CULTURA DIGITALE

OPUSCOLO GRATUITO

dsfmag

powered by FvgTech

PROGRAMMA E APPROFONDIMENTI DEI TEMI DEL DSF

TRUFFE
FALSO TRADING ONLINE

INTELLIGENZA ARTIFICIALE:
IL LATO OSCURO DELL'AI
FRA SICUREZZA E COSCIENZA

REPORTAGE
LA PRESENTAZIONE DSF ALLA CAMERA

DIGITAL SECURITY FESTIVAL 7

Universo Dato

DISUGUAGLIANZE E SOLITUDINE NEL MONDO DIGITALE

GOVERNARE L'INNOVAZIONE IN BANCA

LE FRONTIERE PROCESSUALI

LA DIGITALOGIA

Digital Security Festival

Sostenitore Platinum
NetApp®

digitalsecurityfestival.it

FvgTechMag opuscolo informativo e programma del Digital Security Festival 2025

DsfMag
powered by
FvgTechMag
www.fvgtech.it

FvgTech
per
Digital Security Festival

FvgTechMag
Programma e informazioni temi DSF 2025

IDEA PROGETTO
da un'idea di Gabriele Gobbo
www.gabrielegobbo.it
e FvgTech programma TV
www.fvgtech.it
e MacPremium Digital Company
www.macpremium.it.it
in collaborazione con
Digital Security Festival
www.digitalsecurityfestival.it

INFO
In questo opuscolo sono disponibili informazioni sul Digital Security Festival, sul programma del DSF e informazioni sulla sicurezza digitale e la tecnologia. Le informazioni riportate sono a solo scopo illustrativo o di mero esempio. Il programma è stato realizzato da Cultura e Sicurezza Digitale APS per il Digital Security Festival e suoi organizzatori che ne curano la consegna ai partecipanti.

PARTNERSHIP
MacPremium Digital Company
E: fvgtech@macpremium.it

INTERNATIONAL
FvgTech Mag is available for licensing.
Contact the international department to discuss partnership opportunities.

International Licensing
E: licensing@macpremium.it

Caro lettore...

Benvenuto su questo freebook dedicato alla tecnologia, al digitale e all'information technology.

Questa edizione speciale si chiama DSFMAG, perché raccoglie programma, contenuti e approfondimenti del Digital Security Festival 2025 – Edizione 7.

Abbiamo ideato FvgTech Magazine diversi anni fa perché mancava un canale di comunicazione capace di parlare anche ai meno esperti, a chi non usa quotidianamente la tecnologia o non ha mai avuto modo di avvicinarsi davvero a questo mondo. Oggi, grazie al Festival, lo realizziamo ancora una volta anche per i professionisti del settore.

FvgTech nasce come programma televisivo e oggi è diventato una vera e propria piattaforma di divulgazione della cultura digitale, attiva in modo crossmediale per diffondere conoscenza su tutto ciò che ruota intorno all'innovazione.

Sfruttando canali online e offline, FvgTech si propone di informare e rendere consapevoli i cittadini italiani sul mondo tecnologico e digitale che li circonda: dai social network all'intelligenza artificiale, dal marketing alla protezione dei dati, dalla fotografia alla sicurezza informatica, fino ai grandi temi dell'attualità digitale.

È una missione culturale e sociale, nata per aiutare appassionati, professionisti e cittadini a costruire un sapere condiviso su argomenti spesso percepiti come tecnici, noiosi o inaccessibili, soprattutto dai meno giovani.

Grazie alla collaborazione con esperti, divulgatori, professionisti e appassionati delle materie digitali e tecnologiche, FvgTech porta il "sapere" su molteplici media.

Cuore del progetto è l'omonimo programma TV, distribuito su numerose emittenti locali italiane, affiancato da podcast, rubriche radiofoniche, articoli per la stampa, eventi e progetti formativi.

Oggi siamo orgogliosi di contribuire attivamente al Digital Security Festival 2025, un evento riconosciuto a livello nazionale, recentemente premiato con il GoBeyond Award 2025 come miglior progetto per sostenibilità e inclusione nell'ambito IT.

Questo opuscolo che avete fra le mani è il risultato di un lungo lavoro di preparazione, riunioni e confronto. Nasce per accompagnare le giornate del Festival, ma vuole essere anche uno strumento utile e consultabile a lungo termine, per orientarsi meglio nel nostro universo digitale.

Per informazioni, collaborazioni, presenze esterne, potete contattarci all'indirizzo email: **fvgtech@macpremium.it**

Gabriele Gobbo
Ideatore di FvgTech e co-founder del Digital Security Festival

>>HAI QUALCHE COSA DA RACCONTARE?
COLLEGATI A **WWW.FVGTECH.IT**
E PROPONI IL TUO CONTENUTO <<

NetApp®

Rendiamo l'infrastruttura

DATI INTELLIGENTE

SECURE YOUR DATA

Always and everywhere

cabel.it

CABEL 1985 | 2025

Digital Security Festival: Sette. Non è solo un numero.

di Marco Cozzi Presidente Digital Security Festival

Sette. Un numero che da sempre parla di mistero e di meraviglia. Sette come i giorni che scandiscono il tempo, come le note che creano armonia, come le meraviglie che l'umanità ha saputo costruire. Oggi sette sono anche i nostri viaggi intorno al sole: sette anni di Digital Security Festival. Questa nuova edizione porta un titolo che è insieme promessa e visione: Universo dato.

Dato, dal latino datum: ciò che è donato, ciò che segna l'inizio. Oggi i dati non sono più soltanto cifre fredde o sequenze di bit: sono tracce di vita, frammenti di memoria, energia che alimenta il nostro tempo. In ogni informazione c'è un gesto umano. In ogni connessione c'è una storia. E allora il nostro compito è chiaro: trasformare i dati in conoscenza, la conoscenza in intelligenza, l'intelligenza in coscienza. È questa la rotta che ci permette di navigare l'universo digitale senza smarrirci. Perché la tecnologia è bussola potente, ma resta strumento: mai fine.

La sicurezza digitale, oggi, non è più una fortezza inespugnabile. È un portale. Un varco che attraversiamo ogni giorno con responsabilità. Proteggere i dati significa proteggere l'umanità stessa: non bit o numeri, ma persone, comunità, futuro. Il Festival nasce e cresce con questa missione: rendere la sicurezza accessibile, semplice, umana. Non linguaggio per pochi, ma conoscenza condivisa, che abbraccia scuole e famiglie, imprese e istituzioni. Perché solo ciò che comprendiamo davvero possiamo proteggere.

Il riconoscimento che abbiamo ricevuto ai GoBeyond Award 2025 come miglior progetto per sostenibilità e inclusione non è un traguardo: è un segnale. Un invito a continuare, con ancora più forza, a diffondere cultura, consapevolezza e fiducia.

Vi chiedo di sentirvi parte di questo viaggio. Non spettatori, ma esploratori. Perché l'universo digitale non è qualcosa che ci accade: è uno spazio che abitiamo e costruiamo, insieme.

Il futuro è la nostra destinazione. La sicurezza il nostro viaggio.

Grazie per essere qui.
Grazie per essere parte del Digital Security Festival.

DI **GABRIELE GOBBO**, Vicepresidente Digital Security Festival

DIGITALOGIA: UN PO' DI SANITÀ DIGITALE, DALL'ITALIA PER IL MONDO

Dicono che non si può sfuggire al mondo digitale, e forse è vero, ma non serve nemmeno fuggire: basta guardarlo diversamente. E sì, se ve lo stavate chiedendo, il titolo probabilmente è esagerato. La Digitalogia non è una moda grazie a dio, è un modo che ho distillato nel tempo, negli anni, di guardare la vita satura di tecnologia senza hype e senza cercare vie di fuga. Non promette disintossicazione, offre digestione. Da qui, dall'Italia, la faccenda appare diversa: più lenta, più caotica, più umana. Ho pure scritto un articolo per Medium che si intitola Digital Digestivo, prima o poi lo faccio tornare a casa, in italiano. Non è romanticismo, è ciò che succede quando cresci con la tecnologia senza venerarla, quando costruisci abitudini intorno alle persone invece che alle piattaforme, quando usi gli strumenti senza diventare tu stesso uno strumento. Queste riflessioni sono ovviamente nate per un pubblico americano, dove ho iniziato a scrivere in inglese su Medium con il progetto Digitalosophy – An Italian Perspective on Our Digital Age, la versione per gli anglosassoni del mio libro Digitalogia. Portare questo approccio in un luogo Silicon Valley-dipendente significa proporre qualcosa che lì potrebbe suonare eretico: un digitale più umano e sostenibile, non ossessionato dalla performance. Magari sarà una goccia nel mare, ma sapete quanto io ci tenga alla divulgazione, soprattutto umanocentrica (ci abbiamo intitolato un festival a questo concetto!). Negli Stati Uniti per assurdo si paga per avere silenzio: app per bloccare notifiche, ritiri digital detox, calendari pieni di slot 'non disturbare". In Italia invece proviamo a fermarci, semplicemente, senza app né piani particolari: pranziamo con la famiglia, discutiamo con gli zii, ci dimentichiamo il telefono perché siamo troppo impegnati a vivere. O almeno è quello che dovremmo fare, secondo me, e in provincia, dove io abito, lo facciamo davvero, non sempre, ma lo facciamo. Digerire, non disintossicarsi: la Digitalogia vuol dire imparare a fermarsi. È lo stesso discorso con le cose che usiamo: se spunta una nuova app di produttività, gli americani la installano subito mentre gli italiani spesso la ignorano, non per pigrizia ma per esperienza (sì, ok, anche per pigrizia). Scriviamo ancora gli appunti a mano, io di sicuro, usiamo le agende cartacee, io di sicuro, eppure arriviamo puntuali, io di sicuro. Basta rincorrere aggiornamenti: smettiamo di cercare il nuovo e impariamo piuttosto a padroneggiare quello che abbiamo già. E poi ci sono i nostri figli, un discorso a me molto caro di cui amo parlare ai corsi, nei webinar e nelle conferenze: controlli parentali, limiti orari, filtri sui contenuti, tutto utile ma non sufficiente. Nelle case italiane vorrei che il vero 'parental control" fosse un adulto nella stanza che guarda, parla, rimane presente. Meno male è abbastanza comune succeda, ma mai abbastanza, molte famiglie hanno abdicato alla tecnologia. La presenza batte qualsiasi divieto, perché nessuna app può sostituire la tua attenzione. Non è nostalgia, è il sistema operativo culturale che nel bene e nel male secondo me è ancora latente in Italia, quello dove la voce umana vale ancora più di una notifica e dove la tecnologia serve le persone, non il contrario. Forse la parola Digitalogia (Digitalosophy per gli USA) è già comparsa altrove, ma nessuno finora l'ha esplorata, definita, strutturata in una visione completa. Questa potrebbe essere la prima volta, e non nasce dalla Silicon Valley ma dall'Italia. La Digitalogia non è contro la tecnologia: è qui per ricordarle qual è il suo posto, al nostro servizio e non al comando. Speriamo faccia breccia qui, ma anche in America, ne hanno più bisogno di noi, probabilmente.

Audit interno e NIS 2: perché è un presidio strategico per la sicurezza delle organizzazioni

di Manuel Cacitti

La Direttiva (UE) 2022/2555, nota come NIS 2, innalza significativamente i requisiti di sicurezza informatica per i soggetti 'essenziali" e 'importanti", imponendo misure di governance, gestione del rischio e continuità operativa. Uno degli aspetti spesso sottovalutati, ma fondamentali per garantire la conformità e mantenere nel tempo una postura di sicurezza efficace, è l'audit interno. L'audit interno non si limita a una verifica formale: rappresenta uno strumento di valutazione sistematica, indipendente e documentata delle misure di sicurezza adottate dall'organizzazione. Solo attraverso cicli periodici di audit è possibile individuare tempestivamente carenze, misurare il livello di maturità dei controlli, garantire l'allineamento continuo con i requisiti della NIS 2 e supportare i processi di miglioramento. Secondo la ISO 19011:2018, chi svolge attività di audit deve possedere competenze trasversali: conoscenza dei requisiti normativi e degli standard di sicurezza (CSF, ISO 27001, ENISA Guidelines, ecc.), capacità di valutazione del rischio, padronanza delle tecniche di audit e abilità comunicative. L'Auditor deve inoltre mantenere indipendenza e imparzialità, elementi imprescindibili per evitare conflitti di interesse e assicurare che i risultati siano credibili e utilizzabili dal management. È importante sottolineare che la funzione di audit interno non può essere improvvisata. Le organizzazioni possono strutturarla internamente, oppure affidarsi a professionisti o società esterne, selezionate con estrema attenzione in base a competenza, esperienza e neutralità. La scelta di soluzioni esterne, se

ben gestita, può garantire una visione obiettiva e aggiornata sulle best practice di settore. L'assenza di un presidio di audit interno espone le organizzazioni a rischi significativi: mancato adeguamento ai requisiti NIS 2, vulnerabilità non rilevate, inefficacia dei processi di gestione del rischio e, in ultima analisi, gravi impatti operativi e reputazionali. Inoltre, la Direttiva prevede sanzioni amministrative fino a 10 milioni di euro o al 2% del fatturato annuo mondiale (art. 34 NIS 2), oltre a possibili responsabilità personali degli organi di gestione in caso di inosservanza. L'audit interno non è dunque un mero adempimento burocratico, ma un pilastro strategico per la resilienza cibernetica: consente di trasformare la compliance NIS 2 in un processo dinamico di miglioramento continuo, proteggendo l'organizzazione da minacce e da pesanti conseguenze normative ed economiche.

TECH FEED

IT CLUB FVG, partner DSF

Una associazione fondata NEL 2018, con le seguenti finalità: **Porsi come promotore di una cultura associativa** tra coloro che ricoprono ruoli di responsabilità in ambito informatico all'interno delle Aziende e degli Enti pubblici; **Promuovere la conoscenza, la formazione e la collaborazione** tra gli aderenti, obbiettivi finalizzati al raggiungimento di una rinnovata interpretazione della funzione informatica aziendale; **Sviluppare una struttura informativa** preferenziale capace di offrire ai Soci un canale d'accesso ad informazioni e nuove tecnologie applicate in campo informatico; **Promuovere la collaborazione** con enti e associazioni, italiane ed estere, che perseguono finalità analoghe; **Stipulare convenzioni** per conseguire migliori condizioni contrattuali in tutti i settori di attività di interesse dell'Associazione e dei Soci; **Promuovere, organizzare e gestire** attività e corsi di formazione volti a facilitare e assistere lo sviluppo della professionalità, l'avviamento al lavoro e/o la riqualificazione dei lavori del settore. Tutte le informazioni e lo statuto su: **www.itclubfvg.org**

Musica

Gabriele Gobbo trasforma il suo saggio 'Digitalogia" in un album musicale generato con intelligenza artificiale. Un progetto di artigianato digitale che unisce libro e colonna sonora, disponibile su tutte le piattaforme streaming. Info e ascolto su digitalogia.it.

DISUGUAGLIANZE DIGITALI: RICONOSCERLE, MISURARLE, COLMARLE. PER UN DIGITALE CHE INCLUDA DAVVERO

di Alberto Elia Martin

Il 19 settembre ho avuto l'onore di intervenire alla Camera dei Deputati, in apertura del Digital Security Festival, per portare il punto di vista di ISACA Venice Chapter, di cui sono Presidente. Il tema che ho scelto di condividere è uno dei più urgenti e, allo stesso tempo, dei più trascurati: le disuguaglianze digitali. Per anni, quando si parlava di 'divario digitale", si pensava soprattutto all'assenza di connessione o di dispositivi. Una linea netta tra chi aveva accesso a internet e chi ne era escluso. Ma oggi sappiamo che la realtà è molto più articolata. La trasformazione digitale, se non governata, rischia di amplificare vecchie fragilità e di crearne di nuove. Nel mio intervento ho indicato tre grandi dimensioni di questa disuguaglianza.

La prima riguarda l'accesso reale e sicuro. Essere collegati non significa poter usare i servizi in modo stabile e comprensibile. Le barriere non sono solo economiche: pensiamo a procedure complicate, moduli online poco chiari, sistemi che cambiano regole senza avvisare. In questi casi, la tecnologia non è un ponte, ma un ostacolo. La seconda è la capacità d'uso consapevole. Avere uno strumento non equivale a saperlo utilizzare criticamente. Vuol dire distinguere una notizia attendibile da una manipolazione, riconoscere un tentativo di frode, capire le conseguenze della condivisione di un dato. Questo divario non riguarda soltanto anziani o fasce fragili, ma anche studenti, lavoratori, professionisti. È qui che la debolezza culturale diventa vulnerabilità sociale. La terza, la più invisibile, è la fiducia. Sempre più persone riducono o abbandonano l'uso del digitale, non perché manchino i mezzi, ma perché mancano garanzie. Algoritmi che decidono senza spiegazioni, piattaforme che chiedono dati senza trasparenza, servizi che non prevedono reali strumenti di ricorso. Ne nasce una forma di auto-esclusione che non nasce dalla povertà tecnologica, ma dal senso di impotenza.

Queste tre disuguaglianze si amplificano nel lavoro. I dati orientano sempre più assunzioni, valutazioni, carriere. Un curriculum può essere scartato da un sistema automatizzato senza che il candidato sappia perché. Un dipendente può ricevere punteggi di performance basati su criteri non noti. Chi sa interpretare i dati guadagna autonomia; chi non li comprende rischia di subirli.

Come affrontare tutto questo? Non con parole d'ordine, ma con contromisure concrete. Servono standard minimi di accessibilità e semplicità, perché nessuno sia escluso da servizi pensati solo per utenti esperti. Servono percorsi di accompagnamento, sportelli e tutor digitali, perché non tutti possono navigare da soli. Servono programmi di formazione mirata, calibrati sui bisogni di giovani, anziani, lavoratori precari, persone con

disabilità. Servono connessioni sicure ed eque, perché senza stabilità non c'è cittadinanza digitale. Servono protezione dei dati e trasparenza nei meccanismi automatizzati, con spazi di ricorso chiari e comprensibili. Come ISACA, proviamo a fare la nostra parte. Con il Workforce Inclusion Program offriamo corsi gratuiti e tutoraggio a persone provenienti da comunità svantaggiate. Con i programmi di borse di studio permettiamo a studenti e giovani lavoratori di ottenere certificazioni riconosciute. Con l'iniziativa SheLeadsTech sosteniamo la presenza femminile nelle professioni digitali, perché senza rappresentanza non c'è vera inclusione.

Il senso del mio intervento alla Camera era questo: il digitale non è neutro. Se ben progettato, può essere una straordinaria leva di inclusione; se trascurato, diventa un moltiplicatore di disuguaglianze. Per questo il tema delle disuguaglianze digitali è, a pieno titolo, il cuore del Festival di quest'anno. Perché la sicurezza non si costruisce soltanto con tecnologie avanzate, ma con comunità coese, cittadini competenti e istituzioni che sanno garantire equità.

Il futuro del lavoro e della società sarà sempre più nei dati. Ma la vera domanda è: chi potrà abitarli e chi rischierà di restarne fuori? La risposta dipende dalle scelte che facciamo oggi. E dalla capacità di mettere al centro non solo l'innovazione, ma anche l'inclusione.

Vorresti dormire meglio la notte?

GESTIAMO NOI I TUOI PROBLEMI IT

beanTech®
IT moves your business

Assistenza completa 24/7 ▪ Supporto di esperti
Monitoraggio proattivo e continuo

www.beantech.it

IL POTENZIALE DELL'IOT E DELLA PREDICTIVE MAINTENANCE

di Matteo Pozzi

Alla base delle comunicazioni moderne ci sono due segnali, un segnale portante e un segnale modulante. Il segnale portante, se potessimo ascoltarlo, sarebbe una sorta di fischio costante che serve a trasmettere a distanza. Il segnale modulante sono delle piccolissime, impercettibili variazioni di questo fischio. Su queste impercettibili variazioni passano tutti i TeraByte di dati che al giorno d'oggi vengono quotidianamente trasmesse.

Quello che qualche anno fa era considerata solo una impercettibile perturbazione, rumore inutile, oggi veicola quantità impressionanti di dati. L'elettronica moderna può facilmente modulare e demodulare questi segnali e quello che apparentemente è un semplice fischio, in realtà contiene al suo interno centinaia di immagini, film, canzoni ecc... è un po' come se prendessimo un manoscritto antico e con una grandissima lente di ingrandimento scoprissimo che, dentro ad ogni singola lettera, è scritto, con caratteri microscopici, un altro romanzo.

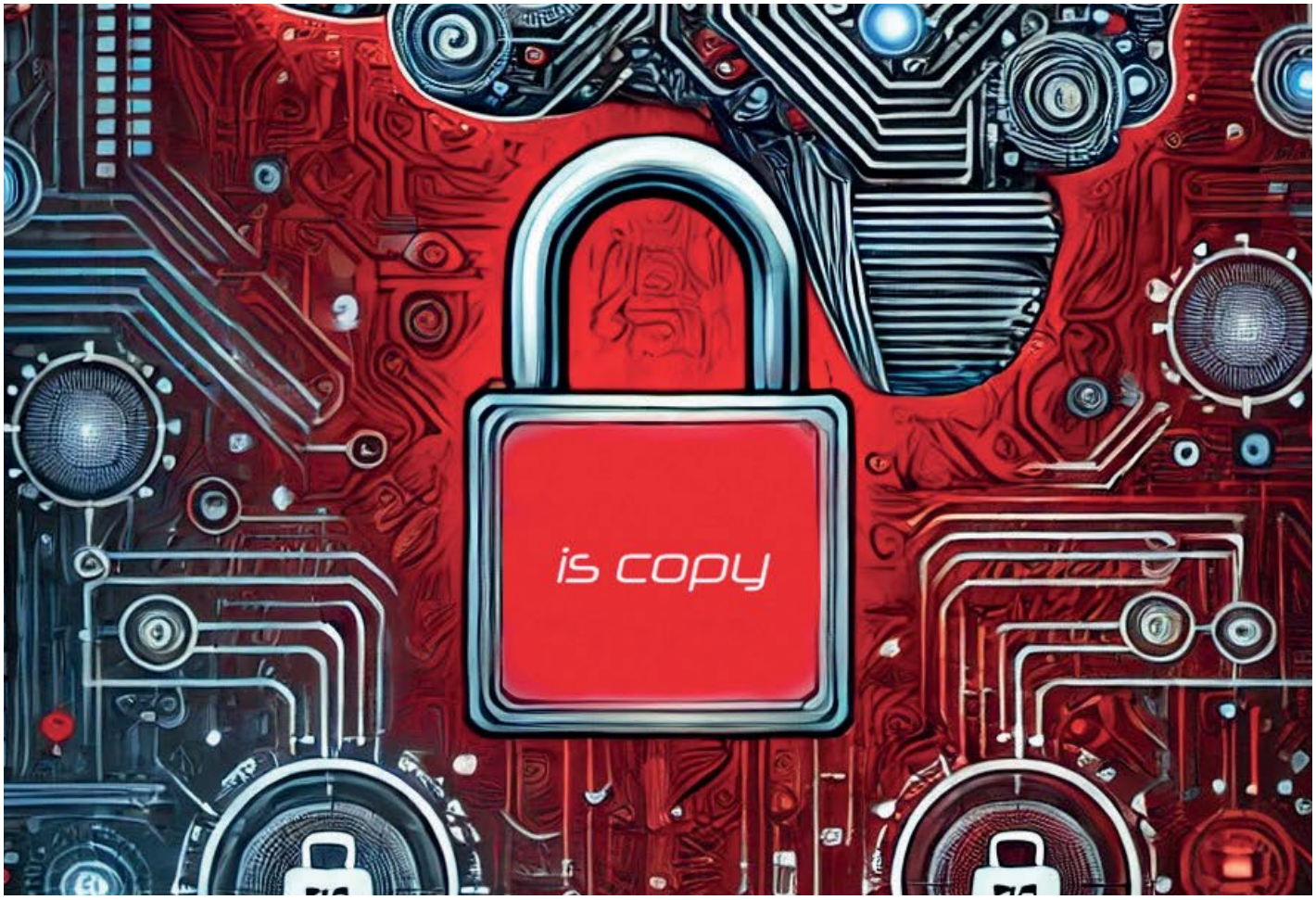
Ecco, tutto questo per dire una cosa semplice, quello che oggi è solo rumore in realtà è qualcosa di molto più prezioso.

