CODIRP
Confederazione Dirigenti della Repubblica

Per il MINISTRO PER LA PUBBLICA AMMINISTRAZIONE

PROPOSTE PER IL PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR)

SCHEDA 3 di 7

CLOUD E DIGITALE

Riprendendo le proposte di carattere generale ed organizzativo focalizziamo ora l'obbiettivo su innovazione e digitalizzazione

L'Europa ha posto la transizione digitale equa e sostenibile come uno dei principali obbiettivi del Recovery Plan e del Next Generation EU.

Sul tema della digitalizzazione, come si è detto nella parte generale ed organizzativa, la proposta è quella di costituire un cloud nazionale pubblico utilizzando le risorse già esistenti nella pubblica amministrazione italiana, incrementandole.

L'idea è di costruire una piattaforma unica italiana integrata al modello europeo su server pubblici gestiti dal CINECA e da altri consorzi universitari.

L'utilizzo di server di proprietà pubblica, costruendo in proprio la piattaforma tecnologica presenta notevoli vantaggi rispetto ad una mera acquisizione della tecnologia sul mercato:

- la costruzione in proprio della tecnologia trasforma la leva finanziaria in leva tecnologica;
- permette l'eliminazione del rischio c.d. di *vendor lock* in, cioè la creazione di un rapporto di dipendenza col fornitore del servizio;
- rende facilmente attuabile l'interoperabilità dei servizi, sia tra PP.AA., sia tra P.A. e privati, con apertura del mercato alle Piccole e Medie Imprese (PMI);
- consente una fattiva protezione dei dati restando la PA titolare degli stessi;
- permette di affidare lo sviluppo delle app anche a studenti o start up universitarie e altre piccole imprese;
- i server possono essere utilizzati non solo per ospitare la banca dati della pubblica amministrazione, costituita secondo il principio del *once only*, ma di utilizzarne la potenza di calcolo per progetti di ricerca scientifica (*grid*

computing) o per ospitare uno spazio virtuale commerciale a favore delle piccole imprese;
- l'utilizzo di app pubbliche e piattaforme dedicate permetterebbe l'eliminazione dei costi degli intermediari e la possibilità di far conoscere anche piccole realtà, altrimenti sconosciute.

Per quanto riguarda il commercio on line questa piattaforma pubblica messa a disposizione delle piccole imprese (agricole, artigianali, del turismo ecc.) permetterebbe di avere una piazza virtuale, con bancarelle virtuali, per il commercio on line di prodotti legati all'artigianato e agricoltura del territorio (e-commerce a km zero).

A questo scopo potrebbero essere coinvolta la rete delle camere di commercio che hanno già nelle loro banche dati tutte le informazioni necessarie.

Una volta che si sia costruito un modello organizzativo basato sulla architettura delle *blockchain*, come sopra richiamato, si potranno attuare progetti di più ampio respiro della semplice digitalizzazione degli attuali processi amministrativi.

Nelle *blockchain* le informazioni vengono registrate e distribuite tra più nodi per garantire sicurezza informatica e resilienza. Le decisioni vengono trascritte in registro pubblico non modificabile senza il consenso della rete, questo consente la trasparenza e la tracciabilità delle decisioni.

L'utilizzo delle *blockchain* permette di scambiare documenti ed informazioni tra le pubbliche amministrazioni ed il cittadino rivoluzionando il concetto di "certificato".

Il suo impiego nell'ambito dell'anagrafe, per esempio, sarebbe in grado di garantire l'inalterabilità dei dati relativi alla nascita del bambino/a oltre che una riduzione dei tempi per il disbrigo delle pratiche.

La *blockchain* è una architettura primariamente organizzativa più che tecnologica, L'Economist la definisce the trust machine cioè la macchina della fiducia, per enfatizzare la possibilità che, all'interno di un'architettura distribuita e decentralizzata (dove tutti possono verificare e dove nessuno da solo detiene il potere del controllo) ci si possa fidare di più. Per questa (astratta) attitudine, la *blockchain* viene vista come lo strumento capace di sostenere la lotta alla corruzione, combattere traffici illegali, avviare processi virtuosi di lotta alla povertà e molto altro.

