TIG THE INNOVATION GROUP

MARZO 2025

IL CAFFÈ DIGITALE

SERVIZIO CLIENTI: L'AI È UNA GRANDE RISORSA, MA ATTENZIONE A USARLA BENE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON…

Ranieri Razzante,
docente universitario specializzato in gestione del rischio di riciclaggio e cybersecurity

LA TRASFORMAZIONE DIGITALE

Tecnologie quantistiche e big tech: a che punto siamo davvero?

NUMERI E MERCATI

Servizi digitali e infrastrutture fisiche fanno evolvere le PA locali

SOMMARIO

L'EDITORIALE
3 Servizio clienti: l'AI è una grande risorsa, ma attenzione a usarla bene
Valentina Bernocco

A COLAZIONE CON
5 Mafie digitali: l'utilizzo criminale di AI, social e dark web
Elena Vaciago

LA TRASFORMAZIONE DIGITALE
7 Accessibilità digitale: perché è fondamentale per un web davvero inclusivo
Valentina Usellini

LA TRASFORMAZIONE DIGITALE
8 Tecnologie quantistiche e big tech: a che punto siamo davvero?
Gianluca Dotti

CYBERSEC E DINTORNI
10 Sanità italiana nel mirino degli hacker: l'opportunità della direttiva NIS2
Elena Vaciago

DIRITTO ICT IN PILLOLE
12 Piano ispettivo primo semestre 2025: su quali ambiti si concentreranno gli accertamenti del Garante
Valentina Frediani

NUMERI E MERCATI
14 Servizi digitali e infrastrutture fisiche fanno evolvere le PA locali
Camilla Bellini

Servizio clienti: l'AI è una grande risorsa, ma attenzione a usarla bene

Valentina Bernocco, *Web and Content Manager*
TIG - The Innovation Group

Quella del **customer service** – non è un mistero – è una delle aree in cui l'**intelligenza artificiale** sta trovando e troverà maggiore applicazione. Molte le sue incarnazioni: assistenti virtuali più o meno evoluti, sistemi di ticketing basati su AI, strumenti di analisi del sentiment e dei feedback dei consumatori, e ancora sistemi di raccomandazione, software di automazione delle procedure e "agenti", cioè sistemi di Agentic AI, capaci di svolgere in totale autonomia alcune procedure e azioni.

Secondo le stime di ResearchAndMarkets, l'anno scorso il mercato delle **soluzioni di AI per il servizio clienti** ha superato i 12 miliardi di dollari di valore e arriverà a **47,8 miliardi di dollari nel 2030**. Tra i principali player spiccano Microsoft, Ibm, Google, Amazon Web Services, Salesforce, Atlassian, ServiceNow, Sap e Zendesk. Un sondaggio di Gartner, realizzato l'estate scorsa su 187 aziende, suggerisce invece che quest'anno il 44% delle realtà del campione sperimenterà l'uso di un *voicebot*.

Per quanto riguarda la nuova frontiera dell'Agentic AI, le previsioni sono incoraggianti: sempre a detta di Gartner, **entro il 2029** gli agenti di AI potranno gestire e risolvere **l'80% delle problematiche di servizio clienti più comuni,** senza alcun intervento umano. Ciò permetterà alle aziende di ridurre, mediamente, del 30% i costi operativi del servizio clienti. *"L'Agentic AI cambia le regole del gioco nel servizio clienti, spianando la strada a esperienze clienti autonome e a sforzo minimo"*, ha commentato **Daniel O'Sullivan**, senior director analyst della Customer Service & Support Practice di Gartner. "*A differenza degli strumenti di GenAI tradizionali, che semplicemente assistono gli utenti fornendo informazioni, l'Agentic AI risolverà proattivamente le richieste di servizio per conto dei clienti, aprendo una nuova era per l'ingaggio dei consumatori*".

Il servizio clienti è un terreno fertile per l'intelligenza artificiale, per diverse ragioni. In questo campo, più che altrove, l'AI può essere addestrata su una grande quantità di dati che nel customer service solitamente abbondano, generati da più fonti, eventi, interazioni. Grazie alle sue capacità di automazione, l'AI può accorciare i tempi del servizio clienti e a differenza degli umani è sempre operative, senza pause, notti o weekend. Il cerchio si chiude nelle attività di marketing, che grazie ai dati transitati dai chatbot di assistenza ai clienti o da altri sistemi di AI possono trarre (magari proprio grazie all'AI) insight preziosi, e su questa base differenziare e personalizzare le comunicazioni.

L'intelligenza artificiale sembra non dispiacere nemmeno ai consumatori. In uno studio di ServiceNow di un anno fa (quando ancora non si parlava di Agentic AI) il 62% degli italiani intervistati diceva di considerare i chatbot

Image by upklyak on Freepik

come un servizio importante che le aziende devono offrire e solo il 21% affermava di non fidarsi della correttezza della risposte fornite dall'AI.

Tutti felici? Sorge spontanea la domanda: l'uso o l'abuso dell'intelligenza artificiale non rischia di togliere, anziché aggiungere valore al servizio clienti? Può creare distacco, disaffezione o anche frustrazione, anziché aiutare a risolvere i problemi? Dipende, come evidenziato da una ricerca (citata dal *Corriere della Sera*) di **Andrea Ordanini**, docente di marketing and service analytics, Bnp Paribas Endowed Chair presso l'**Università Bocconi di Milano**: nelle procedure *front-end,* in cui le aziende si interfacciano direttamente con i consumatori, l'AI non è intrinsecamente utile. Lo è solo se viene accuratamente allineata alle procedure *front-end* più complesse e non automatizzabili, cioè quelle gestite da operatori di customer service umani. Inoltre, spiega ancora Ordanini, le soluzioni di AI potranno diventare sempre più efficaci e ottimizzate, ma questo significherà anche standardizzazione: sarà quindi più difficile, per le aziende, differenziare il proprio servizio clienti da quello della concorrenza. Bisognerà quindi preservare le relazioni umane, che nel customer service saranno sempre più ridotte ma anche più significative.

C'è poi un'altra considerazione da fare, che non riguarda l'efficacia dell'AI ma i suoi potenziali **impatti sull'occupazione.** Gli analisti di ResearchAndMarkets osservano, un po' vagamente, che il settore del servizio clienti "*affronta la sfida di una potenziale perdita di posti di lavoro, che potrebbe condizionare le dinamiche professionali e i tassi di adozione*". Sul tema le opinioni divergono e inoltre qualsiasi previsione rischia di diventare obsoleta rapidamente, data la velocità dell'innovazione. Uno tra gli studi più ampi e più citati è quello realizzato due anni fa da Goldman Sachs, secondo cui nel medio periodo potrebbero sparire a causa dell'intelligenza artificiale generativa circa 300 milioni di posti di lavoro (equivalente a tempo pieno), ovvero il 18% della forza lavoro mondiale. Decisamente più ottimista la visione del World Economic Forum, secondo cui le tecnologie di AI eroderanno 92 milioni di posti di lavoro da qui al 2030 ma ne creeranno 170 milioni. D'altro canto nel report "Future of Jobs" del Wef la professione dell'addetto al servizio clienti viene inserita tra i "ruoli in declino" da qui ai prossimi anni.