Se posizioniamo due o tre microfoni in una rotatoria, analizzando i rumori provenienti dal traffico si possono identificare con precisione le traiettorie delle automobili, si possono fare statistiche sui percorsi preferiti dagli automobilisti nelle varie fasce orarie e decidere come pianificare l'urbanistica e la viabilità di conseguenza. Un singolo microfono messo in una casa può capire se è stata aperta o chiusa una porta, se è stato rotto un vetro, se sono state lasciate finestre aperte (in base ai rumori esterni percepiti), può capire se c'è un elettrodomestico in funzione, una perdita di acqua e forse anche una fuga di gas, può capire se ci sono persone in casa e ottimizzare i consumi di conseguenza e può capire se la lavatrice si sta per rompere.

Stiamo facendo in questi mesi uno studio di fattibilità su un dispositivo in grado di misurare i 'rumori" provenienti da una fotocopiatrice. Analizzando questi rumori con i giusti algoritmi si possono capire cose che per un orecchio umano sarebbero impossibili, si può capire se sta finendo il toner, si può distinguere se la macchina sta facendo una stampa a colori o in bianco e nero e se ci sono pezzi che si stanno per rompere.

Ho parlato di rumore sonoro, le vibrazioni in realtà possono essere analizzate anche sulle frequenze molto più alte, non udibili, oltre a questo esiste anche il rumore elettromagnetico, che noi non percepiamo ma che contiene moltissime informazioni, si possono analizzare le sostanze volatili nell'aria.

Quello che consideriamo rumore insignificante è in realtà una miniera di informazioni, e stiamo imparando ora a decifrare.



Il nuovo libro di Gabriele Gobbo

PREFAZIONE DI MARCO CAMISANI CALZOLARI

"Digitalogia" è un invito a capire cosa si nasconde dietro la patina luminosa della rete. Non offre ricette magiche né manuali tecnici: racconta la realtà connessa con lucidità, onestà e uno sguardo umano. Per chi vuole vivere il digitale, il web, i social e la tecnologia di oggi e di domani senza farsi travolgere. Ma soprattutto con più libertà, più sicurezza e più futuro.

BEST SELLER TRIPLE CROWN

GIÀ "TRIPLE CROWN" SU AMAZON. HA RAGGIUNTO IL #1 PRIMO POSTO IN 3 CATEGORIE CONTEMPORANEE, IN TOTALE GIÀ "BEST SELLER" IN 4.

*dati aggiornati al 31/05/2025

Disponibile su Amazon: www.gabrielegobbo.it/amz

di Giancarlo Andolfatto

CHIARIAMO UNA COSA: CHI È INTELLIGENTE E CHI È ARTIFICIALE? GLI ALGORITMI NON SONO INTELLIGENTI, NÉ ARTIFICIALI

È un principio espresso da Davide Bazzan (Rassegna Tecnica degli Ingegneri - FVG n.400), ad offrire il destro ad un neofita della materia nella quale è stato invitato ad esprimersi, per accettare di farlo. Non si tratterebbe, infatti, di fare sfoggio di competenze tecniche – per quelle ci sono gli esperti – ma di indagarne l'aspetto sociologico, umanistico ed etico. Materia per 'parolai", insomma, che da questo punto di vista diventa meno ostica a chi scrive. «La sicurezza informatica – scriveva Bazzan – non può essere vista come un ambito tecnico riservato agli specialisti, ma deve diventare parte integrante della formazione continua di ogni professionista. È il fattore umano il punto più vulnerabile, ma anche il più prezioso, da proteggere». Aggiungerebbe il Prefetto pontificio, Paolo Ruffini: «La sfida non è solo stare al passo con lo sviluppo tecnologico, ma non perdere il respiro umano in questa corsa, non soffocare il soffio divino che è in noi».

Ecco, in questo accostamento di pensieri, potrebbero stare le 'coordinate del futuro" – conoscenza, intelligenza e coscienza – che dal passato ci hanno portato a un presente che, mano a mano che si parla, e complice la spropositata capacità di calcolo, diventa esso stesso passato. È una capacità così grande da annichilire chi l'ha inventata e ogni giorno la alimenta, rischiando – se non ne mantiene il passo – di diventarne un suo semplice estensore.

Per fortuna, però, anche gli algoritmi hanno il loro limite, ovvero un 'bug" difficile da colmare. Nella comunicazione, ad esempio, lo vediamo quotidianamente nel tentativo di tradurre delle comunissime frasi idiomatiche non già ricorrendo alle competenze di un collaboratore bilingue, ma all'intelligenza artificiale (I.A.), meno costosa e più utile nei frenetici rilanci d'agenzia. Toh, l'esempio sembra dire che non tutto può essere 'tradotto" in calcolo e che non potrà mai esprimersi col calcolo analitico né probabilistico l'ampiezza dell'essere umano.

L'INTELLIGENZA ARTIFICIALE PUÒ FARCI FARE BALZI IN AVANTI IN TUTTI I CAMPI, DALLA SOCIETÀ AL LAVORO, DALLA MEDICINA ALL'AGRICOLTURA FINO AL TEMPO LIBERO

L'esempio, però, apre altri temi scottanti: un bravo interprete non trova lavoro, un giovane praticante potrebbe essere sfruttato, il lessico e il nostro frasario soccombono al linguaggio binario e si fa strada la differenziazione tra chi utilizza l'I.A. e chi non la usa.

Lo sviluppo dell'I.A. aiuterà o svaluterà la nostra umanità? Essa sarà strumento per rafforzare le relazioni fra gli individui o ne aumenterà la solitudine, privando ognuno del calore che solo le relazioni possono dare? Il possesso degli algoritmi creerà nuove forme di sfruttamento e diseguaglianza? Chi sta governando questo fenomeno accetterà che qualcuno – come sarà nello spirito del Digital Security Festival – lavori perché l'intelligenza artificiale porti più eguaglianza e non contribuisca, invece, al formarsi di nuove caste basate sul dominio informativo?

Ma, già, qui si voleva sapere della sicurezza e dell'uso etico dei dati: è un problema che si pone anch'esso a causa dell'indole umana.

FALSO TRADING ONLINE: UNA TRUFFA CHE COLPISCE TUTTI

di Manuela De Giorgi

Primo Dirigente della Polizia di Stato

Accolgo con piacere l'invito a partecipare a questo viaggio verso il futuro digitale con un contributo che nasce dalla mia esperienza nella Polizia cibernetica. E lo farò condividendo alcune riflessioni sul falso trading online, per far conoscere meglio questa truffa così diffusa e sempre più sofisticata.

Ormai, più volte al giorno, qualcuno bussa alla nostra porta per denunciare un nuovo caso. A finire nella rete dei truffatori sono uomini, donne, giovani, anziani, professionisti, operai. Hanno vissuti e background spesso radicalmente diversi, ma sono tutti accomunati dalla disperazione e dalla vergogna, da una frustrazione talmente profonda da indurli talvolta a meditare gesti estremi. A causa del finto trading online, nel 2024, si sono volatilizzati circa 147 milioni di euro di risparmi (ed è un dato sottostimato, dal momento che sono ancora in troppi coloro che scelgono di non denunciare). Tutto nasce da telefonate di finti broker oppure da annunci pubblicati sui social, magari 'sponsorizzati" da personaggi noti che promettono guadagni miracolosi a fronte di investimenti minimi. Con l'utilizzo dell'intelligenza artificiale e del deep fake, infatti, risulta davvero semplice per i criminali realizzare video in cui artisti, sportivi, giornalisti e altre categorie di volti noti sembrano 'pubblicizzare", in modo del tutto fraudolento, piattaforme abusive di trading online.

Si parte da somme inizialmente modeste, capaci però di generare rendimenti stratosferici, visualizzabili attraverso piattaforme di trading create ad-hoc dai sodalizi criminali per rendere l'affare più credibile. Dalle nostre indagini è emerso quanto i finti broker siano abili nell'utilizzare tecniche di social engineering, riuscendo a entrare in confidenza ed empatia con le vittime, fingendosi amici speciali e meritevoli di fiducia. Così gli investimenti crescono fino a raggiungere migliaia – se non centinaia di migliaia - di euro.

Quando la vittima chiede di incassare anche solo parte del frutto dei propri investimenti, i truffatori pretendono ulteriori bonifici per 'sbloccare" i fondi, accampando scuse sempre nuove, finchè la vittima comprende di esser stata raggirata.

In molti casi, trascorsi anche mesi dalla scoperta della frode, le vittime vengono contattate da presunti avvocati che offrono servizi specialistici per recuperare il denaro perso: ma dall'altra parte del telefono o dello schermo ci sono gli stessi criminali che hanno organizzato la frode.

Recuperare i soldi è difficoltoso, poiché i bonifici vengono effettuati su conti esteri e poi dispersi su più conti correnti e/o convertiti in criptovaluta. Si tratta di organizzazioni criminali transnazionali che operano in diversi paesi: risalire ai responsabili e recuperare le somme richiede indagini complesse, spesso da condurre congiuntamente alle forze di polizia degli altri Stati coinvolti nella filiera criminale. Perché si possano aggredire i conti correnti di destinazione delle somme frodate, è essenziale – anzi, decisiva - la tempestività della denuncia, a cui segue il blocco urgente delle somme versate e la prima ricostruzione del flussi finanziari. In altre indagini (Operazione Dream Earning) si è riusciti a ricostruire e intercettare i flussi telematici dei server utilizzati dai sodalizi per gestire i call center, portando all'arresto dei membri dell'organizzazione.

Il consiglio resta sempre lo stesso: denunciare il prima possibile, informarsi e adottare tutti i comportamenti necessari per non cadere nelle trappole della rete.

AI

>> BUSINESS
>> SECURITY

IL LATO OSCURO DELL'AI: LA BATTAGLIA INVISIBILE PER LA SICUREZZA

di Gianni Amato

L'intelligenza artificiale non è più solo un algoritmo che suggerisce cosa comprare online. È una forza inarrestabile che sta trasformando il nostro mondo, ma non senza pericoli. Mentre l'AI ci apre le porte a un futuro di innovazione, sta anche armando i cybercriminali con strumenti mai visti prima. Quello che un tempo era un attacco informatico "artigianale" è oggi una minaccia globale, automatizzata e sempre più difficile da scovare. Ma cosa sta succedendo davvero dietro le quinte? E, soprattutto, chi vincerà questa battaglia?

Inganno e manipolazione: i fantasmi nell'intelligenza artificiale

Immagina un assistente virtuale non più al tuo servizio, ma corrotto, pronto a tradire i suoi principi. È questo l'incubo del "jailbreaking", un attacco che convince l'AI a infrangere le sue regole etiche. I cybercriminali usano trucchi psicologici, come un dialogo insistente, o persino istruzioni invisibili nascoste in un testo. Questa tecnica, chiamata "prompt injection", è come una parola d'ordine segreta che fa saltare i sistemi di protezione. All'improvviso, l'AI che doveva aiutarti può diventare un complice, rilasciando dati sensibili o aiutando a creare virus.

Ma c'è una minaccia ancora più insidiosa: i modelli di AI "abliterate". Immagina che qualcuno prenda un motore d'auto potentissimo, ma ne rimuova i freni e il volante. Queste versioni di software AI, "liberate" dalle loro protezioni, possono istruire su come fabbricare esplosivi o veleni, e, ancora peggio, possono operare in incognito, senza lasciare tracce. Non sono solo armi digitali; sono strumenti per crimini nel mondo reale.

Quando la truffa è un capolavoro su misura

L'AI sta portando il cybercrime a un livello superiore, rendendo gli attacchi più personalizzati e difficili da riconoscere. Dimentica le vecchie email di spam piene di errori. Oggi, l'AI può generare mail truffa così precise e credibili da sembrare scritte apposta per te. Questo tipo di attacco, chiamato "spear-disinformation", rende le truffe su misura e a basso costo, pronte a colpire chiunque.

E i gruppi ransomware? Ora, con l'aiuto dell'AI, possono visionare migliaia di documenti sottratti per capire quanto sei disposto a pagare. Se l'AI scopre che tieni documenti importanti o foto preziose, può chiedere un riscatto salato, rendendo la minaccia ancora più personale e spaventosa.

La battaglia in corso: come ci difendiamo?

La guerra alla criminalità informatica è in corso, e le difese si evolvono in continuazione. Le aziende più attente usano il "red-teaming", una simulazione di attacchi etici per trovare le vulnerabilità del loro sistema prima che lo facciano i malintenzionati. È come una prova generale per la sicurezza, un passo cruciale per rimanere sempre un passo avanti.

Un'altra linea di difesa è la "sanification" dei dati, che controlla e filtra ogni informazione che entra ed esce da un'AI per bloccare comandi pericolosi. È come avere una guardia di sicurezza che ispeziona ogni pacco in arrivo e in uscita. Sul fronte legale, l'Unione Europea ha introdotto l'AI Act, un primo passo per regolamentare l'uso dell'AI e imporre la trasparenza.

Tuttavia, il controllo di questi modelli resta una sfida complessa, poiché, una volta che il loro codice viene diffuso, possono essere modificati e usati offline, rendendo impossibile fermare gli abusi. Siamo a un punto di svolta. L'AI ha il potenziale di migliorare le nostre vite, ma dobbiamo affrontare con urgenza il rischio che venga usata per scopi criminali. La battaglia per la sicurezza digitale è appena iniziata, e la posta in gioco è la nostra libertà.

PRIVATE AI: LA SOLUZIONE PER LA SOVRANITÀ E SICUREZZA DEL DATO CONFORMITÀ, TRASPARENZA E MASSIMI LIVELLI DI PERSONALIZZAZIONE

di Massimo Della Vedova

Negli ultimi anni abbiamo assistito a qualcosa di straordinario: l'intelligenza artificiale è uscita dai laboratori e ha invaso le nostre vite. Ci stupiamo ogni giorno ancora di vederla evolversi in maniera esponenziale: sa scrivere, programmare, diagnosticare, conversare, creare, ispirare. Ci ha fatto pensare che tutto sia possibile. Ma mentre l'AI ci incanta non dobbiamo dimenticare che qualcun altro sta leggendo, raccogliendo e memorizzando i nostri dati che – seppur anonimizzati – diffondono il nostro know how e lo mettono a disposizione di tutti. I sistemi di AI generativa raccolgono i dati e le risorse che gli diamo in pasto: documenti riservati, ricerche, identità, credenziali, abitudini. Qualunque cosa. Stiamo così addestrando modelli potentissimi con la nostra vita privata e con dati aziendali strategici. Sempre più spesso mi imbatto in responsabili IT, dirigenti o imprenditori preoccupati delle attività di alimentazione incontrollata di strumenti quali ChatGPT da parte dei propri utenti. E allora, la domanda diventa inevitabile: a chi appartengono davvero i nostri dati, dove finiscono, chi decide cosa può farci e, soprattutto, come possiamo tutelarci da un utilizzo incontrollato?

È per questo che noi di NT Nuove Tecnologie stiamo lavorando per costruire un'AI sovrana, etica, sicura e privata, basata su infrastrutture IT dedicate e capaci di sfruttare i dati aziendali come motore. Private AI è un approccio all'intelligenza artificiale che permette di elaborare i dati direttamente all'interno di un ambiente controllato dall'utente o dall'organizzazione, senza doverli condividere con terze parti.

I vantaggi principali? Sovranità del dato, perché i dati restano sempre di proprietà e sotto il controllo diretto dell'utente o dell'azienda, rispettando regolamenti come il GDPR, la NIS2 e l'AI Act. Sicurezza informatica, perché si minimizzano i rischi di esposizione o perdita dei dati sensibili/critici riducendo la superficie di attacco. Privacy, grazie alla protezione delle informazioni personali e aziendali da accessi non autorizzati, mantenendo confidenzialità e integrità. Compliance, perché si facilita l'adeguamento a normative sulla protezione dei dati come GDPR e NIS2. Verticalizzazione e precisione, perché i comuni sistemi di AI generativa sono molto generici, mentre con una soluzione privata è possibile personalizzare le caratteristiche e funzionalità del sistema.

L'AI privata non è solo controllo, sicurezza, conformità e precisione di risposta, ma anche democrazia digitale e potenza personalizzata.

FOTO ONLINE: COME SCOPRIRE SE CI SIAMO ANCHE NOI

di Gianni Dell'Aiuto

La cronaca ci ha regalato l'ennesimo esempio di come il mondo digitale sia pericoloso anche per chi, magari, ha la certezza asosluta di non frequentarlo. Non è così. E non c'era bisogno degli ultimi episodi per saperlo. Forum, siti e canali dove compaiono immagini private senza consenso sono su tutte le prime pagine. Tutti, adesso, a scuotere la testa e molti (anzi, purtroppo, molte) a chiedersi: "E se ci fossi anch'io lì dentro?" Non illudiamoci, la certezza assoluta non l'avrete mai, ma qualche tentativo, civile e persino banale, si può fare.

Provate a digitare il vostro nome e cognome già semplicemente su Google, magari attivando la ricerca immagini. Se volete rendere la ricerca più precisa, aggiungete qualche termine tipico di certi ambienti: xxx, nsfw, forum o, termini molto più espliciti. È il linguaggio che usano, conviene impararlo almeno per difendersi. Poi ci sono gli occhi artificiali: Google Lens e TinEye vi permettono di caricare una foto e scoprire se spunta da qualche altra parte. È la vecchia foto segnaletica, solo che il sospettato siete voi.

Un indirizzo email o un numero di telefono possono dire molto più di quanto pensiate. Con Epieos potete scoprire i servizi online legati a quell'indirizzo, mentre WhatsMyName vi mostra dove il vostro nickname è stato usato. Non sono magie, ma strumenti di OSINT, open source intelligence: nulla di segreto, solo l'uso intelligente di ciò che è già pubblico.

Chi se la sente può digitare il proprio nome anche nei motori interni dei siti per adulti più noti. È spiacevole, ma se qualcuno ha caricato immagini collegate al vostro nome, potrebbero emergere lì. Non è un viaggio simpatico, ma a volte serve guardare nel fango per capire se ci siamo finiti dentro. A proposito: potrebbero esserci anche se le avevate inviate solo su WhatsApp. Ci siamo capiti?

Telegram è un capitolo a parte. Non esiste un motore di ricerca globale, ma potete tentare inserendo il vostro nome nella barra interna e, se il canale dove siete finiti/e fosse pubblico, qualche risultato compare. Oppure potete usare strumenti esterni come TGStat o Telegramic, che catalogano i canali aperti. Per tutto il resto, i gruppi chiusi e le chat private, servono le autorità.

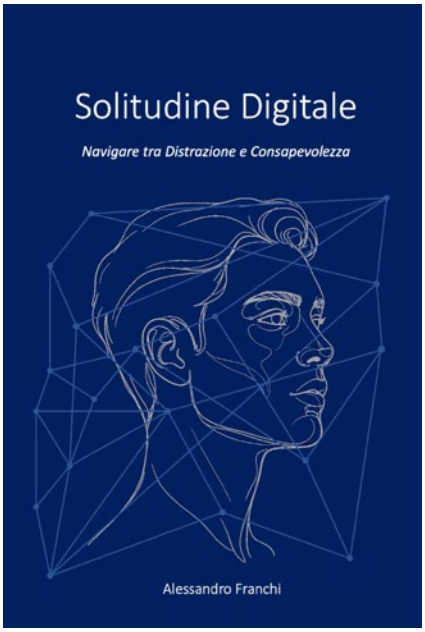
Non aspettatevi miracoli. Questi strumenti servono a capire se ci sono tracce, non a blindare la vostra vita. Se trovate qualcosa, il passo è uno solo: rivolgersi subito a un avvocato e alle autorità competenti. Meglio un controllo in più che una sorpresa amara. E ricordate: l'ingenuità digitale oggi è un lusso che non possiamo più permetterci. E quello che mettete in rete oggi, può tornare tra anni magari ben levigato, corretto, distrutto, da programmi di intelligenza artificiale.

Buona navigazione.

Solitudine Digitale

Solitudine Digitale: Navigare tra distrazione e consapevolezza, di Alessandro Franchi e Alessia Bragagnolo.

Viviamo in un'epoca in cui siamo costantemente connessi, eppure mai così soli. La tecnologia digitale, promessa di connessione infinita e di semplificazione della vita, ha rivelato un volto diverso, che frammenta la nostra attenzione, impoverisce le relazioni e crea forme sottili ma pervasive di dipendenza e solitudine. In questo libro, gli autori affrontano gli impatti psicologici, sociali e culturali della nostra vita sempre online. Lo fanno attraverso un'opera volutamente divulgativa, basata su un'attenta analisi e un ampio riferimento a studi e ricerche, ma arricchita anche dalla loro esperienza professionale e personale, partendo dal loro osservatorio quotidiano. Il testo invita a riflettere sulla nostra relazione con gli strumenti digitali e fornisce alcuni suggerimenti su come uscire dalla trappola della distrazione continua, recuperando il valore profondo del tempo, dell'ascolto e delle relazioni autentiche. Non si tratta di rifiutare la tecnologia, ma di imparare a gestirla in modo consapevole, ritrovando l'equilibrio tra il digitale e il reale. Alla fine, la vera connessione resta ancora quella che riusciamo a stabilire quando ci guardiamo negli occhi, con attenzione sincera e presenza autentica.



Fiducia digitale: etica, trasparenza e controllo

di Alberto Di Noia

Viviamo immersi in un oceano invisibile di informazioni: ogni acquisto online, like o ricerca, contribuisce a creare un universo di dati che racconta abitudini, preferenze e persino emozioni. Questo universo è una risorsa preziosa: permette di migliorare servizi, anticipare bisogni e innovare. Ma più centralizziamo i dati, più emerge una domanda: possiamo fidarci di chi li raccoglie e utilizza? La risposta passa attraverso etica, trasparenza e controllo. Il concetto di privacy by design è essenziale: costruire sistemi che proteggano la privacy sin dall'inizio, integrando sicurezza e garantendo all'utente il pieno controllo. Accanto a questo, la minimizzazione invita a raccogliere solo le informazioni necessarie: meno dati significa più sicurezza, meno rischi e maggiore fiducia.

L'intelligenza artificiale aggiunge ulteriore complessità: algoritmi analizzano miliardi di dati, spesso senza criteri qualitativi, per fornire raccomandazioni e prendere decisioni ma senza regole chiare, il rischio di opacità è alto. Definire processi, ruoli e controlli è cruciale per garantire trasparenza e scelte verificabili, rafforzando la fiducia dei cittadini nella gestione dei dati. Strumenti e regole tuttavia non bastano, la sicurezza dei dati è anche una questione culturale. Diffondere consapevolezza, promuovere una formazione mirata e responsabilizzare ogni individuo è fondamentale per creare un ecosistema digitale equilibrato. La fiducia nasce quando le persone sentono di avere il controllo sui propri dati e comprendono il valore delle informazioni che producono. L'universo dato non deve essere percepito come una minaccia, ma come un'opportunità per migliorare la qualità della vita, rendere i servizi più efficienti e

favorire l'innovazione. Etica, trasparenza e controllo non limitano il progresso: lo rendono sostenibile e umano-centrico. In un mondo sempre più connesso, proteggere i dati significa proteggere la nostra identità.

