APRILE 2023

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

SANITÀ E DIGITALE
VANTAGGI TANGIBILI MA UN PERCORSO ANCORA LUNGO

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Marta Ottaviani
Giornalista

ICT ECOSYSTEM

Il canale ICT si muove sul valore. E scopre il bello dei servizi

AI FORUM

Facciamo il punto sull'Intelligenza Artificiale

IL TEAM DEL CAFFÈ DIGITALE

Roberto MASIERO
Presidente
The Innovation Group

Ezio VIOLA
Co-founder
The Innovation Group

Emilio MANGO
General Manager
The Innovation Group

Elena VACIAGO
Associate Research Manager
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

Loris FREZZATO
ICT Ecosystem

SOMMARIO

Sanità e digitale: vantaggi tangibili ma un percorso ancora lungo

Valentina Bernocco, Web and Content Editor
The Innovation Group

Servizi di telemedicina, semplificazione nei rapporti con medici, ospedali e Asl, una migliore copertura territoriale e una gestione più digitalizzata di tutti i dati e processi. Sono alcune delle direttrici di cambiamento che la sanità italiana sta percorrendo, dopo lo shock di una pandemia che ha reso evidenti le mancanze e inefficienze di un settore ancora troppo poco "digitale" e in cronica penuria di risorse. Ora, anche grazie ai fondi del Piano Nazionale di Ripresa e Resilienza, stiamo andando nella giusta direzione ma non senza ostacoli sul percorso. Il Fascicolo Sanitario Elettronico, per esempio, è oggi un'opera ancora incompiuta e frammentata, per la quale è necessario accelerare i lavori per rispettare le scadenze previste dal PNRR.

Dalla "Digital Healthcare Executive Conference" organizzata da The Innovation Group a Roma lo scorso 18 aprile sono emersi alcuni punti fermi: l'importanza di una collaborazione stretta fra Pubblica Amministrazione centrale e locale; la necessità di creare non solo piattaforme digitali ma anche competenze; l'idea di una telemedicina che non si sostituisca ai servizi di cura tradizionali e alle relazioni umane, bensì li affianchi; una generale trasformazione dell'esperienza del paziente, che ha diritto a tempi e modalità di cura migliori. In tutto questo il digitale non distrugge nulla, ma è un fattore abilitante. Sul tema è intervenuto, tra gli altri, Giuseppe Quintavalle, Commissario Straordinario della Asl Roma 1: "Dopo la pandemia ci sono state delle modifiche assistenziali, e realtà territoriali hanno potuto portare l'assistenza a casa delle persone", ha ricordato. "Sono convinto che l'utilizzo di nuove progettualità debba entrare nel bagaglio formativo e culturale di ogni professionista sanitario".

Quintavalle ha suggerito che alcune materie diventino obbligatorie nella formazione universitaria dei medici, come la robotica e l'intelligenza artificiale. "L'AI è un ausilio", ha sottolineato, "ma l'uomo, il medico, resterà centrale. Oggi si parla di Fascicolo Sanitario Elettronico, tuttavia siamo ancora distanti. Stiamo facendo passi in avanti nella presa in carico domiciliare, nella teleassistenza e nella telemedicina. Le scadenze stringenti del PNRR impongono atti programmatori che si devono calare nella formazione di ogni singolo operatore. La parola d'ordine per me è cambiamento culturale".

Se la carenza di competenze digitali è un limite non da poco, il grande problema alla base del Sistema Sanitario Nazionale è l'insufficienza della spesa pubblica, in

un Paese senescente (l'attuale rapporto tra occupati contribuenti e pensionati è di 1,6 a 1) e in cui circa 23 milioni di persone (38% della popolazione) sono affette da patologie croniche e richiedono, quindi, cure continue. Sul problema ha puntato il dito Francesco Longo, professore associato del Dipartimento di Scienze Sociali e Politiche e direttore dell'Healthcare Sector Observatory dell'Università Bocconi. Presentando i risultati di una ricerca svolta insieme alla RegioneEmilia-Romagna, Longo ha evidenziato che "la coperta è corta", che il rapporto tra il numero di medici di medicina generale (Mmg) e infermieri, da un lato, e abitanti, pazienti cronici e frequenza d'accesso agli ambulatori, dall'altro, non consente livelli di servizio adeguato.

"La digitalizzazione del territorio dovrebbe garantire di raccogliere dati più precisi", ha sottolineato Longo, "ma soprattutto di ridisegnare il format dei servizi e di re-ingegnerizzare i rapporti professionali nella filiera sanitaria, tra Mmg, specialisti ambulatoriali e specialisti dei prelievi. Dobbiamo introdurre elementi di intelligenza artificiale soprattutto per standardizzare di più le cure e ridurre la straordinaria variabilità esistente nelle cure su pazienti con la stessa patologia e la stessa stadiazione". La digitalizzazione (di cui l'AI è, se vogliamo, una delle frontiere più evolute ma non l'unica) non è dunque un optional ma una necessità per il settore sanitario italiano. La logica di fondo è utilizzarla per tutti i processi laboriosi e a scarso valore aggiunto, come la raccolta dei dati e le procedure amministrative, ma anche a supporto del personale medico (e non in completa sostituzione) nelle attività ad alto valore aggiunto, come le cure a distanza (servizi di telemedicina, applicazioni per il monitoraggio dell'aderenza alle terapie) e la formulazione di diagnosi. L'obiettivo finale è realizzare un "patient journey in cui togliamo i processi a scarso valore aggiunto per introdurre nuovi processi ad alto valore aggiunto", ha sintetizzato Longo.

Un nuovo "patient journey"

Il concetto di patient journey, mutuato dal mondo del marketing (dove da anni si parla di customer journey), è importante anche per Elena Bottinelli, head of digital transition and transformation del Gruppo San Donato, cui fanno capo 56 strutture tra Ircss e ambulatori: "Ci siamo posti l'obiettivo di anticipare il cambiamento, di creare un nuovo modo di fare sanità. Per questo abbiamo voluto realizzare una piattaforma che raccogliesse i dati delle soluzioni che abbiamo già in essere: prenotazione online, referti, televisita, Crm e fascicolo sanitario". Il problema? "A oggi abbiamo più di 100mila iscritti alla piattaforma ma solo il 25% la utilizza", ha spiegato Bottinelli. "L'uso sporadico della telemedicina non produce i risultati sperati. Dobbiamo ripensare il patient journey in cui alcuni passaggi sono in digitale e alcuni sono nella dimensione fisica".

Un punto di vista non dissimile è quello espresso da Claudio Caccia, presidente onorario dell'Associazione Italiana Sistemi Informativi In Sanità (AISIS). "Oggi qualsiasi organizzazione sanitaria non funziona senza un adeguato livello di maturità digitale", ha osservato. "Altro tema importante: andremo sempre di più verso una sanità ibrida, in parte in presenza o mista o totalmente online. Questo implica la capacità di progettare nuovi modelli di presa in carico del paziente".

La digitalizzazione non si esprime solo attraverso la telemedicina o gli strumenti self-service per prenotazioni e referti: è anche un supporto per la prevenzione. "Il tema della cronicità per noi è molto forte", ha raccontato Laura Di Dio, head of operations di Humanitas, gruppo a cui fanno capo nove ospedali e dieci centri specialistici."Vogliamo ridurre l'impatto della cronicità tramite la cura preventiva del paziente e creando strumenti che misurino l'outcome. Nel fare prevenzione, la digitalizzazione ci aiuta con sistemi come i Crm, che ci descrivono il nostro paziente e lo gestiscono in modo proattivo, tramite followup".

