

An underwater scene with a fishing hook hanging from a thin line. The water is blue with light rays filtering down. Numerous '@' symbols and small bubbles are scattered throughout the scene.

A PESCA D'IDENTITÀ



Direttore responsabile: Stefano Cuzzilla

Vice Direttrice: Dina Galano

In redazione: Assunta Passarelli,
Antonio Soriero, Valentina Neri

Web Manager: Federico Romani

Provider e sviluppo grafico:

IWS SpA - Industria Welfare Salute

Redazione: Roma – via Ravenna, 14

Telefono: 06-44070236 / 261

progettomanager@federmanager.it

Sito web:

progettomanager.federmanager.it

Editore: Manager Solutions srl

sede legale: Roma - Via Ravenna 14 - 00161

Registrazione Tribunale di Roma n. 297

del 12.12.2013

Tipografia: Artigrafiche Boccia spa

Finito di stampare

Aprile 2024

IN QUESTO NUMERO...

Cybersecurity

Etica

IA

Sostenibilità

Dati

Donne

Digitale

Reti

Ue

Elezioni

Fake news

Privacy

Geopolitica

Rischi

Competenze

Investimenti

Bitcoin



PROGETTO MANAGER

IL MENSILE DI FEDERMANAGER



LEGGI I NUMERI PRECEDENTI

INTERVISTE, APPROFONDIMENTI E ANALISI SUL MONDO
DEL MANAGEMENT E NON SOLO



L'EDITORIALE DI STEFANO CUZZILLA

Per una crescita strutturale

L'ampia **riforma fiscale** voluta dal Governo sta procedendo attraverso gli **step** dei diversi decreti attuativi e può rappresentare un punto di svolta importante per il Paese. Ce lo auguriamo, soprattutto perché la nostra capacità di essere competitivi è strozzata dal peso di un fisco iniquo e da cattiva **burocrazia**.

Dalle premesse che vediamo, alla base della riforma si pone l'intento politico di agire per **ridurre la pressione fiscale** su famiglie e imprese, **semplificare** e rendere comprensibile il quadro normativo e garantire una piena **certezza del diritto**.

Se è giusto intervenire per migliorare l'efficacia delle fasi sanzionatorie e i meccanismi di riscossione, in un Paese come il nostro che patisce un **tax gap** intorno ai **100 miliardi**, non si deve però appesantire il panorama del **contenzioso**, con oltre il **40% delle controversie civili** presso la Corte di Cassazione che riguarda oggi questioni di carattere tributario. Appare pertanto più che opportuno che si proceda spediti sulla via di una modernizzazione e sburocratizzazione di sistema; il che significa sposare il concetto che **per pagare meno tasse è necessario che le paghino tutti**. Altrimenti si ricade nell'usuale malcostume italiano di vessare chi lavora onestamente, come i tanti manager che la nostra Federazione rappresenta, e di permettere a chi fa il furbo di vivere sulle spalle degli altri, beneficiando di servizi a cui non contribuisce. Per crescere in **maniera sostenibile sotto il profilo economico e sociale**, l'Italia ha bisogno quindi di **giustizia ed equità fiscale**, anche e soprattutto per quel **ceto medio** che è il motore dell'iniziativa economica nazionale.

Chi guadagna da 50 mila euro in su non può essere considerato un super ricco, come ha ben sottolineato il Viceministro Leo anche in occasione del nostro **Open day Cida** sulla petizione a salvaguardia del ceto medio. L'intervento riformatorio rappresenta un banco di prova importante per tutti e, affinché il Paese sia in grado di fare uno scatto in avanti, dovranno essere coinvolte al meglio **competenze, professionalità e amministrazioni** diverse. Soprattutto perché, quando parliamo di fisco, parliamo anche di **investimenti** sullo sviluppo e sul progresso dell'Italia. La **leva fiscale** ha difatti assunto, negli ultimi anni, un ruolo preponderante anche come strumento di **politica industriale**, grazie a un significativo strumentario di agevolazioni e crediti di imposta.

Organizzazioni come la nostra vogliono sempre più contribuire a un **dialogo qualificato con tutti i livelli istituzionali** per favorire interventi, sul piano normativo e regolatorio, che producano effetti benefici in termini di **crescita strutturale**. Dal **taglio del cuneo fiscale** ai sostegni di cui le Pmi hanno bisogno per dotarsi di **competenze manageriali innovative**, serve un progetto di riforma affidabile, che premi chi è onesto e rilanci il lavoro.



PROGETTO MANAGER

IL MENSILE

DI FEDERMANAGER

NON

CI

RACCONTIAMO

STORIE



PER RICEVERLO OGNI MESE
ISCRIVITI SUL SITO
progettomanager.federmanager.it

INTERVISTE, ANALISI, APPROFONDIMENTI
SUL MONDO DEL MANAGEMENT E NON SOLO

Al passo con il futuro

Portare a termine un ampio processo di **trasformazione digitale** nel Paese delle antiche vestigia, delle tradizioni, delle consuetudini. Obiettivo non facile, ma abbiamo il dovere di centrarlo.

Anche perché la congiuntura storica non ammette alternative e le risorse a disposizione ci sono. Basti pensare che **la missione n.1 del Pnrr**, denominata *"Digitalizzazione, innovazione, competitività, cultura e turismo"*, prevede lo stanziamento di **oltre 40 miliardi di euro**: una cifra imponente, da gestire con sapienza e lungimiranza.

Del resto, i processi lavorativi all'interno delle organizzazioni stanno traendo indubbi benefici dall'adozione di **nuove modalità operative** e buona parte del merito è da ascrivere allo sbalorditivo **sviluppo tecnologico** degli ultimi anni.

Sviluppo che ha però come contraltare un panorama di **complessità** da fronteggiare. Pensiamo a quanto importante sia oggi un tema come quello della **cybersecurity**, fondamentale per proteggere il **patrimonio industriale** e le preziose **banche dati** delle aziende e della Pubblica amministrazione. Oppure anche al tema dell'integrazione nei processi dell'**intelligenza artificiale**, una rivoluzione che si sta manifestando a **una velocità senza precedenti**, come sottolineato più volte anche da Sam Altman, guru di OpenAI.

Per governare il cambiamento e stimolare una piena **competitività** del sistema Paese, servono certamente **infrastrutture e tecnologie** all'avanguardia, ma servono soprattutto **competenze** al passo coi tempi. È necessario, in altre parole, lavorare a un **nuovo umanesimo** che ponga la persona, con un rinnovato bagaglio di **conoscenze tecniche** e di **soft skill**, al centro dei processi di digitalizzazione.

Su questo fronte, c'è molto da lavorare. Infatti, il recente *"Digital decade report"* della Commissione europea ha evidenziato come, in Italia, solo **il 46% delle persone** possieda competenze digitali di base. E se si guarda nel dettaglio al settore occupazionale, ben si comprende quanto sia urgente procedere attraverso efficaci iniziative di **upskilling** e **reskilling**.

Anche per tali ragioni, la nostra Federazione insiste sul tema della **formazione** e promuove un percorso come **BeManager**, che **certifica le competenze manageriali** di figure quali **l'innovation manager**, in grado di trasformare il modo di fare azienda, soprattutto nelle Pmi.

Ma bisogna guardare anche oltre e, come avvenuto proprio per il **voucher per innovation manager**, vogliamo lavorare di concerto con le istituzioni perché siano previsti fondi che supportino le **Pmi** a inserire, nell'assetto aziendale, figure apicali con specifiche competenze digitali.

Abbiamo un obiettivo chiaro: aggiornare e riconvertire la nostra **forza lavoro**. E per farlo, le opportunità offerte dalla rivoluzione digitale devono essere colte innanzitutto a livello manageriale.



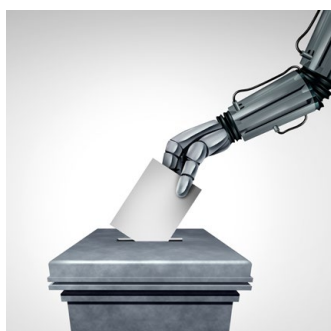


8 A COLLOQUIO CON

Capitali all'opera

AUTORE DINA GALANO

Un piano ambizioso: iniettare 8 miliardi per stimolare la creazione di start-up e investire nell'economia reale. A partire dal comparto AI e cybersecurity. Progetto Manager incontra Agostino Scornajenchi, Ad e Dg di Cdp Venture Capital

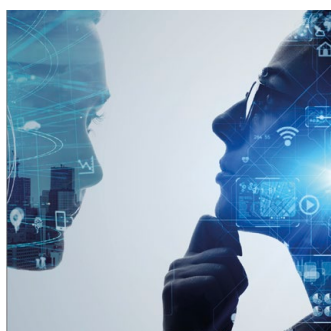


11 SCENARI

Rischio influenze

AUTORE LUCA ZORLONI

Tra intelligenza artificiale, deepfake, fake news e blackout di internet, il 2024, con elezioni che portano al voto metà della popolazione mondiale, è un anno delicato per le democrazie e per le imprese

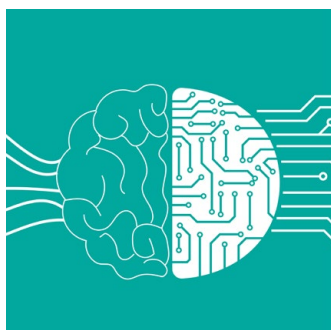


14 STORIE

Le amiche geniali

AUTORE DOMITILLA BENIGNI

Ridurre il divario di genere dei professionisti della cybersecurity, superando gli stereotipi e promuovendo lo sviluppo di competenze innovative. La sfida di Women4Cyber