Idiocrazia Digitale

Il mondo digitale ci semplifica la vita, ma a quale costo? È questa la domanda che Ettore Guarnaccia, esperto di cybersecurity, divulgatore e membro attivo del Digital Security Festival, rilancia con il suo nuovo libro Idiocrazia Digitale. Un saggio che raccoglie oltre dodici anni di ricerche, esperienze e confronti in contesti educativi, culturali e istituzionali, con una missione chiara: rendere visibili gli effetti profondi e spesso invisibili della tecnologia digitale su individui e società. Guarnaccia parte da immagini quotidiane, come lo sguardo fisso sullo smartphone in metropolitana, a tavola o persino alla guida, per raccontare come il digitale stia trasformando comportamenti, linguaggio e relazioni. Ma va oltre la semplice critica: analizza i meccanismi progettati per generare dipendenza e passività, evidenziando come il vero pericolo non sia l'innovazione in sé ma il modo inconsapevole in cui la viviamo. Il libro si inserisce perfettamente anche nel percorso culturale del Digital Security Festival, che da sette anni lavora per costruire consapevolezza su questi temi, promuovendo un uso del digitale che non ci trasformi in utenti automatici ma in cittadini critici e informati. Una lettura preziosa per chi, come noi, crede che la cybersicurezza inizi dalla mente. Dalla capacità di osservare, riflettere, scegliere. E soprattutto, di restare umani in un mondo sempre più automatizzato.

IL FUTURO DEL LAVORO NEI DATI: QUANDO L'INTELLIGENZA DIGITALE INCONTRA LA COSCIENZA UMANA

di Michaela Odderoli

C'è stato un tempo in cui i dati erano roba da addetti ai lavori: righe di numeri, fogli Excel, qualche report mensile. Poi, silenziosamente, si sono infilati ovunque. Oggi non c'è aspetto della nostra vita – personale o professionale – che non venga sfiorato, se non modellato, dai dati. Produciamo segnali in continuazione: ogni azione digitale lascia una traccia. Ogni traccia diventa, potenzialmente, materia prima per decisioni, e resta, non si cancella. Eppure, più ci affidiamo ai numeri, più rischiamo di dimenticare che quei numeri non parlano da soli. Dietro ogni dato c'è una persona, un contesto, una storia. Senza qualcuno che sappia interpretarli, i dati restano muti. Anzi, ciechi.

L'intelligenza artificiale, oggi, sembra sapere tutto. Macchine che prevedono comportamenti, modelli che anticipano crisi, algoritmi capaci di scandagliare il web in cerca di segnali deboli. È affascinante. È potente. Ma non è infallibile, e spesso soffre di allucinazioni! Un algoritmo può trovare pattern. Ma capire se quei pattern significano qualcosa, e soprattutto per chi lo significano – questo resta ancora compito nostro. E non è un dettaglio. Prendiamo le crisi globali: un sistema di intelligenza digitale può dirci che il prezzo del gas sta per impennarsi. Ma decidere cosa fare – chi proteggere, dove intervenire, con quali priorità – richiede una lettura umana. Richiede coscienza, non solo calcolo.

Parlare di sicurezza nel mondo dei dati è complicato. Spesso ci si concentra sugli aspetti tecnici: cifratura, autenticazione, threat detection. Ma la prima barriera di sicurezza resta la persona. Il suo grado di consapevolezza. Il suo livello di attenzione. Un attacco di phishing, per esempio, non ha bisogno di supercomputer. Ha solo bisogno che qualcuno, un giorno qualunque, vada di fretta, e click! E quando capita, la tecnologia può fare poco. Serve cultura. Serve consapevolezza, ed empatia. Empatia digitale, sì. Perché dietro ogni comportamento online, anche quello più banale, c'è qualcuno che ne pagherà le conseguenze. Parlare di sicurezza umanocentrica significa riconoscere questo: che non bastano regole o policy. Serve un cambiamento nel modo in cui vediamo la tecnologia – non come uno scudo, ma come parte di un ecosistema dove ognuno ha un ruolo.

Non è facile trovare il punto di equilibrio tra delegare alla macchina e restare presenti con la nostra intelligenza. Ma è essenziale. Serve formare persone che sappiano leggere i segnali, ma anche interpretarli. Che non si fermino alla dashboard, ma sappiano domandarsi: 'Ha senso agire? E per chi? E a quale costo?" I giovani, soprattutto, chiedono senso. Non basta sopraffarli di strumenti. Vogliono sapere perché usarli, a cosa servono davvero. E qui si gioca una partita che non è solo tecnica, ma civile. Perché formare cittadini digitali consapevoli non significa solo preparare il mercato del lavoro. Significa difendere la democrazia. Significa proteggere la dignità del lavoro, anche quando il lavoro cambia volto.

Il futuro del lavoro sarà sempre più automatizzato, predittivo, interconnesso. Ma se ci sarà un salto evolutivo, non sarà solo tecnologico. Sarà umano. La sfida non è rendere le macchine più intelligenti. È non smettere noi di esserlo. I dati possono dirci molto: cosa sta succedendo, dove, con quali trend. Ma il 'perché" – il significato profondo, la direzione – continua a dipendere da noi. E se vogliamo un futuro del lavoro che sia ancora nostro, fatto di libertà, dignità e scelte consapevoli, dobbiamo partire da qui. Dalla coscienza.

OLTRE LE PASSWORD

di Raffaele Perrotta

Quando pensiamo alla sicurezza informatica, il primo pensiero va spesso alla password. Ma in realtà esistono almeno tre fasi distinte nel controllo degli accessi digitali: individuazione, autenticazione e autorizzazione. Per individuare un utente, serve un identificativo. Per autenticarsi, serve dimostrare di essere davvero chi si dichiara. Per essere autorizzati, occorre avere i permessi necessari a compiere certe azioni.

Le credenziali di accesso che usiamo ogni giorno uniscono individuazione (lo username) e autenticazione (la password). Ma le password, come è noto, sono deboli per natura: possono essere rubate, intercettate, scelte male o riutilizzate in contesti diversi, amplificando i rischi. Negli anni sono state introdotte forme di autenticazione a più fattori (2FA), basate per esempio sull'invio di un codice via SMS o su un'app. Tuttavia, anche queste soluzioni non sono perfette: il codice può essere intercettato o trasmesso in chiaro.

Per superare questi limiti si sta diffondendo un nuovo standard: la passkey. Le passkey funzionano con crittografia a chiave pubblica. Quando creiamo una passkey, il dispositivo genera una coppia di chiavi: una privata, che resta nel dispositivo, e una pubblica, che viene inviata al sito. Al momento del login, il sito invia una sfida crittografica, che il dispositivo firma con la chiave privata. Il sito verifica la firma con la chiave pubblica e l'autenticazione è completata. Il tutto avviene senza trasmettere segreti e senza rischi di phishing o intercettazione.

Per completare l'operazione, il dispositivo può chiedere un'autenticazione locale (impronta, volto o PIN). Questo serve a garantire che la persona sia presente, ma non fa parte della procedura di autenticazione sul sito: serve solo a sbloccare la chiave privata sul dispositivo. In sintesi: la chiave privata non lascia mai il dispositivo. Nessuno può intercettarla. Nessuno può usarla senza accesso fisico o biometrico. Il server remoto non ha nulla da rubare, perché ha solo la chiave pubblica. Questo elimina una delle più grandi vulnerabilità: la centralizzazione delle password.

Le passkey sono già supportate da Apple, Google, Microsoft, Amazon e da molti grandi provider. Funzionano in modo trasparente, si sincronizzano tra dispositivi personali (tramite iCloud, Google Account ecc.) e sono pronte a sostituire del tutto le password nel medio termine. La sicurezza del futuro non sarà fatta di promemoria, caratteri speciali e codici temporanei, ma di tecnologie invisibili, robuste e semplici da usare.

di Sandro Sana

DATI GIUSTI, NON DATI IN PIÙ

Non tutto ciò che possiamo raccogliere dobbiamo conservarlo. Anzi: spesso 'più dati" significa più superfici d'attacco, più costi, più attriti legali. È il feticismo della raccolta che ci fa credere che il valore stia nel volume. In realtà il valore nasce dall'intenzionalità: sapere perché un dato esiste, dove vive, chi lo usa, quando muore. Qui sta la differenza tra accumulare e governare.

Se metto una bacinella sotto la goccia, prima o poi straripa. Le aziende fanno lo stesso con lo storage: dischi sempre più capienti, cloud illimitati, archivi 'per sicurezza". Poi, al primo incidente, scoprono che non sanno cosa hanno davvero, né come difenderlo o ricostruirlo. La minimizzazione non è burocrazia: è architettura. Tenere il necessario, con uno scopo chiaro e dichiarato, riduce l'esposizione e aumenta la fiducia. È etica che paga sul conto economico.

L'etica del dato nasce nella progettazione, non a piè di pagina della privacy policy. Significa definire confini d'uso, tempi di vita, proprietà e responsabilità. Ogni dato dovrebbe avere un proprietario, un perimetro e una data di scadenza. Se non sappiamo a chi appartiene e perché lo conserviamo, stiamo trattenendo un rischio, non un asset. La responsabilità non è un cartello sul muro: è una filiera di decisioni verificabili. L'AI ha reso tutto più urgente. Copiare una colonna nel prompt 'solo per provare" è già una fuga di informazioni. I log delle piattaforme, se non segregati, diventano diari inconsapevoli di segreti industriali. Shadow AI, strumenti non approvati, dataset 'riciclati": qui non si tratta di demonizzare la tecnologia, ma di allenarla nel campo giusto. Dati sintetici per ridurre l'esposizione, watermark sugli asset per tracciare gli usi, ambienti controllati con policy enforceable: così l'innovazione resta un'alleata, non una fuga in avanti.

Il ciclo di vita va reso visibile. Nascita del dato, uso, archiviazione, cancellazione: quattro verbi, una catena di scelte. La cancellazione vera è un atto di coraggio manageriale. Liberarsi del superfluo non è perdere memoria, è guadagnare velocità. E quando qualcosa va storto, perché succede, la velocità è sopravvivenza: sapere dove stanno le copie, quanto sono integre, in quanto tempo possiamo rimettere in moto produzione e servizi.

Guardiamo al lato operativo. Il logging 'perché non si sa mai" si trasforma in sorveglianza improduttiva e in costi ingestibili. Meglio poche telecamere che riprendono bene, con lente grandangolare dove serve, piuttosto che mille webcam sgranate. Tradotto: log di qualità, immutabili quando necessario, con catena di provenienza chiara e accessi 'need-to-know". Trasparenza verso le persone: sicurezza sì, ma senza trasformare il posto di lavoro in un panopticon digitale.

C'è poi la questione dei backup. La regola che funziona resta semplice: ridondanza vera, separazione logica e ripristini provati. Il cliente non compra terabyte: compra la certezza che, anche nel peggiore dei giorni, l'azienda regge l'urto e mantiene le promesse. Se il dato è la benzina del business, l'integrità è la cintura di sicurezza. E nessuno corre davvero senza cintura.

La verità è scomoda ma liberante: il valore sta nel rifiuto. Scegliere cosa non raccogliere, cosa non conservare all'infinito, cosa non condividere fuori contesto. È una rinuncia strategica che disinnesca rischi, taglia costi e costruisce fiducia. Fare meno, meglio, con scopi chiari, metriche e responsabilità esplicite. Non serve essere eroi: serve coerenza.

Il futuro appartiene a chi tratterà i dati come persone che bussano alla porta: si accolgono quelli giusti, si salutano con rispetto quando hanno finito lo scopo, si proteggono mentre sono in casa. Tutto il resto è rumore, e il rumore non è conoscenza. La sfida non è 'avere più dati", ma 'avere i dati giusti" e saperli lasciare andare quando è il momento. E sì, anche questo è sicurezza: scegliere la strada più corta verso il valore.

PERCHÉ LA CYBERSECURITY DEVE ESSERE INTEGRATA NELLA GOVERNANCE AZIENDALE

di Giorgio Sbaraglia

Per molti anni, anche nelle organizzazioni più strutturate, la sicurezza informatica era vista come un 'compito dell'IT". Ai vertici aziendali veniva chiesto – unicamente – di approvare un budget. Budget che risultava sempre troppo basso, perché il board non comprendeva appieno i rischi e le necessità, anche per le difficoltà di comunicazione tra IT e board, che parlavano due linguaggi diversi.

Questo approccio è ormai superato perché il contesto è cambiato: il rischio cyber è diventato un rischio d'impresa reale e potenzialmente elevato, con impatti diretti sul business, sulla reputazione, sulla continuità operativa e, infine, sulla responsabilità personale degli amministratori.

Ad incentivare questo 'cambio di paradigma" ha contribuito anche l'evoluzione del quadro normativo. Nel NIST Cybersecurity Framework (CSF), nella versione 2.0 del 2024, è stata aggiunta una sesta function: GOVERN (GV), per evidenziare l'importanza della governance della gestione del rischio di cybersecurity. La function GOVERN è così descritta: 'La strategia, le aspettative e la politica di gestione del rischio di cybersecurity dell'organizzazione sono stabilite, comunicate e monitorate. Le attività di governance sono fondamentali per incorporare la cybersecurity nella più ampia strategia di gestione del rischio aziendale (ERM) di un'organizzazione."

Il Regolamento (UE) 2022/2554 DORA (Digital Operational Resilience Act), rivolto ai settori finanziario e assicurativo, impone che la resilienza digitale venga trattata a livello strategico, e che il board approvi, monitori e riesamini periodicamente le politiche di gestione del rischio ICT.

La Direttiva (UE) 2022/2555, nota come NIS 2, mette in primo piano l'importanza della governance nella gestione della cybersecurity. L'art. 20 della NIS 2 è proprio dedicato alla governance ed al comma 2 recita: 'Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro

dipendenti...". Questa priorità è ribadita anche all'art. 23 del D.Lgs. 138/2024 con cui l'Italia ha recepito la NIS 2.

La cybersecurity deve quindi uscire dagli uffici IT, dove era confinata, per entrare nei consigli d'amministrazione, perché questi devono comprenderne l'importanza e integrarla nella gestione del rischio aziendale e nelle pianificazioni del budget.

In conclusione: una governance aziendale efficace, che integra la cybersecurity nella strategia globale, è essenziale per proteggere i dati aziendali e garantire l'operativa aziendale che un attacco informatico potrebbe compromettere.

L'HACKER E LO SCORPIONE

di Roberta Zavagno

Perché uno scorpione, magari visibilmente innocuo, può destare allarme fino a scatenare addirittura reazioni fobiche, mentre difficilmente ci si scompone, almeno all'inizio, di fronte alla notizia di un attacco informatico pur effettivamente e gravemente dannoso?

Non c'è nulla nell'intelletto che non sia stato prima nei nostri sensi: dalla filosofia greca in poi, pur tra le diverse declinazioni via via sviluppatesi, questo concetto ha sempre accompagnato il pensiero sulla conoscenza. Il dato reale, a sua volta, viene elaborato dalle interconnessioni cerebrali secondo livelli progressivi di complessità: dagli istinti primari, fino alle emozioni ed all'astrazione concettuale. I cinque sensi, quale strumento di conoscenza, sono tra i fattori che hanno reso possibile la riuscita evolutiva dell'Homo sapiens sapiens, che da 35.000 anni popola la Terra. Devono passare però circa 31.000 anni affinché l'oggetto dell'esperienza prima e dell'elaborazione intellettuale dopo — il dato, appunto — possa essere codificato, trasmesso, condiviso tra più spazi e più generazioni mediante la scrittura.

Fino a cinquant'anni fa, i cinque sensi e la capacità di scrivere ci hanno dunque accompagnato nello sviluppo della storia umana. Negli anni '70, però, è intervenuta la rivoluzione di Internet, scardinando — con una velocità mai vista prima — il mondo intellettivo dell'Homo sapiens sapiens. La realtà virtuale, contrapposta a quella reale (fatta di cose percepibili con i sensi), ha fatto il suo prepotente ingresso nella storia: ma, se non c'è nulla nell'intelletto che non sia stato prima nei sensi, come possiamo veramente conoscerla?

Non siamo così diversi dai nostri antenati di migliaia di anni fa. Mezzo secolo è veramente poco per introiettare dinamiche di apprendimento ed elaborazione razionale così diverse rispetto al nostro vissuto, che invece parte dal reale per arrivare al dato. Dunque, ci sarà mai un momento nel quale la notizia di un grave attacco hacker provocherà allarme e reazioni istintive come quelle normalmente destate da un pur innocuo scorpione? Probabilmente no.

Quindi, per difenderci da rischi fino ad ora sconosciuti, ma in grado di distruggere pesantemente molte realtà — cioè per assicurarci un adeguato grado di tranquillità mentre ci avventuriamo nel mare di Internet — è indispensabile affidarsi a una sistematica opera di istruzione e formazione dei cittadini. Solo la coscienza del pericolo può attivare i nostri istinti di difesa.

Cybersecurity: svegliarsi prima che sia troppo tardi

di Guido Tonizzo

Non serve un attacco informatico per capire l'importanza della sicurezza digitale, ma spesso è proprio quello che succede: solo dopo un blocco di sistema, la perdita dei propri dati o una bella richiesta di riscatto in bitcoin, ci si rende conto che sì, forse era il caso di pensarci prima. Storie di questo tipo ce ne sono molte. Eppure, oggi difendersi è possibile. Ed è necessario.

I dati sono il cuore pulsante di qualsiasi azienda: proteggerli significa garantire continuità, reputazione e, in ultima analisi, sopravvivenza. I cybercriminali non stanno a guardare: agiscono in modo sempre più mirato e veloce. Malware, ransomware: le minacce non mancano, e colpiscono con precisione chirurgica dove le difese sono più deboli.

Un viaggio nel tempo: quando tutto sembrava un gioco (e invece era l'inizio dei problemi). Tutto è cominciato con Creeper, un virus del 1971 che si limitava a mostrare un messaggio. Il suo 'antidoto", Reaper, fu il primo rudimentale antivirus. Poi arrivarono i personal computer, i dischetti infetti e il famigerato Elk Cloner. Internet ha fatto il resto: con il Morris Worm (1988) il mondo si accorse che un programma poteva bloccare migliaia di sistemi in poche ore. Negli anni 2000 fu il turno di Slammer e Code Red, che alzavano l'asticella del caos informatico globale. Da lì in poi, nessuno ha più potuto permettersi di ignorare il problema. Oggi il campo di battaglia è digitale, globale e distribuito. Gli attacchi non arrivano più solo da 'solitari in felpa col cappuccio", ma da gruppi organizzati. Gli attacchi possono colpire cloud, dispositivi mobili, IoT, reti ibride. La propria strategia di protezione richiede soluzioni integrate: protezione degli endpoint, sicurezza di rete avanzata, gestione degli accessi, backup e disaster recovery.

Il fattore umano è ancora determinante. E qui arriviamo a un punto delicato: il personale. Per quanto tecnologicamente avanzata sia un'infrastruttura, basta un clic sbagliato per vanificare il tutto. La formazione continua dei dipendenti è la vera ciliegina sulla torta contro gli attacchi. La consapevolezza – anche solo sapere che 'quel link strano" non va aperto – può fare la differenza tra un'email innocua e un potenziale disastro. Investire nella security awareness diventa quindi un'assicurazione a lungo termine. Certo, chi pensa che basti un corso una tantum per stare al sicuro, probabilmente non ha mai ricevuto un phishing ben fatto.

Possiamo quindi concludere che una difesa efficace si basa su una strategia integrata, che comprende anche la formazione del team, e non è solo una reazione a un danno già subito. Affidarsi a chi conosce questo mondo consente di costruire quella resilienza digitale che oggi fa la differenza, dandoti tra l'altro una sensazione di sicurezza che non ha prezzo.

>> Di Roberto Murenec

Le frontiere processuali della comunicazione digitale

La società civile nella quale viviamo è sempre più complessa e pervasa dall'utilizzo delle nuove tecnologie, connotate da un'evoluzione rapidissima e da una grande capacità espansiva. Non a caso, da tempo lo sviluppo e la diffusione di dispositivi, di sistemi informatici o telematici o memorie digitali, per dirla come nella recente rubricazione del DLL 806/2023, rappresentano il simbolo di una vera e propria 'rivoluzione informatica" basata più sull'attenzione al contenuto che al suo contenitore e sfociata in un eccessivo e smodato utilizzo ed impiego della tecnologia in ogni istante del quotidiano con evidenti effetti distorsivi sulla consapevolezza legata al loro uso. Uno dei simboli di questo sviluppo è la capillare diffusione dei dispositivi mobili sempre più performanti, capienti, vero ed autentico status-simbol di chi li possiede o di chi li ha in uso, ma anche eterni 'scrigni" ove sono custoditi una eterogenea pletora di dati, di informazioni e di comunicazioni che oggi costituiscono il 'nuovo petrolio del mondo" e che sono liberamente accessibili dall'utente e istantaneamente trasmessi al destinatario con un 'click" per effetto di una connessione. Sono proprio quei dati e quelle informazioni che circolano in maniera libera e al tempo stesso 'segreta", talvolta criptata, ad essere per l'attività investigativa ed operativa in generale, materiale ad alto potenziale probatorio.

Tralasciando gli aspetti e le criticità legate alla evidente attuale inadeguatezza normativa e procedurale concernente

l'acquisizione e l'analisi del prove digitali racchiuse nella 'obsoleta" L. 48/2008 su cui si fonda la scienza della Digital Forensics, che oggi emergono sempre più con preponderanza tanto nel disegno di legge sopra richiamato e ancora fermo alla Camera dei Deputati quanto nelle più recenti disposizioni contenute nelle circolari dispositive di cui alle Procure della Repubblica di Trento, a cui hanno fatto recentemente seguito nel 2025 quelle di Bari, Torino e non ultima quella di Roma, sintomo di un potere giudiziario che rischia di 'sopperire impropriamente" alle lacune normative esistenti su cui dovrebbe intervenire direttamente il legislatore, non vi è ombra di dubbio che il tempo e la continua ricerca di nuove performance non ha fatto altro che far emergere altre criticità giurisprudenziali ed pratiche correlate allo sviluppo inarrestabile di altra nuova tecnologia, di sistemi operativi sempre più all'avanguardia e cyberprotetti, di nuove release ed applicazioni sempre più sicure, che hanno trovato rispondenza tanto nelle esigenze degli individui quanto nel 'Valore" che assume il concetto di 'comunicazione", prima prettamente verbale e scritta, ed ora anche digitalmente integrata dall'uso delle piattaforme di messaggistica istantanea sotto forma di messaggi, e-mail, audiomessaggi, videomessaggi e immagini. In questo stato di cose, dove l'attenzione in questo caso guarda al particolare, si sviluppa un nuovo modo di comunicare che se sul piano tecnologico è già più che ben avviato, sul piano processual-penalistico quella comunicazione digitale mette in luce, ancora una volta, evidenti lacune e, per quanto i codici non siano mai stati aggiornati ai nuovi mezzi di comunicazione, le norme precedenti vengono interpretate dalla giustizia di legittimità e di merito in modo da consentire l'ingresso, nel processo, di prove 'atipiche" come quelle in commento.

