei nodi decisionali presenti nei diversi processi, consentendo di esplicitare le ricadute che ogni decisione intrapresa potrà avere sulle diverse proprietà dei dati e delle informazioni trattate.

La *Knowledge Base* che sarà sfruttata dall'assistente intelligente, oltre a contenere questa conoscenza strutturata, conterrà grandi moli di informazioni non strutturate, costituite ad esempio dalla normativa vigente, da documenti di *best practices*, e da documenti testuali che descrivono procedure e processi interni alla PA.

4 Analisi delle criticità e interfaccia cognitiva

Uno degli obiettivi è la definizione di opportuni algoritmi in grado di individuare vulnerabilità per la privacy a partire dalla modellazione esplicita e strutturata dei processi coinvolti nel trattamento delle informazioni, valutando sia la probabilità che l'entità del rischio rispetto agli obiettivi di sicurezza del sistema. L'assistente intelligente sfrutterà i servizi messi a disposizione dalla piattaforma IBM Watson per comprendere ed interpretare la conoscenza non strutturata disponibile nella base di conoscenza.

Tali servizi costituiranno inoltre la base per la progettazione dell'interfaccia cognitiva dell'assistente intelligente, attraverso cui l'utente potrà porre quesiti in linguaggio naturale. Le domande poste saranno interpretate al fine di individuare elementi utili per guidare l'analisi della grande mole di dati non strutturati ed eterogenei, e per individuare elementi utili per fornire una risposta all'utente.

Al termine di ogni interazione, l'utente potrà fornire un feedback relativo alla qualità del supporto ricevuto. Tale informazione sarà utilizzata in un processo di addestramento continuo che consentirà all'assistente intelligente di apprendere dall'esperienza passata.

5 Scenari di validazione

Si prevede di validare il sistema in due differenti scenari applicativi della PA, ed in particolare nell'ambito sanitario ed in quello universitario. Le diverse caratteristiche di tali scenari applicativi consentiranno di verificare la generalità della soluzione proposta e la possibile applicazione in contesti differenti, caratterizzati da criticità eterogenee. In particolare, in ambito sanitario, servizi complessi quali ad esempio la telemedicina e la cura/ospedalizzazione domiciliare, sono basati su processi specifici in cui il trattamento dei dati può avvenire in luoghi differenti, e sotto la responsabilità di differenti attori. D'altra parte, in ambito universitario esistono processi di elevata complessità relativi alla gestione delle carriere degli studenti e dell'intera macchina amministrativa, che comportano una diversa gamma di rischi. In tale dominio, l'assistente intelligente saprà individuare soluzioni adeguate con costi commisurati al valore del rischio stimato.

Riferimenti bibliografici

[Chung *et al.*, 2014] Wingyan Chung, Albert Chan, Daniel Plante, Ray Villalobos, e Joseph Woodside. Intelligence and security informatics: developing curricular modules in context. In *Proceedings of the 45th ACM technical symposium on Computer science education*, pages 708–709. ACM, 2014.

[Lourdes *et al.*, 2015] Gino D Lourdes, Dheeraj Gurugubelli, e Marcus Rogers. A tool for interactive visual threat analytics and intelligence, based on opensoc framework. In *Proceedings of the 16th Annual Information Security Symposium*, page 33. CERIAS-Purdue University, 2015.

[Rao *et al.*, 2016] Josyula R Rao, SN Chari, D Pendarakis, Reiner Sailer, M Ph Stoecklin, Wilfried Teiken, e Andreas Wespi. Security 360°: Enterprise security for the cognitive era. *IBM Journal of Research and Development*, 60(4):1–1, 2016.