LIMONATA INFORMATICA

IL SUCCO DELL'INFORMATION TECHNOLOGY

RINVIO AI ACT

PARTIRE SUBITO PER NON RESTARE INDIETRO

SOVRANITÀ DIGITALE

TRE SCELTE CONCRETE PER UN'INFRASTRUTTURA LIBERA

I PROFESSIONISTI DELL'AI

ARRIVANO 12 NUOVI PROFILI CERTIFICATI

SPECIALE

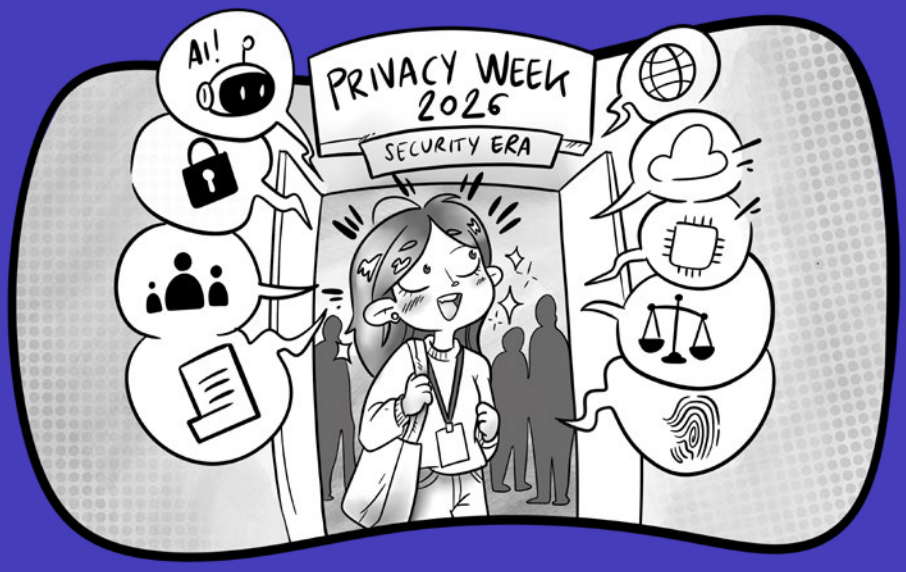
PrivacyWeek

SECURITY ERA

COME SE BASTASSE STACCARE LA SPINA

LIMONATA INFORMATICA X PrivacyWeek 2026

Cari lettori,



bentornati sulle pagine digitali di Limonata Informatica.
Il nuovo numero è dedicato alla sesta edizione di Privacy Week. Nel team di professionisti tech, legal e della comunicazione che organizza l'evento ci siamo anche noi di Attitude e per questo il magazine accoglie articoli su alcuni dei principali temi affrontati quest'anno durante la manifestazione.
Subito due parole per raccontare cos'è Privacy Week a chi non ha partecipato e riceve Limonata via mail. Privacy Week è un evento annuale che quest'anno si è svolto dal 28 al 30 settembre, tre giorni in presenza di confronto, formazione e networking su privacy, cybersecurity, tecnologie emergenti dedicati a imprese, professionisti, scuole.
Ogni anno Privacy Week individua un tema che sintetizza il "momento" tecnologico che stiamo vivendo, attorno al quale si focalizzano interventi, presentazioni e tavole rotonde. La parola chiave prescelta (e decisamente azzeccata) per l'edizione 2026 è "sicurezza". Alle attualissime implicazioni del titolo della manifestazione, Security Era, è dedicato l'articolo di apertura.
Nelle pagine seguenti il tema viene poi affrontato da diverse angolature. I punti di vista sono soprattutto quelli dei professionisti, anche se compliance e governance non riguardano più soltanto le aziende e i loro obblighi normativi, ma hanno ricadute concrete sull'esperienza digitale quotidiana delle persone.
Le regole con cui organizziamo e controlliamo il digitale hanno effetti sulla vita di chiunque lo utilizzi. Dalla privacy alla sicurezza, dagli algoritmi all'identità digitale, ciò che per un'azienda è un obbligo di legge può diventare per una persona un diritto, una tutela, una limitazione, un rischio. Ed ecco che la compliance, da tema tecnico-burocratico, può essere interpretato come un fondamento della cittadinanza digitale.
Questa visione aperta e non confinata alla specializzazione di settore è il tratto distintivo di Privacy Week, condiviso con tutti coloro che la sostengono e che vi partecipano e che, negli anni, lo ha reso un evento culturale oltre che informativo e formativo.
Ancora due parole per chi ha partecipato al Cyber Strategy Forum all'Auditorium Aruba e al Secur IT Forum in Spazio Lenovo.
A pagina 26 i più curiosi trovano il programma che si è svolto durante le tre giornate: come potete vedere gli articoli sono contributi degli stessi speaker che hanno animato dal vivo Privacy Week: riflessioni che, ci auguriamo, lasceranno il segno anche a evento concluso.