Il digitale si presta a ottimizzare anche l'ambito degli screening oncologici, a beneficio sia dei pazienti sia del taglio della spesa sanitaria. "Già oggi i sistemi informativi complessi aiutano gli screening ma potrebbero farlo ulteriormente", ha spiegato Alessandro Carellario, amministratore delegato di Sinapsys, società del Gruppo Maggioli. "Una ricerca svolta negli Stati Uniti sugli screening mammografici ha evidenziato che nel 19% dei casi le pazienti sono state sottoposte a esame donne che non ne avevano bisogno in quel momento, con conseguente stress per le pazienti e innalzamento dei costi". Un'altra ricerca, citata da Carellario, ha dimostrato che analizzando referti mammografici con algoritmi di intelligenza artificiale è possibile accorciare in modo significativo i tempi di diagnosi e creare percorsi di followup personalizzati.

Esempi di innovazione regionale

Oggi alcuni degli ecosistemi in fieri sono quelli della sanità regionale. In Puglia, per esempio, è stato realizzato un Sistema Informativo Sanitario Territoriale (SIST) che ha messo in rete circa quattromila medici di medicina generale, 1.200 farmacie, 900 operatori privati accreditati e duemila specialisti. Dal portale online del SIST i cittadini possono fare prenotazioni che risultano direttamente visibili ai farmacisti.

"La nostra regione ha affrontato l'opportunità di cercare di utilizzare la tecnologia a supporto dei nuovi modelli organizzativi", ha testimoniato Giovanni Delgrossi,

dirigente unità organizzativa Sistemi Informativi e Sanità Digitale, direzione generale welfare della Regione Lombardia. “La tecnologia non potrà risolvere tutti i problemi ma sicuramente potrà facilitare il processo”. Il team di Delgrossi è particolarmente impegnato sul fronte della telemedicina, dove sono stati coinvolti gli operatori delle Case di Comunità (strutture sociosanitarie polivalenti distribuite sul territorio).

Gli ostacoli da superare

Quelli descritti sono solo alcuni esempi del grande potenziale del digitale in sanità. Un potenziale che si scontra però con alcuni problemi di fondo. Uno è, naturalmente, quello delle risorse a disposizione per gli investimenti, cui si associa la difficoltà di realizzare i progetti nei tempi previsti dal PNRR. C’è poi il già citato problema delle competenze e dell’usabilità delle applicazioni, con cui è necessario familiarizzare, e l’opera non può essere demandata al singolo professionista. “Sicuramente l’innovazione tecnologica ci può permettere di risolvere una serie di questioni, nella comunicazione ad esempio”, ha detto Nicola Calabrese, vicesegretario nazionale della Federazione Italiana Medici di Medicina Generale. “Ma ci vogliono tanti investimenti e l’innovazione tecnologica non può essere lasciata in mano al singolo professionista”.

Un altro problema, di natura più tecnica, è quello dell’interoperabilità di dati e piattaforme: se manca, i processi e la gestione dei pazienti rimangono frammentati. L’interoperabilità è particolarmente cruciale per la realizzazione di un Fascicolo Sanitario Elettronico esteso e deve esistere a più livelli (gestione dei dati, infrastrutture, processi). Un punto di riferimento è lo standard HL7 FHIR (Fast Healthcare Interoperability Resources), valido a livello internazionale e utile per lo scambio di cartelle cliniche elettroniche. “La maggior parte dei manager del settore ritiene che la frammentazione degli applicativi e dei sistemi di gestione dei dati a tutti i livelli sia una delle più importanti barriere che impediscono alla sanità nazionale di evolvere”, ha illustrato Lucio Marottoli, market line manager health & public sector di Deda Next, società di Deda Group focalizzata sul settore pubblico. “L’esigenza vera è quella non solo di riuscire a raccogliere tutti i dati ma anche di trovare un linguaggio comune, un esperanto dei dati, per poterli comprendere”.

Concorda Cesare Guidorzi, vice president hospital & public business per l’Italia di Doctolib, software per la prenotazione di visite, esami e altri servizi sanitari. “Non basta creare un’app o un portale per avere un cittadino digitalizzato”, ha detto Guidorzi. “Bisogna metterlo al centro e dargli del potere, questa è un’idea assolutamente valida. Il mondo che abbiamo davanti è a rete, e non più gerarchico. Ma è necessario aprire gli ecosistemi e renderli interoperabili”.

“L’interoperabilità è cruciale per la realizzazione di un Fascicolo Sanitario Elettronico esteso e deve esistere a più livelli (gestione dei dati, infrastrutture, processi). Un punto di riferimento è lo standard HL7 FHIR, valido a livello internazionale e utile per lo scambio di cartelle cliniche elettroniche

Marta Ottaviani
giornalista specializzata su Turchia e Russia

Infowar, ossia, l'informazione come arma di guerra

Elena Vaciago, Research Manager
The Innovation Group

Perché ci interessa la guerra non lineare che si gioca sul web? perché purtroppo è il nuovo modo con cui si farà la guerra negli anni a venire. Adesso abbiamo sotto gli occhi una guerra di natura territoriale, ma si tratta di un caso particolare. Se pensiamo alle potenze che si stanno affacciando al nuovo ordine mondiale multilaterale, come la Cina o l'India, hanno capito che è più importante che occupare territori è oggi acquisire informazioni pregiate e dati delle persone, il vero petrolio del futuro, oltre che essere in grado di influenzare a proprio favore le coscienze e la mente dei Paesi dove ci sono delle democrazie evolute. Quello che per noi è un valore irrinunciabile, ossia la libertà di espressione, per Paesi autoritari potrebbe essere una debolezza da colpire. Su questi temi si è svolta, lo scorso 9 marzo al "Cybersecurity Summit 2023" di The Innovation Group, la conversazione con Marta Ottaviani, giornalista specializzata su Turchia e Russia. Riportiamo le principali considerazioni emerse.

Cosa si intende con Infowar e che cosa implica?

La domanda è importante perché, dall'inizio della guerra in Ucraina, ci siamo tutti focalizzati su quello che stava succedendo sul campo, ma c'è una guerra parallela che si sta combattendo grazie alle nuove tecnologie sul web ed è una guerra che non si vincerà e non si perderà mai completamente. Questo perché la guerra non lineare russa è sempre operativa, è una guerra continua. Domani il conflitto militare in Ucraina finirà, ma poi ci saranno altri motivi e altri temi con i quali la Russia cercherà di manipolare l'opinione pubblica, non solo italiana, anche quella di altri Paesi.

Esempi ce ne sono stati molti: pensiamo solo al referendum sulla Brexit e, in particolare, a un'informativa del Parlamento in cui si sottolineava come i Servizi Segreti avessero sottovalutato gli attacchi hacker e gli sciami di troll che avevano operato durante il periodo della Brexit (facendo campagna sciaguratamente per il Leave). La guerra non lineare russa, prima di tutto, non è una novità; la Russia ha strutturato e pensato questa guerra fin dall'epoca sovietica, quando si era resa conto che non avrebbe avuto più a disposizione il budget che l'Unione

Sovietica destinava all'industria di difesa, e soprattutto si rendeva conto che era sempre un passo indietro rispetto agli americani (che per la Russia sono una vera e propria ossessione, se non addirittura un peccato originale).

Con il tempo, la Russia ha iniziato ad applicare questa guerra non lineare a un numero sempre più importante di Paesi. Il vero turning point per noi è stato il 2013, quando è emersa la seconda direttrice della guerra non lineare russa, ossia la disinformazione sui social. E' stato fatto un upgrade e la disinformazione ha iniziato a diffondere fake news non solo in russo, ma anche in tutte le altre lingue (con precedenza, chiaramente, all'inglese e alle lingue dei Paesi dell'ex blocco sovietico o dell'ex blocco di Varsavia). Infatti, la strategia di Mosca era di colpire prima gli Stati Uniti e la Gran Bretagna e in contemporanea i Paesi che Mosca ritiene ancora orbitanti nel suo cerchio. Poi, in terzo luogo, l'Europa. Quindi il secondo aspetto della guerra non lineare sono gli sciami di disinformazione sui social e il terzo è un sistema di softpower che parte dai Think Tank. Tutti i Paesi hanno Think Tank politicamente orientanti, però un conto è avere Think Tank che hanno delle simpatie e un conto è avere dei Think Tank che sono sostanzialmente alle dipendenze della narrazione del Cremlino e che, soprattutto, producono documenti che non hanno valore scientifico.