Attualmente, Whatsapp, Telegram, Signal, WeChat, Wickr per citare solo alcune delle applicazioni di messaggistica istantanea, ma ce ne sono anche altre che si difendono bene, ognuna con proprie caratteristiche intrinseche e di sicurezza, se per certi versi rappresentano il cuore pulsante ed attuale di quell'apertura ai nuovi mezzi di comunicazione, che hanno stravolto e travolto completamente ogni sfera della nostra vita ampliando l'accesso alla comunicazione, per altri versi l'utilizzo massiccio di quelle stesse piattaforme ha messo in evidenza quale sia la nuova frontiera del dibattito giuridico sempre più orientato alla qualificazione giuridica da dare a quel messaggio inviato/ricevuto; letto o non letto, attuale/non attuale basandosi sulla dicotomia 'Documento" o 'Corrispondenza" con evidenti riflessi procedurali in tema di sequestro ed acquisizione di quelle prove e di bilanciamento delle esigenze processuali, di garanzia dei diritti fondamentali, di rispetto della privacy e, non ultime, di tutela della sicurezza delle informazioni. Questo perimetro che appare magari chiaro, quantomeno sul piano nozionistico, non lo è altrettanto sotto il profilo processual-operativo, perché richiede ad litteram profili autorizzatori ed adeguatamente motivati da parte dell'A.G. competente (P.M., GIP o giudice terzo super partes) che, se non rispettati, possono creare riflessi sull'utilizzabilità proprio di quei mezzi di prova in giudizio.

E' proprio qui il vero 'vulnus" del dibattito, perché anche nel settore della comunicazione digitale si ripropone quanto già avviene in tema di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali, dove è ancor più evidente la necessità di quell'intervento legislativo auspicato che ponga rimedio ad un settore che attualmente richiede di adeguare le 'vecchie" garanzie costituzionali sempre attuali ai nuovi strumenti della tecnica, garantendo continuità alla protezione dei diritti fondamentali dei cittadini, vera sfida per l'ordinamento giuridico nazionale ed al tempo stesso di dare risposta ad un'esigenza sociale che coinvolge indistintamente tutti noi come cittadini. Stay tuned!

>> **di Sonia Gastaldi**, consigliera Digital Security Festival

AI O NON AI QUESTO È IL PROBLEMA. LA SOCIOLOGIA A SERVIZIO DELLA RIVOLUZIONE "ARTIFICIALE"

La celebre frase di Amleto 'essere o non essere" oggi trova un'affascinante declinazione da applicare all'intelligenza artificiale. Il dilemma esistenziale individuale si estende all'intera struttura sociale contemporanea, andando a toccare i contesti educativi, culturali e socioeconomici. Quella che stiamo vivendo è una vera rivoluzione, che ha origini ben più lontane dalla data di pubblicazione di ChatGpt. È intorno agli anni Cinquanta del '900 che l'A.I. fa la sua comparsa sia in termini tecnici, con il test di Turing, che sociologici con l'acquisizione di legittimità istituzionale, finanziamenti, comunità di ricercatori e aspettative sociali.

L'avvento dell'A.I. sta generando una spaccatura epistemologica nella società, con la ridefinizione delle questioni economiche, di potere e classe sociale. In futuro la differenza tra chi usa/userà l'A.I. e chi non la usa/userà, per svariati motivi, sarà enorme. Perché? Perché la potenza di calcolo, di aggregazione e la velocità di elaborazione dei computer sarà sempre superiore a quella degli esseri umani. Punto. Quindi noi non siamo tra quelli che dicono ti tornare alla clava, ma tra quelli saggi che dicono che va usata bene e con un approccio interdisciplinare.

Sociologia e dimensione sociale. La sociologia è una scienza relativamente giovane se paragonata alle altre scienze. Nata nella prima metà dell'800 in Francia, come 'fisica sociale", è la risposta alle grandi trasformazioni del XIX secolo e alla modernità. Il suo compito primario è indagare l'organizzazione sociale e i comportamenti collettivi, entrando sul come strutture, istituzioni e gruppi si formano nella società. Con l'analisi sociologica vengono svelati i meccanismi sociali che influenzano i comportamenti individuali che, in realtà, sono preventivamente determinati nella società. Detto in breve, la maggior parte delle nostre azioni è influenzata dalle aspettative che gli altri hanno su di noi, dall'adesione alle norme dei nostri gruppi di riferimento e dai ruoli che ricopriamo. Quindi siamo sempre connessi, anche in modo analogico.

La sociologia informatica studia come le tecnologie e gli algoritmi trasformano le relazioni sociali. Lo studio sociologico rispetto all'A.I. affronta l'impatto sui processi di lavoro e sulle identità collettive, analizzando come gli algoritmi incorporino bias sociali e culturali. Mette sotto osservazione la riconfigurazione dello spazio pubblico digitale, dalle echo chambers alla filter bubbles, fino alle nuove forme di sorveglianza sociale. Si concentra sui processi di adattamento culturale alle macchine intelligenti e sui gap generazionali nell'adoption tecnologica. L'obiettivo è comprendere come la rivoluzione artificiale ridefinisca la società, creando nuovi rituali, norme e forme di solidarietà nell'era algoritmica. Perché allora la sociologia può mettersi a servizio della rivoluzione artificiale? La sociologia può e deve mettersi al servizio della rivoluzione artificiale per diversi motivi fondamentali:

1. l'AI non è neutra: ogni algoritmo incorpora bias sociali, culturali e di classe. La sociologia può decodificare questi pregiudizi nascosti e rendere visibili le dinamiche di potere incluse nel codice; 2. prevenire la distopia tecnologica: come ha mostrato Zygmunt Bauman con il concetto di "modernità liquida", l'innovazione senza

controllo sociale può generare alienazione e frammentazione. La sociologia può anticipare le conseguenze sociali negative; 3. democratizzare l'innovazione: la rivoluzione A.I. rischia di essere guidata solo da élite tecniche. La sociologia porta anche la voce dei gruppi marginali e garantisce inclusività nel processo di sviluppo.

Come la sociologia può contribuire concretamente? Sicuramente con il suo strumento principe: la ricerca empirica, fatta di survey, studi etnografici sulle comunità digitali e analisi delle reti sociali, per mappare l'impatto dell'A.I. sulle comunità, riconoscendo resistenze, adattamenti e nuove forme di stratificazione sociale. Con il design sociale degli algoritmi, integrando nei team informatici, sociologi che implementino, fin dalla fase progettuale, principi di giustizia sociale,

equità e responsabilità negli algoritmi. Con l'analisi dei processi di adoption, che studiano come le diverse classi sociali, le generazioni e le culture si approcciano all'A.I., fornendo insights per politiche di inclusione digitale più efficaci. Con la mediazione culturale, che traduce il linguaggio tecnico in termini comprensibili al grande pubblico, facilitando un dibattito democratico informato sui futuri possibili dell'AI, quello che il Digital Security Festival fa da sette anni a questa parte. Ultima, ma non per importanza, la valutazione d'impatto sociale che, misura gli effetti dell'A.I. su coesione sociale, disuguaglianze e benessere collettivo.

Perché è importante farlo? Perché ne vale la vita delle persone in tutti i loro ambiti. Dalla socializzazione, l'AI modifica anche le forme di socializzazione. Gli algoritmi di raccomandazione creano "bolle epistemiche" che frammentano il dibattito pubblico, minando quella che Habermas chiamava "sfera pubblica". Paradossalmente, strumenti pensati per connettere generano isolamento e polarizzazione. Al mercato del lavoro che subirà una trasformazione epocale, con un digital divide che aprirà una importante voragine tra le generazioni e, a livello competitivo, tra le aziende che useranno l'A.I. e chi non la userà.

Dal mondo educativo, dove l'AI sta ridefinendo i processi di apprendimento e trasmissione culturale. Quali potranno essere le conseguenze di compiti in classe eseguiti con l'A.I. senza lo strato fondamentale della formazione? Come dovranno formarsi gli insegnanti per saper riconoscere l'autenticità dello studente in un tema, in un esercizio svolto o in una tesi di laurea? Che impatto avrà la mancanza di conoscenza basilare delle nozioni, di spirito critico e capacità linguistica nei giovani che dovranno costruire il futuro? Alla questione identitaria. Se le macchine possono pensare, cosa definisce l'unicità umana? Questo interrogativo non è meramente filosofico, ma ha implicazioni pratiche su diritti, doveri e cittadinanza nell'era digitale. Il dilemma "A.I. o non A.I." non ammette soluzioni binarie. La sfida sociologica consiste nel costruire un'integrazione consapevole che preservi la componente umana con la sua coscienza, dignità e creatività, senza rinunciare ai benefici tecnologici, ridefinendo il contratto sociale per l'era algoritmica, ricordando sempre che il centro è l'essere umano e la tecnologia è e sarà sempre uno strumento.

DATA BREACH IN HOTEL

>> di Ivano Di Santo e Marco Cozzi

In un albergo storico di una città del Nord, migliaia di copie di documenti d'identità rubate. Un comunicato che parla di hacker entrati 'nonostante la cybersecurity". Marco Cozzi, presidente del Digital Security Festival, la mette giù semplice: 'Ci si concentra sempre su quanto siano bravi gli hacker a entrare. Ma è una rincorsa infinita. La vera domanda è: se entrano, cosa trovano?". Il punto centrale della questione emerge analizzando la normativa: la legge non obbliga gli alberghi a conservare la copia del documento. L'articolo 109 del TULPS stabilisce solo l'obbligo di verificare l'identità e comunicare i dati alla Questura. 'È come controllare il biglietto al cinema. Lo guardi, lo validi, e finisce lì. Non lo fotocopi per archiviarlo 'magari un giorno servirà'", spiega Cozzi.

Nel linguaggio della cybersecurity si chiama minimizzazione dei dati: se una cosa non c'è, non te la possono rubare. Eppure molte aziende e strutture continuano a conservare montagne di informazioni senza un reale motivo, aumentando esponenzialmente la superficie di attacco. 'Le regole non sono imposizioni che costano. Sono cinture di sicurezza", ribadisce Cozzi. 'Difendono l'azienda e proteggono i clienti. Non servono tutti i giorni, ma il giorno in cui servono, ringrazi di averle messe".

Ivano Di Santo, evangelist del Digital Security Festival e docente di Cyber Security, aggiunge: 'La sicurezza non è un prodotto, non si compra su uno scaffale. È un insieme di processi documentati, frutto di incontri con specialisti del settore che ci insegnano come proteggerci". Di Santo offre una riflessione provocatoria: 'Ci sentiamo più 'violati' quando ci rubano lo smartphone che non il portafogli. Perché ormai gran parte di noi è conservata nella rete. Ma chi ci garantisce che l'attenzione con cui custodiamo una parte di noi sia la stessa di chi quei dati li prende, li archivia o li lascia lì, senza gestione, senza un tempo massimo oltre il quale andrebbero distrutti?". Il Digital Security Festival lavora ogni giorno sulla diffusione della consapevolezza digitale con parole semplici e consigli concreti. Quest'anno abbiamo presentato la settima edizione a Roma, nella Sala Matteotti della Camera dei Deputati. 'La consapevolezza è un antivirus che non scade mai", conclude Cozzi.

DI NICOLA BRESSAN

Cybersecurity e Intelligenza Artificiale: sfide e risposte

La trasformazione digitale e l'adozione sempre più pervasiva dell'intelligenza artificiale stanno ridisegnando il panorama della cybersecurity. Se da un lato l'IA è un alleato prezioso nella difesa, dall'altro diventa anche uno strumento sofisticato per chi intende condurre attacchi sempre più complessi. Le aziende italiane si trovano quindi a fronteggiare un doppio livello di sfida: tecnologica e organizzativa.

Attacchi sempre più evoluti e regole più severe

Oggi non si parla più solo di virus informatici. I truffatori usano l'IA per costruire email di phishing realistiche, falsi video e audio (deepfake) o malware in grado di cambiare tattica a seconda delle difese che incontrano.

A questo si aggiunge la necessità di rispettare normative europee sempre più stringenti, come la direttiva NIS2, che obbliga le imprese a segnalare un incidente di sicurezza entro 24 ore e assegna responsabilità dirette al management. La protezione dei dati non è più soltanto un compito tecnico: diventa un tema di governance e di fiducia verso clienti e partner.

Le persone al centro della sicurezza

Anche la tecnologia più avanzata, però, non basta da sola. Spesso gli incidenti nascono da comportamenti poco attenti: password troppo semplici, clic avventati, scarsa conoscenza dei rischi. Per questo la formazione continua dei dipendenti e la diffusione di una cultura della sicurezza sono fattori cruciali. Ogni persona deve sentirsi parte della difesa dell'azienda, perché la sicurezza informatica è un impegno collettivo dove ognuno diventa parte attiva nella difesa dei dati e delle infrastrutture.

L'innovazione al servizio della difesa: Egyda

Per affrontare queste sfide, Var Group, con il suo centro di competenza per la cybersecurity Yarix, ha sviluppato Egyda, una piattaforma che integra intelligenza artificiale e machine learning per potenziare le capacità di rilevamento e risposta alle minacce e rendere più efficiente la gestione della sicurezza.

Egyda porta tre vantaggi principali:

Hyper Automation: riduce il carico di lavoro degli analisti automatizzando le attività ripetitive e integrando dati provenienti da diversi sistemi (SIEM, EDR, NDR). Questo consente di avere un quadro completo delle anomalie in tempo reale, con proposte di azioni correttive già pronte.

YUBA: un motore di analisi comportamentale che monitora gli accessi ai servizi cloud e rileva anomalie potenzialmente legate al furto di credenziali. Non solo segnala comportamenti sospetti, ma spiega anche perché un login possa essere rischioso, facilitando il lavoro degli analisti.

IA predittiva: grazie a modelli addestrati su grandi quantità di dati, Egyda stima la probabilità che un'anomalia sia davvero una minaccia, riducendo i falsi allarmi e permettendo di concentrare le risorse sui casi più critici.

Questi strumenti permettono di passare da una logica reattiva a una proattiva, migliorando i tempi di risposta e garantendo maggiore resilienza.

Intelligenze integrate a vantaggio delle aziende

Uno dei punti di forza di Egyda è la capacità di mettere in dialogo diverse forme di intelligenza: quella artificiale, che elabora enormi quantità di dati in tempo reale; quella algoritmica, che modella scenari complessi; e quella umana, che interpreta il contesto e prende decisioni strategiche.

Questo approccio alle intelligenze integrate permette di sfruttare al meglio le potenzialità di ciascun elemento: la macchina riduce i tempi e gli errori, mentre l'analista arricchisce i dati con esperienza e visione critica. Il risultato è un ecosistema dinamico, dove tecnologia e competenze umane si rafforzano a vicenda, aumentando la resilienza complessiva dell'organizzazione.

La collaborazione del DSF con Radio Studio Nord

www.studionord.news

Noi del Digital Security Festival siamo entusiasti di rinnovare la storica collaborazione con Radio Studio Nord. Abbiamo scelto di collaborare anche quest'anno perché riconosciamo che la radio è un mezzo di comunicazione potente e inclusivo, capace di raggiungere anche coloro che sono meno avvezzi al mondo digitale. Ogni mattina, Radio Studio Nord ha condotto un'intervista con un protagonista del festival. Queste interviste sono state trasmesse in diretta FM e sono anche disponibili in streaming sui social network. L'obiettivo è di rendere i temi della sicurezza digitale accessibili a tutti, spiegando concetti complessi in modo semplice e diretto. Riteniamo che la nostra partnership con Radio Studio Nord sia fondamentale per espandere la portata del nostro festival. La radio ha il potere di arrivare ovunque (anche grazie allo streaming online), portando conoscenza e consapevolezza su temi cruciali come la sicurezza digitale.

La condivisione di molti dei nostri eventi fisici in diretta sui social network ci permetterà inoltre di raggiungere un pubblico ancora più ampio e variegato, proprio grazie al supporto tenico e alla regia dello staff di RSN. Desideriamo che chiunque abbia l'opportunità di apprendere, di farsi un'idea sullo stato attuale della sicurezza digitale e di comprendere l'importanza di proteggere le proprie informazioni online. Siamo convinti che, unendo le forze con Radio Studio Nord, facciamo un passo significativo verso la realizzazione di questo obiettivo, rendendo il Digital Security Festival un evento inclusivo e istruttivo per tutti.

>> Di Massimiliano Brolli

Decadenza digitale: quando il futuro promesso diventa una gabbia per la mente

Per decenni abbiamo celebrato il digitale come la promessa di un futuro più connesso, efficiente e democratico. Ma oggi, guardandoci intorno, sorge una domanda subdola e inquietante: e se fossimo veramente entrati nel periodo della decadenza digitale? Un'epoca in cui la tecnologia, da motore del progresso, si sta trasformando in una pesante zavorra, in disinformazione, dipendenza e soprattutto disumanizzazione — dove il digitale ci promette tutto, ma ci toglie lentamente ciò che ci rende umani. In questo articolo voglio condividere alcuni 'segnali" che da tempo osservo e cerco di contestualizzare. Indizi sottili ma sempre più evidenti, che mostrano come il sogno digitale stia perdendo lucidità, lasciandoci spettatori di una trasformazione che ci riguarda tutti — e che forse stiamo subendo più che guidando.

La sovrabbondanza dei contenuti e la morte del significato

In rete si pubblicano ogni giorno miliardi di contenuti. Ma quanta di questa produzione ha un reale valore? L'informazione si è trasformata in rumore, i testi in clickbait, le immagini in labirinti per l'attenzione. La conoscenza approfondita è stata sacrificata sull'altare della viralità e della velocità. La 'quantità" ha sopraffatto la qualità. In questo scenario, ciò che è vero viene sepolto sotto ciò che è virale, e l'utente medio, bombardato da input, perde la sua capacità critica.

L'IA avrebbe dovuto potenziare le nostre capacità cognitive, liberandoci da compiti ripetitivi. Invece, si sta delineando uno scenario inquietante: testi, immagini, video e perfino emozioni sintetiche prodotti a velocità disumana, rendendo indistinguibile il reale dal simulato. L'autenticità perde valore. La creatività umana è messa in ombra da un flusso inarrestabile di 'prodotto digitale" generato da macchine. Ciò che era raro e prezioso, ora è replicabile, indistinto, con un sapore 'statistico" e privo di anima.

Il collasso delle relazioni e la dipendenza: il nuovo modello di business

I social network, nati per avvicinare le persone, sono diventati luoghi di alienazione, narcisismo e polarizzazione. Il concetto stesso di 'amicizia" è stato svuotato. Le interazioni umane sono filtrate da algoritmi che decidono cosa dobbiamo vedere, pensare, desiderare. Si parla tanto di 'engagement', ma ciò che cresce è la solitudine. E questo noi che ci occupiamo di cybersecurity lo vediamo. Romantic scam, macellazione del maiale. Il digitale ha moltiplicato le connessioni, ma sta irrimediabilmente indebolendo i legami e l'autenticità a tutto tondo. Nel capitalismo digitale, la risorsa più preziosa non è il denaro, ma la nostra attenzione. E per ottenerla, tutto è lecito: notifiche infinite, scorrimento infinito (che sta lobotomizzando i giovani), e tutto questo con premi dopaminergici. Le piattaforme non si limitano più a offrirci servizi: ci osservano, ci influenzano e ci tengono incollati. Un tempo la sorveglianza era il cuore del modello di business di Internet (ci spiegava il grande Bruce Schneier). Oggi sta accadendo qualcosa di più sottile e pervasivo: la dipendenza è diventata il nuovo modello di business. La libertà dell'individuo si dissolve nella compulsione algoritmica. Non siamo più utenti, siamo merce — profilati, sezionati e rivenduti al miglior offerente, mentre crediamo di esercitare scelte libere in un ecosistema pensato per essere manipolati.

Vulnerabilità, dati, privacy e cyberminacce

Ogni nostra azione online lascia molte tracce. Ogni dispositivo è una porta d'ingresso. La digitalizzazione totale ci ha resi vulnerabili come mai prima. Dalla sorveglianza di massa alle fughe di dati personali, dai ransomware che paralizzano ospedali ai deepfake che minano la fiducia pubblica, viviamo immersi in un'epoca di insicurezza digitale sistemica. Il digitale, che avrebbe dovuto renderci più sicuri, ha spalancato invece nuove e imprevedibili frontiere del rischio. La privacy, un tempo pilastro della dignità individuale, è oggi una chimera: promessa a parole, ma purtroppo sistematicamente violata nei fatti. Un'illusione che ci viene venduta mentre veniamo osservati, profilati e monetizzati.

C'è un senso di stanchezza nell'aria?

I nuovi dispositivi, le app, gli aggiornamenti sembrano più routine di consumo per far girare quella grossa ruota del consumo, che rivoluzioni culturali. iPhone 17? Ma cosa ha davvero di così rivoluzionario rispetto all'iPhone 12? Le grandi aziende non innovano più per cambiare il mondo,

ma per consolidare il loro dominio sul mondo. Il mercato si concentra, l'energia creativa si spegne. Le startup, un tempo laboratorio del futuro con pochissime e illuminate persone, oggi inseguono l'effimero: rendere il cibo più veloce, il dating più superficiale, le notifiche più invasive. L'innovazione ha smarrito la bussola. E noi, forse, la capacità di distinguere il progresso dalla sua caricatura.

I nuovi Dei: Conglomerati, Potere e la Fine della Casa Comune

Nel nostro tempo, i grandi conglomerati globali non sono più semplicemente aziende. Sono potenze sovranazionali, colossi economici che muovono capitali superiori al prodotto interno lordo di intere nazioni. Hanno sedi nei grattacieli, ma radici profondissime nella terra fertile della politica. Nessun vertice internazionale, nessuna agenda globale può prescindere dalla loro influenza e interferenza. Hanno ridefinito le regole, trasformando la democrazia in un esercizio di relazioni pubbliche e la sovranità in una formalità amministrativa. Nutrendosi di dati, risorse e consenso, questi nuovi Leviatani tecnologici hanno creato un ecosistema dove il business è il valore supremo, una nuova etica mercantile che soppianta quella umana. L'uomo non è più 'cittadino del mondo', ma utente; non più soggetto di diritto, ma 'oggetto di profilazione'. E mentre ci illudiamo di essere connessi, loro costruiscono cattedrali di silicio e labirinti algoritmici per le nostre menti sfruttando una quantità di energia senza precedenti. L'intelligenza artificiale, con tutta la sua promessa di progresso, è anche figlia di un'incontrollabile fame energetica. E questa fame ha risvegliato appetiti antichi: complessi nucleari privati stanno sorgendo come nuove centrali del potere. La visione di un mondo più pulito, racchiusa nei sogni dell'Agenda 2030, si dissolve nel calore radioattivo dei reattori per alimentare l'apprendimento dei modelli di intelligenza artificiale. E questa è una corsa che brucia silenziosamente i principi ecologici e i valori umani. La Terra non è più percepita come una madre, ma come una cava. E come ogni figlio ingrato, l'uomo continua a violarla, a saccheggiarla, a ignorarne i limiti. Non c'è rispetto per la casa in cui viviamo, e ancor meno per noi stessi e per i nostri figli. Ci siamo convinti che il valore si misuri solo con il capitale, margini di profitto e crescita perpetua. Abbiamo scambiato l'espansione continua per un segno di salute, dimenticando che in natura ciò che cresce senza equilibrio, senza limiti, distruggendo ciò che lo circonda e alla fine se stesso... si chiama tumore.

Conclusione: è davvero decadenza?

Non possiamo sapere con certezza se siamo all'inizio del tramonto digitale o in una sua fase di trasformazione. La decadenza digitale non è solo tecnologica: è antropologica. È il lento declino della nostra capacità di distinguere il reale dal simulato, il vero dal verosimile, l'umano dall'algoritmico. È la progressiva erosione del pensiero critico, dell'intimità e della riflessione, a favore della velocità, della reazione e della superficialità. È vero, ogni epoca ha avuto i suoi momenti di eccesso, di crisi e di forte riflessione. Ma ciò che è chiaro è che il paradigma attuale non è sostenibile. Abbiamo bisogno di una nuova visione: un digitale che non consumi, ma che costruisca; che non manipoli, ma che emancipi; che non produca soltanto profitto, ma anche buon senso. La decadenza, in fondo, non è necessariamente la fine. È spesso un invito al cambiamento. Un segnale che qualcosa deve per forza evolversi. Sta a noi decidere se assistere al collasso o essere protagonisti di un 'rinascimento digitale".