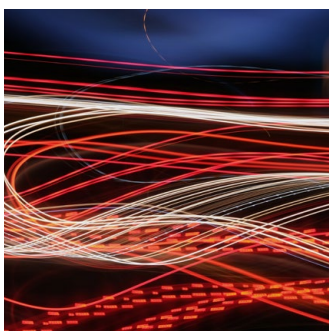


17 RIFLESSIONI

Combinazione di sicurezza

AUTORE STEFANIA SANTUCCI

Intelligenza artificiale, machine learning, deep learning: gli sviluppi tecnologici aprono la strada a innovative soluzioni di sicurezza. Ma le competenze umane rimangono imprescindibili

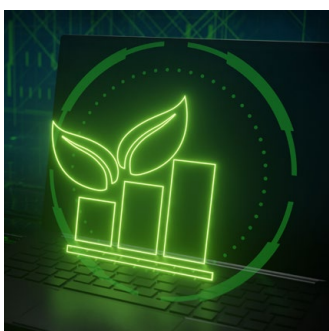


20 A COLLOQUIO CON

Profondo rosso

AUTORE ANNA MARIA SELINI

Cavi per le comunicazioni e per il trasporto di energia. Sotto i mari viaggia una parte consistente degli asset mondiali e i rischi per la sicurezza sono sempre altissimi



23 SCENARI

Senso obbligato

AUTORE STEFANO EPIFANI

Sicurezza digitale e sostenibilità, due obiettivi fondamentali che orientano strategie e processi operativi delle aziende, rivelandosi sempre più interdipendenti

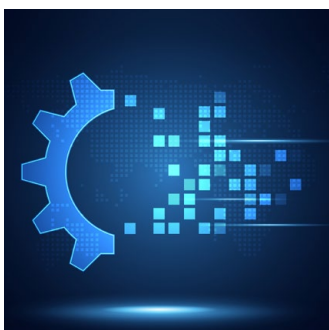


26 DALL'ESTERO

La fabbrica del consenso

AUTORE DAVIDE IPPOLITO

L'intelligenza artificiale generativa irrompe nella campagna elettorale americana con testi e immagini che hanno la capacità di influenzare fortemente l'opinione pubblica



29 RIFLESSIONI

A, B, C, Digitale

AUTORE MAURIZIO PIMPINELLA

Italia dietro la lavagna, con livelli medi di conoscenza di digitale e finanza troppo bassi per un Paese che voglia davvero essere protagonista della competizione globale. E non solo sul piano industriale

A COLLOQUIO CON

CAPITALI ALL'OPERA

AUTORE: **DINA GALANO** - TEMPO DI LETTURA: **3 MINUTI**

The image features a magnifying glass with a black frame, centered over the letters 'Ai' in a large, white, sans-serif font. The background is a deep blue with a subtle grid pattern. In the foreground, there are several stacks of silver coins of varying heights. Overlaid on the coins and the background is a white line graph with several upward-pointing arrows, suggesting growth or investment. The overall composition is clean and modern, with a focus on financial and technological themes.

Ai

Un piano ambizioso: iniettare 8 miliardi per stimolare la creazione di start-up e investire nell'economia reale. A partire dal comparto AI e cybersecurity. Progetto Manager incontra Agostino Scornajenchi, Ad e Dg di Cdp Venture Capital

Agostino Scornajenchi, Amministratore delegato e Direttore generale di Cdp Venture Capital, ha presentato a Milano il nuovo **piano industriale** quinquennale, con un progetto che punta a mobilitare, entro il 2028, ben **8 miliardi di risorse** e a trasformare il **venture capital** «in un'infrastruttura al servizio del Paese, al pari di quelle già esistenti che trasportano acqua, energia, persone», afferma Scornajenchi. Sono “sei più uno” gli ambiti individuati come strategici per l'**economia** italiana: quel “più uno” si riferisce al miliardo di euro dedicato all'**intelligenza artificiale**, l'investimento trasversale agli altri che, per volontà del Governo, arriva a rinforzare lo sviluppo di soluzioni AI in Italia e a fare da moltiplicatore di nuovi investimenti.

L'incidenza del venture capital su nostro Pil è ferma allo 0,1%, in Francia arriva allo 0,4, la media Ue è dello 0,3. Cdp Venture Capital punta a essere un soggetto economico protagonista. Lei dice, però: «Non saremo il supermercato degli incentivi». Cosa vorrete essere?

Vogliamo difendere la nostra posizione industriale, dobbiamo fare le cose, non comprarle da altri. Per questo il nostro piano è a 5 anni, perché per realizzare le cose ci vuole tempo. Noi non intendiamo soltanto finanziare **progetti**, ma diventare imprenditori insieme ai *founder*, con un approccio attivo e non meramente finanziario, sostenendo anche i rischi connessi. L'obiettivo del piano è paragonare almeno la media europea, raggiungendo lo 0,3% su Pil. Perciò occorre una *investment proposition* chiara. Non vogliamo diventare un “investificio”, essere identificati come il supermercato dell'**equity** agevolato. Altrimenti rischiamo di creare un sistema di selezione avversa, in cui le *start-up* migliori non verranno da noi e noi rimarremo dipendenti dal capitale pubblico, che è un bene ci sia, ma solo se serve a spingere altri **investimenti**. Non vogliamo salvare imprese, vogliamo costruire le imprese di domani.

È questa la sua visione del venture capital?

Mi sono occupato a lungo di **infrastrutture** nel-

la mia vita e per me il *venture capital* assume la forma di un'infrastruttura al pari di quelle già esistenti che trasportano acqua, energia, persone, e che, in questo caso, trasmette capitale dal pubblico e dal privato verso l'economia reale. Per riuscirci servono affidabilità e credibilità. Fino al 2020 il **mercato** italiano era poco significativo, nel 2023 si è attestato a **1,4 miliardi di euro**, principalmente grazie al quarto trimestre che è andato molto bene recuperando la penalizzazione degli alti tassi di interesse: anche se sono mancati i *big ticket*, i **deal** sono stati in linea a quelli dell'anno precedente. Il nostro piano mira al **target** di 8 miliardi di euro nel 2028.

L'intelligenza artificiale è un'opportunità unica con un impatto globale impressionante, stimato tra i 2,6 e 4 trilioni di dollari al 2040

Parliamo di AI e cybersecurity. Quanto è strategico investire su questo asset e come intendete farlo?

Il nostro piano si concentra su 7 ambiti che, da un'analisi tassonomica effettuata, risultano strategici per l'Italia – in termini di peso sul Pil e di allocazioni Pnrr dedicate – e sufficientemente maturi nel mercato del *venture capital* – in termini di numerosità di **start-up**, peso dei *deal*, presenza di fondi di Vc settoriali. I 7 comparti sono: *agrifoodtech*, *spacetechnology*, *healthcare & lifescience*, *cleantech*, *industrytech*, *infrastructure & mobility* e *Artificial intelligence & cybersecurity*. Dico che sono 6 + 1 perché l'intelligenza artificiale in realtà riguarda anche tutti gli altri. L'AI è un'opportunità unica, il cui impatto globale è impressionante, stimato tra i 2,6 e 4 trilioni di dollari al 2040. In Italia non abbiamo ancora casi di successo in questo ambito, ma si sta aprendo uno spazio.

Quali cartucce abbiamo?

Penso a tre elementi di vantaggio tutti italiani. Innanzitutto, vantiamo competenze accademiche e tecniche straordinarie. E, sottolineo, che ci farebbe piacere che rimanessero qui. Poi la nostra **cultura umanistica**, che da sempre genera creatività e innovazione. Infine, la nostra capacità imprenditoriale di scalare anche all'estero.

In che modo gli strumenti di *venture capital* possono sostenere le *start-up* italiane ad emergere nel campo dell'AI e a competere con la concorrenza internazionale?

Il *venture capital* può essere determinante nel sostenere lo sviluppo di una via italiana all'intelligenza artificiale, accompagnando la crescita di **campioni internazionali efficienti e concorrenziali** sul mercato globale, assicurando un efficace supporto ai processi industriali di domani e garantendo allo stesso tempo la **sicurezza dei dati sensibili** per il Paese. Sappiamo che l'impatto della AI può essere non sempre positivo, per questo insisto anche sull'aspetto **etico** affinché ci distingua. L'AI è una tecnologia potente che tuttavia pone delle potenziali criticità in termini di discriminazioni, di **privacy**, di sicurezza. Si deve lavorare per garantire anche un approccio etico alle nuove tecnologie che noi dobbiamo sostenere.

Un miliardo di euro per l'intelligenza artificiale, a partire da quando e come?

Partiremo subito con la creazione del Fondo per l'intelligenza artificiale con una dotazione di **500 milioni**, destinati a sviluppare nuovi **modelli di linguaggio** e la parte più infrastrutturale della tecnologia, la cosiddetta "*deep tech*", mentre altri 500 milioni saranno declinati in investimento sugli ulteriori 6 fondi settoriali a cui accennavo. In particolare, investiamo 120 milioni sul **trasferimento tecnologico**: quindi, *ticket* piccoli che servono a supportare ciò che studenti e ricercatori italiani stanno portando avanti. Altri 580 milioni andranno alle *start-up* che già lavorano su applicazioni verticali. Infine, vogliamo contribuire alla costituzione di uno, due *silver bullet* per fare massa critica attraverso la creazione di un soggetto competitivo sul mercato globale - un campione nazionale di AI - con un investimento di 300 milioni.