Quantificare tutti questi impatti non è semplice, il rischio è sempre un po' quello di oscillare tra visioni apocalittiche ed entusiasmi forse eccessivi, e inoltre non possiamo sapere quale sarà la prossima innovazione dirompente dietro l'angolo. Si sente spesso dire (dai vendor soprattutto, ma anche dagli analisti) che le nuove forme di intelligenza artificiale come la GenAI hanno un ritorno sull'investimento rapido, perché per un'azienda può essere sufficiente acquistare un servizio cloud già pronto all'uso o anche solo aggiornare un software all'ultima versione. Ovviamente esistono altre casistiche, per esempio situazioni in cui l'azienda voglia addestrare o perfezionare un modello di AI con i propri dati. E la vera impresa è riuscire a integrare l'AI nei processi di lavoro esistenti, o magari ridefinire questi ultimi.

Ma concediamo all'intelligenza artificiale il vantaggio di avere un ROI veloce e, probabilmente, dei risultati tangibili sulla produttività: resta comunque da capire quali saranno **i ritorni nel lungo periodo** e forse, azzardiamo, gli impatti sociologici dell'AI. Per i consumatori diventerà sempre più difficile riuscire a parlare con qualcuno, avere dall'altra parte della chat o del telefono una persona reale, senza dover transitare dagli strumenti di automazione che le aziende tenderanno a proporre? Tutti conosciamo la frustrazione di attendere in linea per minuti che sembrano ore, con una registrazione in sottofondo, prima di riuscire a parlare con un operatore. L'AI dovrà servire innanzitutto a evitare questa frustrazione, e quindi la disaffezione del cliente, senza però imporsi come un muro che separa le persone, i consumatori dalle aziende.

Mafie digitali: l'utilizzo criminale di AI, social e dark web

Elena Vaciago, *Research Manager*
TIG - The Innovation Group

Le organizzazioni criminali stanno sfruttando le nuove tecnologie, dall'intelligenza artificiale alle criptovalute, per potenziare le loro attività illecite. La criminalità organizzata utilizza il dark web, il riciclaggio automatizzato e persino l'AI per il reclutamento e la propaganda. Le istituzioni stanno reagendo, ma tra carenze di risorse e normative frammentate, la sfida resta complessa. Servono più investimenti e una cooperazione internazionale efficace per contrastare questi fenomeni.
Riportiamo l'intervista su questo tema con **Ranieri Razzante, Docente universitario specializzato in gestione del rischio di riciclaggio e cybersecurity,** già Componente del Comitato per l'AI, Presidenza del Consiglio Speaker del Cybersecurity Summit 2025, il 19 e 20 marzo a Milano.

TIG. Nel suo ultimo libro "Algoritmo criminale", lei analizza il legame tra criminalità e nuove tecnologie. Cosa sappiamo di questo rapporto?

Ranieri Razzante. Le mafie sono avanti a noi di almeno 15 anni nell'uso del web e dell'intelligenza artificiale. Operano online da molto prima di noi e dispongono di tecnici specializzati, sia interni sia reclutati dall'estero. Attualmente è in corso una fase di reclutamento di hacker e di affinamento delle strategie per consolidare la loro presenza nello spazio digitale. Questo fenomeno è spesso sottovalutato a livello internazionale, poiché si continua a pensare a una "Mafia 2.0" senza coglierne l'evoluzione. In realtà, le mafie dimostrano una grande lungimiranza: operano nel web da almeno 15 anni, utilizzano le criptovalute e sfruttano il dark web per i loro traffici, allo scopo di ridurre i tempi di infiltrazione nell'economia legale.

TIG. L'utilizzo delle nuove tecnologie da parte della criminalità è dunque molto maturo. E per quanto riguarda l'intelligenza artificiale? Quali potrebbero essere le conseguenze del suo impiego?

Ranieri Razzante. L'AI triplica le potenzialità di attacco e infiltrazione, riducendo il bisogno di hacker, poiché consente di automatizzare molte attività. Questo significa che la facilità di penetrazione nel web e la capacità di commettere reati e riciclare denaro sono almeno raddoppiate. Il principale pericolo legato all'uso dell'AI è proprio questo. Le mafie, infatti, non conducono direttamente attacchi informatici, ma li subappaltano, utilizzandoli per acquisire visibilità e rafforzare la loro presenza sul territorio.
Uno degli aspetti più preoccupanti riguarda il reclutamento delle nuove generazioni. Sui social media circolano video manipolati con l'AI che esaltano l'appartenenza a gruppi criminali, diffondendo modelli devianti. Studi condotti dalla Fondazione Magna Grecia (in particolare, il rapporto "Le mafie al tempo dei social" scaricabile online) evidenziano come le mafie sfruttino i social per attrarre nuovi affiliati, attraverso immagini e chat che ne esemplificano le dinamiche.
Purtroppo, la nostra capacità di reazione non è

comparabile alla velocità con cui questi contenuti sono diffusi. Sarebbe auspicabile un impiego dell'AI in chiave difensiva, per potenziare le capacità di risposta e di contrattacco, anche derogando alla privacy dei criminali quando necessario. Tuttavia, attualmente siamo vincolati da limiti normativi, come quelli previsti dall'AI Act, che non facilitano questo tipo di interventi.

TIG. Riciclaggio e finanza illecita: l'AI può diventare un'alleata nel contrasto al riciclaggio di denaro? Quali sono gli strumenti più promettenti?

Ranieri Razzante. Sì, si stanno sperimentando applicazioni virtuose dell'AI nella lotta al riciclaggio, in particolare per l'analisi delle transazioni finanziarie. L'Unità di Informazione Finanziaria (UIF), presso la Banca d'Italia, già utilizza sistemi di machine learning per monitorare grandi volumi di operazioni, prevalentemente lecite, ma in cui è possibile individuare tempestivamente anomalie sospette.
L'AI è già impiegata nella rilevazione preventiva di schemi illeciti e fenomeni atipici nei conti bancari e nei circuiti finanziari. Successivamente, l'attività di contrasto è svolta dalle forze dell'ordine e dagli organi investigativi. In Italia, strumenti come l'Anagrafe dei rapporti finanziari e l'Anagrafe immobiliare sono già operativi. Inoltre, la Guardia di Finanza ha recentemente introdotto "Molecola", un software basato su AI capace di analizzare miliardi di dati in fase investigativa.
Da questo punto di vista, possiamo dire di essere all'avanguardia: i risultati nel contrasto al riciclaggio e al finanziamento illecito, incluso quello a fini terroristici, sono promettenti.

TIG. Come le criptovalute e la finanza decentralizzata stanno influenzando le attività di riciclaggio e finanziamento illecito?

Ranieri Razzante. Le mafie operano sempre più in maniera decentralizzata, sfruttando i vantaggi offerti dalle nuove tecnologie finanziarie, come costi ridotti e rapidità nei trasferimenti di denaro. Le criptovalute, in particolare, pur essendo strumenti leciti, mancano ancora di una regolamentazione adeguata, il che le rende appetibili per la criminalità organizzata.
Da almeno 15 anni, le organizzazioni mafiose le utilizzano sistematicamente, e rappresentano ad oggi l'unico strumento per il pagamento dei riscatti in caso di attacchi ransomware. La mancanza di una tracciabilità immediata su questi flussi finanziari è una delle principali criticità, ed è urgente intervenire con normative adeguate a regolamentare questo ambito.