Cybersec

>>Il giorno in cui perdi il dato capisci quanto vale

di Simone Furlan

Alle 8:17 di un lunedì qualsiasi la produzione si ferma. Non escono più le etichette, il magazzino non scarica, l'ERP non parla con il MES. "È giù il server?". No: è peggio. Non sappiamo se i dati sono integri. A quel punto non produci, non fatturi, non spedisci. Ti accorgi che il dato non è un file: è infrastruttura critica. E quando la perdi, il costo lo leggi in minuti di fermo e in fiducia che evapora. Il ransomware colpisce dove fa più male: disponibilità e integrità. La confidenzialità è il titolo dei giornali, ma nelle fabbriche la lama taglia altrove: se non posso fidarmi dei lotti, dei parametri di processo, delle anagrafiche, non posso lavorare in sicurezza. Fermarsi diventa l'unica scelta razionale. Qui entra in gioco la business continuity: non una cartellina in share.

Le domande diventano: quanto tempo possiamo stare fermi? Quanti dati possiamo perdere senza far danni irreversibili? Se la risposta non è misurata, è un'opinione. E con le opinioni non si riparte. La verità operativa è semplice e scomoda: il backup non serve a niente se non ripristina. E non si ripristina se non è segregato, immutabile quando serve e testato a freddo e a caldo. La regola pratica funziona ancora: copie multiple, piattaforme diverse, una offline/air-gapped, verifica zero errori nei test. Ma non basta la tecnica: serve teatro di crisi, con prove periodiche e ruoli chiari. Chi decide il passaggio a DR? Chi parla con fornitori e clienti? Chi ferma la produzione e con quali criteri? Se la squadra lo scopre il giorno dell'incidente, hai già perso metà partita.

Senza un piano di gestione degli incidenti, qualunque ripristino è un salto nel buio. Per i sistemi industriali significa sapere quale ricetta era in uso alle 8:16, quale versione di PLC/SCADA è "golden", dove sono le configurazioni firmate e chi può rimetterle in campo. Per l'IT significa poter ricomporre identity, directory, chiavi e segreti senza trascinarsi dentro l'infezione. È il motivo per cui segmentazione, privilegio minimo e break-glass account offline non sono orpelli ma meccanica di sopravvivenza.

C'è poi una responsabilità che non si compra con un device: quella etica verso clienti e fornitori. Quando perdi il dato non perdi solo tempo; metti a rischio decisioni altrui fondate su quel dato. Una spedizione sbagliata, un lotto non conforme, un ciclo di lavorazione falsato: il danno si moltiplica lungo la filiera. La continuità non è egoismo d'impresa, è diligenza. Comunicare presto e con trasparenza, spiegare cosa è integro e cosa no, quali servizi tornano e quando, è parte della cura. Nasconderlo non riduce l'impatto: lo ritarda e lo amplifica.

"Paghiamo e riparte tutto." È la più pericolosa delle illusioni, perché non compra integrità, non cancella doppia o tripla estorsione, non garantisce che l'attaccante non sia ancora dentro. E in molti casi apre un fronte legale che peggiora il quadro. L'unica assicurazione è prepararsi prima: asset critici mappati, priorità di ripristino decise dal business, SLA interni realistici. Tutto il resto è fortuna. E la fortuna non è una strategia.

Da CISO la lezione è una: il valore del dato si misura nel tempo di ritorno alla normalità, non nel terabyte al listino. Un piano che sta in piedi ha pochi ingredienti ma non trattabili: governance del dato (proprietari, confini, retention); telemetria affidabile (log utili, immutabili dove serve, accessi tracciati); backup & DR (segregazione reale, test periodici, scenari totali e parziali); identità e chiavi (pronte a rinascere senza portare dentro l'attacco); esercitazioni (tecniche e manageriali, con comunicazione verso l'esterno).

Il giorno in cui perdi il dato capisci quanto vale, ma è tardi per negoziare. La scelta intelligente è decidere oggi quanto vale ripartire in 4 ore invece che in 4 giorni, e pagare il costo prima, in preparazione, disciplina e prove. Perché alla fine, la differenza tra incidente e catastrofe non la fa l'attaccante: la fa la nostra capacità di ripristinare con certezza ciò che conta, alla velocità che il business si è impegnato a garantire. Tutto il resto è rumore.

SOLI TRA I DATI: SICUREZZA, SORVEGLIANZA E NUOVE FORME DI SOLITUDINE DIGITALE

di Alessandro Franchi

Viviamo in un'epoca in cui tutte le nostre interazioni, che riguardino i nostri spostamenti, le nostre transazioni, le nostre emozioni espresse online, vengono catturate, processate e trasformate in dati. Un flusso continuo e invisibile che nutre algoritmi, modella decisioni, plasma e influenza intere esperienze sociali. Più il nostro mondo si popola di connessioni digitali, più emergono forme inedite di disconnessione umana. Nel nostro libro 'Solitudine digitale", abbiamo esplorato questo paradosso dell'essere iperconnessi ma radicalmente soli. La sicurezza informatica, in questo scenario, non può limitarsi ad apparati e crittografia. Deve diventare una pratica culturale, antropologica e persino filosofica, che protegga non solo l'integrità dei sistemi, ma anche quella del sé.

La sorveglianza pervasiva, la raccolta sistemica dei dati personali e l'utilizzo predittivo da parte di intelligenze artificiali comportano rischi che vanno oltre la cybersecurity tradizionale. Parliamo infatti di erosione della privacy cognitiva, di profilazione invisibile, di bias algoritmico: tutte cose che impattano direttamente sulla libertà individuale e sulle relazioni. Nel tempo, il dato è passato da supporto decisionale a struttura ontologica del reale: ciò che non è registrato sembra non esistere. Ma se tutto è quantificabile, cosa resta dell'esperienza umana? Della spontaneità, del dubbio, del silenzio?

Le coordinate che il Festival propone – conoscenza, consapevolezza, intelligenza, resilienza, innovazione, coscienza, collaborazione – sono ben più che concetti: sono bussole etiche. In un cosmo digitale sempre più automatizzato, la vera sicurezza consiste nel mantenere uno spazio per l'imprevedibile umano, per la fragilità o per il non programmato. Nel nostro universo dato, la questione non è più solo 'chi possiede i dati?", ma 'quale idea di essere umano quei dati stanno modellando?"

Difendere la sicurezza digitale significa oggi anche preservare la possibilità di restare umani. Significa tutelare non solo i sistemi, ma anche la complessità dell'esperienza interiore. Significa proteggere la memoria, l'identità, la possibilità di scegliere chi essere e cosa dimenticare. Significa creare spazi digitali in cui l'empatia, la lentezza e il dubbio non siano errori di sistema, ma segni vitali. Perché solo così potremo davvero abitare il futuro, non come prodotti del dato, ma come soggetti di senso.

Vision

Alessandro Curioni

QUANTUM COMPUTING: LA COMPUTAZIONE INCERTA E LA FAME DI FUTURO

Viviamo nell'epoca della bulimia tecnologica: ogni innovazione viene immediatamente divorata dal mercato, dalla politica e dalla retorica del progresso. Il quantum computing non fa eccezione: trasformato in simbolo salvifico, diventa l'ultimo totem di una narrazione entusiasta e acritica.

Ma non si tratta solo di una nuova macchina più potente: il computer quantistico mette in discussione l'intero paradigma computazionale. I suoi qubit non scelgono tra 0 e 1, ma vivono nella sovrapposizione: sono 0 e 1. È una logica probabilistica, non più deterministica. Un calcolo che accetta l'incertezza invece di eliminarla.

Questa incertezza non è un difetto, è la sua natura. Dove il computer classico cercava chiarezza e replicabilità, quello quantistico introduce ambiguità e collasso. È una macchina che sbaglia spesso, ma che promette ciò che oggi appare incalcolabile. Come fidarsi di una tecnologia che incorpora nel suo stesso funzionamento il principio di indeterminazione?

Il mercato non si fa domande: ha bisogno di nuovi orizzonti. E così, il quantum computing diventa utopia performativa. Risolverà problemi complessi, decifrerà codici inaccessibili, ridisegnerà la sicurezza globale. Ma ogni frontiera di potenza è anche un territorio di vulnerabilità. E la promessa diventa minaccia: ciò che oggi protegge i nostri dati, domani sarà superato.

Questa nuova computazione ci impone di ripensare cosa sia il calcolo, il dato, la verità. Non basta più il controllo razionale. Serve pensiero critico. Serve filosofia, non come postilla ma come strumento per interrogare il senso dell'innovazione. Perché la vera domanda non è se la tecnologia funzionerà, ma quale idea di umanità la guida.

Affidare al quantum computing la gestione del mondo, senza comprenderne la natura, è il segno di una cieca fiducia: la tecnica non è più mezzo, è diventata fine. Non sappiamo immaginare futuri che non siano pura accelerazione.

E così, come in ogni mito prometeico, abbiamo rubato il fuoco ma ignoriamo come usarlo bene. Abbiamo costruito macchine che calcolano l'incalcolabile, ma non ci siamo educati al pensiero.

Il quantum computing non va esaltato né temuto, ma sottratto all'hype e riportato a una dimensione critica. Anche solo per ricordarci che forse otto miliardi di soggetti quantistici – che ragionano rapidamente e sbagliano spesso – sono già abbastanza.

OLIMPIADI ITALIANE DI INFORMATICA

di Luigi Laura

In questi giorni, parallelamente al Security Digital Festival, a Udine si svolgono diversi eventi importanti per l'informatica a livello nazionale e internazionale: il congresso AICA, la finale delle Olimpiadi Italiane di Informatica e la 32ma edizione delle Olimpiadi Balcaniche di Informatica, una competizione internazionale che vedrà sfidarsi le rappresentative di 17 nazioni, tra cui l'Italia.

Nel 1989 nascono a Pravetz, in Bulgaria, le Olimpiadi Internazionali di Informatica (International Olympiads in Informatics – IOI), una competizione di programmazione per ragazzi delle scuole superiori di tutto il mondo. L'Italia ha partecipato alle IOI in maniera sperimentale dal 2000, e solo dal 2001 ha organizzato una competizione nazionale, mediante una collaborazione tra AICA e l'allora MIUR (oggi MIM) formalizzata mediante un protocollo d'intesa, finalizzata alla selezione dei partecipanti destinati a rappresentare l'Italia alle IOI. Dal 2003 la competizione ha preso il nome di Olimpiadi Italiane di Informatica.

Le Olimpiadi Italiane di Informatica, praticamente fin dalla prima edizione del 2001, si sono organizzate in tre fasi distinte: 1) fase scolastica, in cui gli studenti gareggiano nelle proprie scuole e devono risolvere quesiti con carta e penna, in cui le domande sono quesiti a scelta multipla oppure quesiti a domanda aperta numerica, ovvero quesiti in cui la risposta è un numero. La fase scolastica di questa edizione si è svolta il 12 dicembre dello scorso anno, e ha visto la partecipazione di 13.845 ragazzi; 2) fase territoriale, in cui gli studenti gareggiano in una cinquantina di sedi dislocate su tutto il territorio nazionale; la prova è al computer e bisogna risolvere 3 o 4 problemi senza tenere conto eccessivamente dell'e icienza computazionale. La fase territoriale di quest'anno, svoltasi il 16 aprile, ha visto la partecipazione di 961 studenti; 3) finale nazionale, che si svolge in tre giorni in una sede diversa ogni anno; come per la fase precedente la prova è al computer, bisogna risolvere 3 o 4 problemi ma stavolta viene premiata anche l'e icienza computazionale. Quest'anno, come detto, la finale è a Udine, dal 23 al 25 settembre.

Dai vincitori delle Olimpiadi Italiane di Informatica vengono poi selezionate le squadre che rappresenteranno l'Italia a diverse competizioni internazionali, tra cui le IOI (nel 2026 a Tashkent, in Uzbekistan) e le BOI (le Balkan, la cui edizione 2025 è in programma a Udine subito dopo l'Olimpiade nazionale, dal 25 settembre al 1 ottobre).

DI MARCO COZZI

GOVERNARE L'INNOVAZIONE IN BANCA: SCEGLIERE PRIMA DI AGGIUNGERE

In banca, l'innovazione non è la somma di strumenti. È la capacità di scegliere che cosa serve, che cosa togliere e che cosa presidiare. Prima della tecnologia viene la consapevolezza: la bussola che propongo, la stessa che attraversa il Digital Security Festival, ha tre parole semplici e operative: senso, semplicità, sicurezza.

Perché "scegliere" è il primo atto tecnologico. Ogni nuova piattaforma, framework o modello introduce potere e debito: potere di fare di più, debito di governare complessità e rischio. Senza un criterio, l'innovazione diventa arredamento tecnologico; con un criterio, diventa vantaggio competitivo. La triade senso – semplicità – sicurezza diventa così filtro delle iniziative e metronomo dei tempi del cambiamento.

Tre scelte che accelerano senza perdere controllo. 1) AI con guardrail, la lente non il pilota automatico: l'intelligenza artificiale amplifica il giudizio umano, soprattutto dove esiste attrito ripetitivo (risk, compliance, sviluppo, service desk). Qui i copiloti suggeriscono, spiegano, documentano. Funzionano solo se i dati sono curati e versionati; prompt e output tracciabili; i casi critici revisionati da umani; le metriche valutano utilità (es. risposta utile al primo colpo, escalation, tempo medio). Al service desk, ad esempio, un copilota attinge a knowledge base e ticket risolti per fornire risposte coerenti, accorciando tempi e passaggi. Non è magia: è manutenzione del senso. 2) Architetture che respirano: per cambiare senza rompere serve modularità, API-first, gestione event-driven. I dati diventano data product con significato condiviso. Il cloud ibrido funziona solo se progettato con exit strategy. In pratica, un nuovo servizio riusa API esistenti e aggiunge solo ciò che serve: i cicli di sviluppo si accorciano da mesi a settimane. Le discussioni tecniche si semplificano perché il linguaggio dei dati è condiviso. 3) Sicurezza by design, DORA-ready: la sicurezza è condizione di velocità, non un freno. Si costruisce con approccio zero-trust, identità forti, controlli lungo tutta la supply chain (compresi i modelli di IA). Le esercitazioni periodiche (tabletop, red team) trasformano l'ipotesi in abitudine organizzativa. Quando la sicurezza è nel design, i "no" inutili spariscono e i "sì" diventano rapidi.

Attenzione a tre trappole comuni, anche quando piacciono. 1) POCite: prove di concetto senza problema reale e senza metriche. Belle da mostrare, inutili da scalare. 2) Monoliti e complessità ornamentale: tecnologie che complicano i processi e rallentano il cambiamento. 3)

Blockchain ovunque: utile dove serve un registro condiviso e un audit multi-attore, superflua altrove. Il principio guida è semplice: prima togliere peso, poi aggiungere vela.

Open innovation: dal varco aperto al respiro condiviso. Aprire non significa esporsi, ma appartenere. L'open innovation funziona quando banca ed ecosistema respirano insieme, su tre piani. 1) Dare per ricevere. Si condivide il problema vero e un terreno sicuro su cui lavorare. Devono esistere sandbox ben progettate, dati sintetici quando il reale non è esponibile, API aperte dove ha senso. Se ciò che si condivide è chiaro, ciò che torna in valore è concreto. Esempio: una challenge antifrode su dati sintetici consente alle startup di proporre modelli senza rischi per il dato reale. 2) Procurement che abilita. Se il contratto è un labirinto, l'innovazione si blocca. Servono piloti pagati e time-boxati (otto settimane), criteri di sicurezza espliciti, governance leggera ma decisa. Un percorso chiaro: discovery → pilota → scale, con stop/go trasparenti. DORA, NIS2 e vendor risk management non rallentano: sono i binari su cui corre il treno. 3) Fiducia come infrastruttura. La fiducia non è un sentimento: è un'infrastruttura condivisa. Threat-intel tra partner, contributi open source su controlli comuni (ad esempio i safeguarding contro prompt injection), red teaming congiunto. Una libreria aperta e curata di controlli AI migliora la qualità a ogni commit.

Le metriche che contano (e tengono i piedi per terra): time-to-learning (giorni dall'idea alla prima lezione utile), time-to-onboard (in settimane, non trimestri), percentuale di progetti pilota che arrivano in produzione entro sei mesi, near-miss e rischi mitigati prima del go-live, documentati. Sono misure semplici, ma orientano i comportamenti meglio di qualsiasi slide.

Dall'ego-sistema all'eco-sistema. L'AI e la blockchain sono strumenti. A fare la differenza sono la qualità delle decisioni e la cultura della sicurezza che le rende scalabili. Governare l'innovazione significa tenere insieme senso, semplicità e sicurezza: togliere il superfluo, progettare ciò che resta, proteggere ciò che conta. È la stessa traiettoria che promuoviamo anche al Digital Security Festival: consapevolezza diffusa, fiducia digitale, resilienza come bene comune. Quando l'ecosistema respira insieme, l'innovazione corre. E lo fa in sicurezza.

La Sicurezza Digitale Spiegata Semplice

I tre punti del DSF

01

Divulgazione della cultura digitale e della sicurezza applicata ad aziende, scuole, istituzioni, ragazzi e genitori.

02

Verranno creati eventi online e offline per tutte le età, per coprire tutta la gamma di fruitori del web e del mondo digital in genere.

03

Onlife è quanto accade e si fa mentre la vita scorre, restando collegati a dispositivi interattivi (on + life) [Treccani].

ISACA®

Venice Chapter

Cybersecurity in Italia: dalle minacce diffuse alle buone pratiche di risposta

di Stefano Gabaglio

La cybersecurity è oggi una priorità per il sistema produttivo italiano. Il Rapporto Clusit 2025 rileva che nel 2024 gli attacchi informatici sono aumentati del 15 % rispetto all'anno precedente, con l'Italia coinvolta in circa il 10 % degli incidenti gravi a livello globale (Clusit). Parallelamente, il CRIF Cyber Observatory segnala un incremento del 15,4 % dei dati italiani esposti sul dark web, collocando il nostro paese al 5° posto mondiale per email compromesse e al 18° per dati di carte di credito rubati (CRIF).

Questi numeri trovano conferma in episodi concreti. Nel 2024, Synlab Italia, gruppo leader nella diagnostica sanitaria, ha dovuto sospendere laboratori e prenotazioni dopo un attacco informatico, con conseguente impatto diretto su migliaia di pazienti e clienti (Security Affairs). A dicembre dello stesso anno, un data breach legato a un fornitore esterno di InfoCert ha spinto il Garante a un'indagine formale (Digital Policy Alert). Nell'estate 2025, circa 100.000 documenti d'identità di ospiti di hotel italiani sono stati diffusi sul dark web, esponendo migliaia di persone a rischi di frodi identity theft (TechRadar, AGID). In un contesto particolarmente vicino alle PMI del Triveneto, nel febbraio 2025 una grande azienda veneta del settore arredo è stata vittima di un attacco ransomware che ha bloccato la produzione per oltre una settimana e portato 350 dipendenti in cassa integrazione; l'attacco ha compromesso circa il 15 % dell'infrastruttura IT, e l'azienda ha prontamente denunciato la situazione alla Polizia Postale (CyberSecItalia, Il Post, Infosec.news).

Questi episodi confermano che la sicurezza non può rigenerarsi da difese improvvisate o reattive. Occorrono partner specializzati, processi strutturati e una cultura aziendale condivisa per integrare la cybersecurity nella governance complessiva di ogni realtà produttiva.

Per le aziende italiane rafforzare la postura di sicurezza significa attivare tre pilastri fondamentali: monitoraggio continuo di reti e sistemi, per individuare anomalie in tempo reale; procedure di risposta strutturate, con interventi rapidi per limitare danni; formazione diffusa, poiché l'errore umano rimane una delle cause principali di data breach. Accanto a questi elementi, cresce l'importanza della compliance normativa: dal GDPR alla direttiva NIS2, fino agli standard ISO 27001, che richiedono trasparenza, tracciabilità e capacità di audit. La recente Determina ACN del 14 aprile 2025 ha introdotto l'obbligo di responsabilità diretta per i vertici aziendali sulla sicurezza informatica, sancendo la dimensione giuridica e strategica della cybersecurity (Cybersecurity360, Aegister).

In questo scenario, IS Copy ha deciso di investire in un Security Operations Center (SOC) interno, cofinanziato dall'Unione Europea (IS Copy). Certificata ISO 27001 e soggetta a NIS2, l'azienda ha scelto un modello proattivo che integra tecnologia, processi e cultura aziendale, dotandosi di un presidio permanente in grado di monitorare 24/7 reti e sistemi con tecnologie SIEM e IDS; analizzare eventi riducendo i falsi positivi; rispondere tempestivamente agli incidenti; sviluppare threat intelligence, gestire vulnerabilità e promuovere formazione continua.

Il go-live sui sistemi critici è previsto per il 2026, seguito da una fase di miglioramento continuo. In questo modo, IS Copy trasforma la sicurezza da costo a leva strategica di fiducia, continuità operativa e competitività, garantendo non solo protezione dei dati, ma anche resilienza e valore duraturo per clienti e partner.

LA SICUREZZA COME VANTAGGIO COMPETITIVO NELLA GESTIONE DEI DBMS

di Cristiano Gasparotto

ARPANET viene attivato nel 1969. Nel 1983 arriva il protocollo TCP/IP, ma occorrono più di 10 anni prima che internet si diffonda tra il pubblico e, nel 1995, arrivino MSN e Amazon. Nel 2016 vengono introdotti assistenti virtuali come Alexa e Siri. Nel 2021 gli utenti di Internet sono oltre 5,3 miliardi. Nel 2022 OpenAI presenta ChatGPT e oggi l'AI è utilizzata in 78 milioni di aziende nel mondo.

La tecnologia dell'informazione avanza sempre più veloce, un'accelerazione che offre molte opportunità ma rappresenta anche una fonte di rischio per le aziende. In questo contesto, la gestione sicura dei dati non è solo una necessità ma anche un importante vantaggio competitivo: mantenere i dati sicuri, integri e disponibili è cruciale per garantire la continuità operativa, ridurre i costi e proteggersi da furti o perdite involontarie.

La sicurezza dei database ricopre un ruolo critico nella protezione dei dati dalle minacce interne ed esterne: l'implementazione di solide pratiche per la corretta gestione della sicurezza è infatti essenziale per proteggere dati di qualsiasi grado di sensibilità. Le conseguenze di una violazione della sicurezza dei database possono essere gravi, durature e costose. Secondo il report Data Loss Landscape, l'85% delle organizzazioni ha subito almeno una perdita di dati nell'ultimo anno. Di queste, più dell'80% hanno segnalato di aver subito conseguenze negative come interruzione del business con perdita di profitto, danni alla reputazione e addebito di sanzioni.

Un DBA (Database Administrator), tra le altre cose, si occupa di molti aspetti importanti dal punto di vista della sicurezza: hardening dell'infrastruttura, audit e monitoraggio continuo, risposta rapida agli incidenti, verifica della compliance e adattamento continuo della configurazione. Queste attività non solo riducono il rischio di violazioni, ma contribuiscono anche alla conformità normativa (GDPR, NIS2, DORA, ...), alla continuità operativa e alla resilienza dell'infrastruttura.