Come riuscirete a selezionare le *start-up* o i potenziali campioni di AI? Come mettere a sistema le opportunità in un settore così innovativo?

A livello di *governance*, bisogna favorire il cambiamento delle **competenze** disponibili. Come Sgr abbiamo bisogno di esperti, di ruotare il nostro modello organizzativo, dobbiamo introdurre specifiche competenze negli *advisory board*, nei comitati di valutazione. Ciò detto, il cambiamento di approccio riguarda tutte le aziende e il loro management. È necessario un "*layer trasversale*" su questi temi per la **classe dirigenziale** del Paese, perché l'intelligenza artificiale diventa un'opportunità se ci si arriva preparati, un rischio invece se ci si arriva spiazzati.

Vogliamo contribuire alla costituzione di uno, due *silver bullet* per fare massa critica attraverso la creazione di un soggetto competitivo sul mercato globale - un campione nazionale di AI - con un investimento di 300 milioni



Agostino Scornajenchi, Amministratore delegato e Direttore generale di Cdp Venture Capital

RISCHIO INFLUENZE

AUTORE: **LUCA ZORLONI** - TEMPO DI LETTURA: 4 MINUTI



Tra intelligenza artificiale, deepfake, fake news e blackout di internet, il 2024, con elezioni che portano al voto metà della popolazione mondiale, è un anno delicato per le democrazie e per le imprese

Nel 2024 circa **metà della popolazione mondiale** è attesa alle urne. Tra elezioni nazionali e locali, si vota in 76 Paesi, tra cui otto dei più popolosi. Dall'India agli Stati Uniti, solo per citarne alcuni. Si è partiti con Taiwan, dove il **voto** ha segnato i futuri rapporti con la Cina, e si chiuderà con la scelta del futuro inquilino della Casa Bianca, un ruolo conteso tra l'attuale Presidente statunitense Joe Biden e l'ex Donald Trump. Nel mezzo, circa **400 milioni di persone** dovranno scegliere i propri rappresentanti all'Europarlamento, che poi provvederà a selezionare i componenti della Commissione europea.

È un anno delicatissimo. Perché i risultati di questa imponente tornata elettorale determineranno i **futuri equilibri del globo**, mentre le tensioni internazionali, tra invasione dell'Ucraina, guerra in Medio Oriente, tensioni nel mar Rosso surriscaldano la situazione complessiva a livello mondiale. Per questo, preoccupano le possibilità che il voto possa essere manipolato. E preoccupano gli usi deleteri di alcune tecnologie che rischiano di far deflagrare i tentativi di incursione di chi vuole inquinare le **campagne elettorali** e l'esercizio del voto.

Sorvegliata speciale è l'**intelligenza artificiale**. E in particolare l'uso di **deepfake**, ossia la sintesi di immagini e video con l'AI per sovrapporre e combinare il materiale originale con quello manipolato dagli algoritmi. A gennaio ne è stato fatto uso negli Stati Uniti per simulare una chiamata da parte del Presidente Joe Biden che invitava i sostenitori del Partito democratico a non andare a votare alle primarie del New Hampshire. Un rischioso **boomerang** per il corretto svolgersi della selezione del candidato alle elezioni nazionali. E l'antipasto dei **pericoli** che questa tecnologia rappresenta. Sostenitori di Trump, per esempio, hanno prodotto una serie di immagini **deepfake** in cui il magnate è immortalato in mezzo a sorridenti elettori della comunità afroamericana. L'obiettivo è chiaro: avvicinare all'ex Presidente una

fetta di elettorato distante dal manifesto politico del **tycoon** e le modalità per farlo sono piuttosto pedestri, perché le foto false sono state smascherate in un lampo. Conta, però, la facilità con cui si possono inondare **social media e chat** di messaggistica di immagini manipolatorie.

Le società che sviluppano sistemi di intelligenza artificiale hanno promesso provvedimenti per impedire **usi distorti** della loro tecnologia. Così hanno fatto i **social network**: Meta, per esempio, ha promesso di inserire una filigrana per distinguere i contenuti prodotti da modelli di AI generativa. OpenAI che ha sviluppato ChatGPT, a sua volta, assicura maggiore trasparenza. Midjourney, un altro dei sistemi di AI generativa, sta valutando di impedire di creare alcuni tipi di immagini a sfondo politico.

Preoccupa, in particolare, l'uso di deepfake, ossia la sintesi di immagini e video con l'AI per sovrapporre e combinare il materiale originale con quello manipolato dagli algoritmi

Tuttavia, le prime analisi da parte di organizzazioni ed enti di ricerca indipendenti hanno dimostrato che questo tipo di misure sono fallimentari e facilmente aggirabili. Le **big tech** non possono ignorare la faccenda. Troppo lassismo potrebbe comportare una stretta **normativa di urgenza** e legare le mani alle aziende di intelligenza artificiale. Già in Europa le aziende del digitale hanno il loro bel daffare. Da alcuni mesi i principali **social network** e i motori di ricerca più grandi sono soggetti al nuovo regolamento europeo sui **servizi digitali**, il *Digital services act* (Dsa), che include anche obblighi

per le **piattaforme** affinché impediscano un uso distorto dei loro sistemi ai fini elettorali. Tutte hanno annunciato maggiore trasparenza sulle inserzioni pubblicitarie a scopo politico e centri *online* dove trovare indicazioni su come segnalare le violazioni e verificare le informazioni. A sua volta, la Commissione ha chiesto lumi e promette di stabilire una strategia per mettere al riparo il voto per l'Europarlamento. Il timore principale è che la Russia possa manipolare la campagna per minare la stabilità delle **istituzioni comunitarie**.

Il problema, però, è che non basta. Ci sono spazi *online*, come gruppi sui *social* o *chat* nelle *app* di messaggistica che sfuggono a questo controllo. E spesso non serve fare ricorso a tecniche sofisticate come il *deepfake*. Montaggi di immagini e video per simulare finti articoli di giornale funzionano ancora per diffondere *fake news*. Così come le attività di siti e portali votati ad alimentare **complotti e dietrologie**. Non solo. A mettere a repentaglio il corretto svolgimento delle elezioni sono anche metodi come il **blackout di internet**, adoperato in paesi dove si vuole impedire la partecipazione al voto azzeccando le comunicazioni. È già successo in Pakistan, alle Comoros e in Senegal.

Lo strettissimo sentiero delle elezioni 2024 non rappresenta solo una prova esistenziale per la democrazia e un momento decisivo per le aziende tecnologiche per assumersi le responsabilità che il loro ruolo comporta, ma anche un momento delicato per le imprese in generale. La costante **instabilità politica** che il lungo processo di voto comporta rappresenta di suo un motivo di fluttuazione dei mercati e di incertezza per gli investimenti. Se a una contesa accesa si somma il gioco sporco di tecnologie manipolatorie, il clima per le imprese potrebbe peggiorare.

Non solo: un affinamento delle tecnologie di *deepfake*, sperimentate in una campagna coordinata sul campo elettorale per poterlo manipolare, potrebbe portare a riutilizzarle successivamente in contesti come lo **spionaggio industriale** o attacchi coordinati a una impresa. Già oggi sistemi di simulazione della voce vengono utilizzati

per imitare i ruoli di manager e responsabili di azienda e rubare informazioni sensibili, denari o **asset strategici**.

Non solo. Un proliferare di contenuti falsi provocherà anche una generale disillusione e un senso di smarrimento e sfiducia verso **il mondo dell'informazione e della comunicazione**, minando la fiducia dei consumatori che è un potente motore dei mercati. In Australia Pwc ha messo in guardia le aziende: «Su una scala meno globale ma comunque potenzialmente drammatica, anche le singole aziende dovranno essere consapevoli delle implicazioni dei video *deepfake*.

Un proliferare di contenuti falsi provocherà anche una generale disillusione e un senso di smarrimento e sfiducia verso il mondo dell'informazione e della comunicazione, minando la fiducia dei consumatori che è un potente motore dei mercati

In un'epoca di attivismo degli azionisti e macchinazioni aziendali, non è certamente difficile immaginare che la **manipolazione** video venga utilizzata per danneggiare il marchio e la **reputazione** da parte di concorrenti, ex dipendenti (o ex come nel caso del porno di vendetta) o truffatori professionisti. Mentre le aziende potrebbero dedicare tempo a istruire il personale su come individuare video falsi (e ci sono modi, come strani schemi di lampeggiamento, manipolazione di **pixel e metadati**, audio dal suono metallico), la tecnologia continuerà a migliorare, fino al punto in cui sarà praticamente impossibile identificare un falso senza un'analisi forense approfondita». Un rischio che non siamo pronti a correre, ma che non possiamo ignorare.



STORIE

LE AMICHE GENIALI

AUTORE: DOMITILLA BENIGNI - TEMPO DI LETTURA: 4 MINUTI

Ridurre il divario di genere dei professionisti della cybersecurity, superando gli stereotipi e promuovendo lo sviluppo di competenze innovative. La sfida di Women4Cyber

La sempre maggiore interconnessione del **cyberspazio** sta comportando un crescente intreccio tra mondo digitale e fisico, esponendo cittadini, imprese e Stati a nuovi rischi come gli attacchi informatici.