La validazione su *blockchain* aggiunge un ulteriore livello di sicurezza ai sistemi di firma digitale e biometrica.

Tra le priorità di investimento del Recovery Plan c'è senza ombra di dubbio anche la digitalizzazione degli appalti. La digitalizzazione deve andare di pari passo con il rafforzamento della Banca dati nazionale dei contratti pubblici presso ANAC. Sono strumenti indispensabili per garantire efficienza e trasparenza della spesa.

La gestione degli appalti digitalizzata garantirebbe da un lato maggiore celerità e dall'altro trasparenza degli affidamenti. Questo obiettivo è già previsto dalle direttive UE in tempi stretti, con verifiche di attuazione già nel 2023.

Si può pensare all'utilizzo delle *blockchain* anche in questo ambito, partendo dalla citata revisione della banca dati nazionale degli appalti, operativa presso l'ANAC. Con la *blockchain* si potrebbe monitorare la velocità della spesa, limitare gli appesantimenti burocratici a carico delle PP.AA. rendendo possibile l'attività di verifica dei requisiti dichiarati dai concorrenti. In tal modo le amministrazioni potrebbero concentrarsi solo sulle strategie di acquisto con eliminazione del contenzioso.

L'utilizzo della *blockchain* comporterebbe l'obbligo di sottostare a standard di controllo rigidi che assicurino il dato. Dati corretti aumenterebbero il valore delle imprese, che partecipano alle gare di appalto, o ancora nel turismo delle imprese che offrono servizi al cittadino e così via nei diversi settori, dove la PA potrebbe avere un ruolo fondamentale (si pensi che la Svizzera in poco più di un anno è diventato un hub europeo)

Utilizzando apposite piattaforme si potrebbe tracciare l'intero processo produttivo del Made in Italy, con benefici al "marchio Italia" costituito dalle piccole imprese.

DIGITALIZZAZIONE IN SANITA'

Robotica ed intelligenza artificiale sono considerate tra le tecnologie emergenti destinate a trasformare il mondo in generale, e la sanità in particolare, nei prossimi anni. Basta leggere Pubmed per trovare un numero elevatissimo di articoli indicizzati (87.600) con la parola chiave "intelligenza artificiale" e questa, in ambito sanitario, viene già utilizzata come supporto per le decisioni cliniche. Archivi digitali delle immagini radiografiche, linee guida, registri elettronici, materiale di ricerca, studi clinici. L'intelligenza artificiale pone anche potenziali conseguenze devastanti per la società in termini di tutela della sicurezza e della privacy. L'Unione Europea, non a caso ha emanato nuove linee guida sull'etica dell'intelligenza artificiale e sulla privacy.

L'Autorità Garante per la protezione dei dati personali nella Relazione sull'attività svolta nel 2018 ha affermato:

«*Il 2018 è stato definito, l'anno peggiore relativamente alla sicurezza cibernetica, così costantemente esposta a minacce da configurare una sorta di cyber-guerriglia permanente. In ambito sanitario l'incremento ha toccato l'acme del 99% rispetto all'anno precedente, con effetti tanto più gravi che in altri settori perché l'alterazione dei dati sanitari può determinare errori diagnostici o terapeutici. La protezione dei dati è un fattore determinante di efficienza*

sanitaria, funzionale anche alla correttezza del processo analitico fondato su big data.»