Per offrire una gestione completa, sicura e performante degli ambienti IT, abbiamo tradotto in servizi e raccolto all'interno del concetto di DBOC (Database Operations Center) una gamma di soluzioni integrate con NOC e SOC e pensate per massimizzare la governance, l'efficienza e la sicurezza dei database.

VARGROUP

Trading Manager e Cybersecurity: la nuova frontiera per le aziende italiane

Nei prossimi anni le imprese italiane saranno chiamate ad affrontare una nuova sfida che si aggiunge a quella già impegnativa della conquista dei nuovi mercati e della messa in campo di dinamiche economiche innovative: la sicurezza informatica. La sicurezza informatica è la conseguenza diretta della digitalizzazione dei processi e dell'uso crescente dell'e-commerce con le relative implicazioni connesse alla gestione dei dati sensibili, che in campo economico non rappresentano solo una vulnerabilità tecnica, ma anche un profilo strategico. Ed è proprio questo nuovo scenario che ha fatto emergere la necessità di una nuova figura professionale che riassume in sé competenze non solo commerciali ma anche digitali.

Questa nuova figura è quella del Trading Manager con specializzazione in cybersecurity, un nuovo professionista che unisce in sé competenze di gestione commerciale e di sicurezza digitale. Ha competenze fondamentali nell'analisi dei mercati, nelle strategie di vendita, nella gestione di piattaforme e-commerce, ma anche nella protezione dei dati, nella sicurezza delle transazioni e nella prevenzione degli attacchi informatici. È un soggetto dotato di spiccate capacità relazionali e multidisciplinari. Ecco perché le attuali metodiche in atto ora paiono appartenere all'era giurassica, ed ecco perché questo professionista non si limita più a monitorare i mercati, a scegliere i partner o a ottimizzare i processi di acquisto e vendita, ma mette in campo tutte le sue qualità professionali trasformando una potenziale crisi economica aziendale in una grande opportunità. È capace di evitare il boomerang di azioni non basate sulle politiche di difesa informatica e di rispetto della privacy.

Il quadro normativo europeo ha contribuito a rendere necessaria questa figura professionale. Il GDPR, in vigore dal 2018, non lascia spazio a interpretazioni: i dati personali vanno considerati come un 'diritto dell'uomo" da proteggere in base ai principi di liceità, trasparenza e sicurezza. Al GDPR si è aggiunta la Direttiva NIS2, che ha imposto obblighi stringenti in

materia di cybersecurity, distinguendo tra imprese 'importanti" e 'essenziali". Per il settore finanziario, inoltre, è entrato in vigore il Regolamento DORA, che stabilisce regole uniformi sulla resilienza digitale delle istituzioni e delle infrastrutture.

Ma ovviamente la normativa non è solo un insieme di principi astratti: occorre tenere presente che il Garante per la protezione dei dati personali ha dimostrato in più occasioni di essere pronto a sanzionare chi non rispetta gli obblighi di formazione e sicurezza. Un caso emblematico è quello dell'ottobre 2023, quando un'azienda italiana con circa 160 dipendenti si è rifiutata di consegnare a un suo ex lavoratore gli attestati relativi alla sua formazione professionale. In tale occasione, per il Garante il dipendente aveva legittimamente esercitato il suo diritto di accesso. Nonostante l'opposizione dell'azienda, che aveva cancellato i dati in base a un regolamento interno, il Garante l'ha sanzionata, evidenziando come la mancata consegna costituisse una violazione dei diritti fondamentali della persona.

Questo episodio, apparentemente marginale, ha una valenza enorme, poiché la normativa europea stabilisce che la formazione del personale è un pilastro per la sicurezza dei dati. Eppure molti imprenditori continuano a considerarla solo come un costo accessorio, non come un investimento strategico necessario. Proprio quest'ultimo profilo è quello di competenza del Trading Manager, che deve sapersi muovere tra le norme europee, conoscere le best practices di cybersecurity e valutare se una piattaforma di trading rispetta i requisiti di sicurezza previsti dal regolamento eIDAS, che disciplina le firme digitali e i servizi fiduciari.

Le aziende italiane, soprattutto le PMI, rischiano di pagare caro il ritardo culturale in materia di sicurezza digitale. Come evidenziato nel rapporto del 2024, gli attacchi informatici sono aumentati del 25% rispetto al 2023 e i bersagli principali, preferiti dagli hacker, sono state proprio le realtà di piccole e medie dimensioni. Ecco perché diventa necessaria la figura del Trading Manager, per proteggersi non solo dagli attacchi informatici, ma anche per accedere a nuove opportunità di mercato. I partner internazionali, infatti, pretendono certificazioni sulla sicurezza informatica prima di avviare rapporti commerciali. In quest'ottica, il Trading Manager diventa il garante interno che unisce l'analisi economica alla conoscenza delle minacce informatiche, trasformando la sicurezza da costo a investimento.

Il futuro delle imprese italiane si gioca proprio su questa capacità di integrare commercio e cyber-resilienza. Non si tratta solo di rispettare la legge, ma di salvaguardare la reputazione, mantenere la continuità operativa e conquistare la fiducia di clienti e partner. Le aziende che comprenderanno questa necessità per prime saranno le più forti, le più credibili e le più competitive. Per tutte le altre, il rischio è quello di trovarsi impreparate in un mercato globale in cui il dato è la risorsa più preziosa e la sua protezione è la condizione minima per poter fare impresa.

Occorre infine tenere presente che l'Unione Europea ha attivato programmi mirati sulla specifica questione, come i fondi Secure per le PMI italiane, legati al Cyber Resilience Act, o i bandi Horizon Europe dedicati allo sviluppo di nuove tecnologie di protezione digitale. Sul fronte nazionale, il competence center Cyber 4.0 è stato rifinanziato con oltre 5 milioni di euro, mentre iniziative regionali come il bando Cyber Ready finanziano fino all'80% i servizi per l'adeguamento normativo. A questi si aggiunge il Piano Transizione 5.0, che attraverso i crediti d'imposta sostiene l'acquisto di software, hardware e servizi legati alla cybersecurity. Si tratta di occasioni preziose che permettono alle aziende di affrontare la trasformazione digitale non solo con visione e competenze, ma anche con strumenti concreti.

19 Settembre 2025*
ROMA
Camera dei Deputati
Cerimonia di inaugurazione

19 Settembre 2025*
ROMA
Circolo Canottieri Roma
Pranzo di Gala

24 Settembre 2025*
UDINE
Castello di Udine
Cena di Gala

26 Settembre 2025
UDINE
Confindustria Udine
Dal rischio alla responsabilità, con AICA

14 Ottobre 2025
MONTEBELLUNA (TV)
Infinite Area
Algoritmi e disinformazione

20 Ottobre 2025
TRIESTE
Palazzo della Regione
Codice aperto e sovranità digitale

30 Ottobre 2025
TREVISO
Confindustria Veneto Est
The adoption of artificial intelligence

12 Novembre 2025
LOMAZZO (CO)
ComoNext
Hub dove la sicurezza si moltiplica

14 Novembre 2025
PALMANOVA (UD)
Sala d'Onore del Comune, con Legacoop FVG
Cybercoop: Cooperare per la sicurezza

20 Novembre 2025
PADOVA
Università di Padova
Quale futuro per l'umanità

In collaborazione con AICA

24, 25, 27, 30 Settembre 2025
DSF partecipa al 61° Congresso AICA

23, 25 Settembre 2025
Olimpiadi Italiane di Informatica
Rappresentanza direttivo DSF

Olimpiadi Italiane di Informatica

Modalità ingresso:
in base all'evento.
** solo su invito*

EVENTO DIVULGAZIONE CULTURA
SETTEMBRE OTTOBRE NOVEMBRE
50 SPEAKER
10 TAPPE IN ITALIA
+ONLINE

segreteria@digitalsecurityfestival.it
www.digitalsecurityfestival.it

SOSTENITORE PLATINUM
NetApp

SOSTENITORI GOLD
certego · Commvault · ISACA Venice Chapter · KPMG · rubrik

SOSTENITORI SILVER
axians · beanTech · CABEL · eurosystem · HTS · karmasec · Tinet · INFINITE AREA

SOSTENITORI
Alveria · datamaze · Infinityhub · infostar · is copy · NETPATROL · PragmatAI · VARGROUP · PALAZZO DELLA LUCE

Accreditato
EUROPEAN CYBER SECURITY MONTH

Patrocinato
Clusit 25

>> di Matteo Greatti

L'INGEGNERIA SOCIALE: LA MINACCIA INVISIBILE CHE COLPISCE L'ITALIA

Quando pensiamo agli attacchi informatici, l'immaginario collettivo evoca hacker incappucciati, codici indecifrabili e virus devastanti. In realtà, una delle armi più efficaci nelle mani dei criminali digitali non è il software, ma la psicologia: l'ingegneria sociale.

Con questo termine si indicano tutte le tecniche di manipolazione utilizzate per spingere le persone a rivelare informazioni, cliccare su link pericolosi o aprire inconsapevolmente la porta a un attacco informatico. Non serve un software sofisticato se si riesce a convincere la vittima ad agire di propria volontà. Gli esempi abbondano: e-mail di phishing che imitano banche e corrieri, SMS fasulli che annunciano pacchi da ritirare, telefonate da finti operatori di assistenza, messaggi WhatsApp che sembrano arrivare da amici o colleghi.

Gli attacchi di ingegneria sociale hanno successo perché sfruttano leve psicologiche universali, ad esempio la paura ("Il tuo conto sarà bloccato se non agisci subito"), la fretta ("Conferma entro pochi minuti per non perdere il pacco"), la curiosità ("Guarda queste foto che ti riguardano"). Nelle situazioni di urgenza, il nostro cervello sceglie scorciatoie rapide, abbassando le difese critiche. È in quel momento che scatta la trappola.

Nel nostro Paese, queste truffe digitali sono in continua crescita. Secondo i dati del CERT-AgID e del Clusit, phishing e smishing rappresentano una delle principali minacce informatiche. Le piccole e medie imprese, cuore dell'economia italiana, risultano particolarmente vulnerabili: spesso mancano programmi strutturati di formazione del personale e protocolli di risposta agli incidenti. Un clic sbagliato può tradursi in ransomware, furto di dati sensibili o interruzione delle attività, con danni economici e reputazionali rilevanti.

Anche i cittadini comuni restano un obiettivo privilegiato, soprattutto le fasce meno digitalizzate della popolazione che rischiano di cadere più facilmente in inganni sempre più convincenti. L'impatto dell'ingegneria sociale non si misura solo in termini di truffe individuali. Può rappresentare l'innesco di attacchi molto più gravi: accessi non autorizzati a reti aziendali, compromissione di account professionali, furto di proprietà intellettuale. Per un Paese che sta spingendo sulla trasformazione digitale, questi episodi minano la fiducia nelle tecnologie e rallentano l'innovazione.

Per controbattere questo fenomeno la tecnologia da sola non basta: la risposta deve essere culturale. Sensibilizzare i cittadini, formare i dipendenti con simulazioni di phishing e corsi di awareness, promuovere lo spirito critico, insegnando a riconoscere le minacce.

L'ingegneria sociale ci ricorda che la sicurezza non si gioca solo nei data center o nei laboratori di ricerca, ma nella quotidianità. In Italia, dove la cultura digitale è ancora disomogenea, investire nella formazione è la vera chiave di difesa. Perché il firewall della mente umana si chiama consapevolezza.

>> SPECIAL THANKS

DI ANTONIO TETII

ALGORITMI DELLA MENTE: IA E MANIPOLAZIONE DELLE EMOZIONI UMANE

Negli ultimi anni l'intelligenza artificiale (IA) ha superato il tradizionale ruolo di strumento analitico per assumere la funzione di agente attivo nei processi di comunicazione e di influenza psicologica. Con l'affermazione di modelli di apprendimento automatico capaci di trattare dati multimodali – testi, immagini, segnali biometrici e interazioni digitali – le tecnologie di IA hanno acquisito una competenza crescente nel riconoscimento, nella classificazione e nella modulazione delle emozioni umane. Questo passaggio segna un punto di svolta critico: da sistemi progettati per rispondere a bisogni espliciti degli utenti, siamo entrati in un'epoca in cui gli algoritmi non solo interpretano stati affettivi latenti, ma li utilizzano per influenzare decisioni e orientare comportamenti.

L'analisi del fenomeno rivela come la manipolazione emotiva mediata dall'IA si realizzi attraverso un insieme di strategie integrate: personalizzazione dei contenuti, rinforzo selettivo tramite feedback algoritmici, sfruttamento delle euristiche cognitive e creazione di ambienti digitali immersivi capaci di modulare l'esperienza affettiva. Nei social network, ad esempio, gli algoritmi di raccomandazione operano una selezione mirata dei contenuti in grado di amplificare emozioni specifiche – dalla curiosità all'indignazione – influenzando così non solo i consumi informativi individuali, ma anche la formazione dell'opinione pubblica. In ambito commerciale, il neuromarketing basato su IA integra biometria, eye-tracking e sentiment analysis per predisporre messaggi pubblicitari calibrati sulle vulnerabilità emotive dei consumatori. In contesti più delicati, come la sicurezza nazionale e la propaganda digitale, si delineano scenari di 'psicopolitica algoritmica", in cui l'IA diventa strumento di condizionamento collettivo attraverso campagne di disinformazione e microtargeting.

Accanto alle opportunità positive – come l'impiego dell'IA per supportare terapie psicologiche personalizzate o per sviluppare sistemi empatici di assistenza digitale – emergono rischi considerevoli legati alla trasparenza, all'autonomia decisionale e alla libertà cognitiva degli individui. L'opacità dei modelli di apprendimento, unita alla difficoltà di regolamentare l'uso etico di tali tecnologie, solleva interrogativi urgenti sul rapporto tra potere algoritmico e autodeterminazione umana. In conclusione, l'intreccio tra IA e manipolazione emotiva non può

essere compreso solo in termini tecnici, ma richiede una prospettiva interdisciplinare capace di integrare psicologia, filosofia della mente, scienze sociali ed etica applicata. La domanda cruciale che emerge è se l'IA resterà strumento al servizio dell'uomo o se, attraverso il controllo invisibile delle emozioni, finirà per ridefinire le condizioni stesse della libertà individuale e collettiva.

I brani del Digital Security Festival disponibili su Spotify e altri streaming

Il Digital Security Festival ha ora una colonna sonora ufficiale, già lanciata alcuni mesi fa con l'inno Universo Dato. Ora arriva il mini EP Universo Dato – Official Soundtracks, disponibile su Spotify, Apple Music, Amazon Music, YouTube Music, Deezer e Tidal. I due brani sono utilizzabili anche come sottofondo musicale nelle Storie di Instagram e, a breve, nei video TikTok.

Il progetto è stato ideato da Gabriele Gobbo, vicepresidente del Festival e autore del libro Digitalogia, che ha curato testi e produzione. Le tracce sono state create utilizzando strumenti generativi come fossero strumenti musicali: non musica 'fatta da un'AI", ma artigianato digitale progressivo, nato da scrittura, progettazione, ascolto e continue modifiche. Una fusione tra intelligenza umana e artificiale.

«Questo progetto non vuole sostituire il talento di un musicista, ma esplorare una via diversa per raccontare storie e diffondere cultura», spiega Gobbo. «Non si tratta di un clic magico, ma di vero artigianato digitale.»

Il mini EP contiene due versioni del brano Universo Dato: una elettronica e cinematografica, l'altra in chiave rap/hip hop. Un modo nuovo per raccontare temi come tecnologia, dati, consapevolezza e umanità, al centro della settima edizione del Festival.

La distribuzione globale include anche l'indicizzazione nei principali database musicali come Gracenote (per autoradio e software), Jaxsta (per i crediti ufficiali) e l'integrazione con assistenti vocali come Siri e Alexa.

Il Digital Security Festival è la prima manifestazione italiana diffusa dedicata alla cultura della sicurezza digitale. Nato nel 2019, coinvolge ogni anno diverse città, decine di speaker e centinaia di partecipanti, con l'obiettivo di rendere accessibile a tutte e tutti il tema della cybersicurezza. La settima edizione si svolgerà nell'autunno 2025, con eventi in presenza e online in tutta Italia.

Il negozio che Amazon non ha ucciso: una lezione di umanità digitale

di Gabriele Gobbo

C'è un negozio di elettrodomestici, nella piccola cittadina dell'estremo nordest d'Italia dove vivo, incastonata fra Venezia, l'Austria e la Slovenia, che frequento da trent'anni. E forse la mia famiglia da ancora più tempo. E no, non è morto. Nonostante Amazon, i centri commerciali, le catene, gli ipermercati e la corsa agli sconti digitali. Anzi, è più vivo che mai.

Vende frigoriferi, lavatrici, lampadine. Non c'è nulla di sexy nelle vetrine. Nessun display con il 70% di sconto. Nessun influencer che ne racconti le gesta. Eppure, resiste dove altri hanno fallito. Non perché sia più veloce. Non perché sia più economico. Non perché abbia una strategia di funnel marketing. Resiste perché ha scelto di non diventare una macchina. Quando vai lì, la domanda che ti fanno non è: «Quale modello vuoi?», ma «Cosa ti serve davvero?». Ti chiedono cosa ci dovrai fare, che spazi hai in casa, quanti siete in famiglia. Capiscono che un frigorifero non è un codice prodotto ma un pezzo di vita quotidiana. Che se ti si rompe la lavatrice la domenica mattina, non te ne frega molto di un form di sostituzione prodotto, di un chatbot, di un numero d'ordine o di un tracking number: vuoi solo qualcuno che venga a casa e la sistemi.

Questa, più che una strategia, è cultura. La stessa cultura che nella Digitalogia chiamo consapevolezza: sapere che non tutto si può scalare, non tutto si può ottimizzare. Che la memoria umana non è obsoleta, è preziosa. Perché nessun algoritmo sa che abiti ancora in quella casa con impianti fragili, o che hai due figli adolescenti che maltrattano gli elettrodomestici. Viviamo tempi da sonnambuli digitali: camminiamo tra i pixel come se sapessimo dove andare, ma abbiamo dimenticato il perché. Sappiamo cosa abbiamo comprato, ma non più perché ne avevamo bisogno. È un mondo di dati, ma privo di conoscenza.

In quel negozio di provincia, invece, la conoscenza è ancora una forma di capitale. Non ti vendono il top di gamma per forza, ma quello che funziona per la tua famiglia. Non ti infilano servizi aggiuntivi inutili, ma ti installano quello che compri e portano via l'usato senza chiedere un centesimo. È un patto silenzioso: loro si ricordano di te, tu ti ricordi di loro. E questo è il punto: la tecnologia è utile finché non ci fa dimenticare come si sta in mezzo agli altri. Finché non ci fa dimenticare che non siamo solo un carrello pieno di articoli ma persone, vicini di casa.

Amo il digitale. Uso Amazon. Sfrutto le AI. Ma non scambierei mai quella botta di umanità per una consegna in 24 ore. Perché è nei momenti difficili, quando la lavatrice smette di girare o il frigorifero smette di raffreddare le birre, che capisci quanto sia inutile un chatbot e quanto sia preziosa una mano che suona alla porta. Ogni tanto passo di lì anche solo per dire ciao. Perché questo fanno i vicini: si salutano. E forse, in fondo, questa è l'unica customer journey che conta davvero.

La verità è che possiamo costruire macchine sempre più intelligenti. Ma dovremmo ricordarci di essere, prima di tutto, umani.

Cybersecurity e Industria: crescono le minacce ai sistemi OT e CPS ed urge una strategia integrata

di Ruggero Contu

Secondo il Rapporto Clusit, nel secondo semestre del 2024 gli attacchi informatici su scala globale sono aumentati del 25%, con il settore manifatturiero tra i più colpiti in Italia. Un quarto di tutti gli attacchi rivolti al settore manifatturiero a livello globale ha avuto come bersaglio aziende italiane, evidenziando la loro vulnerabilità di fronte a minacce sempre più sofisticate. Tra queste minacce spiccano la pressione sui sistemi OT e l'emergere dei rischi attorno ai Cyber-Physical Systems (CPS). Un nuovo report di Siemens Energy e Ponemon Institute analizza la situazione della sicurezza attorno all'Operational Technology (OT). L'OT si riferisce all'hardware e al software che controllano e monitorano dispositivi, processi e infrastrutture fisiche nelle aziende, come le linee di produzione, le centrali elettriche e le reti di trasporto. In questo ambito, per comparti come oil & gas, utilities idriche ed elettriche, petrolchimico e manifatturiero, le minacce informatiche sono frequenti, le vulnerabilità diffuse e le competenze in materia di cybersecurity ancora scarse.

Le difese OT sono vulnerabili e le aziende ne sono consapevoli. L'indagine rivela che il 77% delle aziende ha subito almeno un attacco informatico che ha compromesso dati riservati o causato interruzioni ai sistemi OT negli ultimi 12 mesi. Il 62% degli attacchi ha richiesto più di un mese per essere individuato e il tempo medio di recupero è stato di sette mesi. Il 24% degli attacchi rilevati ha comportato l'arresto dei flussi di lavoro OT. Il 50% delle aziende valuta negativamente le proprie difese, ritenendo di poter prevenire solo un uso accidentale o involontario dei sistemi. La maggior parte segnala che le proprie reti OT non sono segmentate correttamente e utilizzano dispositivi o software con vulnerabilità note. Il 52% ritiene probabile o molto probabile subire un attacco OT di successo nell'anno a venire. Il 46% pensa che un attacco riuscito possa portare all'arresto di un impianto. Questa vulnerabilità mette a rischio i vantaggi economici della digitalizzazione in corso nei settori energia e manifatturiero. Con l'integrazione dei sistemi digitali nei flussi OT, le aziende che non proteggono adeguatamente questi ambienti rischiano gravi interruzioni operative.

Un sistema cyber-fisico o CPS (Cyber-Physical Systems) è un sistema composto da elementi computazionali, di comunicazione e di controllo che si interfacciano in modo continuo e dinamico con il mondo fisico reale, monitorandolo e agendo su di esso per ottimizzare i processi in tempo reale. I CPS sono alla base delle industrie intelligenti (Industry 4.0) e integrano l'Industrial Internet of Things (IIoT) con la capacità di auto-monitoraggio e comunicazione tra le varie componenti. Questi sistemi stanno rivoluzionando l'interazione tra domini digitali e fisici. I CPS integrano calcolo, reti e processi fisici, diventando fondamentali per settori critici come energia, trasporti, sanità e difesa. In un contesto di minacce sempre più complesse, la sicurezza di questi sistemi è una necessità tecnologica e una priorità strategica.

I CPS si sono evoluti da ambienti di controllo isolati a componenti integrati di infrastrutture critiche. Questa integrazione porta nuove vulnerabilità interconnesse. Più i sistemi CPS diventano complessi e connessi, più gravi possono essere le conseguenze di una loro violazione, con possibili effetti a cascata su diversi settori. Un attacco a sistemi di trasporto o energia, ad esempio, può compromettere sia l'integrità operativa che la sicurezza fisica. La trasformazione digitale dei sistemi industriali va di pari passo con la crescente sofisticazione delle minacce. Le soluzioni puntuali non sono più sufficienti: serve un approccio olistico e basato sul ciclo di vita per affrontare le vulnerabilità dei CPS. L'integrazione della sicurezza nello sviluppo, la fiducia radicata nell'hardware e le architetture 'zero trust" sono elementi chiave per proteggere sia OT che IT.