L'ampia diffusione delle tecnologie digitali nelle nostre vite ha innalzato il costo e l'impatto degli **attacchi informatici**, rendendo la sicurezza informatica una priorità cruciale volta a garantire la **sicurezza** e la stabilità delle nostre attività digitali, della società nel suo complesso e delle nazioni. Senza una robusta difesa informatica, i diversi **assets** divengono vulnerabili a una vasta gamma di minacce che possono arrivare a compromettere la stessa sicurezza nazionale. A livello di business, vi è poi il rischio che vengano compromessi i **dati sensibili** delle imprese, nonché la loro reputazione e la continuità operativa.

Le Pmi sono particolarmente esposte a questi rischi perché spesso non sono dotate delle **risorse e competenze** sufficienti in materia di sicurezza informatica per far fronte alle minacce informatiche, divenendo vulnerabili ad esse. Pertanto, investire in soluzioni e pratiche di sicurezza diventa cruciale per **proteggere i dati** e garantire la sostenibilità delle attività aziendali. Il costante aumento delle minacce cibernetiche sta determinando una crescente **domanda di professionisti qualificati** nel settore, rendendo la **cybersecurity** un campo stimolante per intraprendere una carriera. Il settore sta infatti registrando una crescita esponenziale, sproporzionata rispetto alla capacità reale del mercato di fornire forza lavoro.

Le competenze specializzate risultano essenziali per prevenire, individuare e rispondere alle minacce alla sicurezza. Le imprese devono **investire nella formazione** e nell'aggiornamento del personale, garantendo l'acquisizione delle competenze necessarie per proteggere efficacemente le risorse digitali delle aziende. In que-

sto contesto, il **valore del personale qualificato** diventa fondamentale per la sicurezza e la prosperità delle imprese italiane.

Purtroppo, però l'aumento nella richiesta di competenze non corrisponde in assoluto all'offerta disponibile nel **mondo del lavoro** e inoltre, nel quadro di questa generale difficoltà a reperire le competenze necessarie, si riscontra un ulteriore ambito di assenza femminile nella rivoluzione digitale in corso. Molteplici statistiche mettono in evidenza un **gender gap significativo**, in particolare nel settore Ict. In Italia, la disparità raggiunge l'apice nelle aree di *cloud computing*, ingegneria dei dati e intelligenza artificiale. E nel **cyber** la percentuale rimane ancora molto bassa, con una media di un lavoratore su dieci donna.

Molteplici statistiche mettono in evidenza un gender gap significativo, in particolare nel settore Ict. In Italia, la disparità raggiunge l'apice nelle aree di cloud computing, ingegneria dei dati e intelligenza artificiale

Ben consapevoli della gravità sistemica di questo problema abbiamo dato vita a delle iniziative per l'**inclusione delle donne nella cybersecurity**. Questo slancio ha motivato la costituzione della Fondazione europea Women4Cyber, nata nel 2019 in seno a Ecso - European Cyber Security Organization -, con attualmente 27 capitoli nazionali in Europa ed ancora in fase di espansione. Suo obiettivo è contribuire a **ridurre il divario di genere** dei professionisti della **cybersecurity**, concentrandosi sulla sfida agli stereotipi di genere, sulla promozione e svi-

luppo di competenze digitali e *cyber* tecniche e la riqualificazione di professioni tradizionali, ivi comprese quelle di taglio umanistico (giuridiche, economiche, linguistiche) di crescente applicazione nel settore *cyber*.

In Italia abbiamo voluto dare un segnale nazionale forte costituendo **il capitolo italiano di Women4Cyber**, iniziativa che vede accanto a me, che ne sono Presidente, Rita Forsi (Vicepresidente e Direttore del Comitato tecnico scientifico), Selene Giupponi (Segretario generale), Giorgia Pontetti, Costanza Matteuzzi e Irene Sorani (membri del *board*). La *mission* di questa iniziativa ha motivato grandi personalità a darci il loro sostegno: la Professoressa Paola Severino in qualità di Presidente onorario, e altri illustri soci onorari tra i quali ricordo il Prefetto Frattasi e la Dottoressa Ciardi, rispettivamente Direttore e Vice direttore dell'Acn, Ivano Gabrielli, Direttore della Polizia postale e con loro davvero tanti altri. È stato poi istituito, in seno a Women4Cyber Italia, un Comitato tecnico scientifico, cui hanno aderito prestigiose personalità provenienti da università, pubblica amministrazione, aziende e settori specialistici e che ha promosso accordi di collaborazione tecnico-scientifica e per l'incremento della consapevolezza delle opportunità presentate all'**universo femminile dal mondo cyber** con le Università Luiss, Campus Biomedico e Università di Pisa.

L'associazione, con i suoi membri, partecipa e patrocina eventi, *webinar* e conferenze in collaborazione con università, enti e imprese per sensibilizzare sui temi della trasformazione digitale, della ricerca e dell'**innovazione**, della *cybersecurity* e ovviamente dell'inclusione femminile in questi processi. Si impegna in programmi di *mentorship*, attività sui media e conversazioni con importanti *role model*.

Tutto ciò mira ad evidenziare come l'azione di Women4Cyber Italia parta dalla volontà di mettere in luce la **necessità di un contributo attivo delle donne al settore**. Queste ultime possono contribuire in modo sistematico a colmare il divario delle competenze, con un apporto diversificato di talenti e competenze, a beneficio dell'innovazione.

Questo processo deve essere accompagnato da un cambiamento culturale che contribuisca a superare radicati pregiudizi, in nome di una maggiore uguaglianza di genere. Su questi presupposti desideriamo contribuire all'**edificazione di un mondo digitale, sostenibile** ed inclusivo per il bene del sistema Paese.

Promuovere l'inclusione delle donne nella *cybersecurity* richiede un impegno duraturo da parte degli attori coinvolti. Per potenziare le **sinergie nell'ecosistema della cybersecurity** e promuovere una maggiore inclusione delle donne, è essenziale adottare un **approccio olistico** che coinvolga diversi attori e implementi una serie di strategie coordinate, potenziando il partenariato pubblico-privato. Questo approccio, rispecchiato nel *modus operandi* di Women4Cyber Italia, mira a creare un ambiente in cui le donne possano contribuire pienamente alle sfide e alle opportunità del settore, migliorando così la **sicurezza cibernetica** globale.

Women4Cyber Italia mira a creare un ambiente in cui le donne possano contribuire pienamente alle sfide e alle opportunità del settore, migliorando così la sicurezza cibernetica globale

Per questo motivo desideriamo agire da catalizzatore di energie. Farci motore per sensibilizzare gli *stakeholder* pubblici e privati sulle tematiche legate al divario delle competenze e al divario di genere, nonché sulla necessità di investire negli uomini e nelle donne.

È cruciale dare priorità all'istruzione e alla formazione. Nella società digitale di oggi, questo è un passaggio imprescindibile che va salvaguardato quale diritto di accesso a un'**istruzione** (digitale e non solo) **di qualità e qualificante** per il **mercato del lavoro del futuro**, che possa davvero aprire le porte verso il progresso e la prosperità.

COMBINAZIONE DI SICUREZZA

AUTORE: **STEFANIA SANTUCCI** - TEMPO DI LETTURA: **3 MINUTI**



Intelligenza artificiale, machine learning, deep learning: gli sviluppi tecnologici aprono la strada a innovative soluzioni di sicurezza. Ma le competenze umane rimangono imprescindibili

L'aumento esponenziale degli attacchi informatici (secondo il recente rapporto Clusit, dal 2018 + 61,5% a livello mondiale, e in Italia addirittura + 300%) nonché la rapidissima diffusione e crescita delle tipologie di minacce, mette a dura prova i **team di sicurezza**, che oggi devono affrontare molte sfide: attacchi sofisticati, esplosione dei volumi di **dati**, superficie di attacco in espansione e crescente complessità delle infrastrutture (anche a causa del sempre maggiore ricorso a tecnologie Cloud).

I **software** intelligenti applicati alla **cybersecurity** offrono un valido supporto ai professionisti per acquisire consapevolezza del panorama delle **minacce**, percepire e analizzare i pericoli e decidere i rimedi e le azioni da compiere.

Prima di entrare nel dettaglio delle funzionalità che l'intelligenza artificiale mette a disposizione della **sicurezza informatica** è bene però ricordare alcune definizioni. L'**intelligenza artificiale** è una qualsiasi tecnica capace di imitare l'intelligenza umana, applicando regole di logica e adottando processi decisionali interni, mentre il **machine learning** è un sottoinsieme dell'intelligenza artificiale che utilizza tecniche statistiche complesse che elaborano le informazioni e i dati raccolti dal sistema nello svolgimento delle proprie mansioni, con lo scopo di perseguire il miglioramento continuo delle **performance**. La **deep learning**, invece, è un sottoinsieme del **machine learning** che comprende algoritmi utili al **software** per allenarsi nello svolgimento delle attività per cui è stato predisposto, ad esempio riconoscere immagini, voci oppure individuare determinate informazioni esaminando una grande quantità di dati.