Leggi l'intervista completa a Ranieri Razzante sul canale cybersecurity di TIG.

Accessibilità digitale: perché è fondamentale per un web davvero inclusivo

Valentina Usellini, *General Manager*
TIG Factory

Oggi si parla spesso di inclusione, ma troppo spesso questa parola resta confinata a slogan e buone intenzioni. L'inclusione vera significa creare ambienti, anche digitali, in cui le differenze siano accolte e valorizzate, offrendo a tutti pari opportunità e diritti. Questo vale anche — e soprattutto — per il web.
Informarci, acquistare beni e servizi, prenotare prestazioni mediche o accedere a servizi digitali sono attività che dovrebbero essere quotidianamente garantite a tutti, senza distinzioni. Purtroppo non è sempre così se consideriamo i milioni di siti web che presentano errori di accessibilità ostacolando o impedendo l'accesso alle persone con disabilità.

Come si può intervenire per abbattere queste barriere e favorire l'inclusività digitale?
In TIG Factory partiamo dal **Design System**: un insieme di regole, componenti e linee guida che definiscono l'aspetto e il funzionamento di un sito web fin dalle prime fasi della progettazione. Adottare il principio di accessibilità by design significa incorporare i requisiti di accessibilità direttamente nelle fondamenta del progetto, evitando correzioni successive spesso costose e poco efficienti.
Gli interventi si sviluppano su tre livelli fondamentali:

User Interface (UI) che riguarda l'aspetto visivo e l'interazione immediata dell'utente con il sito: Contrasto colori – Font Leggibili con spaziatura e interlinea adeguata– sfondi neutri e poco invasivi – pulsanti grandi e facilmente cliccabili
HTML e Programmazione: interventi sul codice TAG Semantici – Parametri che migliorano l'interpretazione dei contenuti (Attributi ARIA) – compatibilità con tecnologie assistive quali screen Reader e navigazione da tastiera

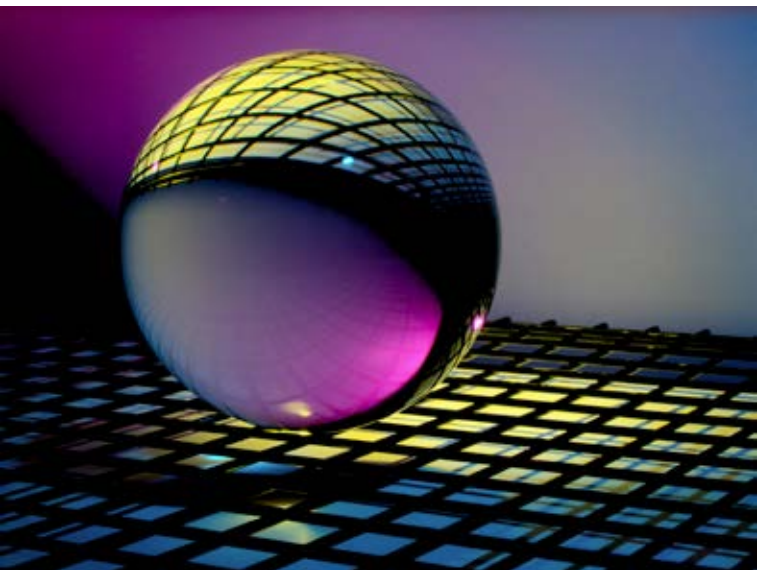
User Experience (UX) e writing semplice e intuitivo con linguaggio diretto, contenuti ben organizzati, messaggi di errore chiari

I vantaggi di un sito accessibile non riguardano solo gli utenti, ma anche i brand. Investire nell'accessibilità significa, infatti, rafforzare la reputazione aziendale e trasmettere un'immagine di attenzione, inclusione e responsabilità sociale. Inoltre, i siti accessibili tendono a essere meglio ottimizzati per i motori di ricerca, migliorando il posizionamento e aumentando la visibilità online.
Per progettare un sito davvero accessibile, è indispensabile una **formazione specifica** sulle linee guida **WCAG e AgID**. In vista delle nuove normative sull'accessibilità digitale abbiamo investito tempo e risorse affinchè il nostro team di designer, sviluppatori e content creator completassero un percorso formativo specifico.
Il risultato è che oggi in **TIG Factory** abbiamo integrato il tema dell'accessibilità a monte del processo, rendendolo parte integrante del workflow migliorando l'efficienza e garantendo i risultati attesi.

Image by Freepik

Tecnologie quantistiche e big tech: a che punto siamo davvero?

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group



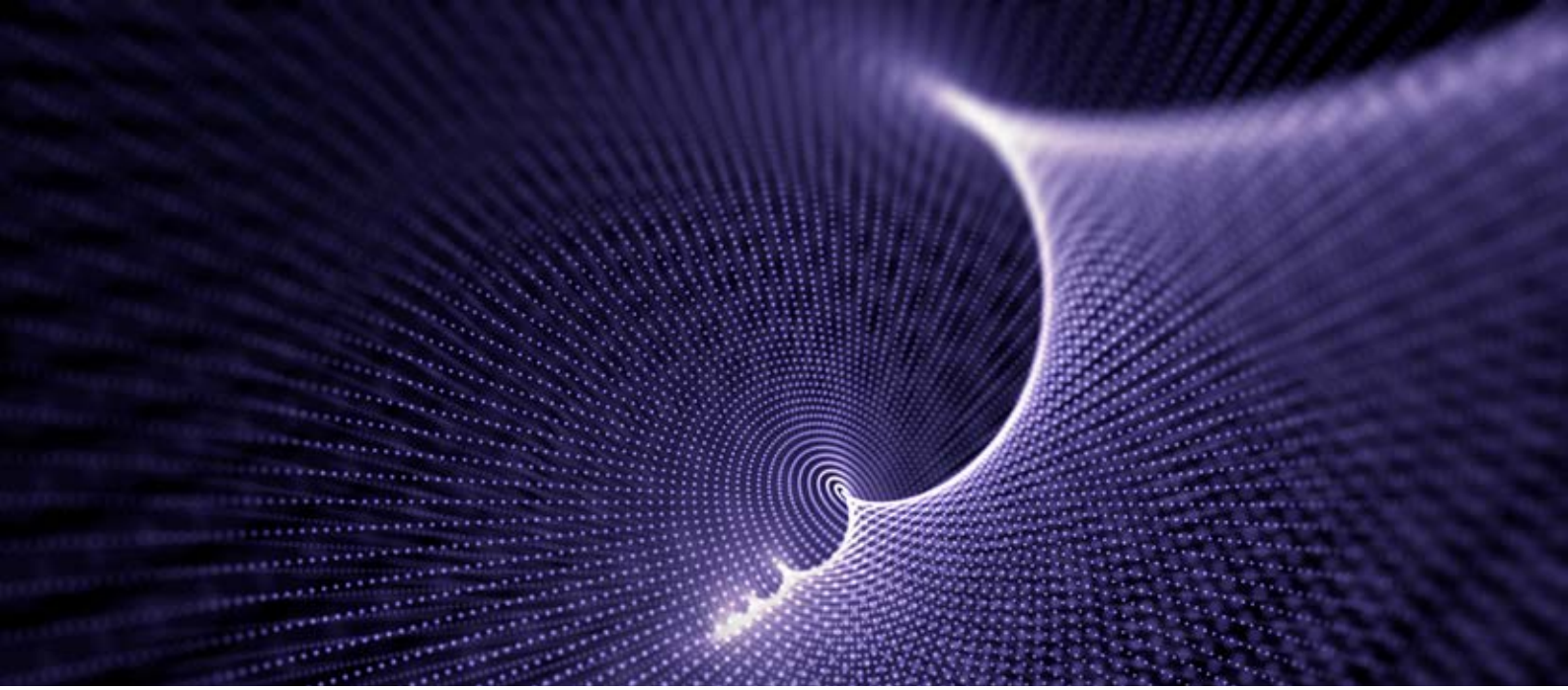
La corsa alla **supremazia quantistica** sembra proprio essere entrata in una fase di sprint. Con le recenti novità annunciate a gran voce da **Google**, **IBM**, **Microsoft** e **Amazon**, il settore sta puntando a un traguardo che fino a pochi anni fa sembrava distantissimo o addirittura irraggiungibile: la costruzione di un **computer quantistico su larga scala**, capace di risolvere problemi computazionali che vanno al di là della portata dei supercomputer classici.