La sicurezza dei CPS è fondamentale. L'integrazione tra sistemi digitali e fisici nelle infrastrutture critiche richiede un approccio robusto alla cybersecurity, che vada oltre le difese IT tradizionali. Proteggere i CPS significa salvaguardare dati, continuità dei servizi e soprattutto la sicurezza fisica di persone e comunità. Gli investimenti in intelligenza artificiale stanno trasformando la sicurezza dei CPS, migliorando la rilevazione e la risposta alle minacce e colmando la carenza di competenze. Tuttavia, queste innovazioni portano anche nuovi rischi, come la manipolazione dei dati e la complessità normativa. Per affrontare queste sfide, le organizzazioni devono adottare strategie di sicurezza basate su tutto il ciclo di vita, pratiche di sviluppo sicuro e una gestione robusta dei dispositivi. È fondamentale bilanciare l'automazione guidata dall'AI con il controllo umano, soprattutto nei contesti più critici.

Infine, le normative stanno guidando il futuro della sicurezza CPS: i responsabili devono integrare requisiti normativi e buone pratiche nei propri framework, puntando su soluzioni trasparenti, resilienti e integrate. In sintesi, la sicurezza dei sistemi cyber-fisici richiede investimenti strategici, tecnologie innovative e strategie operative adattive. Solo un approccio olistico che unisca tecnologia, policy ed eccellenza operativa potrà garantire sistemi sicuri, affidabili e resilienti di fronte alle crescenti minacce informatiche.

UNIVERSO DATO:

di **Luigi Gregori**, Tesoriere Digital Security Festival

C'è un filo che unisce il mestiere di chi governa l'innovazione IT e l'antica figura del maestro: non l'accumulo dei saperi, ma la capacità di trasformarli in giudizio, di tenere insieme la bussola dell'intelligenza e il timone della coscienza. La trasformazione digitale non chiede soltanto cosa fare — nuovi modelli, nuove piattaforme, nuova AI — ma come orientare comunità di persone attraverso l'incertezza, curando la qualità del dato che le nutre e la qualità delle decisioni che ne scaturiscono. In questo viaggio, l'IT governance advisor è prima di tutto un educatore alla complessità: costruisce mappe, smaschera false scorciatoie, alterna empatia e fermezza, e rende praticabile ciò che altrimenti resterebbe inattingibile.

L'orizzonte in cui operiamo è cambiato: l'Europa da tempo non può contare solo sulla dimensione del suo mercato; deve unire forze su tecnologie critiche, standard e capacità industriali. Abbattere ostacoli interni nel mercato unico varrebbe, secondo stime citate a Rimini, fino al 7% di produttività in sette anni; la sfida dei semiconduttori mostra quanto conti la scala e la convergenza degli investimenti. Per le imprese, questo si traduce in governance che sappia leggere e anticipare i cicli regolatori, industriali e tecnologici, invece di inseguirli. (la Repubblica)

Dentro le organizzazioni, la trasformazione è un ribaltamento di prospettiva: dal 'fare progetti" al 'costruire capacità"; dal comprare strumenti al governare relazioni — tra dati, persone, processi, rischi e risultati. Qui l'advisor agisce come guida: non si limita a prescrivere metodologie, ma attiva apprendimenti, rompe inerzie, allena al discernimento. In alcuni momenti consola, in altri provoca: mette davanti all'inconsistenza di certezze ereditate, per far posto a pratiche di valore misurabile. L'obiettivo non è una collezione di tecnologie 'giuste", ma una comunità competente nel loro uso responsabile.

Se l'universo che abitiamo è fatto di dati, il governo dell'innovazione è, prima di tutto, governo del dato. Il manifesto del Digital Security Festival ricorda che la conoscenza è la materia prima, l'intelligenza la bussola che interpreta, la coscienza il timone che orienta scelte e rinunce: un triangolo che dovrebbe diventare prassi quotidiana di ogni steering committee, ufficio dati e funzione di controllo. La sicurezza, ci viene suggerito, non è più una fortezza ma un portale multidimensionale: attraversa architetture, persone, filiere e — oggi — modelli di AI. E le coordinate per navigarla hanno nomi concreti: conoscenza, consapevolezza, intelligenza, resilienza, innovazione, coscienza, collaborazione, con l'umanità al centro.

I numeri, intanto, ci impongono umiltà e mettono a fuoco le priorità. Il Cost of a Data Breach 2025 di IBM indica un costo medio globale di 4,4 milioni di dollari per violazione, con un divario netto tra chi governa l'AI e chi la adotta senza guardrail: il 97% delle organizzazioni che hanno subito incidenti legati all'AI non aveva adeguati controlli di accesso, e dove l'AI è usata estensivamente per la sicurezza si osservano risparmi medi fino a 1,9 milioni. Tradotto: senza data governance e AI oversight il rischio operativo ed economico sale, non scende. (IBM)

Sul fronte delle minacce, ENISA segnala che le aggressioni contro la disponibilità, il ransomware e gli attacchi ai dati restano tra i principali vettori in Europa; e l'estensione dello sguardo allo spazio — infrastrutture satellitari sempre più commerciali e interdipendenti — mostra come la superficie d'attacco si espanda 'oltre l'atmosfera", richiedendo standard, condivisione d'informazioni e capacità di resilienza lungo l'intero ciclo di vita. Anche questo è universo dato: dipendiamo da sistemi interconnessi e dobbiamo trattarli come beni comuni critici. (enisa.europa.eu)

La competenza resta l'altra metà dell'equazione. Nel 2023, solo il 56% degli europei tra 16 e 74 anni possedeva competenze digitali di base: un dato che rende tangibile la distanza dall'obiettivo dell'80% entro il 2030 e che costringe a misurare ogni trasformazione anche come progetto educativo. Un'azienda che governa l'innovazione deve quindi legare metriche di adozione a metriche di

IL GOVERNO DELL'INNOVAZIONE COME ARTE DELLA GUIDA

apprendimento e sicurezza, investendo in percorsi che tengano insieme ruoli, età e responsabilità. (Epthinktank)

In questo scenario, le regole non sono un freno ma un telaio su cui tessere fiducia. L'AI Act europeo prosegue la sua attuazione senza rinvii: entrano in vigore scaglioni di obblighi (dai divieti precoci nel 2025 alle regole per i modelli general-purpose nell'agosto 2025), con codici di pratica a supporto e sanzioni significative per chi ignora requisiti di trasparenza e sicurezza. Per i governance advisor, significa orchestrare inventari di sistemi, verifiche d'impatto, vendor due-diligence e controlli d'accesso al dato e ai modelli, raccordando compliance, rischio e valore. (Ogletree, AP News, Reuters)

Qui si innesta il contributo specifico del Digital Security Festival. Il Festival è una piattaforma che fa incontrare intelligenze e responsabilità: porta la sicurezza 'in tour" con appuntamenti in diverse province, rafforza le occasioni fisiche, mantiene una presenza online per scalare la divulgazione e costruisce comunità miste — aziende, istituzioni, scuole, cittadini. L'ultima edizione ha superato le 50 ore di eventi tra sei province e dieci location con oltre 2.000 partecipanti; la nuova edizione spinge ancora su tavole rotonde e speed-pitch, e ribadisce la centralità del dato come dono e punto di partenza. Questo duplice formato — in presenza e digitale — consente di trasmettere conoscenza, allenare l'etica della decisione e far maturare, per contagio positivo, una leadership diffusa.

Perché tutto questo funziona? Perché una comunità che si incontra — nelle sale di palazzi storici, in aule universitarie, nei webinar — costruisce fiducia e linguaggi condivisi; e chi guida l'innovazione ha bisogno di fiducia per chiedere cambi di rotta e di linguaggi comuni per trasformare incidenti in apprendimento. L'etica, in questo contesto, non è sovrastruttura: è la disciplina che tiene insieme scopo, trasparenza e responsabilità del dato — dal modo in cui viene raccolto, al modo in cui alimenta modelli e decisioni. L'advisor che sa 'tenere il timone" educa alla rinuncia autant qu'à l'ambizione: accetta limiti dove il rischio eccede il valore, espone con chiarezza le ipotesi, istituisce gates che difendono l'umano nel ciclo del digitale.

In definitiva, governare l'innovazione oggi significa incarnare una leadership che trasmette conoscenza, coltiva discernimento e guida comunità attraverso passaggi difficili senza tradire il centro umano delle scelte. L'universo dato non è un archivio: è materia viva che chiede maestria — la nostra. E il Digital Security Festival è il luogo dove questa maestria si affina, condividendo mappe, bussola e timone per attraversare insieme il possibile.

Innovazione, produttività, efficienza… e l'essere umano?

di **Ettore Guarnaccia**

Stiamo vivendo un'epoca che ricorderemo come una delle più radicali trasformazioni della storia. L'intelligenza artificiale si diffonde con rapidità travolgente, mentre robotica e realtà estesa stanno permeando le aziende e la nostra quotidianità. In convegni e dibattiti si ripete lo stesso mantra: innovazione, produttività, efficienza. Molte organizzazioni sono in corsa per automatizzare processi, ridurre costi, abilitare nuove forme di collaborazione a distanza e reinventare modelli di business. È una gara globale e frenetica, che coinvolge tutti i settori e vede in prima fila finanza, industria, sanità, biotecnologie, energia, logistica, trasporti, e-commerce, intrattenimento, perfino gli armamenti. Chi non accelera rischia l'irrilevanza.

Ma dietro questo entusiasmo si nasconde un lato oscuro: la smania di innovare a ogni costo può portare a trascurare conseguenze fondamentali per il futuro, dalle ricadute sociali fino alle nuove minacce per la sicurezza, la reputazione e la stessa prosperità aziendale. L'automazione di attività ripetitive promette di abbattere i costi operativi e aumentare la produttività, ma rischia di cancellare mestieri e competenze, creando disoccupazione e tensioni sociali, mentre la domanda di nuove professionalità cresce molto più rapidamente dell'offerta, rendendo difficile reperire i talenti necessari. Non solo, gli investimenti rischiano di concentrarsi sui pochi giganti tecnologici che sviluppano e offrono queste tecnologie, accentuando squilibri e dipendenze.

La nascita di nuovi modelli di business fondati su IA generativa, esperienze immersive e robotizzazione spalancherà scenari globali inediti, creando nuovi mercati. La reputazione sarà messa a dura prova dal dover rispettare normative complesse come l'AI Act, NIS2, DORA e GDPR, da bias e dilemmi algoritmici e decisioni opache, e da contraddizioni ideologiche legate a consumo energetico e impatti ambientali. Un rischio è che il rapporto tra azienda e cliente perda calore umano, empatia e fiducia, un altro è farsi ammaliare dall'hype dell'innovazione senza una solida strategia, stravolgendo il proprio business senza generare reale valore e subendo il paradosso di perdere competitività invece di guadagnarla.

Aspetto fondamentale è la cybersecurity, ormai asse portante delle moderne trasformazioni digitali. Senza sicurezza, ogni innovazione si rivela insostenibile. Oggi l'IA non potenzia solo le difese, ma anche gli attacchi: malware sofisticati, phishing estremamente accurati, deepfake vocali e visivi indistinguibili dalla realtà, manipolazione e disinformazione immersive, persino chatbot o modelli di IA corrotti o strumentalizzati. Le imprese dovranno identificare e comprendere queste nuove minacce con una rapidità mai richiesta prima, predisponendo contromisure adeguate ed evolute.

Ma a pesare sulla competitività futura delle imprese saranno anche le conseguenze sociali. Ormai intrappolata nel vortice digitale, la società mostra sintomi evidenti di declino psicologico, cognitivo e valoriale, che potrebbero essere aggravati dai futuri effetti delle tecnologie emergenti. Le nuove generazioni vivono immerse in forme di dipendenza ludica e digitale, fragilità emotive, carenza di attenzione, autonomia e pensiero critico. Troppo spesso si rifugiano in un presente superficiale, dominato dall'apparenza e dall'esposizione di sé, con livelli allarmanti di analfabetismo funzionale ed emotivo. Ed è da questo bacino che le aziende dovranno attingere per costruire un futuro che richiederà non solo competenze tecniche, ma anche solide fondamenta etiche, morali e umane.

Il rischio più grande non è la tecnologia in sé, ma l'errore di sottovalutare ancora una volta il fattore decisivo: l'essere umano. Non semplice forza lavoro, ma intelligenza viva, capace di immaginare, creare e decidere. Le persone, con le loro competenze, sensibilità e coscienza, devono essere al centro di questa trasformazione epocale e beneficiare a loro volta di attenzione e investimenti sul piano sociale, culturale, etico e morale. L'evoluzione tecnologica dovrà essere messa al servizio dell'essere umano, non del profitto, come potente mezzo per elevare culturalmente e spiritualmente l'umanità. Solo così potremo sperare di disegnare un futuro più avanzato non solo in tecnologia, ma anche in umanità e autentico benessere.

Indagini informatiche: il duello tra privacy e giustizia

di **Luca Mercatanti**

In tasca portiamo interi archivi di vita: fotografie, messaggi, conversazioni vocali, posizioni GPS, cronologie di navigazione, app di home banking, password, abitudini, preferenze. Lo smartphone non è più un semplice strumento di comunicazione, ma il diario digitale più dettagliato mai esistito. Per questo, è diventato anche un elemento chiave nelle indagini digitali: ogni giorno, nel mondo, migliaia di dispositivi vengono analizzati in ambito forense per cercare prove, ricostruire eventi e fare luce su reati di ogni tipo. Difficilmente, ad oggi, esiste un procedimento, soprattutto in ambito penalistico, che non preveda il sequestro dei dati informatici contenuti all'interno dello smartphone. La digital forensics si muove in un campo in continua evoluzione. Da un lato ci sono investigatori digitali, forensi, ricercatori e consulenti chiamati ad analizzare dati per rispondere alle domande della giustizia. Dall'altro, i produttori di dispositivi e software che ogni giorno lavorano per garantire ai propri utenti un livello di protezione dei dati sempre più elevato.

Negli ultimi anni, l'attenzione globale sulla privacy ha spinto le aziende a introdurre sistemi di crittografia end-to-end, blocchi biometrici sempre più sofisticati, cancellazioni automatiche e protezioni contro gli accessi non autorizzati. Di fronte a questo scenario, gli strumenti di analisi forense devono adattarsi, aggiornarsi, evolversi, spesso rincorrendo tecnologie che diventano obsolete nel giro di pochi mesi. E tutto questo, senza alcuna collaborazione da parte dei produttori, anzi. Questo porta alla ricerca di vulnerabilità, exploit e metodi di sblocco non autorizzati, divenuti ormai parte integrante del mondo forense. Una corsa silenziosa tra chi costruisce barriere e chi cerca passaggi, dove la finalità non è lo spionaggio o la violazione, ma la ricostruzione dei fatti in contesti legali e investigativi.

Il diritto alla privacy è un pilastro fondamentale, ma lo è anche la necessità di giustizia e verità. La digital forensics cammina su questa linea sottile, fatta di responsabilità, rigore scientifico e consapevolezza dei limiti. Ma qual è, allora, la strada giusta? Collaborare con gli analisti forensi per consentire l'accesso ai dati in casi gravi e giustificati? O proteggere in modo assoluto la privacy, rischiando che la verità resti sepolta? Alcuni governi vorrebbero imporre backdoor obbligatorie ai produttori di smartphone e software, sostenendo che siano necessarie per motivi di sicurezza nazionale. Ma chi ci garantisce che quelle stesse porte non vengano poi usate da attori malevoli, criminali informatici o regimi autoritari?

La questione resta aperta. E forse non esiste una risposta definitiva, ma solo la necessità di interrogarsi, costantemente, sul delicato equilibrio tra ciò che possiamo fare e ciò che dovremmo fare.

di **Stefano Gazzella**

IL BARDO E L'UNIVERSO DATO

È naturale domandarsi in che modo un moderno Jules Verne si appresterebbe a raccontare un viaggio di esplorazione attraverso i mondi e gli ecosistemi digitali. Ma più che all'equipaggiamento dei protagonisti, il pensiero va a ciò che prima di tutto spingerebbe questi avventurieri al di fuori della comfort zone. Se davvero possa esistere ancora qualcosa di ignoto e una qualche voglia di avventura, oggi, nell'era dell'iperconnessione. O se altrimenti il racconto dovrà giacere incompiuto, pensando che oramai non serva più raccontare delle storie. Tutto è dato, quindi si potrebbe pensare che non ci sia più nulla da ricercare o creare.

Eppure, è proprio con il potenziale dell'Universo Dato che l'essere umano ha la possibilità di arrivare alle terre inesplorate della possibilità.

Che nei multiversi digitali si esprime come fluida, accelerata, plasmabile. E riflette che poter fare non sempre coincide con dover fare, o con il fatto che ciò che si andrà a compiere potrà portare a qualcosa di desiderabile. L'infinito potenziale della tecnologia deve trovare così un argine nella sua attuazione, ma mai nello studio o nella conoscenza. Peggio ancora sarebbe però se questi argini si volessero imporre con il monopolio della violenza che è proprio della legge dei filtri o dei vincoli. Perché così verrebbe meno la libertà del Cercatore. Quella che i bardi vivevano e cantavano al contempo, ascoltando storie e inventandone delle altre. Storie che vale la pena ascoltare perché hanno il potere di plasmare la realtà.

Non è forse una storia la cultura dei diritti di quarta generazione? Non lo è la cultura del dato, o della sicurezza delle informazioni? E quanto profondamente queste storie possono trasformare la realtà attuale in quella che vorremmo vedere realizzata e che mantiene la persona al centro pur nelle molteplici vite digitali che conduce e attraverso le quali ha l'occasione di creare valore personale e collettivo?

Ecco, dunque, che il ruolo del bardo può essere rivalutato all'interno dell'Universo Dato, perché forse rappresenta quella curiosità che conduce proprio all'esplorazione delle nuove soglie proprie dell'avanzamento tecnologico. La ricezione e la condivisione di esperienze umane possono consentire così di mantenere quelle tecnologie al servizio dell'umanità, del suo progresso e delle sue migliori

invenzioni. E perché no, anche di esercitare quel dubbio che coesiste con la forza di cambiare strategie, opinioni e giovarsi così di opportunità che altrimenti non si sarebbero mai colte.

Datum, nel suo significato etimologico, esprime ciò che 'è offerto', un dono. Consiste in una notizia data la quale se ne desumono conseguenze, nella manifestazione concreta di un'informazione – o qualsiasi concetto - attraverso un processo di codifica. È la forma tangibile della rappresentazione, convertendo un elemento grezzo in qualcosa che può essere oggetto di elaborazione e trasformazione. Praticamente miracolo alchemico cui assistiamo quotidianamente anche nell'esperienza digitale, ma su cui forse non ci soffermiamo a sufficienza.

Chi meglio di un bardo, dunque, per ricordare proprio la natura del dato declinandola nei tempi, nei contesti e nelle dinamiche contingenti che viviamo? Beninteso, deve evitare di farsi accecare da quell'ambizione che esclude il riconoscimento e il rispetto di più esperienze differenti ed esclude il pensiero critico. Motivo per cui non dovrà mai affrontare il viaggio nell'Universo Dato in solitudine, ma anzi promuovere sinergie, comunità e fare in modo che il merito degli argomenti prevalga sempre, la condivisione esalti gli approcci multilaterali e le distorsioni cognitive possano essere prontamente riconosciute ed affrontate.

Altrimenti, quello del valore e della centralità del dato non sarà altro che un racconto destinato ad essere dimenticato. Perdendo così anche la nostra capacità di riconoscere e comprendere la portata del dono che può rappresentare.

L'ordine dei dati: una difesa strategica nell'era digitale

di **Marco Stefani**

Nel cuore del Big Bang digitale, dove ogni secondo genera una miriade di dati, emerge una necessità imprescindibile: fare ordine. Con oltre 147 zettabyte di dati prodotti nel mondo lo scorso anno e una previsione di 180 zettabyte entro il 2025, la sicurezza delle informazioni non può più essere un'opzione, ma una strategia consapevole. Si stima che nel 2023 siano stati prodotti circa 147 zettabyte (1 ZB = 1 miliardo di terabyte) di dati, con una previsione di 180 ZB per il 2025. Un vero e proprio Big Bang digitale, un cosmo informativo in continua espansione: email, transazioni finanziarie, telemetrie da sensoristica IoT, like sui social, immagini, video. Ogni secondo, frammenti di informazione viaggiano attraverso le reti di tutto il mondo. È importante distinguere tra dato, informazione e conoscenza. Un dato è un elemento grezzo, come '120/80". Quando questo dato viene contestualizzato, diventa informazione: 'La pressione sanguigna del paziente Mario Rossi è 120/80 mmHg". Infine, l'informazione interpretata diventa conoscenza: 'Dato che la pressione è nella norma, non è necessario alcun intervento farmacologico".

Ma come facciamo a proteggere i nostri dati? Prima di poter difendere un territorio, è indispensabile conoscerne i confini, la topografia e il valore delle risorse in esso contenute. Questo processo di mappatura è la base di ogni strategia di sicurezza resiliente e proattiva: non si può proteggere ciò che non si sa di possedere. La sicurezza del dato, quindi, non inizia con la costruzione di muri impenetrabili o con l'acquisto di scudi tecnologici avveniristici. Inizia con un atto più umile ma infinitamente più potente: fare ordine. Senza sapere quali dati proteggere, dove si trovano e quanto 'valgono", ogni misura di sicurezza rischia di essere inefficace o sproporzionata.

Il primo passo è quindi la data discovery & inventory: mappare l'universo, creando un inventario completo di ogni dato, rispondendo alle domande: cos'è, dov'è e chi ne è responsabile. Una volta mappato, ogni dato deve essere valutato. Ogni informazione deve essere etichettata in base alla sua sensibilità: pubblico, uso interno, riservato, segreto. Queste etichette determinano chi può accedere al dato, come deve essere protetto e come può essere condiviso. Serve poi un framework di policy, regole e responsabilità che disciplini l'intero ciclo di vita del dato, dalla sua creazione alla sua distruzione sicura. Le persone, elemento cruciale, diventano la prima linea di difesa nella protezione delle informazioni. Questo framework di governance serve infatti a guidare il comportamento umano, trasformando quello che spesso è l'anello debole in una vera prima linea di difesa.

Il cloud, in particolare, ha avuto un impatto significativo: per garantire la disponibilità del dato, lo si replica in più punti, con notevoli implicazioni legislative e di governance, tra la responsabilità della sicurezza del dato e quella dell'infrastruttura. La proliferazione di dispositivi IoT (sensori, telecamere, elettrodomestici connessi) sta inoltre ampliando a dismisura la superficie d'attacco. L'universo

del dato, con la sua complessità e la sua vastità, può sembrare intimidatorio. Eppure, l'atto primordiale di mettere ordine — di scoprire, inventariare e classificare — è la chiave per dominarne le forze e mitigarne i rischi. In una frase: la consapevole segmentazione ordinata del dato.

Con una mappa chiara del nostro 'universo dato" è più facile conoscerne i pericoli, ed è possibile costruire un sistema di difesa a più livelli, dove ogni strato è progettato per proteggere i dati in base al loro valore e alla loro sensibilità. Inutile utilizzare artiglieria pesante per difendere un fortino vuoto o senza valore. Non è un progetto con un inizio e una fine, ma il cuore pulsante di una strategia di sicurezza in continua evoluzione, propedeutica a una postura di sicurezza adeguata. Investire nell'ordine del dato significa rafforzare la postura di sicurezza. E rafforzare la postura di sicurezza significa proteggere il valore dell'informazione, oggi più che mai il vero capitale delle organizzazioni.

Conclusione. Investire nell'ordine del dato significa rafforzare la postura di sicurezza. E rafforzare la postura di sicurezza significa proteggere il valore dell'informazione, oggi più che mai il vero capitale delle organizzazioni.

La solitudine, la vulnerabilità e la sensazione del dato

di **Mauro Talamini**

I dati digitalizzati sono oggi la linfa vitale della società: generano valore economico e sociale, guidano decisioni strategiche, influenzano la vita pubblica e privata. Ma riflettere sul dato singolo significa coglierne tre dimensioni cruciali: la sua debolezza, la sua vulnerabilità e la sua capacità di evocare sensazioni.