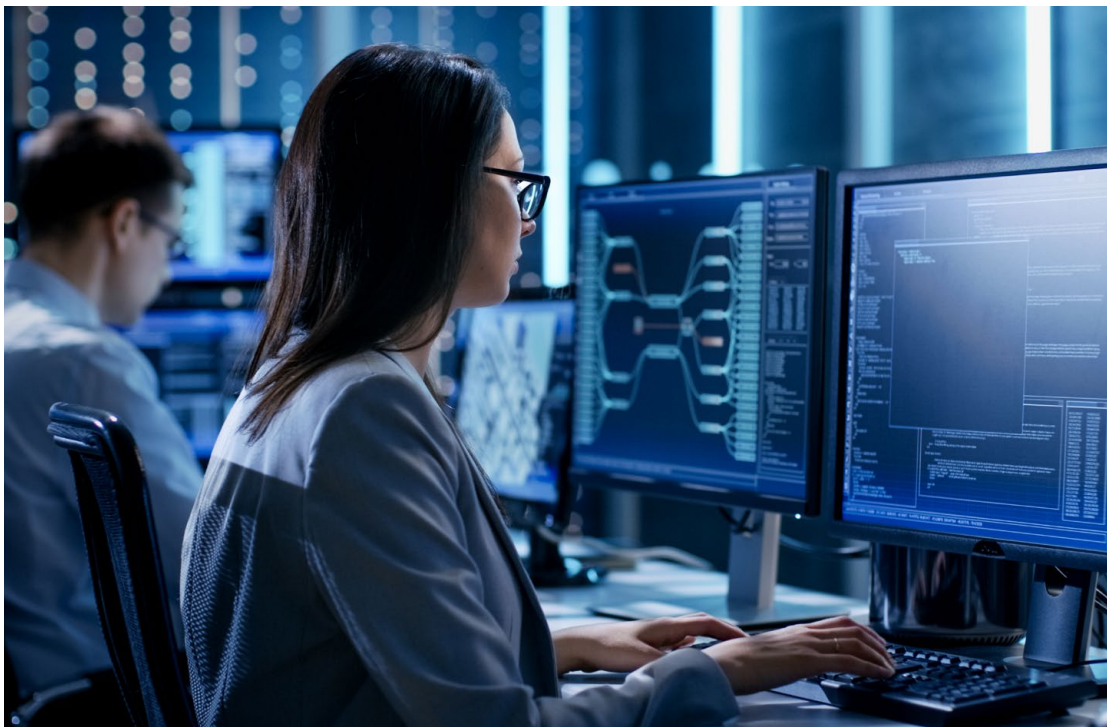
Da un lato, tutti questi strumenti possono certamente essere manipolati e sfruttati anche da **attori malintenzionati** allo scopo, ad esempio, di sviluppare e distribuire **malware**, alimentare la creazione di **disinformazione e contenuti non autentici** (*deep fake* e *fake news*), o per ampliare le capacità degli aggressori di automatizzare e velocizzare i loro attacchi. L'IA genera-

tiva può supportare la gestione di truffe come il **phishing** diventando uno strumento utile agli **hacker** per creare rapidamente comunicazioni e materiali su misura sempre più convincenti e coinvolgenti, che inducano le vittime ad aiutare inconsapevolmente gli aggressori.

Secondo il recente rapporto Clusit, c'è un aumento esponenziale degli attacchi informatici: dal 2018 + 61,5% a livello mondiale e in Italia addirittura + 300%

D'altra parte, però, è bene ricordare che l'intelligenza artificiale interviene anche a supporto e in aiuto delle soluzioni di **sicurezza informatica**. Infatti proteggere i sistemi informatici dagli attacchi, mitigando i rischi e difendendo l'integrità e la disponibilità dei dati richiede tempo e comporta la necessità di eseguire operazioni ripetitive e continue di **monitoraggio e analisi dei sistemi informatici**, per tenere sempre aggiornati gli apparati e individuare in modo tempestivo possibili minacce. Con un'**automazione intelligente e adattiva**, i **team di cybersecurity** possono ricevere consigli tempestivi su problemi appena scoperti, ottenere suggerimenti sulle opzioni con cui procedere, o anche disporre di sistemi per modificare automaticamente le impostazioni in base alle criticità e alle esigenze individuate.

L'utilizzo di tecnologie di intelligenza artificiale, **machine learning** e **deep learning** aiuta a ridurre il **tempo di risposta alle minacce**, certamente una delle metriche più importanti per l'efficacia di un **team di cybersecurity**, consentendo di intervenire più rapidamente possibile per prevenire e identificare le minacce e mitigare eventuali danni.



La sicurezza assistita da *machine learning* può aiutare a **classificare e clusterizzare i dati** per individuare dei profili, dei *pattern* che caratterizzano i comportamenti “nella norma” di persone e sistemi, contribuendo così all’identificazione di eventuali anomalie in modo automatico e veloce. L’identificazione di **nuove minacce** è un altro fattore che ha un impatto determinante sui tempi di risposta ai cyberattacchi. La costante evoluzione degli attacchi è un motivo di preoccupazione nell’ambito delle attività di difesa della rete. Ma i **cyberattacchi** raramente vengono creati da zero. Poiché sono spesso basati su comportamenti, *framework* e codici sorgente utilizzati in passato, l’**algoritmo** di *machine learning* ha a disposizione un **percorso preesistente** da cui partire evidenziando i punti in comune tra la nuova minaccia e quelle identificate in precedenza, che semplifica l’identificazione delle caratteristiche del nuovo attacco. Attraverso l’analisi dei *set* di dati storici basata su *machine learning* i sistemi possono anche individuare e consigliare una serie di interventi mirati a **migliorare le misure di sicurezza**, fino a sviluppare, nelle soluzioni più avanzate e sofisticate, capacità **preventive, predittive e proattive**. Tutte queste attività, basate sulla **raccolta, analisi e rappresentazione** di enormi quantità di dati e informazioni, sono qualcosa che gli esseri umani

non riescono a fare in modo efficace e tempestivo. L’utilizzo sempre più esteso di soluzioni basate sull’intelligenza artificiale può certamente aiutare ad alleviare gli **skill gap** nel campo della *cybersecurity*. Ma è possibile che le soluzioni basate sulle tecnologie più avanzate sostituiscano completamente i professionisti della *cybersecurity*? Certamente non a breve, perché non è ancora possibile, allo stato attuale, che l’intelligenza artificiale possa interpretare i risultati con le stesse capacità di un essere umano. Il settore continua ad avere bisogno di più esperti di *cybersecurity* con **competenze** specifiche su intelligenza artificiale e *machine learning* che siano in grado di utilizzare al meglio le tecnologie e i risultati che queste generano, ma anche di sviluppare una programmazione efficace in questo campo, gestendola e modificandola in base alle esigenze. È indubbio che il *pool* di persone formate e qualificate è ancora troppo ridotto rispetto all’immensa **domanda globale di personale** in grado di fornire e gestire queste soluzioni. I **team umani** saranno ancora essenziali poiché il pensiero critico e la creatività saranno fondamentali per supportare il processo decisionale. La sfida del futuro si giocherà appunto sulle **persone**. Ossia sul far funzionare la collaborazione uomo-macchina tra IA ed esperti, combinando le forze tra intelligenza artificiale e umana.

A COLLOQUIO CON

PROFONDO ROSSO

AUTORE: ANNA MARIA SELINI - TEMPO DI LETTURA: 3 MINUTI

Cavi per le comunicazioni e per il trasporto di energia. Sotto i mari viaggia una parte consistente degli asset mondiali e i rischi per la sicurezza sono sempre altissimi

Le guerre ibride saranno sempre di più anche subacquee. Basti pensare a quanto successo al gasdotto Nord Stream 2 e alla distruzione di tre cavi, per le comunicazioni tra Asia ed Europa, nel Mar Rosso. Ne abbiamo parlato con **Alessandro Gili**, analista dell'osservatorio di Economia dell'Ispi.

Quando parliamo di infrastrutture strategiche sottomarine che cosa intendiamo?

Ci riferiamo a due grandi macrocategorie: i cavi sottomarini *digital*, che sono circa 450 e che garantiscono le comunicazioni a livello internazionale e poi la categoria energetica, cioè gasdotti e cavi sottomarini per il trasporto di energia elettrica.

Quali sono le minacce a cui sono soggetti i cavi? Come si proteggono?

Come abbiamo visto, possono esserci **attacchi di carattere geopolitico**, ma i rischi sono anche naturali. Sono cavi che non hanno un diametro molto grande, circa 20 mm, e non sempre sono posati a grandi profondità. Tanto che rischiano di essere danneggiati anche dalle semplici attività di pesca, per esempio dalle ancore. Oppure durante **grandi eventi naturali** come terremoti o eruzioni vulcaniche, come è successo all'isola di Tonga, che è rimasta scollegata dal resto del mondo a lungo.

Possono essere soggetti anche a dinamiche di spionaggio? Come?

Sì, diciamo a dinamiche **cyber**. Sulle coste, per esempio, ci sono centri di raccolta **dati** e infrastrutture terrestri legate a quelle sottomarine, che possono essere il punto più critico per carpire dati e informazioni. Si cerca di ovviare al problema con la cosiddetta ridondanza: non si dovrebbe mai essere collegati ad un altro Paese attraverso un solo cavo, ma attraverso differenti **infrastrutture sottomarine**, per avere la possibilità di *switchare* e spostare il traffico su altri canali. È quello che è avvenuto nel Mar Rosso: tre cavi sono stati danneggiati, ma non è successo granché.

Non è una contraddizione che infrastrutture così importanti siano così fragili ed esposte?