Il Comitato Nazionale di Bioetica, in un documento del gennaio del 2017, sollecitava l'elaborazione di una normativa per la protezione dei dati personali e la tutela dei cittadini/utenti da rischi sociali dell'abuso dei dati. Vi si affermava che le tecnologie informatiche possono presentare dei rischi che riguardano soprattutto il trattamento e la protezione della vita privata e dei dati a carattere personale, la trasparenza, la qualità dell'informazione, la dipendenza, il principio di giustizia partecipativa e la governance. Il problema consiste non tanto nell'uso dei dati, quanto piuttosto nell'uso "appropriato" dei dati per il bene dell'uomo e della sua salute. L'obiettivo dovrebbe essere quello di coinvolgere attivamente gli utenti e consentire la presa di coscienza critica dei problemi etici emergenti delle nuove tecnologie. Bisogna sollecitare il MIUR a redigere e diffondere nelle scuole Linee Guida per un corretto uso delle tecnologie sociali. In una parola bisogna investire ricerca sui sistemi bioeticamente compatibili.

Se pensiamo alla sanità come spesa è indubbio che la trasformazione digitale sia un'opportunità di diminuzione della spesa, che taluni quantificano nel 5%. Le nuove tecnologie permettono di agevolare la competitività e l'efficienza del sistema, sempre che tutto ciò sia equamente diffuso, altrimenti le diseguaglianze già presenti provocherebbero un allargamento della forbice sociale. Un patrimonio informatico può migliorare la programmazione sanitaria e favorire la prevenzione, che riduce la spesa, ma anche la diagnosi e la cura delle malattie. Ma è soprattutto il confronto dei dati clinici il grande vantaggio.

Si parla sempre più di "digital health" salute digitale. Telemedicina, fascicolo sanitario elettronico, ricetta elettronica, referti inviati per via informatica, sono strumenti che permettono un trattamento sempre più personalizzato ma a patto che la consapevolezza dei propri ruoli sia alla base di un corretto rapporto. Può certamente migliorare il rapporto medico paziente, ma non è facile parlare con pazienti che entrano nell'ambulatorio con domande, supposte diagnosi e soprattutto terapie, lette e suggerite sul web. La rete diventa l'informatore privilegiato e, di conseguenza, quello con lo specialista medico rischia di diventare un contenzioso dialettico tra sordi. Spesso si finiscono per ascoltare più voci rischiando un labirinto di incertezze. Quando uscirono anni fa le enciclopedie mediche assistemmo allo stesso problema, diffusione di conoscenze aspecifiche a chi non poteva avere la capacità di selezionarle. Oggi la digitalizzazione ha esasperato il problema ed il medico si vede spesso costretto a difendere le proprie scelte in una confutazione che non ha nulla di scientifico. Uno scenario potenzialmente migliore ma a rischio per "l'incultura" del paziente.

Non vogliamo e non possiamo ostacolare il progresso, ma non vogliamo essere sostituiti dal mezzo elettronico. L'intelligenza artificiale non può essere

combattuta ma deve essere utilizzata, essere un mezzo, uno strumento per migliorare la professione medica. Ma non vogliamo che un robot faccia diagnosi dopo che sono stati inseriti migliaia di casi clinici nella sua memoria. Non vogliamo che un computer esprima il suo referto su immagini TC dopo che sono stati inseriti nel suo data base milioni di possibilità. Non vogliamo che, inseriti target e dosi limite, sia il robot che decida come conformare un piano di radioterapia per un paziente oncologico.

Per quanti dati si possano inserire, nessun caso sarà mai uguale ad un altro. Anche con la stessa malattia esistono presentazioni diverse. Il cervello umano non è sostituibile perché si basa sul vissuto, sull'esperienza, sull'essere singolo. Nessun cervello artificiale può sostituirsi all'uomo. L'uomo immette i dati ma il ragionamento è ben diverso dall'analisi di una sommatoria di input. C'è un'etica, una filosofia che non potranno mai essere introdotti in una macchina. Parliamo sempre più di personalizzazione della medicina ed allora la standardizzazione della macchina non può essere la soluzione!