Come avviene il processo decisionale all'interno di una multinazionale come la vostra?

La scelta dei fornitori e dei provider viene gestita a livello corporate e non ci sono margini per agire localmente. La scelta centrale si è orientata verso il cloud pubblico, ma è allo studio la possibilità di dotarsi anche di cloud privato per alcune tipologie di applicazioni e dati. Come già indicato, gran parte dell'azienda è ormai migrata, mentre la produzione progredirà in direzione dell'edge computing per ragioni di opportunità e di business. In generale, riteniamo che il cloud vada interpretato soprattutto come una soluzione, in grado di alleggerire.

Perché l'Italia si è trovata impreparata?

Siamo impreparati perché abbiamo visto tutti cosa è successo nel 2016, negli Stati Uniti, con le elezioni americane: le manipolazioni sui social hanno evidentemente avvantaggiato

Donald Trump. C'è anche stato un altro warning nel 2014 da parte dell'Ucraina. L'Ucraina affermava di aver subìto attacchi hacker e che la Russia continuava a fare controinformazione sui social, a far passare solo la sua versione dei fatti. Questo è molto pericoloso, perché rischia di ingannare non solo il cittadino comune, ma anche un giornalista che si occupa di esteri come me. Ora si parla della guerra tra Russia e Ucraina, ma la guerra non lineare si applica a tutto, anche ai grandi temi di attualità. Ne cito uno per tutti: i vaccini.

Cosa dobbiamo fare e cosa stiamo facendo per prepararci?

Soprattutto a livello Europeo e a livello NATO c'è un coordinamento crescente in questo senso. Come singoli dobbiamo anzitutto imparare a capire che questa guerra esiste, questa Infowar, come la chiamano i russi, esiste. Dobbiamo cercare di informarci cum grano salis selezionando attentamente le nostre fonti, e tenere sempre bene a mente che la moltiplicazione di fonti (purtroppo) non è direttamente proporzionale alla qualità delle informazioni. Ma, soprattutto, dobbiamo, a mio parere, essere più educati dal punto di vista digitale a tutti i livelli.

Le piattaforme potrebbero fare qualcosa in più?

Le piattaforme devono fare qualcosa in più. Io l'altro giorno ho inviato a Twitter una segnalazione per i tweet dell'ambasciata russa, particolarmente attiva nel nostro Paese. L'account è una fucina di fake news praticamente H24, così ho mandato una segnalazione a Twitter dicendo "guardate che questa è una fake news, c'è dell'incitazione all'odio" e loro mi hanno risposto "Cara Marta non notiamo nulla che violi le nostre regole della community". Non ci siamo sicuramente.

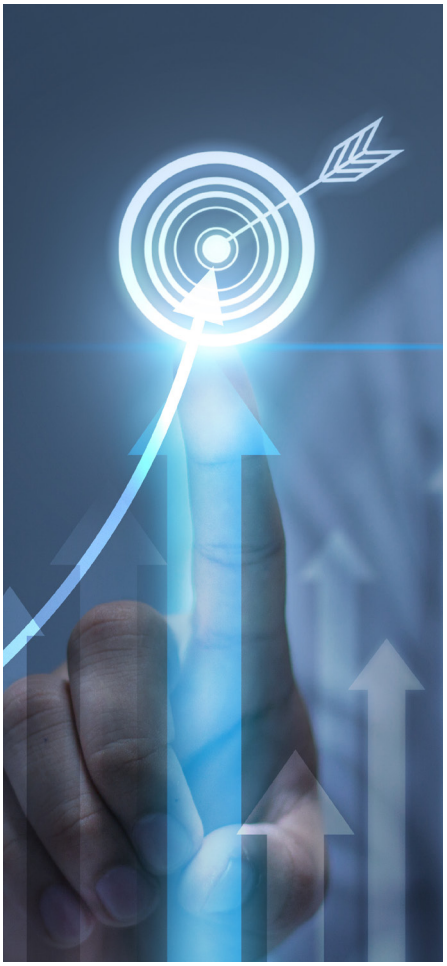
Che cos'è la dottrina Gerasimov?

La dottrina Gerasimov non esiste perché è un nome che, come spiego nel mio ultimo libro ("BRIGATE RUSSE, La guerra occulta del Cremlino tra troll e hacker"), gli ha dato Mark Galeotti, che è un grandissimo studioso di Russia e di Unione Sovietica. È la dottrina dell'approccio olistico al danno, quindi, colpire il nemico da più parti senza che esso se ne accorga, per poi procedere con le quattro direttrici di cui parlavo prima.

Sul canale Cybersecurity di TIG è disponibile il video completo dell'intervista

Pnrr, a che punto siamo?

Arianna Perri, Research Analyst
The Innovation Group



L'attuazione del Piano Nazionale di Ripresa e Resilienza prosegue con cinquanta scadenze previste e un'accelerazione della spesa.

In questi primi mesi del 2023 si iniziano a tirare le somme circa lo stato di avanzamento dei milestone e target raggiunti in ambito Pnrr. È la fase più delicata del processo attuativo in quanto sono previste 50 scadenze, alle quali corrisponde un'accelerazione attesa della spesa del 190 per cento rispetto al triennio 2020-2022. Nella valutazione di impatto sulle dimensioni Desi (Digital Economy and Society Index), pesano soprattutto gli investimenti relativi all'integrazione delle tecnologie digitali, concentrando in essi, nel 2023, quasi il 45% della spesa programmata. Il profilo di spesa relativo alle altre dimensioni Desi risulta essere più distribuito nel tempo, ma è chiaro che il 2023 rimane una fase critica poiché coincide con il momento in cui gli investimenti devono iniziare a tradursi in cantieri.

Ma a che punto è l'Italia? Il verdetto da Bruxelles è che il nostro Paese si trova in grande difficoltà: si assiste in particolare a un ritardo nel cronoprogramma che potrebbe potenzialmente aumentare. Le tempistiche risultano infatti essere uno degli elementi più critici nell'attuazione del Piano Nazionale di Ripresa e Resilienza. Inoltre, un nuovo decreto del governo, che mira alla modifica di diversi aspetti della governance del Pnrr, dovrà nel breve periodo diventare operativo. Anche un nuovo codice appalti, entrato in vigore il 1° aprile 2023, avrà delle implicazioni e ricadute sull'andamento dei progetti del piano. In questa fase però non ci si possono permettere dei blocchi nell'attività di investimento o una decelerazione nell'avanzamento dei progetti già avviati.

A questo scenario si aggiungono, naturalmente, il rialzo dei prezzi dei beni energetici e le tensioni inflazionistiche con le conseguenti ricadute che quest'ultima avrà sui progetti che sono già stati finanziati dal Pnrr. Bruxelles in questo senso rassicura chiarendo che nella definizione del Piano sono stati considerati questi fattori eccezionali. Molti Stati, tra cui l'Italia, hanno iniziato a rivedere alcuni progetti per far fronte all'inflazione. In questo senso, sembra quindi esserci una certa flessibilità nello sviluppo del Piano da parte della Commissione Europea. La scadenza per presentare eventuali proposte di modifica al Pnrr è fissata per il prossimo 30 aprile 2023. Il governo dovrà quindi dedicarsi all'approfondimento delle misure già in corso, delle relative potenzialità e problematiche al fine di decidere se modificare o meno alcuni aspetti del Pnrr.

Ad oggi, il governo sta aspettando un responso sull'ultima tranche effettuata alla fine del 2022, la cui scadenza prevista era marzo 2023, ma che è stata prorogata alla fine del mese di aprile. In particolare,

> **Per il primo semestre 2023 è prevista la realizzazione di 54 obiettivi, ma a febbraio nessuno di questi era ancora completato**

il governo è in attesa dell'arrivo dei correttivi per sbloccare questa terza tranche da 19 miliardi.