Sì, lo è, ma queste infrastrutture hanno un percorso anche di migliaia e migliaia di chilometri. Quindi sarebbe difficile l'installazione di cavi di grande diametro, diventerebbe più complessa la posa e aumenterebbero i costi, rendendo il tutto non conveniente e infattibile. Sicuramente è un problema serio, infatti, nel marzo 2023 la **Nato** e l'**Unione europea** hanno dato vita a una *task force* congiunta, per la sorveglianza delle infrastrutture critiche sia nel Mediterraneo che nel Mare del Nord. È diventato uno dei domini fondamentali per il controllo e la sicurezza.

Secondo una stima a livello internazionale, circa 10 trilioni di dollari di transazioni finanziarie internazionali passano attraverso i cavi sottomarini ogni giorno. Oltre che il 95-98% del traffico internet

Qual è il valore dei cavi *digital* o del traffico che generano?

Secondo una stima abbastanza diffusa a livello internazionale, circa 10 trilioni di dollari di transazioni finanziarie internazionali passano attraverso i cavi sottomarini ogni giorno. Oltre che il 95-98% del traffico *internet*.

Da chi vengono regolamentati?

A livello europeo la Commissione Ue dovrebbe approvare quest'anno un primo documento che prevede l'aumento del coordinamento tra gli Stati membri, per l'individuazione di cavi di interesse europeo e quindi per **ridurre i rischi** e aumentare l'autonomia strategica dell'Ue. L'obiettivo sarebbe anche quello di garantire una crescita dimensionale delle aziende europee - come la francese Alcatel, l'italiana Prysmian e Sparkle per la gestione

- per competere con i giganti americani e con la sempre più crescente Huawei Marine cinese.

Quali sono i cavi che interessano l'Italia e che rischio c'è ad agire nel Mar Rosso, secondo lei, con la missione Aspides, per proteggere le navi dagli attacchi degli Houthi?

Per quanto riguarda l'Italia le nostre connessioni fondamentali sono quelle che passano dal corridoio Est, verso l'Asia, ma anche quelle che garantiscono la **connettività** nel Mediterraneo. Abbiamo *hub* di collegamento da cui partono molti dati importanti per il Mediterraneo e per l'Africa e ovviamente l'Asia. Inoltre, abbiamo anche un interesse dal punto di vista energetico, come il gasdotto Green Stream che ci connette al Nord Africa. Ma soprattutto questa connettività è fondamentale nell'attuale fase di **transizione energetica**, per la produzione di energie rinnovabili, ma anche di idrogeno verde. Il progetto H2 stream, per esempio, dovrebbe connettere il Nord Africa fino alla Germania e l'Italia dovrebbe diventare fondamentale *hub* di collegamento del gas nel Mediterraneo e in futuro anche dell'idrogeno. Queste infrastrutture importantissime necessitano ovviamente di controllo e anche di dispositivi militari. Il recente dispiegamento italiano nel Mar Rosso ovviamente aumenta le possibilità che l'Italia diventi in futuro un *target*, anche se per ora è stato escluso dagli Houthi. Il problema fondamentale nel mar Rosso è più che altro legato all'interruzione delle catene del valore internazionali, perché gran parte delle merci provenienti dall'Asia passa dal canale di Suez.

Secondo lei, questa sarà una delle guerre ibride del futuro?

Sicuramente sarà uno dei domini di possibile guerra.

Il controllo dei cavi sottomarini riflette la situazione geopolitica mondiale? La Cina sta avanzando anche sott'acqua?

La Cina controlla il 10-15%, la maggior parte dei cavi sono degli Stati Uniti, che cercano di limitare la concorrenza cinese, agendo anche sulle grandi società americane. Google, Meta e Amazon ormai vogliono gestire in autonomia tutto il quadro della rete, dalle società di costruzione alla gestione dei cavi sottomarini, di cui sono

proprietarie, per garantirsi la connettività a livello internazionale. A partire da Trump, per questioni di **sicurezza nazionale**, si cerca di impedire che cavi sottomarini colleghino per esempio la California ad Hong Kong, perché nei vari passaggi si potrebbero carpire informazioni fondamentali.

A margine del vertice del G20 in India, è stata avanzata la proposta del G7 di creare un corridoio India-Middle East: sostanzialmente un canale di tipo **logistico**, ma in previsione ci sarebbe anche un cavo sottomarino e un nuovo gasdotto per il trasporto dell'idrogeno verde. E sarebbe molto interessante, perché andrebbe a saltare il canale di Suez.

La Cina controlla il 10-15% dei cavi, la maggior parte sono degli Stati Uniti, che cercano di limitare la concorrenza cinese, agendo anche sulle grandi società americane



Alessandro Gili, analista dell'osservatorio di Economia dell'Ispis

SENSO OBBLIGATO

AUTORE: **STEFANO EPIFANI** - TEMPO DI LETTURA: **4 MINUTI**



Sicurezza digitale e sostenibilità, due obiettivi fondamentali che orientano strategie e processi operativi delle aziende, rivelandosi sempre più interdipendenti

In un mondo dove il **digitale** permea ogni aspetto della vita sociale ed economica, diventa fondamentale riconoscere che ogni interazione, sia essa aziendale, istituzionale o personale, è profondamente radicata nel digitale. Parallelamente, la **sostenibilità**, intesa come la capacità di soddisfare i bisogni attuali senza precludere alle **generazioni future** le stesse opportunità, emerge come un imperativo globale. Tutti gli attori della società - dalle aziende ai Governi, fino ai singoli individui - sono chiamati a contribuire a questo obiettivo, che è sempre più inscindibilmente legato agli obiettivi di **business**. Di qualsiasi business. Da una parte, quindi, la trasformazione digitale ridefinisce i modelli di business riarticolarlo le **catene del valore**, dall'altra la sostenibilità traccia la direzione di tale processo di ridefinizione. È il tema della **sostenibilità digitale**, da non confondere con quello della tecnologia sostenibile e che - oggi - deve essere al centro delle scelte strategiche di ogni organizzazione.

Allo stesso tempo ogni manager deve chiedersi come evolva il suo ruolo, così come quello della sua organizzazione. Ma, in quella che è una vera e propria **rivoluzione di senso**, la trasformazione digitale impone l'acquisizione di nuovi livelli di consapevolezza anche in relazione a tematiche che fino a pochi anni fa erano di dominio specifico solo di quanti, in azienda, si occupavano di digitale.

Cybersecurity e sostenibilità: sempre più punti di contatto

Tra le tematiche sempre più trasversali, una delle più impattanti è quella della *cybersecurity*. La pervasività del digitale incrementa infatti esponenzialmente la **superficie d'attacco dei sistemi**. Allo stesso tempo, tale incremento della superficie d'attacco dei sistemi aumenta contestualmente i punti di contatto - nelle scelte manageriali - tra le questioni legate alla **sicurezza informatica** e quelle relative alla sostenibilità nelle sue dimensioni sociali, ambientali, economiche.

Come tutelare i diritti dei lavoratori e promuovere un ambiente di lavoro sicuro e protetto per tutti, come richiamato dall'Sdg8 dell'Agenda 2030? Come garantire sicurezza e resilienza di **infrastrutture** fisiche ed assicurare la continuità dei servizi, come evidenziato dall'Sdg9? Come tutelare le informazioni riservate garantendo i propri utenti, i propri concittadini, le aziende e gli *stakeholder*, come sottolineato sempre dall'Sdg9, così come dall'Sdg11? Come controllare l'**impatto energetico dei sistemi informativi** in relazione alla rilevanza delle informazioni gestite, in accordo all'Sdg13?

La trasformazione digitale ridefinisce i modelli di business riarticolarlo le catene del valore e la sostenibilità traccia la direzione di tale processo di ridefinizione

L'elenco dei punti di contatto sistemici tra sostenibilità, digitalizzazione e sicurezza potrebbe continuare, ma questi pochi quesiti bastano ad evidenziare come sicurezza e sostenibilità - unite dal digitale - non siano più considerabili quali entità distinte, ma diventino elementi fortemente complementari, facendo della *cybersecurity* uno strumento ineludibile di sostenibilità, e allo stesso tempo della sostenibilità un criterio di indirizzo per lo sviluppo di sistemi di sicurezza che, nel tutelare i sistemi, garantiscano i **diritti** dei loro utenti.

La percezione di Cio e Ciso

Per questo motivo, in un contesto ancora troppo poco approfondito, con la **Fondazione per la sostenibilità digitale**, in un gruppo di lavoro che ha visto coinvolti Cio e Ciso di alcune tra le più importanti aziende italiane, con il supporto di

Gyala - startup italiana finanziata da Cdp specializzata in *cybersecurity* – è stata realizzata una delle prime ricerche¹ che analizza in modo sistematico il **rapporto tra cybersicurezza e sostenibilità**, esplorando le intersezioni tra questi due temi e proponendo un quadro di riferimento che guidi verso una *cybersecurity* che sia al contempo sostenibile e motore di sostenibilità, sottolineando l'importanza di stabilire priorità chiare all'intersezione di questi due ambiti, essenziali per orientare le **strategie di innovazione** di enti pubblici e privati.

Il quadro che ne emerge, condiviso con un *panel* di oltre cento Cio e Ciso, vede tra le principali caratteristiche di sostenibilità della *cybersecurity* tre elementi: *in primis* **l'integrazione tra IT e OT**. Con lo sviluppo delle tecnologie IoT (Internet of Things) è sempre più importante garantire l'integrazione tra le componenti digitali dell'IT e quelle fisiche dell'OT. Questo può avere forti impatti su diversi Sdg e sulle caratteristiche specifiche della sicurezza in termini di sostenibilità. In altre parole, quindi, i Cio intervistati evidenziano come l'integrazione IT/OT sia fondamentale per supportare i processi legati alla **salvaguardia ed alla tutela dell'ambiente**, anche in relazione alla tenuta delle infrastrutture critiche ed al loro valore economico.