IL PRINCIPIO FONDAMENTALE: QUBIT E CALCOLO QUANTISTICO

A differenza dei calcolatori tradizionali, che operano con bit binari, i computer quantistici utilizzano **qubit**, che – per dirla in una frase – possono consistere di una sovrapposizione di stati grazie ai principi della meccanica quantistica. Questo consente di eseguire operazioni su una scala di tutt'altro ordine di grandezza rispetto ai computer convenzionali. Tuttavia, i qubit sono estremamente **instabili** e **soggetti a errori**, il che rappresenta la principale sfida nel rendere questa tecnologia realmente applicabile.
Per affrontare questi problemi, i centri di ricerca e le aziende stanno esplorando diversi approcci, tra cui la correzione d'errore tramite **codici quantistici**, l'uso dei cosiddetti **qubit topologici** e l'integrazione di hardware avanzato per migliorare la **coerenza quantistica**, ossia il tempo di sopravvivenza di un qubit. In parallelo alle innovazioni tecnologiche, le questioni economiche giocano un ruolo fondamentale: il quantum computing richiede ingenti investimenti e modelli di business che possano giustificare le enormi spese di ricerca e sviluppo, da cui si comprende come mai il panorama sia dominato dalle *solite* **big tech**, seguite da uno sciame di **startup**, **scaleup** e **imprese** che lavorano su tutto ciò che sta intorno al *core* computazionale. Per questa volta, diamo uno sguardo a quel che stanno facendo le big.

IL PANORAMA ATTUALE: LE STRATEGIE DEI COLOSSI DEL SETTORE

Google ha recentemente presentato **Willow**, un chip quantistico che ha segnato un avanzamento nella correzione degli errori. La sua architettura ha dimostrato che aggiungere più qubit fisici può ridurre il tasso di errore, invertendo un paradigma da tempo radicato nel settore. Secondo Google, Willow è in grado di risolvere problemi che richiederebbero ai supercomputer più potenti di oggi un tempo più lungo dell'età dell'universo. Sebbene il risultato sia ancora teorico, sarebbe un bel passo in avanti nella scalabilità del calcolo quantistico. L'azienda ha anche annunciato nuovi investimenti in **infrastrutture** per il quantum computing, con la costruzione di un centro di ricerca da 1 miliardo di dollari dedicato alla realizzazione di un computer quantistico che possa avere applicazioni commerciali entro il 2029 (tutte le date sono da prendere con le molle, al momento).
IBM continua a essere un protagonista chiave nel settore, con un focus su processori quantistici modulari. Il suo chip **Condor** è attualmente il secondo più grande mai costruito, mentre **Heron**, con 133 qubit, riduce significativamente il tasso di errore. IBM ha optato per un approccio basato sulla **mitigazione degli errori** anziché la tradizionale correzione, concentrandosi sulla qualità delle operazioni quantistiche e sulla scalabilità attraverso architetture modulari. L'azienda ha inoltre



annunciato una roadmap dettagliata per i prossimi anni, con l'obiettivo di raggiungere i 1.000 qubit operativi già entro il 2026. Il modello di business prevede l'integrazione dei computer quantistici con il **cloud computing**, permettendo alle aziende di accedere a risorse quantistiche senza dover possedere fisicamente l'hardware.

Microsoft ha intrapreso un percorso differente con lo sviluppo di qubit topologici, una tecnologia che potrebbe garantire maggiore stabilità grazie all'uso di stati quantistici *protetti*. Il suo più recente chip, **Majorana 1**, sfrutta stati di materia che non appartengono a solidi, liquidi o gas, potenzialmente migliorando la resistenza agli errori senza sofisticati sistemi di correzione. Tuttavia, parecchi esperti si sono espressi ritenendo che questa tecnologia sia ancora in una fase sperimentale, dunque difficile da valutare. Dal punto di vista economico, Microsoft si sta concentrando anche su un ecosistema di **sviluppo software per il quantum computing**, con strumenti come Azure Quantum. Questo approccio permette alle aziende di iniziare a sperimentare algoritmi quantistici senza dover investire direttamente in hardware.

Da ultima, ma non certo per importanza, **Amazon Web Services (AWS)** ha annunciato il chip **Ocelot**, basato su qubit superconduttori e focalizzato sulla riduzione degli errori quantistici fino al 90% rispetto ai metodi convenzionali. L'integrazione di tecnologie come i cosiddetti *cat qubits* (in onore del gatto di Schrödinger) e la compatibilità con i processi di produzione dell'industria elettronica potrebbero accelerare l'adozione del quantum computing su scala commerciale, in particolare tramite soluzioni **cloud-based**.

Amazon ha anche sviluppato servizi come **Braket**, una piattaforma che consente alle aziende di eseguire **simulazioni quantistiche su hardware classico** e accedere a computer quantistici reali tramite cloud. Questo modello riduce i costi iniziali e permette – secondo le strategie di marketing – una più ampia diffusione delle tecnologie quantistiche nel settore ICT.

TECNOLOGIE QUANTISTICHE E DOVEROSE CAUTELE

Nonostante i progressi indubbi e significativi, il settore è ancora lontano dalla realizzazione di un vero e proprio computer quantistico in grado di funzionare senza errori e per tempi sufficientemente lunghi da essere utile su scala industriale. La tecnologia è ancora nelle fasi iniziali, dunque al di là degli annunci mediatici non vanno dimenticati i **rischi di hype e di generare aspettative irrealistiche**.