Le tempistiche risultano dunque essere uno degli elementi più critici nell'attuazione del Pnrr. Sarà importante ragionare in ottica prospettica e non prestare attenzione solo al singolo target o milestone da raggiungere. L'obiettivo non deve essere di costruire opere o implementare servizi entro il 2026, bensì dal 2026 in poi: pensare cioè a ciò che accadrà da giugno di quell'anno, data di scadenza del Pnrr.

I prossimi traguardi

Per il primo semestre 2023 è prevista la realizzazione di 54 obiettivi del Pnrr, ma alla data del 13 febbraio 2023 nessuno di questi era stato completato, il 61% risultava in corso e il 37% solo avviato. Il 65% degli obiettivi italiani si concentra nella missione 1, "Digitalizzazione, innovazione, competitività, cultura e turismo", per un totale di 21 obiettivi, e nella missione 6, "Salute", per un totale di quattordici obiettivi. Circa la metà degli obiettivi da realizzare nel corso del primo semestre 2023 è dunque riferibile al Dipartimento per la Transizione Digitale e al Ministero della Salute.

Nell'ambito della digitalizzazione, dovranno essere conseguiti i target relativi alla migrazione del 50% delle scuole e università all'anagrafe nazionale e alla connessione delle strutture sanitarie alle reti ultraveloci. Inoltre, dovranno essere aggiudicati i contratti

di cinque progetti relativi alle tecnologie satellitari e all'economia spaziale. Per quanto riguarda la presidenza del Consiglio dei ministri, i traguardi da raggiungere entro il primo semestre 2023 coinvolgono la digitalizzazione della Pubblica Amministrazione, la digitalizzazione del sistema produttivo e l'inclusione sociale. Nello specifico, faranno riferimento alla digitalizzazione della PA, alla cura dei servizi digitali e alla cittadinanza digitale con la diffusione dell'utilizzo delle piattaforme nazionali di Identità Digitale, come Spid e Cie; seguono l'estensione dell'anagrafe nazionale digitale (Anpr) e la digitalizzazione delle grandi amministrazioni centrali (Inps, Inail e il Consiglio di Stato).

Relativamente alla digitalizzazione e la sicurezza nella PA, ci si sta muovendo verso l'attuazione di azioni a favore del Servizio Civile Digitale, mentre sul tema della digitalizzazione, innovazione e competitività nel sistema produttivo, gli interventi su cui ci si concentrerà saranno le tecnologie satellitari nell'economia spaziale (con i progetti quali SatCom, Osservazione della Terra, Space Factory e InOrbit Economy.

Focus sulla Missione 1: M1C1 e M1C2

La missione 1, "Digitalizzazione, innovazione, competitività, cultura e turismo", riveste uno dei ruoli più rilevanti: si pone lo scopo di trasformare l'Italia strutturalmente. Per raggiungerlo, sono stati stanziati circa 40 miliardi di euro dal Dispositivo di ripresa e resilienza e circa 8 miliardi dal Piano complementare, per un totale di 48 miliardi di euro. Per quanto riguarda, nello specifico, le componenti M1C1 e M1C2 sono stati stanziati 33,61 miliardi di euro. È importante sottolineare quanto l'obiettivo della M1 sia trasversale a tutte e sei le missioni del Pnrr: riguarda infatti la scuola, la sanità, l'industria, la Pubblica Amministrazione, ecc. Nel complesso, il Paese sembra iniziare a adottare il modello "government as a platform" per lo sviluppo e l'erogazione di servizi pubblici digitali; in questo contesto la Pubblica Amministrazione diventa una vera e propria piattaforma di innovazione. Nel processo di trasformazione digitale, la digitalizzazione degli enti pubblici, componente 1 della missione 1, riveste infatti un ruolo fondamentale: gli obiettivi sono sfidanti (13 milestone e 27 i target per il 2023) e coinvolgono tutti gli aspetti fondanti della Pubblica Amministrazione. Il digitale riveste sicuramente in questo contesto un ruolo di primaria importanza: è il propulsore del cambio di paradigma, è l'acceleratore di un processo che richiede intrinsecamente rapidità. Non è un caso che proprio la Pubblica Amministrazione sia uno dei soggetti maggiormente coinvolti nel processo di trasformazione digitale dal Piano. Investimenti significativi, in ambito "PA Digitale", si stanno effettuando in termini di azioni concrete volte alla formazione del capitale umano e al miglioramento generale di efficacia della macchina organizzativa. Sarà lanciata Syllabus, una piattaforma digitale che consentirà di muoversi con rapidità per acquisire competenze fondamentali ed è stato già aperto il portale Inpa affinché tutte le procedure concorsuali siano digitali, consentendo di conseguenza di stringere i tempi nel processo di acquisizione delle risorse.

Fonte: MEF website

Traguardi e criticità

Nel Pnrr il processo di digitalizzazione prevede in primo luogo la creazione di infrastrutture digitali attraverso la realizzazione del Polo Strategico Nazionale (Psn), ambiente cloud dove confluiranno le informazioni provenienti da tutte le amministrazioni, consentendo l'interoperabilità dei dati e con l'obiettivo finale di sviluppare un'offerta integrata di servizi digitali per i cittadini. Contestualmente è iniziata la migrazione di dati, anche se, a fronte di oltre 11.000 data center attualmente presenti nelle PA italiane, si è ancora lontani dalla loro completa migrazione in cloud. Inoltre, pur essendo stato attestato il conseguimento del traguardo, la Pcm ha evidenziato come la lista degli enti pubblici che hanno completato lo spostamento verso il Psn sarebbe in realtà conseguenza di un errore materiale: il processo di migrazione non può essere materialmente implementato laddove l'infrastruttura non sia stata già oggetto di collaudo con esito positivo. Nel corso dell'anno 2023, le risorse complessive dell'investimento ammonteranno a 900 milioni di euro e saranno in buona parte destinate alle attività di migrazione degli enti di Pubblica Amministrazione Centrale e delle Asl. L'attività di migrazione della Pac non è ancora iniziata e si prevede una concentrazione della spesa dalla metà del 2023 e nelle annualità 2024 e 2025.

Per assicurare un buon funzionamento del sistema di digitalizzazione è indispensabile monitorare e garantire uno standard di cybersicurezza; a ciò sono stati dedicati ingenti e articolati investimenti nel piano, tra cui l'istituzione della nuova Agenzia per la Cybersicurezza Nazionale (Acn). A questo proposito, è stato decretato il raggiungimento dei risultati previsti e dei relativi tempi impiegati nel rispetto degli obblighi contratti con l'Unione Europea. I dati forniti dall'Acn e le evidenze finanziarie registrate in Regis mostrano che gli obiettivi previsti per il 2022 e riferibili alle risorse del Pnrr sono correttamente adempiuti. Protezione degli asset strategici nazionali, risposta delle minacce, risposta alle crisi cyber nazionali e sviluppo sicuro delle tecnologie digitali tramite strumenti volti a supportare centri di eccellenza e imprese sono gli obiettivi ancora da raggiungere. Resta il dubbio che gli investimenti stanziati per la tematica cybersicurezza siano in realtà ancora troppo bassi per soddisfare questi importanti obiettivi.

Il cittadino al centro

In ogni caso ci stiamo muovendo verso il modello del "government as a platform", raggiungendo importanti traguardi. Infatti, gli obiettivi che sono stati completati nei tempi previsti dal cronoprogramma fanno riferimento all'attuazione del Portale digitale unico; all'adozione della piattaforma PagoPA da parte del 60% delle PA e all'utilizzo da parte del 30% delle PA del front-end dell'app IO. In particolare, PagoPA vede più di 19.000 enti aderenti, più di 400 prestatori di servizi di pagamento coinvolti nella piattaforma e circa 650 milioni di transazioni effettuate, per un valore di oltre 126 miliardi di euro. Per il 2023 resta da raggiungere l'obiettivo finale europeo del numero di enti presenti nell'app IO (occorre giungere all'80% entro il 2026 e ad oggi siamo al 68%).