Il settore della sanità è uno dei più a rischio per la possibilità di rubare i dati dei pazienti ed è quello maggiormente esposto agli attacchi informatici. La sanità è un obiettivo che fa gola perché estremamente redditizio per il mondo del cybercrimine. I sistemi operativi della maggior parte delle strutture sanitarie è vulnerabile. Nel mirino sono gli apparecchi elettromedicali, perché i dati generati da ogni dispositivo, pensiamo solo agli apparecchi per imaging, hanno un grado di attendibilità ed un valore molto elevato. I dati ripuliti possono tornare nel circuito ufficiale rielaborati sotto forma di statistiche sanitarie. Come se non bastasse la "profilazione" degli utenti, ora anche i nostri dati sanitari raccolti dai dispositivi medici diventano una miniera d'oro. E la privacy? Purtroppo non c'è violazione perché il dato generato dall'apparecchio è anonimo. Certo sono immagini apocalittiche ma hackerando una pompa di insulina, un pacemaker si potrebbe commettere un delitto. Si possono fare ricette elettroniche false, falsi certificati telematici di invalidità.

L'Italia ha elaborato linee guida, in conformità con l'Europa per gestire gli attacchi informatici nelle sue attività "vitali" pubbliche e private, inclusa la sanità. Questo, dopo aver recepito il 16 maggio scorso la direttiva NIS, Network and Information Security, dell'Unione Europea. Coordinati dal Dipartimento informazioni e sicurezza della Presidenza del Consiglio, i ministeri di Sviluppo, Trasporti, Economia, Salute ed Ambiente, autorità competenti all'attuazione della normativa Ue, hanno elaborato le misure con le Regioni. Obiettivo: gestire i rischi e prevenire/mitigare degli incidenti con impatto rilevante su continuità e fornitura dei servizi essenziali. In Italia nel 2018 per la prima volta si è saputo di 17 «incursioni» ai danni di siti di ospedali e Asl perché «rivendicati» dagli attivisti di Anonymous: è solo la punta di un iceberg. Il Rapporto Clusit 2019 di Bicocca sulla sicurezza ICT (Information and Communications Technology), ha confermato l'esplosione di cyberattacchi, e

in particolare di ransomware (39% degli attacchi), software malevoli usati per estorsioni online che bloccano le strutture colpite. Dalla sottrazione di dati sensibili al loro uso contro strutture o pazienti per ricattarli, dall' interruzione di servizi essenziali, all'attacco personale a un paziente collegato a un dispositivo come nei film di fantascienza, tutti i rischi sono da considerare La sicurezza è spesso vista come un fatto solo tecnologico di competenza dell'Ict, ma in realtà, siccome l'informatica interessa da vicino i processi clinico ed assistenziale, dipende sempre più dalla connessione tra aspetti informatici ed organizzativi, dalla disponibilità di dati corretti ed affidabili e dalla presenza di funzionalità volte a supportare interamente e con continuità i processi. I sistemi informativi di aziende sanitarie pubbliche e private sono in massima parte strutturati come insiemi di applicazioni eterogenee e basate su tecnologie diverse, è quindi complesso assicurare livelli di sicurezza omogenei ed adeguati. Urge una visione del sistema informativo integrata con l'organizzazione dei servizi, in un'ottica di "gestione del processo" e di "governo del dato". Regolamenti come NIS e GDPR vanno nella giusta direzione.

Occorre anche procedere alla riorganizzazione dei percorsi attuali per il riconoscimento dei benefici correlati alla disabilità.

A oggi, c'è una duplicazione di percorsi amministrative e medico-legali che determina un appesantimento burocratico.

Una rete che connetta tutte le Amministrazioni coinvolte determinerebbe lo snellimento delle fasi sia amministrative che medico-legali e la massima trasparenza con razionalizzazione delle risorse.

Inoltre, bisogna considerare che la semplificazione dell'accertamento della condizione di disabilità produrrebbe enormi vantaggi per una fascia di popolazione particolarmente fragile.

Roma, 21 marzo 2021

Il Segretario Generale
Tiziana Cignarelli