Dal punto di vista economico, comunque, il quantum computing sta attirando miliardi di dollari in investimenti, sia da parte di aziende private sia di governi. L'Unione Europea ha stanziato oltre un miliardo di euro per il **Quantum Flagship**, mentre la Cina sta investendo massicciamente in ricerca quantistica con l'obiettivo dichiarato di diventare leader mondiale nel settore. Anche gli Stati Uniti hanno intensificato i finanziamenti, con iniziative come il National Quantum Initiative Act, e le Nazioni Unite – nella ricorrenza dei 100 anni dallo sviluppo della Meccanica quantistica – ha ufficialmente dichiarato il 2025 **Anno Internazionale della Scienza e della Tecnologia Quantistica** (IYQ2025).

L'elenco delle sfide da superare resta comunque lunghissimo. Il costo di sviluppo dei chip quantistici è estremamente elevato e la domanda di applicazioni pratiche è ancora limitata. Il mercato delle tecnologie quantistiche **potrebbe esplodere nei prossimi dieci anni** (difficilmente più in fretta), ma solo se si riuscirà a dimostrare un chiaro vantaggio economico rispetto alle soluzioni classiche.

Ma c'è una grossa notizia di fondo: gli sviluppi degli ultimi mesi indicano che il quantum computing sta superando barriere storiche, aprendo la strada a nuove applicazioni nella **chimica computazionale**, **nella crittografia** e nell'**intelligenza artificiale**. A dominare la scena sarà chi saprà trasformare questi prototipi in soluzioni accessibili e scalabili per l'industria ICT.

Sanità italiana nel mirino degli hacker: l'opportunità della direttiva NIS2

Elena Vaciago, *Research Manager*
TIG - The Innovation Group

Il settore sanitario è tra i più colpiti dai cyber criminali in tutto il mondo. L'analisi "Health Threat Landscape 2023" dell'Enisa ha messo in luce come gli attori dei servizi sanitari dell'UE, soprattutto gli ospedali, siano stati i più colpiti dagli incidenti tra gennaio 2021 e marzo 2023, rappresentando il 42% del totale degli incidenti. Altri attori come enti e agenzie sanitarie (per il 14%) e industria farmaceutica (per il 9%) sono stati anch'essi bersagliati dal cyber crime. Il ransomware rappresenta la principale minaccia contro la sanità (54% degli incidenti), anche per l'impatto relativo che aumenta quando si hanno importanti violazioni di dati sensibili come quelli sanitari.

QUALI SONO LE MINACCE CYBER PER IL SETTORE SANITARIO ITALIANO

Il report ACN di fine 2024, "La minaccia cibernetica al settore sanitario – analisi e raccomandazioni - gennaio 2022 – dicembre 2024", evidenzia come, a partire da gennaio 2022, si siano verificati sul territorio nazionale in media 2,6 eventi malevoli di cybersecurity al mese ai danni di strutture sanitarie. La metà di questi avrebbero causato "incidenti", ovvero impatti effettivi sui servizi sanitari erogati, conseguenze negative sia in termini di disponibilità sia di riservatezza oltre che il blocco con gravi ripercussioni a danno dell'utenza, anche per quanto concerne la privacy. Nel 2024, gli incidenti sono aumentati nel settore sanitario italiano in modo sostanziale rispetto al 2023 (57 contro 12), anche a causa di un attacco alla IT supply chain di luglio 2024. Secondo l'ACN, le principali minacce nel settore sanitario restano il ransomware, gli attacchi tramite credenziali compromesse e le infezioni da malware, in crescita rispetto agli anni precedenti. Dalla rilevazione emerge che gli impatti più comuni nel settore sanitario sono stati:

- Blocco temporaneo dei servizi sanitari, con differenti livelli di compromissione.
- Esfiltrazione di dati, talvolta con cifratura.
- Modifiche all'integrità dei dati.

L'analisi ACN ha inoltre indagato il **livello di vulnerabilità dei servizi sanitari esposti su internet:** si è visto così che la "superficie di attacco esposta" comprende molte soluzioni e dispositivi presenti su internet con configurazioni errate e vulnerabilità critiche. Sono stati analizzati passivamente oltre 50.000 indirizzi IP associati al settore sanitario: tra gli indirizzi IP analizzati dal 1° luglio 2023 al 31 dicembre 2024, mediamente ogni giorno 2.174 sono risultati esporre pubblicamente dei servizi. Su questi ultimi è stato identificato un numero elevato di criticità (spesso sullo stesso servizio ne sono presenti diverse), alle quali è stato anche attribuito un livello di gravità.
Dai risultati emerge che molte vulnerabilità derivano da pratiche di sicurezza inadeguate o da scarsa formazione del personale. La protezione delle infrastrutture digitali sanitarie richiederebbe una continua identificazione delle vulnerabilità nei sistemi per mitigare i rischi legati alla privacy e alla sicurezza delle informazioni mediche. Le criticità sono:

- Vulnerabilità critiche che permettono il controllo del servizio da parte di attaccanti.
- Configurazioni errate, che indicano una scarsa manutenzione dei sistemi.
- Servizi esposti inutilmente su Internet.

L'adozione di misure correttive dovrebbe seguire una classificazione del rischio, con aggiornamenti software per mitigare vulnerabilità e miglioramenti nelle configurazioni per ridurre le esposizioni inutili. La maggioranza delle problematiche rilevate riguarda configurazioni errate e servizi non adeguatamente protetti.

COME PREVENIRE LE MINACCE CYBER NEL SETTORE SANITARIO

L'ACN ha identificato le principali carenze di sicurezza nel settore sanitario, che dipendono dai seguenti aspetti:

1. **Gestione decentralizzata dei sistemi IT:** reparti e uffici gestiscono hardware e software in modo indipendente, senza policy centralizzate di sicurezza.
2. **Obsolescenza dei dispositivi:** apparecchiature medicali datate non possono essere aggiornate, mantenendo vulnerabilità sfruttabili.
3. **Carenza di personale dedicato alla cybersecurity:** la sicurezza è spesso gestita da personale IT senza competenze specifiche.

Gli errori più diffusi includono la mancata segmentazione della rete, l'assenza di autenticazione multi-fattore, gli aggiornamenti software irregolari e l'uso di protocolli obsoleti. Le contromisure suggerite sono quindi:

- Adozione di policy di gestione centralizzata degli asset IT.
- Investimenti in cybersecurity e aggiornamenti tecnologici.
- Formazione continua del personale sanitario sulla sicurezza informatica.
- Monitoraggio costante delle vulnerabilità e implementazione di strategie di difesa avanzate.

La crescente digitalizzazione nel settore sanitario richiederebbe quindi un rafforzamento della sicurezza per proteggere dati sensibili e garantire la continuità dei servizi, adottando un approccio strutturato e proattivo alla cybersecurity.

LA DIRETTIVA NIS2 RILANCIA LA CYBERSECURITY SANITARIA

La direttiva NIS2 introduce requisiti più stringenti per la sicurezza informatica nel settore sanitario, imponendo un approccio proattivo basato su valutazioni continue delle vulnerabilità, threat intelligence e una maggiore cooperazione pubblico-privato per migliorare la capacità di risposta agli incidenti. Cosa cambierà in sostanza nei prossimi anni?