In questo contesto sarà quindi necessario focalizzarsi sul miglioramento delle competenze digitali di base, formando non solo coloro che erogano i servizi, ma anche e soprattutto gli utenti e, quindi, l'intera popolazione italiana. Al fine di migliorare le competenze digitali di base e superare il digital divide, il Pnrr ha previsto un importante investimento volto a migliorare le competenze digitali e la citizen inclusion. L'inclusione, secondo il Piano, coincide con il concetto di miglioramento dell'accessibilità dei servizi pubblici digitali: dovrà essere sviluppata un'offerta integrata e armonizzata di servizi digitali all'avanguardia orientati al cittadino, garantendo la loro adozione diffusa tra le amministrazioni centrali e locali e migliorando l'esperienza degli utenti.

Il ruolo strategico della cyber security in un'epoca di radicali mutamenti geopolitici

Mark William Lowe, Risk & Security Partner

Vedetta 2 Mondialpol

Cambiamento geopolitico

Fino a poco tempo fa, molte organizzazioni pensavano di poter ignorare la geopolitica: oggi non più. Non solo le relazioni e gli scenari internazionali bilaterali e multilaterali stanno cambiando, ma un certo numero di Paesi ha requisiti e obiettivi strategici che avranno un impatto diretto sulla cyber security. I professionisti della cyber security giocheranno quindi un ruolo sempre più strategico nella tutela degli interessi sia aziendali che nazionali.

Beijing ha fissato l'autonomia tecnologica come obiettivo prioritario strategico: per raggiungere questo ci sarà inevitabilmente un aumento dello spionaggio digitale. Nuova Delhi ha obiettivi economici ambiziosi e un'esigenza cronica di creare occupazione attraverso lo sviluppo di nuove industrie: lo spionaggio aziendale rappresenta in questo caso una scorciatoia. Mosca, non estranea ad azioni dirompenti, attribuisce grande importanza alla guerra informatica come forma di strategia offensiva e difensiva.

Questi esempi sono ben noti, anche se lo spionaggio digitale, e lo spionaggio aziendale in generale, non vengono affrontati con la necessaria diligenza. Ciò che è meno noto è quello che ci riserva il futuro. In termini di geopolitica, l'attuale realtà globale è caratterizzata da un susseguirsi di cambiamenti rapidi e radicali e quindi da un aumento delle minacce e delle sfide. Chi ha responsabilità per la difesa informatica si trova di fronte a un'accentuazione dei rischi esistenti e a un numero sempre crescente di minacce emergenti.

Una conseguenza del cambiamento geopolitico, e in particolare del sostegno ideologico alla Russia, è il preoccupante aumento delle azioni da parte di attori allineati allo Stato.

Ideologia: una minaccia crescente

Il 19 aprile scorso, il National Cyber Security Center (NCSC) del Regno Unito ha pubblicato un avviso riguardante la crescita di una nuova classe di avversari informatici russi: gruppi allineati allo Stato che sono motivati ideologicamente piuttosto che finanziariamente. A differenza dei gruppi sostenuti dallo Stato, gli attori allineati allo Stato non sono soggetti ad alcuna forma di controllo statale e quindi le loro azioni sono meno vincolate e i loro obiettivi sono più ampi rispetto agli attori tradizionali.

Forse la considerazione più allarmante è che l'NCSC considera gli attivisti allineati allo Stato molto meno prevedibili degli attori legati allo Stato, una preoccupazione molto significativa in quanto "meno prevedibile" può essere interpretata come priva di limiti imposti.

Le azioni promosse o approvate da uno Stato generalmente rispettano determinati limiti in quanto le conseguenze di un attacco, e le conseguenti misure di ritorsione, vengono prese in considerazione prima che qualsiasi azione sia autorizzata.

Questa mancanza di controllo è una delle principali preoccupazioni in quanto i gruppi "allineati allo Stato" non possiedono la capacità di comprendere appieno le conseguenze delle loro azioni e ciò potrebbe portare a situazioni molto gravi come attacchi distruttivi contro infrastrutture nazionali critiche.

Conclusioni

Gli attori statali (coloro sponsorizzati dagli Stati) e gli interessi privati sono alla base delle azioni cyber che conosciamo, mentre la crescita degli attori allineati allo Stato è una minaccia che dobbiamo ancora comprendere appieno.

I professionisti della cyber security dovranno adattarsi a un panorama altamente imprevedibile che si sta trasformando più velocemente di quanto possa essere mappato tramite i tradizionali controlli del rischio. Pur rimanendo minacce molto gravi, gli attacchi DDoS, le deturpazioni dei siti Web, la crittografia dei dati, o il furto dei dati dei clienti sono gli scenari migliori.

Alcuni potrebbero obiettare che per il momento i gruppi allineati allo Stato non hanno la capacità di lanciare attacchi distruttivi, una considerazione legittima, ma tuttavia questo è solo un vantaggio a breve termine.

Nel tempo gli attori ideologici acquisteranno maggiore capacità e quindi la sfida di oggi è quella di prevederli e prevenirli.

L'adattamento della normativa al processo tecnologico

Edoardo Gabbrielli, Consultant

Colin & Partners

Negli ultimi anni stiamo assistendo ad un'importante espansione del mondo digitale, il quale ha portato con sé una serie di sfide, che hanno riguardato anche il tema della protezione dei dati personali. Proprio su quest'ultimo tema ci siano stati diversi interventi normativi da parte degli Stati e degli Organismi Sovranazionali, come l'Unione Europea, (la quale ha introdotto il "Regolamento generale sulla protezione dei dati – GDPR), la realtà è che l'adattamento delle normative alla realtà digitale risulta essere, ad oggi, un processo lento e difficile, il quale non riesce a stare al passo con l'evoluzione tecnologica, poiché siamo in un'epoca in cui i dati personali vengono raccolti, elaborati e trasferiti con sempre maggior frequenza e in modi sempre più sofisticati.

Questo adattamento rappresenta sempre di più una sfida complessa da affrontare per due fattori fondamentali:

- In primo luogo, il mondo digitale ha portato con sé un'enorme espansione nella quantità di dati raccolti. La connettività dei dispositivi ha aumentato il potenziale per la raccolta di dati personali in modo crescente. Inoltre, i dati personali possono essere raccolti e utilizzati in modo sempre più invasivo e con tecnologie complesse: ad esempio attraverso il monitoraggio continuo delle attività online degli utenti in caso di uso dei social media e delle piattaforme di e-commerce. Queste ultime raccolgono una vasta quantità di dati sui comportamenti degli utenti, tra cui le loro preferenze di acquisto e di navigazione. Questo ha reso più difficile, per le persone, comprendere per quale motivo vengono utilizzati e soprattutto con quali modalità sono impiegati. Ciò significa che gli utenti si trovano spesso a dover conferire i propri dati senza capire le reali intenzioni di chi li raccoglie.
- In secondo luogo, la complessità della tecnologia digitale ha reso sempre più difficile proteggere adeguatamente i dati personali. Ci sono innumerevoli modalità attraverso cui i dati possono essere compromessi o violati, a partire dalle vulnerabilità del software fino alla perdita fisica del dispositivo. Inoltre, la tecnologia digitale sta evolvendo rapidamente e ciò rende arduo per le aziende e per le pubbliche amministrazioni mantenere il passo con le minacce alla sicurezza dei dati.