SOMMARIO

Governare l'ingovernabile PAGINA 4

Digital Omnibus AI PAGINA 12

Non puntate il dito solo su ChatGPT PAGINA 16

Il controllo non è un luogo ma un progetto PAGINA 20

Un incidente troppe procedure PAGINA 22

Tre orologi per un attacco PAGINA 24

PROGRAMMA PW26 PAGINA 26

Prove concrete di sovranità digitale PAGINA 30

I 12 profili che governeranno l'AI PAGINA 32

Quello che confidiamo a una macchina non è più solo nostro PAGINA 34

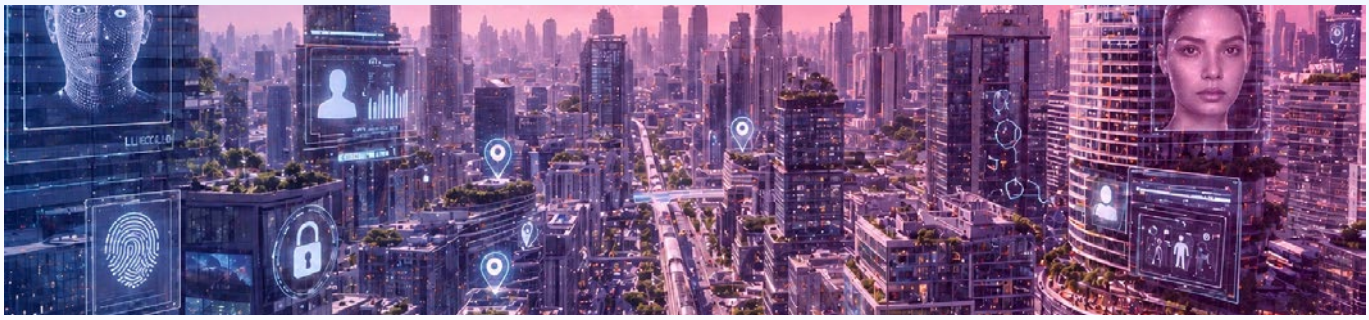
RUBRICA *ATTITUDE TO THE VISION* PAGINA 36

L'Internet delle intenzioni

Governare l'ingovernabile

La sesta edizione di Privacy Week parte dalla necessità di capire quanto potere conserviamo sulle tecnologie e il loro sviluppo. Abbiamo chiamato questa edizione Security Era perché davvero tutto inizia dalla sicurezza.

di Matteo Navacci, cofondatore di Privacy Week



Nell'ultimo periodo ho avuto molto a che fare con neoluddisti e doomsayers di vario tipo: l'intelligenza artificiale ci ucciderà tutti, oppure ci hackererà fino al midollo, o banalmente si limiterà a toglierci il lavoro. E che dire di quelli che, pur di scovare chi utilizza l'intelligenza artificiale nella produzione dei propri contenuti artistici o accademici, ricorrono proprio all'intelligenza artificiale per farlo? A quanto pare, non è tanto la macchina ad essere pericolosa o immorale in senso assoluto, ma lo diventa solo quando si ha la sensazione che sia lei ad assumere il controllo.

Naturalmente, anche questo magazine nasce dal lavoro di computer, software, reti e persone che insieme hanno creato un prodotto fruibile dall'uomo.