C'è poi il tema della **sovranità digitale**. La modalità in cui uno Stato regola ed esercita il governo della tecnologia e dei servizi utilizzati in vario modo all'interno del perimetro nazionale (sovranità digitale) vede nella sicurezza informatica un elemento di grande criticità e, contestualmente, rappresenta un tema centrale in termini di sostenibilità. Gli intervistati evidenziano una centralità della sovranità digitale nella sicurezza per garantire la sostenibilità economica, così come per la dimensione della sostenibilità sociale.

E infine la **privacy**. Sicurezza informatica e *privacy* corrono spesso il rischio di essere considerati come elementi in contrapposizione tra loro. È invece di fondamentale importanza, in un contesto di sostenibilità, evidenziare come la sicurez-

za informatica vada perseguita nel rispetto della *privacy* degli utenti, ed allo stesso tempo la sicurezza informatica sia un importante strumento di sostenibilità.

Emerge con forza la necessità che ogni manager diventi non un “tecnico”, ma un “tecnologo”, in grado di leggere come le tematiche della sicurezza informatica agiscano sui processi, sul business, sulla propria realtà di riferimento

La sfida delle competenze

Uno degli elementi che emerge con maggior forza nella ricerca è costituito dalla necessità che ogni manager diventi non certo un “tecnico” in grado di comprendere nello specifico le tematiche della **sicurezza informatica**, ma senz'altro un “tecnologo”, in grado cioè di leggere come esse impattino sui processi che gestisce, sul business, sulla propria realtà di riferimento. Ed in questo la relazione tra sostenibilità e *cybersecurity* diviene ancora più centrale, rappresentando quello schema di riferimento in grado di correlare le questioni legate alla sicurezza informatica in un quadro più ampio, che si collega in maniera sistemica alle scelte strategiche e che trasforma la sicurezza, così come la sostenibilità, in un **asset di valore** e non in un vincolo. Sicurezza sostenibile e sostenibilità della sicurezza divengono quindi vere e proprie competenze trasversali, in un contesto nel quale i manager devono comprendere come tali elementi possano impattare così profondamente sul *business* al punto di ridefinirlo. Comprendere le dinamiche e la direzione di questo percorso di ridefinizione del *business* può fare la differenza tra subire il cambiamento e cavalcarlo.

¹ La ricerca può essere scaricata gratuitamente sul sito della Fondazione per la Sostenibilità Digitale al seguente indirizzo: <https://sostenibilitadigitale.it/ricerca/sostenibilita-e-cyber-security>

DALL'ESTERO

LA FABBRICA DEL CONSENSO

AUTORE: DAVIDE IPPOLITO - TEMPO DI LETTURA: 3 MINUTI



L'intelligenza artificiale generativa irrompe nella campagna elettorale americana con testi e immagini che hanno la capacità di influenzare fortemente l'opinione pubblica

C'è un dato poco noto in Italia riguardante le **elezioni americane**, fondamentale per comprendere meglio il sentimento del paese e ciò che sta accadendo e accadrà da qui alle imminenti elezioni di novembre, che vedranno di nuovo fronteggiarsi Joe Biden e Donald Trump, esattamente come 4 anni fa: **un americano su cinque** è ancora convinto che le ultime elezioni siano state truccate.

Nonostante tutte le prove dimostrino il contrario e nonostante uno sforzo senza precedenti, anche da parte delle grandi **aziende della Silicon Valley**, per contenere il fenomeno delle **fake news**, questa idea resta radicata in una percentuale troppo alta di americani. Negli ultimi 10 anni, ogni elezione si sta rivelando un terreno sempre più fertile per la **disinformazione** e le interferenze volte a influenzare le elezioni. Questa elezione del 2024 si appresta ad affrontare nuove sfide con un'eccezionale vulnerabilità agli attacchi della propaganda, amplificati dalle potenzialità sempre più sofisticate dell'**intelligenza artificiale (AI)**.

Mi ha molto colpito una recente intervista letta su The Guardian al professor Renée DiResta, responsabile della ricerca tecnica presso l'Internet Observatory di Stanford, un programma universitario che studia **gli abusi della tecnologia dell'informazione**. Il professore ha analizzato come gli ultimi sviluppi nell'AI stiano influenzando le campagne elettorali e su come la società si stia adeguando a una nuova realtà creata artificialmente. Se ci pensiamo, il tema dei **deepfake** (video generati dal computer di un evento mai accaduto) non è nuovo.

Già ai tempi di Obama vi furono tentativi di intrusione con video generati dal computer, e la tecnologia era già abbastanza matura nei risultati finali. Cosa sta quindi realmente cambiando ora? Ci sono stati due importanti sviluppi in due diversi campi negli ultimi mesi: quello di **generazione testuale** e quello di **generazione di**

immagini. Il primo è l'ascesa di ChatGPT, diventato disponibile a un mercato di massa che ha permesso alla maggior parte dei cittadini, anche con scarse **competenze informatiche**, di rendersi conto di quanto sia facile utilizzare questi tipi di strumenti e delle potenzialità che offrono. Il secondo è la possibilità di creare immagini foto-realistiche di cose che non esistono nella realtà con Stable Diffusion o Midjourney (due applicativi molto diffusi e disponibili *online*).

Negli ultimi 10 anni, ogni elezione si sta rivelando un terreno sempre più fertile per la disinformazione

Queste due cose oggi fanno paradossalmente molto più paura di un video e possono avere effetti molto più catastrofici di un video deep fake in una attività di propaganda. Il motivo è semplice: per usare il video in un ambiente politico devi davvero colpire nel segno con il contenuto del messaggio. In un video ci sono tanti indizi rivelatori, molti modi in cui puoi determinare se è generato artificialmente o è reale e, inoltre, quando un video ha un impatto molto forte, è visto da milioni se non miliardi di persone che a quel punto hanno modo di verificarlo e interagire.

Potremmo definirla una risposta immunitaria naturale. Testi e immagini, invece, hanno tutto il potenziale per un impatto maggiormente incisivo in uno **scenario elettorale** perché possono essere più sottili e duraturi. Le elezioni richiedono mesi di campagna durante i quali le persone si fanno un'**opinione**.

Con questo tipo di intelligenza artificiale è molto più facile generare contenuti altamente personalizzati e automatizzarne la diffusione. Solo pensando alle elezioni di quattro anni fa, la grande

paura delle attività di propaganda politica era legata all'utilizzo di **Bot**, programmi per computer progettati per imitare o sostituire le azioni di un essere umano eseguendo attività automatizzate e ripetitive. Twitter o Meta non facevano nulla per fermare il fenomeno, anche se paradossalmente era molto facile da smascherare; molti degli account dicevano esattamente la stessa cosa allo stesso tempo, in quanto troppo costoso e dispendioso in termini di tempo generare un messaggio unico per ciascun **account** falso. Ora, però, con l'AI generativa si possono generare contenuti altamente personalizzati e **automatizzare** la loro diffusione senza sforzo, decidendone tempi e modi di somministrazione. Sono la scala e la portata del fenomeno a fare paura aprendo a scenari inediti e rendendo questo fenomeno profondamente diverso. Le persone sono sempre state in grado di utilizzare strumenti di **propaganda**; questo

ne cambia in maniera mostruosa la velocità di propagazione.

A questo punto, una delle vere sfide è quella educativa. Quando i media hanno iniziato a parlare dei *deepfake*, le persone hanno iniziato a capire che stavamo entrando in un mondo in cui i video potrebbero non essere ciò che sembrano.

Diventa però irragionevole aspettarsi che gli utenti che interagiscono con qualcuno su una piattaforma di **social media** possano essere in grado di capire se la persona con cui stanno parlando è reale.

Saranno le piattaforme a dover prendere provvedimenti per identificare contenuti generati artificialmente. La domanda finale diventa quindi: come pensano le grandi **aziende tech**, strumento principale di disseminazione di queste informazioni, di muoversi rispetto alle loro **responsabilità** e quali saranno le figure manageriali preposte per fronteggiare questa sfida inedita?



A, B, C, DIGITALE

AUTORE: MAURIZIO PIMPINELLA - TEMPO DI LETTURA: 3 MINUTI



Italia dietro la lavagna, con livelli medi di conoscenza di digitale e finanza troppo bassi per un Paese che voglia davvero essere protagonista della competizione globale. E non solo sul piano industriale

In base alle stime del Fondo monetario internazionale, l'Italia è l'ottava economia a livello globale mentre a livello europeo è la terza, la seconda invece sotto il profilo manifatturiero.

Il nostro Paese, quindi, rappresenta un punto di riferimento di primo piano per l'economia mondiale in particolare nei settori espressione della macroarea del **made in Italy**.

La **digitalizzazione** dell'economia e dei servizi, tuttavia, ci pone la necessità di allontanarci dal modello prettamente manifatturiero e rappresenta una rivoluzione che impone alle aziende, alle amministrazioni pubbliche e ai lavoratori l'assunzione di due processi correlati tra loro: la **riqualificazione delle competenze** e il loro reindirizzamento verso i settori produttivi di maggiore incidenza di tali **tecnologie**.