Un ulteriore elemento che rende più complicata la corretta applicazione delle normative in materia di protezione dei dati personali è la consapevolezza degli utenti riguardo alla riservatezza e l'uso dei loro dati personali. Come già anticipato, è generalmente bassa la conoscenza delle implicazioni rispetto alla condivisione dei propri dati personali online, così come delle norme che aziende e pubbliche amministrazioni sono tenute a rispettare; anche, le modalità di raccolta e di trattamento possono essere poco chiare e comprensibili per gli utenti

Inoltre, con l'evoluzione tecnologica e lo scambio di informazioni e dati su larga scala, la protezione dei dati è diventata una questione globale e non un fenomeno strettamente locale, necessita, quindi, di una cooperazione internazionale, soprattutto per le aziende che hanno sede in diversi Stati. Infatti, esse devono essere in grado di rispettare le normative in diversi paesi e regioni, il che può essere un compito faticoso, considerando che queste ultime possono variare notevolmente da un paese all'altro.

Fortunatamente su tutti questi ultimi aspetti, il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea, entrato in vigore nel maggio 2018, ha rappresentato un passo avanti significativo per la data protection, in quanto stabilisce obblighi molto stringenti in materia di trasparenza e informazione verso l'interessato di cui vengono trattati i dati personali e trova applicazione in tutti gli Stati membri dell'Unione Europea. Tuttavia, anche se il GDPR ha stabilito norme severe, l'adeguamento al Regolamento sembra essere un'impresa difficile per molte aziende e P.A., soprattutto sul tema della sicurezza, nonostante siano passati 5 anni dalla sua entrata in vigore.

Infatti, secondo l'ultimo report del Clusit, gli attacchi, nel 2022, sono cresciuti del 60% rispetto a quelli rilevati nel 2018. Non a caso, l'Autorità Garante per la Protezione dei dati Personali nel periodo dal 1° gennaio al 31 dicembre 2021 ha ricevuto 2.071 notifiche di violazioni da parte di soggetti pubblici (50,5% dei casi) e privati (49,5% dei casi).

Non deve essere solo la norma a indurre aziende e Pubbliche Amministrazioni ad adempiere all'obbligo di dotarsi di misure di sicurezza (anche di ordine organizzativo) volte alla prevenzione di breach, ma anche l'interesse a proteggere know how, reputazione e credibilità sui mercati.

Oltre che sugli aspetti relativi alla protezione dei dati personali, l'Europa è particolarmente attenta anche al tema cybersecurity, tanto è vero che ha recentemente approvato la direttiva NIS 2 che, ne siamo certi, sarà di stimolo per ripensare tale materia non solo rispetto ai sistemi informativi, ma nell'intera organizzazione.

Sicurezza e tutela continuano, dunque, a rappresentare la sfida attuale e futura per molte organizzazioni. Alcune non dispongono, a oggi, di risorse necessarie per garantirle in modo efficace, altre non sono in grado di adempiere adeguatamente alle normative in materia per carenza di cultura specifica sul tema.

Diviene quindi fondamentale fotografare in modo trasparente e obiettivo la propria realtà. Un'analisi accurata è imprescindibile. La compliance può diventare un'amica; un intento continuativo e un impegno costante per garantire il proprio operato e le possibilità di crescita in contesti tecnologici e giuridici estremamente in fermento. Istituzioni e Autorità di Controllo dovrebbero provare ad accelerare il processo di produzione delle norme, laddove possibile, andando anche ad anticipare la disciplina di nuovi fenomeni. Così come riteniamo fondamentale un approccio proattivo da parte del mondo produttivo o delle pubbliche amministrazioni, anche a livello legislativo non si può giocare una partita in rimessa. Questo se si mira a sviluppare una consapevolezza globale sufficiente a consentire di godere degli enormi vantaggi che il progresso tecnologico può offrire a tutti i livelli.

Il canale ICT si muove sul valore. E scopre il bello dei servizi

Loris Frezzato, Channel Area Manager
The Innovation Group

Il mercato ICT pare essere stagnante, ma mostra buone prospettive dall'offerta a valore e lascia intendere di poter sperare in bene per la seconda parte dell'anno. A dirlo è Context, la società di analisi che monitora il venduto attraverso la distribuzione, monitorando il sentiment di un canale di terze parti ICT che in questo periodo di incertezze ha bisogno di trovare nuove strategie e nuovi modelli di approccio ai clienti, sempre più esigenti e bisognosi di strumenti che agevolino il proprio business.

E i dati raccolti da Context per questi primi mesi dell'anno indicano per il primo trimestre 2023 un mercato ICT italiano in calo dell'1% comparato con lo stesso periodo dello scorso anno. Ma sul fronte del canale ICT il bilancio è allettante, come ci spiega Isabel Aranda, country manager di Context per l'Italia, interpellata da IctBusiness Ecosystem per avere un quadro sull'andamento del canale nel nostro Paese. Un tema che Context avrà modo di esporre in maniera dettagliata e aggiornata in occasione dell'intervento previsto all'interno dell'ICTBusiness Ecosystem Summit del 6 giugno, l'evento che The Innovation Group dedica annualmente ai protagonisti del canale ICT italiano.

Mercato flat, ma la distribuzione cresce

"Complessivamente, per quanto riguarda la distribuzione, l'anno è iniziato molto bene con un inatteso +13% realizzato a gennaio, frutto anche di una crescita a doppia cifra per quanto riguarda il mercato TLC, dovuto soprattutto al mercato degli smartphone e in concomitanza con la consegna dei nuovi modelli

iPhone, i quali hanno dato un forte impulso a tutto il comparto" afferma Aranda.

Una crescita alla quale, già da febbraio 2023, è seguito un lento declino, con febbraio e marzo in negativo, rispettivamente -9 e -7%. E anche aprile, complici i ponti e le festività, si prevede sarà caratterizzato da una domanda piuttosto calma. Come da tradizione, del resto.

"Il mercato della distribuzione è, soprattutto da quest'anno, trainato dai prodotti e soluzioni a valore" riprende Aranda "Dopo la "sbornia" delle vendite a volume del periodo pandemico e immediatamente successivo, ora l'orientamento è verso il valore, un mercato che da almeno cinque mesi consecutivi sta crescendo a doppia cifra e che ha chiuso il Q1 a +15%".

Il canale a valore sente gli effetti boost delle scuole

A questo contribuisce uno spostamento degli investimenti, soprattutto da parte del settore education, verso le infrastrutture in cloud e il software, con la parte di security che cresce parecchio. Le scuole, inoltre, avranno accesso, secondo i piani, a ulteriori fondi nella seconda parte dell'anno, continuando probabilmente a contribuire alla crescita del mercato sui temi digitali e di connessione.

"Vero è che per molti versi si stanno ancora godendo gli effetti di back order dello scorso anno, ma rimane comunque un mercato che mantiene una domanda attiva" commenta la country manager.

La parte di software per la cybersecurity non smette di dare soddisfazioni, registrando una crescita del 19%, addirittura oltre quanto realizzato dall'intero mercato a valore.

Anche gli switch crescono e lo fanno di oltre il 60%, grazie soprattutto agli strascichi dei progetti dello scorso anno che stanno proseguendo, sia da parte della PA sia dalle aziende private.

L'incertezza regna sul mercato del Q2

Anche se in questo attuale momento i progetti stanno rallentando per la graduale aumento dell'incertezza dei mercati dovuti all'inflazione ancora alta, pur in leggero decremento rispetto lo scorso anno, agli alti tassi di interesse e un timore di una ristretta del credito e agli effetti dell'incertezza sui mercati globali per la situazione geopolitica scatenata dal conflitto Russo-Ucraino.

Un segnale di calo dell'inflazione che però non è detto si traduca immediatamente in un abbassamento dei prezzi alla distribuzione. Alcune categorie di prodotti come stampanti e networking, hanno infatti visto un aumento dei prezzi, mentre altre categorie hanno avuto addirittura delle riduzioni.

"Per la fine di aprile è attesa la terza tranche del Pnrr, dalla quale si attende un po' di stimolo a un mercato che è molto turbato dalla situazione macroeconomica attuale. Ma la ripartenza vera è prevista a partire dal Q3".

I partner a valore trainano il mercato del canale ICT

Chi porta porta avanti il mercato nella distribuzione è, comunque, il canale business dei prodotti e soluzioni a valore, che vede i corporate reseller e system integrator come protagonisti principali.