La NIS2 non solo impone di rafforzare le tecnologie di cybersecurity: chiama anche tutte le organizzazioni sanitarie che rientrano nel perimetro della norma ad adottare una serie di misure organizzative, che vanno dalla definizione di un'opportuna governance di questi processi (modelli e strutture organizzative adeguate, responsabile della cybersecurity); all'utilizzo di opportune metodologie per l'analisi del rischio e la prioritizzazione degli interventi; attenzione alla sicurezza della supply chain; misure specifiche per la continuità operativa e la gestione sicura degli accessi; gestione degli incidenti e formazione del personale (per citare le aree più importanti).

La Direttiva NIS2 introduce quindi un approccio strategico alla sicurezza informatica nelle aziende sanitarie, con un forte coinvolgimento dei vertici nella gestione del rischio. Oltre agli aspetti organizzativi, la Direttiva vuole promuovere un cambiamento culturale, obbligando dirigenti e dipendenti a interessarsi del tema, sviluppare le competenze che servono e adottare comportamenti responsabili.

In sintesi, la NIS2 sarà una leva normativa per aiutare le aziende sanitarie a rafforzare la propria resilienza in un contesto di minacce informatiche sempre più avanzate.

Piano ispettivo primo semestre 2025: su quali ambiti si concentreranno gli accertamenti del Garante

Valentina Frediani, *Founder and CEO*
Colin & Partners

Piano ispettivo primo semestre 2025: su quali ambiti si concentreranno gli accertamenti del Garante
La pubblicazione del nuovo piano ispettivo del Garante per la protezione dei dati personali, relativo al primo semestre del 2025 offre alle organizzazioni un quadro ben preciso di quelle che saranno le attività che verranno condotte nei prossimi mesi, ponendosi da un lato in continuità con le ispezioni del semestre precedente e approfondendo al contempo nuovi ambiti di interesse.
Nello specifico, il piano di ispezioni deliberato lo scorso 19 dicembre proseguirà gli accertamenti nei settori già avviati, in primis sui sistemi di trattamento dei dati nelle banche e negli istituti di credito, seguiti dalle società che gestiscono sistemi di video-allarme e dagli istituti scolastici *"in ordine al trattamento dei dati svolto attraverso i registri elettronici"*.
L'obiettivo dell'Autorità non sposterà il mirino nemmeno dal tema del telemarketing, con specifico riferimento al trattamento dei dati effettuato dai gestori di call center e servizi di e-mail marketing che - come hanno rilevato numerosi accertamenti - sono spesso divenuti destinatari di sanzioni per aver utilizzato *"in modo illegittimo indirizzari e banche dati"*.
Il prossimo semestre registrerà, inoltre, *"la conclusione del ciclo di ispezioni sui gestori dell'identità digitale* ***(SPID)*** *e sulla filiera dei soggetti di cui essi si avvalgono per il rilascio di servizi fiduciari (SPID e firma digitale)"*.

Oltre a questi ambiti di ispezione "noti" vediamo quali novità vengono introdotte nel nuovo piano di

accertamenti. I controlli ispettivi dei prossimi sei mesi affronteranno, infatti, aree di intervento sinora inesplorate quali il settore della statistica *"in ordine a specifici progetti, inseriti nel PSN, comportanti utilizzo di big data e dati sintetici"*. Rispetto alla definizione di questi ultimi, ossia dei dati sintetici, con molta probabilità il Garante offrirà maggiori chiarimenti, non essendo di fatto qualificabili come dati personali.
Tra i campi di indagine di nuova entratura anche *"l'utilizzo di dati biometrici per l'ammissione agli esami della patente di guida presso gli uffici della Motorizzazione civile"*.
Volendo trovare un comune denominatore ai var settori oggetto delle ispezioni del Garante vi è senza dubbio l'attenzione posta ai trattamenti su larga scala ai quali – coinvolgendo un significativo numero di interessati – è associabile un fattore di rischio elevato soprattutto laddove la qualità dei dati, la loro acquisizione e - non ultimo - il loro utilizzo non siano stati condotti in maniera conforme.

Quello delle banche dati a ben vedere è un tema molto sentito dall'Autorità e lo stesso viene approcciato secondo tre prospettive differenti:

- Sicurezza e accessibilità: in particolare gli accertamenti si focalizzano sui *"data breach che hanno interessato negli ultimi mesi banche dati pubbliche di particolare rilievo e delicatezza"*.
- Prevenzione e gestione delle violazioni: il settore di indagine in tal caso interessa – nell'ambito delle banche dati degli istituti di credito - l'analisi delle misure adottate per rilevare rapidamente e prevenire violazioni di dati personali.
- Utilizzo illegittimo: in quest'ultimo caso il focus è l'uso non autorizzato di indirizzari e banche dati, con particolare riferimento al trattamento di dati effettuato da imprese operanti nel settore dei call center e dei servizi di e-mail marketing.

L'IMPATTO PRATICO DEL PIANO ISPETTIVO SULLE IMPRESE

Le organizzazioni sono chiamate nei prossimi mesi ad affrontare il tema della protezione dei dati con particolare impegno, rafforzando le procedure di protezione e tenendo alta la guardia sulle misure di sicurezza che devono essere costantemente monitorate e aggiornate. L'accountability deve quindi trovare una traduzione sul piano pratico, piuttosto che restare un principio teorico e non applicato alla quotidiana pratica di business. Il primo alleato a disposizione di enti ed aziende che diventa parte integrante ed imprescindibile per una corretta gestione dei dati resta il Data Protection Impact Assessment, da considerare non solo un obbligo normativo, ma soprattutto il miglior strumento a disposizione per dimostrare la privacy by design e l'attenzione posta dal titolare al tema della data protection. In sede di eventuale controllo è fondamentale essere in grado di dimostrare il percorso di conformità svolto e di comprovare gli adempimenti realizzati, le scelte attuate e le misure tecniche ed organizzative adottate.
Il percorso di conformità rappresenta un processo continuo che non si limita a rispondere alle disposizioni solo in fase di implementazione: il titolare deve infatti tener conto di eventuali evoluzioni del contesto sia interno all'organizzazione che rispetto alla normativa o alla tecnologia in uso. Le valutazioni devono quindi essere monitorate con costanza e revisionate, nell'ottica di mantenere elevato il livello di controllo sulle attività di trattamento effettuate. In questo processo di conformità va da sé che anche la formazione giochi un ruolo fondamentale e sia uno degli aspetti più vagliati in sede di controllo: garantire percorsi di formazione adeguati - e costantemente aggiornati - alla popolazione aziendale favorisce la consapevolezza che la sicurezza non sia un mero "obbligo", bensì un elemento chiave per garantire la protezione del patrimonio informativo aziendale e goda pertanto di una priorità strategica.