Allo stato attuale, quanto a competenze digitali, l'Italia ricopre, la 18° posizione dell'Indice europeo di digitalizzazione (Desi), in crescita rispetto alla 25° della precedente rilevazione. Tale dato indica immediatamente due fattori: il primo e più importante è che questo mal si concilia con la rilevanza dell'economia italiana. Il secondo fattore mostra che, nonostante una evidente crescita nella serie storica rispetto al recente passato, la strada da percorrere è considerevole.

Quanto illustrato, trova riscontro anche nel livello di **alfabetizzazione** degli italiani nel contesto finanziario. Nell'ultimo decennio, infatti, digitale e finanza si sono notevolmente avvicinati e ai servizi e ai prodotti finanziari tradizionali si sono aggiunti quelli innovativi offerti ora in modalità **online** e tramite **app** con i rispettivi pro e contro, opportunità e criticità. Dal 2017, la Banca d'Italia svolge con cadenza triennale un'indagine campionaria sull'alfabetizzazione finanziaria degli adulti in Italia. L'edizione 2023 ha messo in risalto un'evidente crescita rispetto a quella precedente non considerabile però ancora soddisfacente. Nel 2023, rispetto al 2020, il livello di alfabetizzazione finanziaria degli adulti in Italia, pur rimanendo

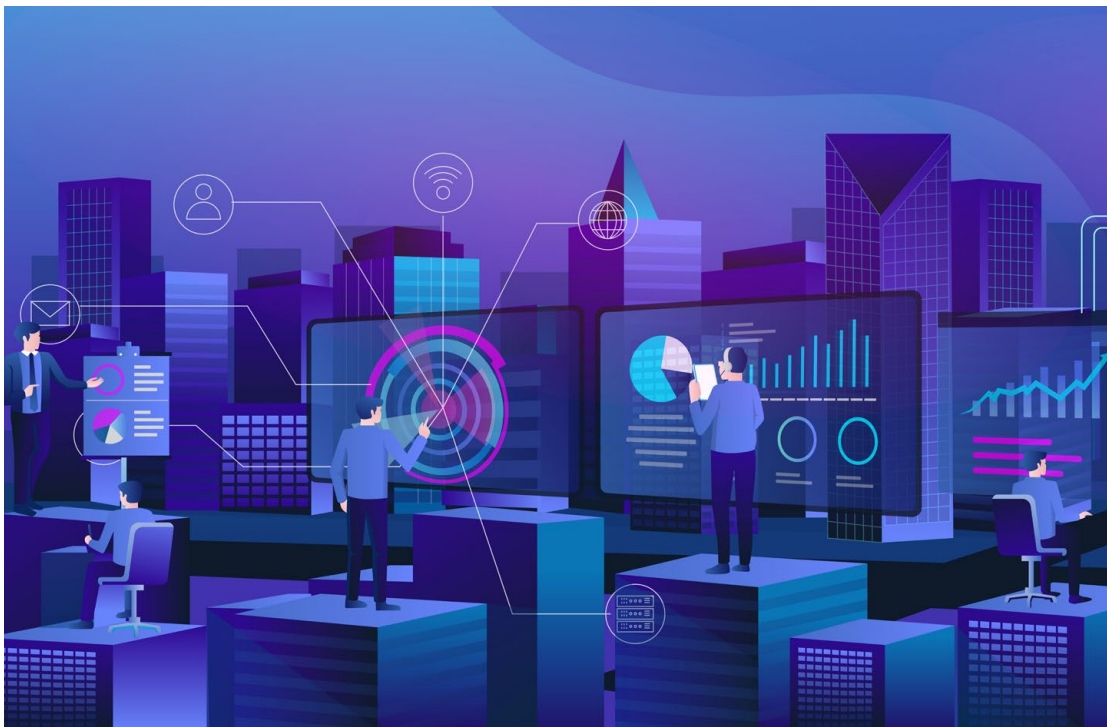
basso, è lievemente aumentato (da 10,2 nel 2020 a 10,6 nel 2023, su una scala da 0 a 20). Il miglioramento è guidato dai comportamenti e dagli atteggiamenti in campo finanziario. Per quanto riguarda poi la **finanza digitale**, il punteggio degli italiani è in media pari a 4,4 su una scala da 0 a 10. I punteggi sono maggiori tra chi è più istruito e nella classe di età tra 35 e 64 anni. Nel punteggio complessivo di finanza digitale vi è inoltre un **divario di genere** che penalizza le donne.

Il tema dell'alfabetizzazione digitale e finanziaria è poi strettamente collegato a quello della sicurezza degli strumenti finanziari e di **pagamento elettronici**. Posto che i sistemi di incasso e di pagamento sono sicuri e pienamente funzionanti, in questo ambito (così come in molti altri) la sicurezza si declina in una duplice veste.

Da un lato, infatti, si pone la **sicurezza degli strumenti digitali** in quanto tali, dall'altro l'uso scorretto che ne fanno gli utenti.

Nel 2023, rispetto al 2020, il livello di alfabetizzazione finanziaria degli adulti in Italia, pur rimanendo basso, è lievemente aumentato: da 10,2 nel 2020 a 10,6 nel 2023, su una scala da 0 a 20

Con l'esplosione delle **criptovalute** e delle applicazioni della moneta digitale, alfabetizzazione e sicurezza diventano centrali. La forsennata crescita del valore del **Bitcoin** che, ad oggi (e mi scuso per eventuali imprecisioni causate dalle frequenti oscillazioni), ha sfondato il muro dei 73 mila dollari di valore, rappresenta per molti l'illusione del guadagno rapido e facile, salvo poi perdere tutto a causa di un investimento improvvido, senza contare poi le numerose truffe che ruotano attor-



no a questi **asset digitali**. Un esempio di ciò è il caso del furto di Bitcoin dalla piattaforma Mt. Gox nel 2014, che ha portato alla perdita di centinaia di milioni di dollari di criptovalute. Questo dimostra l'importanza di comprendere le vulnerabilità delle piattaforme e l'adozione di pratiche di sicurezza robuste, come l'uso di **portafogli hardware** e l'autenticazione a due fattori. Giova ricordare poi che non sono infrequenti i casi in cui, perdendo, dimenticando o non avendo a disposizione le chiavi crittografiche anche il patrimonio diventa di fatto irraggiungibile. Una stima di Cypherock, suggerisce che circa 6 milioni di Bitcoin siano irrimediabilmente persi, per un valore di circa **165 miliardi di dollari**.

La **privacy** è un altro aspetto che giustifica in parte il ricorso alle criptovalute e su cui la Bce sta ragionando per quanto riguarda l'euro digitale. È evidente che sia necessaria l'individuazione di una soluzione di compromesso che consenta la giusta tutela di riservatezza con l'esigenza della sicurezza, ed è a questa esigenza che rispondono le caratteristiche delle Cbdc (le valute digitali delle banche centrali), i cui progetti stanno emergendo un po' in tutto il mondo. Come affermato da Christine Lagarde, Presidente della Bce: «La regolamentazione delle criptovalute deve **bilanciare la sicurezza con l'innovazione** per garantire un ambiente finanzia-

rio stabile e sicuro». A differenza del Bitcoin, una Cbdc poggia su basi più solide sia sotto profilo della *governance* sia sotto quello puramente economico, potendo contare sul supporto di una Banca centrale e di asset concreti, proprio a differenza delle criptovalute decentralizzate *by design*.

Scopo delle istituzioni finanziarie globali, in questo periodo di grandi rivoluzioni tecnologiche, è garantire quindi una **governance efficace**, tesa sì a tutelare consumatori e investitori ma anche impegnata non solo a non soffocare l'innovazione ma, anzi, a valorizzarla.

In conclusione, l'educazione finanziaria fino ad ora in Italia non ha dato i frutti sperati. L'alfabetizzazione digitale e finanziaria sono ancora un coacervo indefinito di norme, tecnologie ed esperienza di cui si parla da anni fraintendendone la portata. Troppo spesso ci si rapporta in termini presuntuosi ai consumatori e alle imprese ritenendo che mettere a loro disposizione servizi equivalga a garantirne la fruizione.

Dobbiamo, invece, migliorare in termini tecnico/pratici, ma anche sotto il profilo comunicativo in modo che si riesca a tramutare il grande valore tecnologico nella capacità delle persone di essere parte integrante del cambiamento. Questa sarà un giorno la vera alfabetizzazione: fornire alle persone gli strumenti utili per essere veri **cittadini digitali**.



ASCOLTARE, COMUNICARE, INNOVARE

Il Fasi, nella ricerca di soluzioni innovative volte a potenziare la conoscenza del valore della tutela offerta, è lieto di presentare **“Fasi In a Box”**: una pagina web progettata per semplificare e rendere sempre più immediato il rapporto tra il Fondo, le Aziende aderenti e i Dirigenti iscritti.

“Fasi In a Box” è molto più di un semplice kit informativo: è un hub completo di risorse e informazioni essenziali, accessibile con un clic, e rappresenta un’evoluzione del tradizionale plico cartaceo inviato in passato.

Al suo interno è possibile trovare la Circolare Fasi per il 2024, una panoramica dettagliata delle ultime novità introdotte dal Fondo, e tutti i link utili al sito istituzionale per consultare le informazioni e i documenti più importanti in modo semplice e rapido.

**Se non lo hai ancora navigato controlla la tua mail
e scopri come avere il Fasi sempre a portata di mano!**

Fasi In a Box

Il plico informativo diventa digitale

PER LE
AZIENDE



PER I
DIRIGENTI





progettomanager.federmanager.it