Con i corporate reseller che guadagnano continuamente share nella compagine dell'ecosistema del canale italiano: 3 punti nel Q1 2023 rispetto allo stesso periodo dell'anno precedente, crescendo dell'11% in fatturato. Sono questi gli operatori preferenziali che interfacciano la PA e le aziende di livello entrerprise, per forniture di grandi dimensioni.

Questo per quanto riguarda il canale, mentre il target di riferimento più proficuo rimane quello delle aziende Small and Midsize, che rappresenta il 41% del mercato della distribuzione, di competenza delle realtà del canale più piccole, i reseller, che su questo ambito hanno visto anche una crescita dell'1% nel primo trimestre 2023. "Un target di utenza che ha un alto potenziale di crescita, probabilmente più lento rispetto ad altri, ma che sta anch'esso via via diventando recettivo all'offerta a valore, anche se trasferibile da un canale di reseller di dimensioni più piccole" commenta Aranda.

Un aiuto anche dalla sostenibilità

Alti e bassi, equilibri interni in altalena ma che per fine anno dovrebbero, secondo le previsioni di Context, tirare le somme con un +1% di crescita complessiva del mercato ICT. Risultato al quale non va dimenticato di assommare gli effetti derivanti dalla crescente attenzione al tema della sostenibilità, con gli obblighi a breve termine per le grandi aziende e, poco dopo, anche per le PMI, e che sta interessando sempre di più anche gli operatori del canale.

Stimolo che è anche nelle carte del Pnrr, che indica l'adesione a criteri di sostenibilità per le aziende che partecipano ai progetti finanziabili con quei fondi. Attivando un processo di digitalizzazione progressiva che può così contribuire attivamente all'ecosostenibilità.

Facciamo il punto sull'Intelligenza Artificiale

Elena Vaciago, Research Manager
The Innovation Group

Stiamo assistendo a un'ondata di innovazione legata all'AI (Artificial Intelligence), ma è evidente che le sfide per rimanere competitivi in questo campo sono molteplici: servono competenze diffuse, diversificate, complementari. Serve una collaborazione forte tra accademia, istituzioni ed aziende utenti finali. Serve un disegno a breve, medio e lungo termine, perché le realizzazioni siano in linea con una concezione socialmente ed economicamente sostenibile di questa tecnologia.

A che punto siamo oggi con gli sviluppi AI e in che direzione stiamo andando? Il tema, molto ampio e complesso, è stato approfondito lo scorso 5 aprile nel corso dell'AI Forum 2023, principale momento di confronto italiano tra tutti gli stakeholder sul tema: dalle associazioni, agli esperti, alle aziende che oggi già stanno applicando queste innovazioni al proprio interno. È emerso così un quadro molto variegato, la necessità di fare sempre più sistema, di contaminare i saperi in gruppi di lavoro diversificati, in modo che si possa arrivare in tempi brevi a sviluppi innovative e contestualmente ritagliati sulle esigenze specifiche del singolo caso.

Come procedono gli sviluppi AI. "Oggi vediamo che nel mondo AI c'è un forte interesse per il sottoinsieme delle tecnologie Machine Learning, ossia, come apprendono le macchine – ha detto Gianluigi Greco, Presidente di AIxIA (dal 1988 la principale fondazione sul tema AI, arriva a contare oggi 1.500 soci tra professori e ricercatori) -. Turing si chiedeva se le macchine possono pensare: oggi invece ci chiediamo se e come le macchine apprendono. La qualità del riconoscimento immagini è diventata superumana: dal 2017 le macchine hanno superato le capacità dell'uomo". Con riferimento all'impegno di Università e Ricerca italiane, oggi abbiamo secondo AIxIA 53 atenei che trattano l'AI in Italia. Una rivoluzione che è avvenuta in pochi anni, e nessuna area geografica italiana è scoperta. Abbiamo corsi su AI in 45 diverse classi di laurea, non solo quelle più tecniche come ingegneria e scienze, segnale che questo tema sta diventando sempre più pervasivo in tutte le lauree. Cosa

si studia? “Il Machine learning, soprattutto, nel 19% dei casi, ma anche tutto il resto: data mining, computer vision, robotics, agent based systems, natural language processing. Ora è d’interesse anche il tema dell’etica per l’AI” ha spiegato Gianluigi Greco.

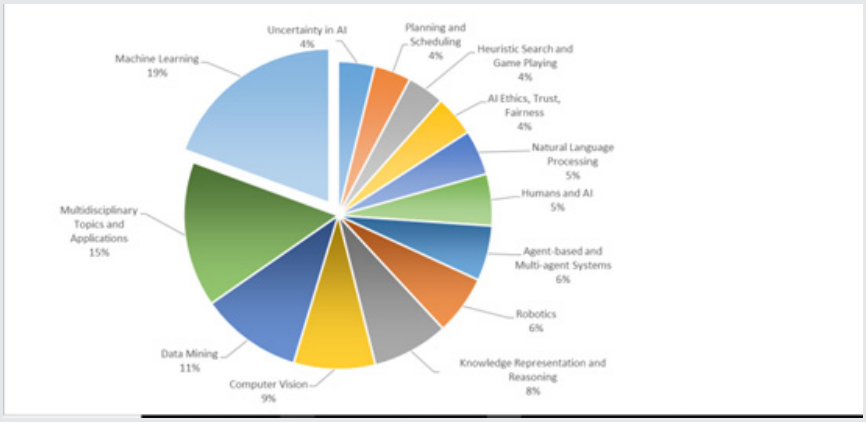
Con riferimento invece all’adozione di tecnologie AI nelle aziende italiane, la crescita continua ad essere impetuosa (il mercato dell’AI ha raggiunto i 500 milioni di euro nel 2022, con un aumento del 32% in un solo anno) ma permane ancora un forte divario tra grandi e piccole aziende. Se le statistiche vedono un 34% delle grandi imprese già in fase di implementazione dell’AI nel business, il 33% in cammino e il 33% in attesa, invece, tra le PMI, solo il 15% è in fase di implementazione, il 33% in cammino e la maggioranza, il 62%, rimane ancora in attesa (stime del Politecnico di Milano).

Parlando di implementazione di tecnologie AI in azienda, Antonella Periti, Deputy Chief Information Officer di Edison, ha osservato: “Noi abbiamo iniziato sette anni fa con una strategia per l’AI che ha messo le basi per diversi use case. Essendo una società energetica, per noi gli ambiti dove portare questa tecnologia sono ad esempio le bollette dei clienti o la produzione energetica sostenibile. Una Data platform abilita progetti di successo: abbiamo un progetto di cloud computing da 4 anni per modernizzare l’infrastruttura. Ora siamo in grado di utilizzare tecnologie innovative, come ad esempio la blockchain. Tramite metodologia agile, abbiamo applicato l’AI sulle centrali termoelettriche, per ottenere risparmi su costi umani ed energetici. Abbiamo visto che cambiano molto le competenze richieste alle persone, noi ne abbiamo sviluppate di nuove con attività di formazione verticale: ci hanno aiutato in questo le startup. Il suggerimento che do per questi progetti complessi è che l’accuratezza del dato è molto importante. Inoltre, il cliente interno deve vedere questa soluzione come un valore aggiunto”.