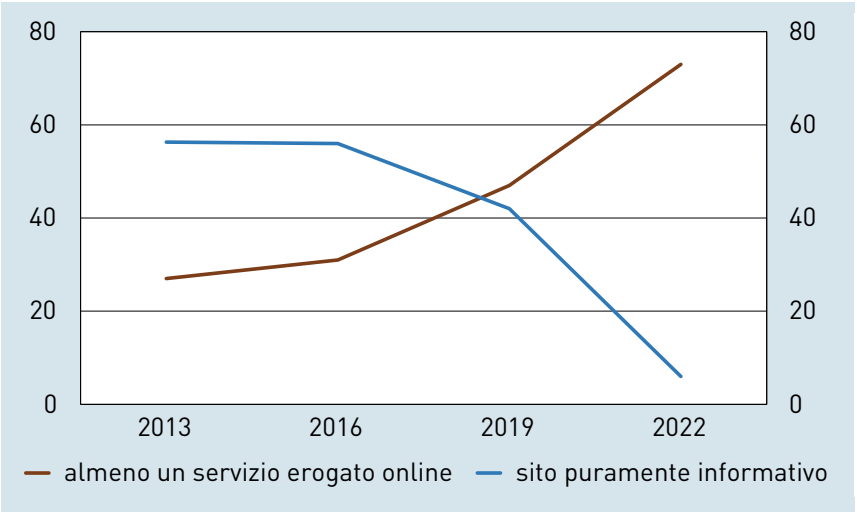
Servizi digitali e infrastrutture fisiche fanno evolvere le PA locali

Camilla Bellini, *Research & Content Manager*
TIG - The Innovation Group


Image by Freepik

Banca d'Italia ha recentemente pubblicato un'analisi sullo stato della digitalizzazione degli enti locali del Paese e sulla diffusione dell'e-government, approfondendo l'evoluzione sia dell'offerta dei servizi pubblici digitali, sia della trasformazione digitale del capitale fisico e umano degli enti locali.
È ormai un dato di fatto che la pandemia da Covid-19, con la conseguente emergenza sanitaria che ne è derivata, abbia avuto un ruolo di acceleratore rispetto al processo di digitalizzazione dei servizi pubblici erogati agli italiani. Lo confermano anche le analisi di Banca d'Italia sulle caratteristiche dei siti web degli enti e sulla loro capacità di erogazione di servizi interamente digitali: se nel 2019 la percentuale di enti con un sito web non interattivo era del 42%, questo dato nel 2022 è sceso al 6%, influenzando la performance soprattutto delle strutture di piccole dimensioni; inoltre, la quota di enti che sono in grado di erogare almeno un servizio interamente online è passata in tre anni dal 47% al 73%, dove anche in questo caso la dimensione dell'ente influisce sulla capacità di passaggio ad una modalità interamente digitale.

CARATTERISTICHE DEI SITI WEB DEGLI ENTI
(valori percentuali)

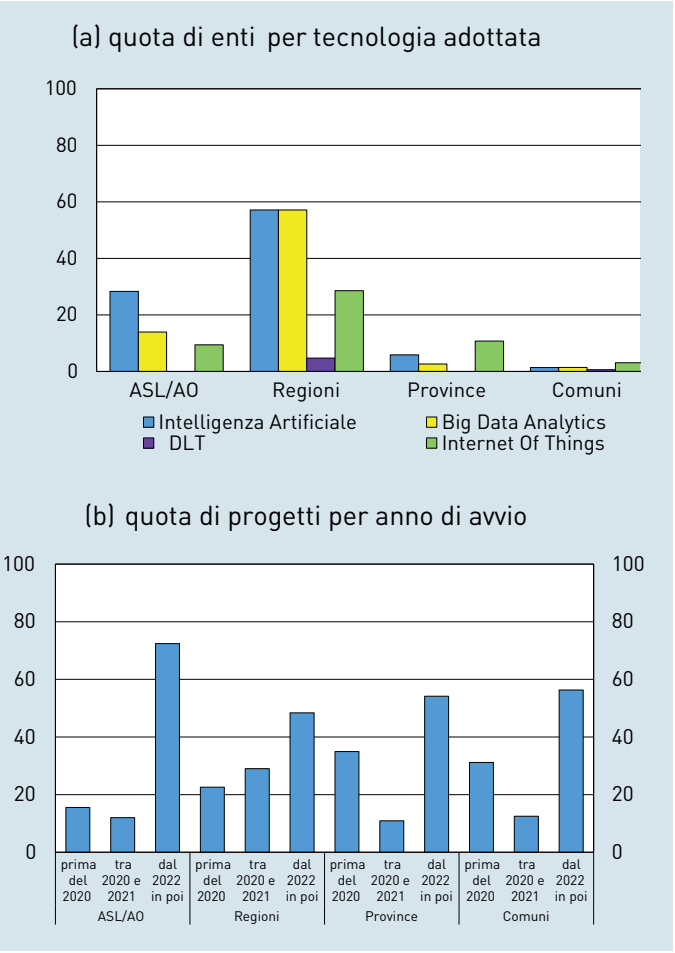


Fonte: IDAL, 2023; Indagine sull'informatizzazione nelle amministrazioni locali, 2022, 2018, 2014.

REGIONI, PROVINCE E COMUNI: IL GRADO DI DIGITALIZZAZIONE NEI SERVIZI

Dall'analisi risulta che 16 Regioni su 21 hanno digitalizzato, anche solo in parte, il processo di erogazione di un set di servizi, quali il pagamento del bollo auto, la presentazione dei bandi per l'accesso ai fondi da parte di imprese e cittadini (che è il servizio più digitalizzato), il catasto per gli impianti termici (il meno digitale) e i certificati di prestazione energetica; 6 Regioni invece li hanno completamente digitalizzati. Le Regioni più digitalizzate da questo punto di vista si trovano nel Centro Italia e nel Nord Ovest, il Sud e le Isole sono invece ancora fanalino di coda.
A livello di Province e Comuni, lo scenario è ancora in divenire. Tra le Province, dove i servizi considerati sono quelli relativi alle autorizzazioni a imprese e cittadini e alle imposte tributi e canoni, è la metà che viene erogato, solo in parte, in modalità digitale, un quarto lo offre invece completamente online. Per quanto riguarda i Comuni, invece, il 62% degli enti svolge in modalità digitale, anche solo parzialmente, servizi quali i servizi demografici, quelli sociali e scolastici, lo Sportello Unico per le Attività Produttive (SUAP) e lo Sportello Unico per l'Edilizia (SUE); li eroga interamente online "solo" il 28%.
Nei Comuni, inoltre, la principale modalità di accesso ai servizi online avviene tramite

UTILIZZO DI APPLICAZIONI INNOVATIVE AVANZATE (1) (valori percentuali)



Fonte: IDAL 2023. (1) Il **grafico a** mostra la quota percentuale di enti che ha adottato una determinata tecnologia avanzata. Nel **grafico b** è illustrato la quota di applicazioni tecnologicamente avanzate in base al periodo in cui sono state introdotte dall'ente, distinta per ciascuna tipologia di enti.

SPID, sia per quanto riguarda i servizi alle famiglie sia alle imprese. È questo un servizio che appare ormai consolidato, e che supporta nel garantire la sicurezza e la privacy nell'accesso a questi servizi.