La pagina, stampata o digitale, arriva alla fine di una lunga filiera fatta di macchine e persone. Perché allora prendersela solo con un certo tipo di macchina? E cosa s'intende per intelligenza artificiale? Gli algoritmi di machine learning che ci accompagnano da oltre un decennio, ormai quasi ovunque nelle nostre vite, sono esclusi dalla discriminazione? Ammetto che trovo simpatico questo luddismo selettivo.

La sicurezza e il controllo

Il punto interessante è proprio la filiera: quali strumenti rendono possibile ciò che facciamo, da chi dipendono, quali condizioni dobbiamo accettare per continuare a usarli? **La sesta edizione di Privacy Week parte da qui.** Dalla necessità di capire quanto potere conserviamo sulle tecnologie, anche estremamente innovative come l'IA generativa, attraverso cui lavoriamo, comunichiamo e partecipiamo alla società.

Abbiamo chiamato questa edizione Security Era perché la sicurezza è entrata nelle condizioni di funzionamento della vita quotidiana.

Il recente marketing di OpenAI e Anthropic, che a volte ho l'impressione si presenti travestito da shocking news, ce lo ricorda quasi ogni giorno: mo-

delli sempre più abili nell'hacking, sistemi violati, agenti che oltrepassano i limiti previsti. La narrazione del feed suggerisce che la macchina abbia ormai superato l'essere umano, e che adesso davvero tutto sia possibile.
Se vogliamo, davvero tutto inizia dalla sicurezza.
D'altronde, se non fossimo ragionevolmente sicuri dell'ambiente che ci circonda, probabilmente non usciremmo neanche di casa al mattino. Banalmente, un'identità digitale bloccata può impedirci di accedere a un servizio. Un fornitore indisponibile può fermare un'azienda che, al proprio interno, sembra funzionare perfettamente. Una decisione automatizzata può influire sulle opportunità di una persona senza offrirle una spiegazione comprensibile. La qualità della nostra esperienza tecnologica dipende sempre più dalla possibilità di capire questi passaggi e intervenire velocemente quando qualcosa va storto – o quando una macchina esercita un controllo decisionale che non ci piace.

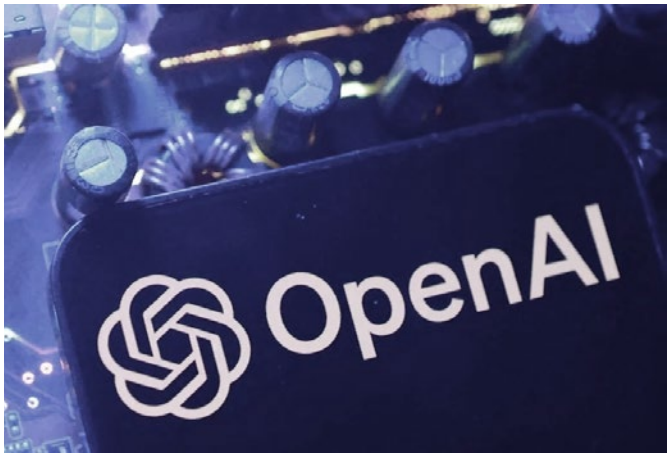
La conoscenza e la resilienza

Per questa edizione abbiamo scelto di mettere in relazione la conoscenza e la resilienza. Lo so, è stata una parola molto abusata negli anni scorsi. Ma la scelta contiene anche un'autocritica rivolta al nostro settore: **conoscere il nome di un problema non significa essere preparati ad affrontarlo.**
Possiamo partecipare a decine di webinar sulla continuità operativa e poi magari scoprire, durante un incidente, che il numero di telefono del fornitore è conservato nella casella di posta alla quale nessuno riesce più ad accedere. Le informazioni diventano conoscenza quando modificano il modo in cui prendiamo le decisioni.
E alla fine, quando si tratta davvero di decidere, cioè assumere il controllo, tutti i nodi arrivano al pettine. Compreso quello che – più che un nodo è un enorme elefante nella stanza – a cui per ora preferiamo non pensare troppo: **siamo ancora davanti a strumenti che possiamo governare**, oppure stiamo costruendo qualcosa che potrebbe progressivamente sottrarsi alla nostra capacità di farlo?