Nel settore assicurativo, l’utilizzo di modelli di machine learning è già applicato da tempo, ad esempio per ottimizzare i tempi di liquidazione, o per l’antifrode. “Da quando è nata, l’assicurazione si basa sui dati – ha detto Massimo Natale, Head of Data & Platform Governance di Generali Italia -. Oggi l’AI si applica bene anche nell’interfaccia con il cliente finale. Nel processo di liquidazione sinistri, abbiamo rivisto l’intero processo: oggi è gestito tramite una App telefonica molto veloce e user friendly, che all’interno del processo utilizza un motore AI. Partendo dal video del danno, stima il danno e propone al cliente in determinate condizioni una pronta liquidazione. Si tratta per ora di una prima sperimentazione, però il vero scopo è quello di lavorare a nuovi sistemi AI: prima bisogna provare, fallire, portare in produzione qualcosa che funziona, quindi creare conoscenza interna. Oggi anche gli Stati cercano di riportarsi il know-how strategico in casa: noi come gruppo di lavoro abbiamo questo obiettivo e, dove dovessero esserci esternalizzazioni, anche in questo caso cerchiamo di portare la conoscenza in casa. I dati devono essere di qualità, di trust elevato e certificato. La vera sfida per i prossimi anni sarà avere un dato di qualità, in futuro la vera benzina nel motore. Siamo in un ambito molto regolamentato, il GDPR prevede multe elevate, per cui quando approcciamo questi temi abbiamo presente il rischio di una cattiva gestione del dato”.

Qual è la maturità raggiunta oggi dall’AI. Oggi abbiamo alcune tecnologie (ChatGPT è una di queste) che hanno raggiunto capacità superumane, hanno performance molto elevate e prestazioni irraggiungibili nella creazione di testi, ma poi cadono quando ricevono domande che ne testano le capacità logiche, di ragionamento. Si tratta di un’AI che non sa ancora risolvere un problema, e che in realtà non è progettata per questo: analizza grandi quantità di dati, ma

Presenza dei Topics nei Corsi



Fonte: Intervento di Gianluigi Greco Presidente di AIxIA all’AI Forum del 5.4.23, Milano

non fornisce una risoluzione a problematiche complesse con esigenze di ragionamento. Manca quindi di capacità di astrazione: se torniamo alla domanda originaria di Turing, “Le macchine sanno pensare?”, vediamo che ancora non ha avuto risposta.

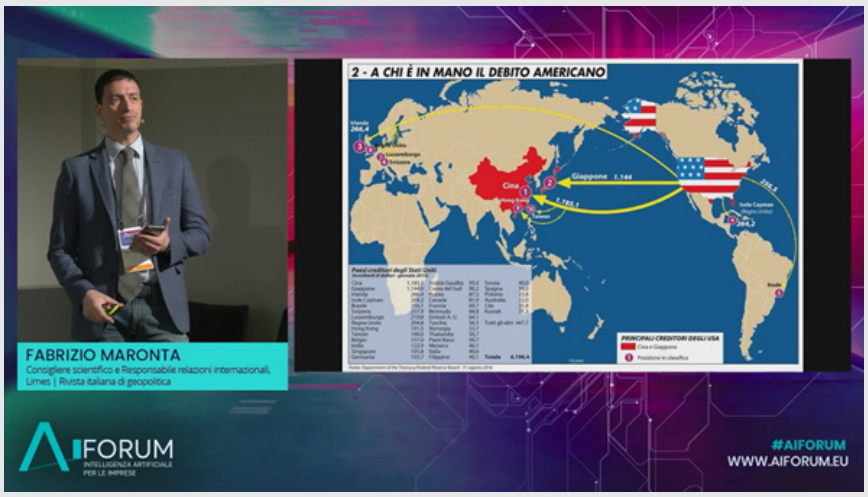
Con riferimento al blocco di ChatGPT da parte del Garante privacy italiano (disposto lo scorso 31 marzo in quanto, secondo il Garante, manca una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati personali allo scopo di “addestrare” gli algoritmi sottesi al funzionamento della piattaforma), è intervenuto Guido Scorza, Componente del collegio del Garante della protezione dei dati personali. “Il rapporto tra le regole per la protezione dati, lo sviluppo degli algoritmi e il progresso tecnologico connesso all’addestramento non è facile: è ovvio che abbiamo un problema di asimmetrica dal punto di vista del calendario. Il ritmo del progresso non è comparabile con il ritmo dei processi di regolamentazione e applicazione delle regole” ha detto Guido Scorza. “Il GDPR era un testo illuminato e moderno, il mondo intero ce l’ha invidiato e in parte anche copiato. Concepito nel 2014 è entrato in vigore nel 2016, quindi accusa ora un po’ di ritardo rispetto agli sviluppi rapidissimi della tecnologia”.

Ad esempio, i modelli del linguaggio come ChatGPT non erano contemplati nel regolamento fino a qualche mese fa: la norma aveva provato a normare l’AI senza poter prevedere però queste applicazioni. Cosa fare quindi in attesa di trovare la soluzione, per bilanciare l’esigenza del progresso tecnologico con una disciplina

che possibilmente riguardi tutti? “Un punto molto rilevante è il fatto che l’addestramento presuppone la raccolta e il trattamento di una mole di informazioni sovrabbondante, inclusi i dati personali. Una risposta può essere individuata guardando all’universo della ricerca, eccezione più importante contenuta nel GDPR – ha detto Guido Scorza -. Pensiamo ad esempio a chi raccoglie dati per necessità statistica: anche in questo caso, non si può prescindere dalla trasparenza assoluta non tanto nei confronti dell’utente del servizio, piuttosto nei confronti di chi, pur non usando il servizio, ha i suoi dati trattati. Chi si trova coinvolto in una ricerca di qualsiasi genere, ha sempre la possibilità di sottrarsi, ad esempio dicendo che i suoi dati non devono esserci”.

Quanto lo sviluppo dell’AI sarà influenzato dagli scenari geopolitici. “Il paradigma uscito vincente dalla guerra fredda è stato la vittoria della democrazia liberale e del capitalismo di matrice statunitense – ha detto Fabrizio Maronta Consigliere scientifico e Responsabile relazioni internazionali, Limes | Rivista italiana di geopolitica -. L’adesione a questo disegno dal mio punto di vista è stato un grandissimo esperimento geopolitico, con gli USA che hanno cercato di assimilare al proprio modello sociale, economico e politico, Paesi che fino a poco tempo prima erano stati dall’altra parte della barricata. La Russia doveva essere teoricamente parte di questo processo. Come è stato fatto? Con lo stesso strumento utilizzato dagli USA dopo la Seconda guerra mondiale con Europa e Giappone, ossia, l’interdipendenza economica, un processo che poi è andato molto oltre, diventando interdipendenza industriale, diplomatica e finanziaria”.

La globalizzazione è stata in gran parte negli ultimi 25 anni un matrimonio d’interesse tra Cina e USA, in cui, semplificando al massimo, la Corporate America ha sfruttato i vantaggi competitivi della Cina per delocalizzare. In questo modo, l’economicità delle merci cinesi ha puntellato il potere di acquisto della classe media americana che nel frattempo perdeva posti di lavoro, reddito e status sociale. Intanto, con gli attivi commerciali maturati, la Cina acquistava varie cose, tra cui il debito pubblico americano.



Fonte: Intervento di Fabrizio Maronta Consigliere scientifico e Responsabile relazioni internazionali di Limes all’AI Forum del 5.4.23, Milano

“Oggi siamo in un contesto – ha aggiunto Fabrizio Maronta – in cui viene messa in discussione l’interdipendenza che dal 2001, con l’ingresso ufficiale della Cina nella WTO, l’organizzazione mondiale del commercio, ha strutturato il nostro mondo economico. Oggi si aprono quindi partite di reindustrializzazione, che riguardano soprattutto gli ambiti più innovativi. Per fare questo l’Europa rischia però di essere il vaso di coccio in mezzo ai vasi di ferro: deve ristrutturarsi e questo non sarà indolore, non sarà consensuale. Tutti questi discorsi non dovrebbero farci mai scordare che gli aspetti prettamente tecnologici (con i risvolti morali, sociali, giuridici che l’evoluzione della tecnologia comporta), non sono avulsi, perché in realtà sono considerati da attori statali come strumenti di competizione geopolitica e internazionale. Quindi sono anche contrastati, agevolati, usati dai diversi Paesi per i propri scopi”.

ISCRIVITI ALLA NEWSLETTER MENSILE!

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

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it