CAPITALE FISICO DIGITALE A SUPPORTO DEGLI ENTI LOCALI

Focus della ricerca è anche il livello di diffusione e disponibilità delle infrastrutture tecniche nelle amministrazioni pubbliche locali. Queste sono infatti considerate dei fattori abilitanti l'offerta di servizi pubblici digitali, il cui monitoraggio è importante al fine di comprendere anche le direttrici evolutive del percorso di digitalizzazione degli enti. Di seguito alcuni trend in corso:

- per quanto riguarda le dotazioni tecnologiche personali, il 79% dei dipendenti ha un pc desktop, mentre solo un quarto utilizza un dispositivo mobile;
- due terzi degli enti utilizza soluzioni e sistemi di cloud computing; più diffuse le soluzioni di cloud storage e di Software as a Service, mentre è più contenuto il ricorso a soluzioni Platform as a Service;
- per quanto riguarda l'adozione di tecnologie e paradigmi tecnologici più innovativi, come i Big Data analytics, l'Internet of Things, le Distributed Ledger Technology o l'Intelligenza artificiale, tra i rispondenti il 5,3% dichiara di aver utilizzato o stare utilizzando una di queste tecnologie, l'1,8% anche più di una. Tra le più utilizzate emerge l'intelligenza artificiale, mentre quelle più rare sono le tecnologie DLT.

In generale, dall'analisi dell'istituto emerge come le Regioni siano gli enti più digitalizzati e più innovativi, che si contraddistinguono sia per l'uso di soluzioni cloud più avanzate come i servizi PaaS, sia in termini di adozione di tecnologie più innovative, dove circa 1 su 2 dichiara di utilizzare soluzioni e strumenti di Big Data e intelligenza artificiale.

LE COMPETENZE DIGITALI FANNO LA DIFFERENZA NELLA TRASFORMAZIONE DEGLI ENTI

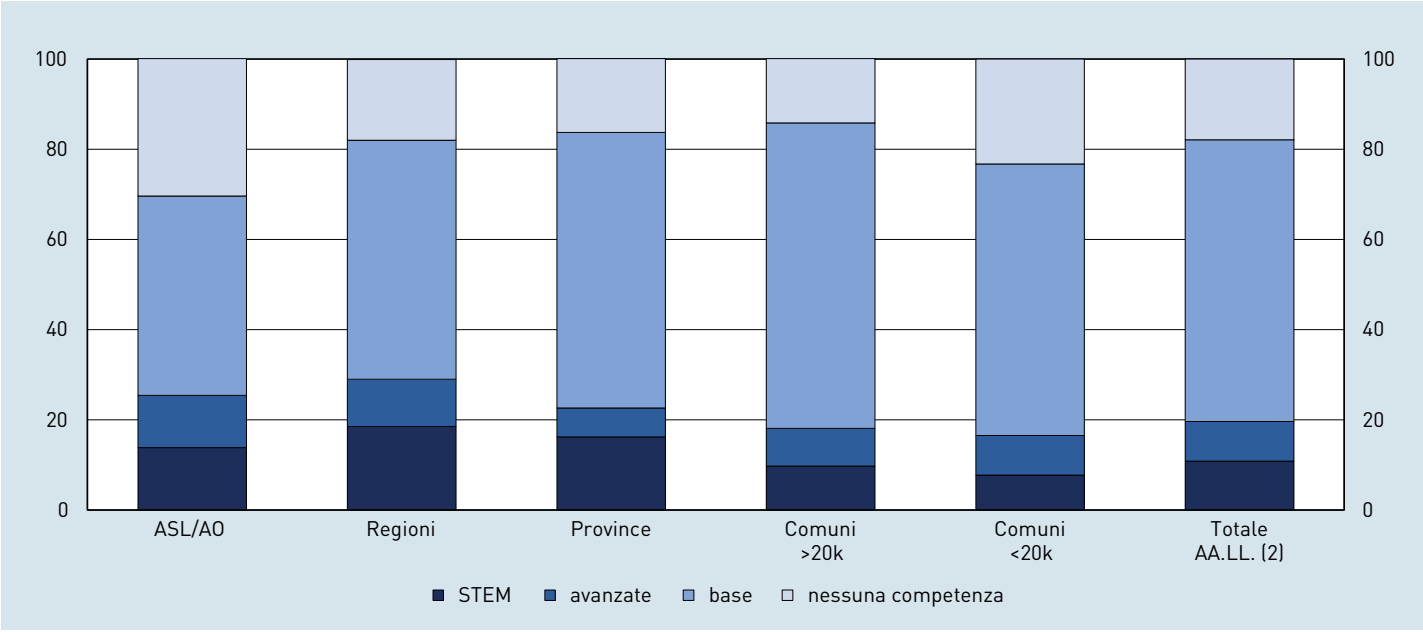
Così come già evidente dal posizionamento del nostro paese nell'indicatore DESI sugli ambiti del capitale umano, anche la rilevazione di Banca d'Italia evidenzia una ridotta disponibilità di personale con competenze digitali, in particolare per gli enti locali. Dall'analisi emerge che tra il personale delle amministrazioni locali il 36% possiede una laurea, e l'11% ha una laurea in materie STEM. Inoltre, è il 17,9% che dichiara di avere competenze avanzate in ambito tecnico e digitale, anche in assenza di un titolo STEM. Risulta invece che la maggioranza degli addetti ha solo una competenza di base o addirittura nessuna conoscenza informatica. Per cercare di colmare questo gap, le pubbliche amministrazioni hanno quindi intrapreso dei percorsi di formazione in materia di ICT, con circa il 37% degli enti locali che dichiara di aver svolto questo tipo di attività per i propri dipendenti.

LA SPESA MEDIA IN INFORMATICA DELLA PAL IN CRESCITA RISPETTO AL PERIODO PRE-PANDEMICO

In generale, nel biennio 2021-2022 la spesa media per investimenti informatici degli enti locali è risultata superiore a quella del periodo 2019-2020, con meno del

6% delle amministrazioni che ha dichiarato un calo della propria spesa in questo ambito.
Rispetto alle fonti di finanziamento a supporto della spesa ICT, sono soprattutto le Regioni che hanno fatto leva anche su iniziative e fondi nazionali ed europei, mentre Province e Comuni, così come le ASL e le aziende ospedaliere pubbliche (anche esse rappresentate nel campione), hanno utilizzato soprattutto risorse interne. Nel complesso, i fondi del PNRR sono comunque considerati un importante riferimento per aiutare le aziende pubbliche locali in questo percorso: tutte le Regioni, due terzi delle Province e quasi tutti i Comuni hanno preso parte ad almeno un bando del PNRR, anche se, tra chi non ha aderito, si lamentano soprattutto la mancanza di risorse a disposizione, di conoscenza dei bandi e di domanda per i servizi oggetto del bando.

DISTRIBUZIONE DEGLI ENTI PER COMPETENZE INFORMATICHE POSSEDUTE DAL PROPRIO PERSONALE (1) (valori percentuali)



Fonte: IDAL 2023 e Conto Annuale RG8 2022. (1) I grafici riportano la distribuzione percentuale degli Enti, per ogni categoria considerata, in base alle competenze possedute dal personale nel proprio organico. Per le ASL si esclude il personale sanitario. (2) Il totale si intende al netto delle ASL/AO.

IL CAFFÈ DIGITALE

Ricevi gli articoli degli analisti
di **TIG - The Innovation Group**
e resta aggiornato sui temi
del mercato digitale in Italia!

ISCRIVITI ALLA NEWSLETTER MENSILE!

TIG | THE INNOVATION GROUP