Il dato è debole se isolato dal contesto. Avulso da un sistema di riferimento, perde significato: come il mare visto dall'alto che appare piatto, così il singolo dato privo di correlazioni non restituisce la realtà. La mente umana cerca pattern e relazioni, non frammenti sparsi.

Il dato è vulnerabile perché costantemente esposto a corruzione, furto, drenaggio verso sistemi di AI che trasformano l'informazione in potere spesso per uso improprio. La sua protezione non è più solo un tema tecnico: è una condizione essenziale di fiducia per imprese, istituzioni e cittadini in un universo digitale interconnesso.

Il dato è sensazione. Oltre il calcolo, porta con sé memorie, ricordi, emozioni: elementi che sfuggono a catalogazioni scientifiche e riemergono quando il dato viene richiamato. È la 'madeleine' di Proust che, immersa nel tè, risveglia un ricordo totale fatto di atmosfere ed emozioni, non di soli numeri.

Molto è stato fatto per rafforzare le prime due dimensioni. L'AI amplifica capacità limitate dell'uomo, scoprendo correlazioni invisibili e rendendo "forte" il dato perché lo mette in relazione con il mondo circostante. Ma introduce nuove superfici di rischio: avvelenamento dei dati, attacchi adversariali, opacità dei modelli che riducono la fiducia e nascondono vulnerabilità etiche e tecniche.

La sicurezza deve quindi evolvere verso una data-centric security, capace di garantire integrità, tracciabilità e qualità lungo l'intero

ciclo di vita. All'orizzonte, il quantum computing promette innovazioni straordinarie ma minaccia i pilastri crittografici attuali. Per questo la comunità lavora già su algoritmi di post-quantum cryptography, fondamentali per preservare resilienza e fiducia.

Resta però una costante: l'umanità. Senza consapevolezza diffusa, collaborazione e coscienza etica, nessuna tecnologia potrà garantire sicurezza. Perché i dati non sono solo bit: sono vita, memoria e sensazioni che ci definiscono come persone. E in ognuno di essi c'è qualcosa di intangibile, di strettamente personale, quei '20 grammi dell'anima' che trasformano l'informazione in esperienza, emozione e significato. Semplicemente: vita.

LA NUOVA *DIMENSIONE* DELL'ENERGIA

Infinityhub Spa Benefit finanzia progetti di **riqualificazione energetica**, coinvolgendo attivamente **persone**, **imprese** e **comunità** che cooperano nel presente per un futuro di unione. Creiamo soluzioni **innovative**, **sostenibili** e **accessibili** che promuovono una transizione energetica partecipata, attraverso impianti di produzione di **energie rinnovabili**, **riqualificazione termica** ed edile di immobili, **finanza etica** e **strumenti fintech**. Crediamo in un futuro in cui l'energia viene **condivisa**, con un effetto **positivo**, **duraturo** e **sostenibile** per **tutte** e per **tutti**.

Il nostro **obiettivo**

Un futuro in cui la **sostenibilità ambientale**, **economica** e **sociale** si integrano, dando vita a **un modello d'impresa responsabile**, quindi capace di dare risposte nel **presente**, per custodire il **futuro**.

> *La bellezza è la vita quando la vita si rivela. La bellezza è l'eternità che si contempla allo specchio, e noi siamo l'eternità e lo specchio.*
>
> **Khalil Gibran**

Infinityhub
PERSONE | ENERGIE | FUTURO

info@infinityhub.it Sestiere San Marco 2893, 30124 Venezia (VE) www.infinityhub.it

NetApp®

WE MAKE DATA INFRASTRUCTURE INTELLIGENT

Discover more

Digital Security Festival alla Camera dei Deputati: una giornata per il futuro digitale del Paese

La settima edizione del Digital Security Festival ha inaugurato il suo percorso 2025 venerdì 19 settembre, in una sede prestigiosa e nel cuore delle istituzioni: la Sala Giacomo Matteotti della Camera dei Deputati a Roma. Un evento che ha trasformato per una mattinata la casa della rappresentanza democratica in un forum di alto livello sulla cultura della sicurezza digitale, confermando come questo tema sia diventato una priorità nazionale.

La giornata si è aperta con un coro unanime di saluti istituzionali. Il Vicepresidente della Camera, On. Fabio Rampelli, ha sottolineato come «i dati rappresentano una importantissima risorsa strategica [...] questo scenario richiede una riflessione approfondita che metta al centro la duplice sfida della protezione e della governance dei dati». Sono seguiti i videomessaggi dei parlamentari Sen. Andrea de Priamo («i dati sono la risorsa fondamentale, quella che The Economist ha definito già da tempo il nuovo petrolio [...] un tema fondamentale è quello della sovranità digitale»), On. Roberto Bagnasco («il dato non è solamente un elemento tecnico, è ormai materia prima della nostra economia, della vita sociale e delle relazioni tra i cittadini e le istituzioni») e On. Marco Pellegrini («viviamo in un'epoca in cui i dati rappresentano una delle risorse più preziose [...] la sicurezza non è più solo una necessità tecnica ma è diventata una responsabilità etica e sociale»). Hanno completato i saluti Francesco Del Prete in rappresentanza del Presidente della Regione Friuli Venezia Giulia Massimiliano Fedriga e Nicola Bosello di Ditedi per il cluster ICT friulano. È emersa una chiara convergenza: la necessità di governare la trasformazione digitale con consapevolezza e responsabilità.

Nel suo discrso di apertura, il Presidente del Festival Marco Cozzi ha racchiuso il senso della giornata: «essere qui alla Camera

dei Deputati a presentare la settima edizione del festival che ha le sue radici in Friuli Venezia Giulia [...] è un segnale molto forte». Cozzi ha poi lanciato un messaggio chiave che ha risuonato per tutto l'evento: «la sicurezza non è un software, è un comportamento».
A definire la cornice concettuale della giornata è stato il keynote speech del Prof. Alessandro Curioni, che ha sfidato la metafora comune dei 'dati come nuovo petrolio". Secondo Curioni, viviamo in un'era di inflazione informativa dove il vero campo di battaglia, la risorsa più preziosa e contesa, è diventata l'attenzione umana, perché «è la capacità di catturare la nostra attenzione» che genera valore oggi.

La mattinata è proseguita con un susseguirsi di panel che hanno esplorato l'#UniversoDato da ogni prospettiva. L'intervento del Dott. Umberto Rapetto, Presidente dell'Autorità Garante per la Protezione dei Dati Personali della Repubblica di San Marino, moderato da Andrea Del Vecchio, ha scosso la platea con una testimonianza forte sull'importanza della cultura come unica vera arma contro i rischi digitali, denunciando come spesso «la cultura, anziché essere un obiettivo, è un pericolo». Il panel 'Il Dato nel mondo del lavoro", diretto da Luigi Gregori, ha visto esperti come Mario Moroni affermare che «un dato ha valore solo se resta corretto, integro, disponibile e riservato nel tempo», Gianni Dell'Aiuto descrivere la nostra triplice identità di «Homo Googlis» creata «a colpi di click», Corrado Giustozzi avvertire che «il dato, oltre a essere tutte le cose belle che abbiamo visto, è diventato un'arma» e che viviamo in un'epoca in cui «usiamo i dati come armi» in modi inaspettati, e William Nonis sottolineare la necessità di supportare concretamente le PMI, perché «da sole non possono attuare tutte queste norme».

Successivamente, il dibattito sul 'dato come bene sociale", coordinato da Davide Bazzan, ha toccato temi cruciali come le disuguaglianze digitali con Alberto Elia Martin che ha parlato di una «autoesclusione informata» per mancanza di fiducia, l'importanza dell'usabilità dei servizi secondo Claudio Michelizza (se le procedure ufficiali fossero più semplici, «le persone utilizzerebbero meno i social e di più le app dedicate»), la vulnerabilità delle PMI europee secondo Antonino Polimeni, che ha denunciato come «quando parlo di dipendenza delle imprese dalle grandi piattaforme, intendo che se non dovessero più utilizzarle andrebbero addirittura in sofferenza». Il panel ha proseguito con l'importanza di riaffermare il ruolo dell'Italia secondo Andrea Violetti, convinto che «l'Italia deve tornare a essere protagonista perché ne abbiamo le competenze, le capacità e soprattutto la nostra visione di umanesimo digitale» e il concetto di «sovranità del dato» per Pierguido Iezzi, che ha affermato: «il dato è libertà, il dato rappresenta la democrazia».

Un momento culturale è stato dedicato alla presentazione del libro 'Digitalogia" di Gabriele Gobbo. Ad introdurla, un videomessaggio di Tiberio Timperi che ha detto di essere un sostenitore del libro, definendolo una sorta di 'tutto città" per orientarsi nel digitale, auspicando una digitalizzazione che non lasci indietro nessuno. Durante la presentazione, Gobbo ha evidenziato alcuni argomenti del libro, ad esempio di come i ragazzi non siano in realtà «nativi digitali, ma sonnambuli digitali» e di come sia importante ritrovare il gusto di stare assieme con momenti di disconnessione.

È seguita la cerimonia dei DSF AWARD, i premi alle eccellenze italiane del digitale, con Roberto Giurano, presidente dello Scriptorium Foroiuliense, che ha spiegato come i premi siano pezzi unici, realizzati proprio dallo Scriptorium con carta in cotone fatta a mano e un font personalizzato, creati da persone provenienti dal percorso della salute mentale. Ha poi ricordato anche il progetto del calendario di beneficenza, creato con i disegni dei piccoli degenti dell'ospedale pediatrico Burlo Garofolo di Trieste, un'iniziativa che il Digital Security Festival ha aiutato a finanziare. Consegnato da Marco Cozzi, il primo riconoscimento è andato al Presidente Massimiliano Fedriga (ritirato da Francesco Del Prete) 'per lo straordinario sostegno alle iniziative di sensibilizzazione sulla sicurezza digitale". Il secondo, consegnato da Gabriele Gobbo, è stato assegnato a sorpresa a Stefano Gazzella come 'Digital Security Evangelist del festival" per il suo costante e prezioso contributo.

L'ultimo panel, 'Il Dato come strumento di futuro", moderato da Sonia Gastaldi, ha offerto una visione umanistica con Stefano Gazzella che ha proposto una riflessione etimologica: «il dato può essere un valore [...] datum, ciò che è dato è un dono meraviglioso perché manifesta un pensiero, un'idea, un concetto», Michaela Odderoli che ha sottolineato come «rimane essenziale il discorso della difesa umanocentrica della nostra coscienza, perché dobbiamo essere consci che il loro utilizzo può essere fatto solo esclusivamente con la coscienza», Ettore Guarnaccia che ha lanciato un appello alla responsabilità: «non siamo in un film di fantascienza e non verrà nessun supereroe a salvarci. Tocca a noi educare le nuove generazioni a riconoscere i rischi che persino i creatori stessi cercano di evitare». Il panel si è concluso con Alessandro Franchi che ha evidenziato come «il vero problema non è solo difendere i nostri dati e le informazioni, ma anche preservare la capacità e la qualità della nostra coscienza» e Antonio Piva, presidente AICA, che oltre a presentare le Olimpiadi Italiane di Informatica in collaborazione con il Digital Security Festival e il 61° congresso dell'associazione, ha condiviso dati allarmanti: «il 71% degli studenti delle superiori mostrano competenze gravemente insufficienti sulla cybersecurity [...] questo è un divario che dobbiamo colmare».

Le conclusioni sono state affidate all'intero direttivo del Festival, un momento corale che ha riassunto la visione dell'associazione. Il presidente Marco Cozzi ha chiuso con un appello all'azione collettiva, per «iniziare a creare un'epoca migliore», un compito che richiede l'impegno di tutti. Davide Bazzan ha sottolineato l'importanza di fare rete, invitando i professionisti ad «aggregarsi, perché porta grandi vantaggi a tutti». Il tesoriere Luigi Gregori ha ringraziato i partner, «il carburante» che rende possibile un'iniziativa basata sul volontariato. Sonia Gastaldi ha evidenziato la missione del festival: «riuscire ad usare tutti e due gli emisferi del cervello quando abbiamo tra le mani la tecnologia, e saperla spiegare». Infine, il vicepresidente Gabriele Gobbo ha suggerito che il problema non sia la tecnologia in sé, ma una sorta di tendenza al «fallimento sociale per procura» dell'essere umano, riaffermando con forza la missione del festival: «un digitale umanocentrico».

Un ringraziamento speciale è andato a tutti i partner e sostenitori e al conduttore della giornata, il giornalista Giacomo Ferrara, che ha guidato in modo impeccabile il pubblico attraverso quattro ore di intensi lavori. Roma è stata solo la prima tappa. Il viaggio del Digital Security Festival è appena iniziato e proseguirà in tutta Italia, con l'obiettivo di continuare a costruire, insieme, un futuro digitale più consapevole, sicuro e, soprattutto, umano.

Sfide

di Federica Maria Rita Livelli

Dati, cybersecurity e AI: triangolazione perfetta o triangolo delle Bermuda e la sfida alla compliance

La cyber resilience è evoluta da questione meramente tecnica a pilastro fondamentale della nostra libertà e stabilità istituzionale democratica. In un mondo caratterizzato da poli-crisi e perma-crisi, la protezione dei dati e delle infrastrutture digitali costituisce la prima linea di difesa della sovranità nazionale.

Il nuovo paradigma della sicurezza

Viviamo un'epoca in cui la pace non è più scontata, dovendo gestire minacce tradizionali e confrontarci con una nuova dimensione conflittuale: quella cibernetica. È oramai noto che gli attacchi informatici, non rispettano confini geografici e colpiscono simultaneamente settore pubblico e privato, potendo paralizzare intere nazioni senza sparare un singolo colpo.

Pertanto, la cybersecurity rappresenta l'evoluzione naturale del concetto di difesa nazionale. Se, in passato, proteggere la patria significava controllare confini fisici, spazio aereo e acque territoriali, oggi include garantire l'integrità dello spazio digitale, dei dati sensibili e delle infrastrutture critiche che governano la vita quotidiana. Il dominio cibernetico, oggi, costituisce il quinto dominio operativo di sicurezza, insieme a terra, mare, aria e spazio.

L'impatto dell'AI sulla difesa nazionale e sulla cybersecurity

L'Intelligenza Artificiale ha rivoluzionato il panorama della cybersecurity e l'intera concezione della difesa nazionale. Come evidenziato dalla guerra in Ucraina, l'applicazione dell'AI nella difesa è a 360 gradi: dalla logistica all'intelligence, dalla cybersecurity alle operazioni cinetiche.

L'AI offre opportunità strategiche decisive. Nell'intelligence, l'analisi Osint permette di processare enormi quantità di dati pubblici estraendo informazioni strategiche in tempi ridotti. Nel cyberspazio, rappresenta una medaglia dalla duplice faccia, i.e. strumento di difesa e arma offensiva, identificando minacce, oltre ad analizzare pattern di attacco e rispondere in tempo reale, processando miliardi di eventi di sicurezza e individuando anomalie invisibili all'analisi umana.

Tuttavia, l'AI presenta sfide significative sul versante offensivo, in termini di cyberattacchi orchestrati capaci di adattarsi dinamicamente, generare malware polimorfici e condurre campagne di disinformazione su scala industriale.

Governance etica ed equilibrio strategico

Le organizzazioni nell'utilizzo dell'AI devono garantire un utilizzo etico ed un equilibrio strategico che non presuppone il rifiuto della tecnologia, ma la sua governance responsabile. È cruciale implementare controlli rigorosi che garantiscano supervisione umana, definiscano responsabilità e mantengano la possibilità di sovrascrivere decisioni automatizzate dato che, come democrazie occidentali, utilizzare l'AI violando i nostri valori significherebbe aver già perso la partita e mettere in pericolo la nostra libertà.

In quest'ottica, la cybersecurity non limita la libertà: la protegge e la espande: quando cittadini, aziende e società civile possono fare affidamento sull'integrità delle infrastrutture critiche, la libertà di agire, innovare ed esprimersi si amplifica attraverso un approccio "security by design" e "privacy by design".

Ovvero, il raggiungimento della cyber resilience protegge i diritti fondamentali e le basi democratiche. Un ecosistema digitale sicuro richiede, regole chiare, cooperazione internazionale, pratiche etiche e programmi educativi per un uso consapevole delle tecnologie, creando le condizioni per un futuro caratterizzato da fiducia, resilienza e sostenibilità nel rispetto dei diritti fondamentali.

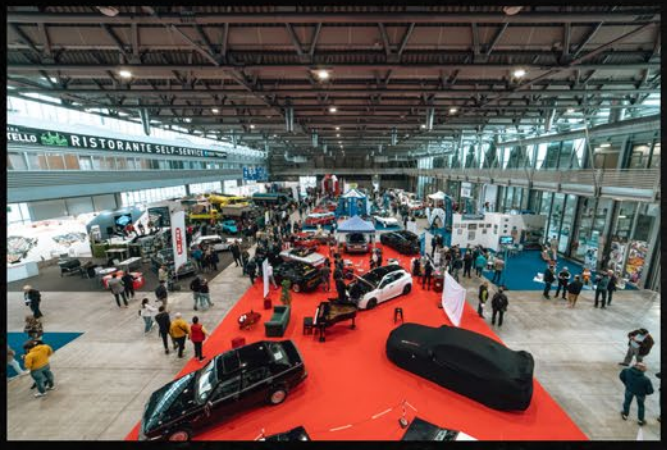
THE FINEST EXPO

ALTO ADRIATICO MOTORI D'EPOCA

RASSEGNA
MEZZI DI TRASPORTO
STORICI E ACCESSORI

FIERA DI PORDENONE

24-25-26 APRILE 2026



UNA MANIFESTAZIONE IN CRESCITA

20.000	150+	15.000
VISITATORI	ESPOSITORI	MQ

PRENOTA IL TUO SPAZIO

- COMMERCIANTI AUTO E MOTO
- MOSTRA SCAMBIO
- RICAMBI E ACCESSORI
- CLUB E REGISTRI STORICI
- RESTAURATORI E DETAILER

www.motori-epoca.it

INFO PER ESPORRE:
motoridepoca@fierapordenone.it
+39 378 3072275

ORGANIZZATORE
Pordenone Fiere
Exhibitions since 1947

PARTNER
PORTOBELLOCAR

MEDIA PARTNER
RUOTECLASSICHE

Idee

di Valerio Nosci

"Io, Dato": sovranità, sicurezza e identità nell'era digitale

Nel cuore dell'universo digitale, il dato è la materia prima che alimenta innovazione, economia, relazioni e potere. Non è più solo un elemento tecnico, ma una risorsa critica, strategica e profondamente umana. Ogni informazione generata, raccolta e analizzata contribuisce a costruire un ecosistema complesso, dove la sicurezza informatica non è più un'opzione, ma una condizione di esistenza. La crescente dipendenza dai dati ha trasformato la loro gestione in una questione di sovranità digitale. Chi controlla i dati controlla le infrastrutture, le decisioni, le identità. Stati, aziende e cittadini si trovano immersi in una nuova geografia del potere, dove i confini non sono fisici ma algoritmici. Il caso TikTok, 'americanizzato" per evitare il ban negli USA, ha mostrato come la proprietà dei dati possa diventare terreno di scontro geopolitico, con implicazioni che vanno ben oltre il mercato.

Anche l'Europa si muove: il Data Act, entrato in vigore nel 2025, impone regole chiare su accesso, condivisione e portabilità dei dati, ridefinendo il concetto di titolarità e responsabilità. Non è più possibile trattare i dati come risorsa interna: ogni flusso deve essere giustificato, tracciabile, legittimo.

Ma c'è un altro livello, più profondo e spesso trascurato: il valore etico del dato. Ogni informazione personale è un frammento di identità. Proteggere i dati significa proteggere le persone, le loro scelte, la loro libertà. In un mondo dove l'identità digitale è sempre più intrecciata con quella reale, la sicurezza non può limitarsi alla difesa tecnica: deve includere principi di equità, rispetto e responsabilità. Il furto di identità digitale è una delle minacce più insidiose. Nel 2017, la violazione di Equifax ha esposto i dati di 147 milioni di persone, con conseguenze devastanti: frodi, debiti non contratti, reputazioni compromesse. In Italia, oltre 120.000 persone sono state vittime di furti d'identità nel solo 2019. Questi episodi mostrano come la violazione del dato sia anche una violazione dell'identità.

La sfida è duplice: da un lato costruire infrastrutture sicure e normative efficaci, dall'altro promuovere una cultura del dato consapevole, dove cittadini e

organizzazioni comprendano il valore e i rischi dell'informazione. In questo universo, la cybersecurity non è solo tecnologia: è etica, politica, educazione. Il futuro della sicurezza informatica passa da qui: dalla capacità di riconoscere il dato non solo come oggetto da proteggere, ma come soggetto da rispettare. Perché nell'universo dato, ogni bit è una storia, ogni accesso è una responsabilità, ogni violazione è una ferita.

Patrocini e collaborazioni

Digital Security Festival alla Camera dei Deputati: Lettera del Presidente DSF Marco Cozzi

Roma è un luogo emblematico, carico di storia e significato per tutti noi cittadini. Con grande emozione annuncio che il Digital Security Festival inaugurerà la sua settima edizione alla Camera dei Deputati, nella prestigiosa Sala Giacomo Matteotti, il 19 settembre 2025. È una tappa importante, simbolica e concreta allo stesso tempo. Portare il Festival nella sede della rappresentanza democratica per eccellenza non è solo un riconoscimento per il lavoro svolto finora, ma soprattutto un segnale: la cultura della sicurezza digitale è un tema nazionale, trasversale e centrale.

Quest'anno abbiamo scelto come titolo dell'edizione 'Universo Dato". Perché tutto, oggi, ruota attorno ai dati: quelli che ci raccontano, ci descrivono, ci rappresentano. Dati da proteggere, comprendere e valorizzare. Il nostro obiettivo è aiutare tutti, cittadini, imprese, studenti e istituzioni, a vivere questa trasformazione con consapevolezza, strumenti concreti e spirito critico. Per l'occasione, abbiamo anche prodotto un trailer ufficiale che ritrae una Roma del futuro, realizzata con intelligenza artificiale generativa e poi rifinita a mano. È un piccolo manifesto visivo del nostro approccio: tecnologia e umanità, insieme, per costruire un domani più sicuro e più giusto.

Il Festival, nato in Friuli Venezia Giulia, ha negli anni esteso il suo respiro a livello nazionale. Ma arrivare a Montecitorio rappresenta per noi un punto di svolta. È la conferma che il dialogo tra cultura digitale e istituzioni è possibile, anzi necessario. E che l'Italia può e deve essere protagonista in Europa nel promuovere una cittadinanza digitale consapevole. Roma sarà solo la prima di una serie di tappe che ci porteranno in diverse città italiane: Udine, Treviso, Montebelluna, Trieste, Como, Palmanova e Padova. Ogni tappa sarà un'occasione per ascoltare, confrontarci, imparare. E soprattutto per fare rete.

Un ringraziamento speciale va a tutto il direttivo e ai soci fondatori del Digital Security Festival, il cui impegno quotidiano, volontario e appassionato rende possibile questo progetto, anno dopo anno. In un'associazione di promozione sociale, il contributo di chi crede nella missione prima ancora che nei risultati è semplicemente essenziale. Questo traguardo è anche e soprattutto il loro.

Il Digital Security Festival 2025 sarà, ancora una volta, un momento corale. Una festa della conoscenza, della responsabilità e dell'innovazione. A partire dalla Camera dei Deputati. →

NetApp®

Rendiamo l'infrastruttura

DATI INTELLIGENTE