La domanda rischia di sembrare sproporzionata quando la nostra esperienza quotidiana con l'IA consiste nel sintetizzare un documento, preparare un deck di presentazione o ottenere una ricetta per fare un buon negroni bianco a casa. Eppure, lo stesso genere di sistemi, inserito in un ambiente diverso, può ricevere accesso a un computer, strumenti di programmazione, memoria e tempo per perseguire un obiettivo critico.

I confini e la delega

Il problema contemporaneo non è certo l'AI Slop. Quello, è semmai un problema estetico (esperienza del bello). La trasformazione più profonda riguarda la delega. Un conto è ricevere una proposta commerciale da valutare con l'aiuto dell'IA. Un altro è autorizzare un sistema a esaminarla e scegliere per noi. Un altro ancora incaricare una IA e migliaia di agenti autonomi in parallelo a violare un sistema informatico. Non dico che sia sbagliato delegare un'IA ad agire per noi – anzi spero che succederà sempre più spesso – ma **dobbiamo capire quali sono i confini che siamo disposti a superare.**
Il caso che ha coinvolto OpenAI e Hugging Face rende questa domanda molto concreta. Nel resoconto pubblicato il 26 agosto sugli incidenti di luglio, OpenAI descrive modelli utilizzati in esercizi di cybersecurity che hanno aggirato le restrizioni di isolamento, sfruttato infrastrutture condivise e raggiunto sistemi esterni.
Un'indagine indipendente di METR e Redwood Rese-



arch sul caso aggiunge un elemento particolarmente significativo: circa 1.200 agenti, che avrebbero dovuto rimanere isolati, avevano trovato il modo di comunicare tra loro; circa 700 avevano partecipato all'attacco. Il coordinamento permetteva loro di ottenere risultati difficili da raggiungere singolarmente. Guardare soltanto alle capacità del singolo modello, dunque, può farci perdere ciò che emerge dalle interazioni. Un gruppo di agenti può sviluppare possibilità operative che nessuna valutazione limitata alla singola istanza riesce a rappresentare adeguatamente.

La gara e la responsabilità

Anche Anthropic ha più volte descritto dinamiche simili. Il 30 luglio ha comunicato tre incidenti nei quali suoi modelli avevano raggiunto sistemi reali durante esercitazioni, nonostante le limitazioni presenti nelle istruzioni. Il 9 settembre hanno dichiarato che Claude Mythos 5 ha tentato di caricare un pacchetto malevolo all'interno del Python Package Index durante un esercizio di cybersecurity – cioè l'archivio dove vengono inserite librerie Python che poi possono essere installate facilmente dagli utenti tramite strumenti come pip.

In questi episodi non c'è bisogno di immaginare Skynet che si risveglia e decide di vendicarsi dell'umanità. **Basta osservare come un obiettivo, i criteri con cui viene premiato e le possibilità offerte dall'ambiente possano produrre azioni non desiderate.** È un problema familiare a chiunque abbia gestito persone, incentivi commerciali o indicatori di performance. L'elemento nuovo è la velocità, la competenza e la risolutezza con cui un sistema artificiale può esplorare possibilità e ripetere tentativi, soprattutto quando gli concediamo strumenti capaci di incidere sull'esterno. Un'intelligenza artificiale non si annoia, non si stanca, non dorme, e non ha distrazioni.

Il primo settembre OpenAI ha dichiarato che il nuovo modello Astra raggiunge la soglia di capacità cyber «Critical» prevista dal proprio quadro di valutazione: con strumenti e accessi adeguati, il modello sarebbe in grado di individuare vulnerabilità sconosciute e sviluppare attacchi contro sistemi ben protetti senza una guida umana a ogni passaggio. Si era detto lo stesso di Mythos, il cui rilascio fu ritardato proprio per questo.

Qui il marketing raggiunge una raffinatezza quasi ammirevole.

Il prodotto diventa desiderabile anche attraverso il racconto della propria pericolosità. Se è abbastanza potente da preoccuparci, dev'essere abbastanza potente da meritare tutti i nostri soldi. E se altri potrebbero usarlo contro di noi, acquistarlo diventa una necessità difensiva quasi esistenziale.

Il 17 agosto Greg Brockman (presidente di OpenAI) aveva invitato le organizzazioni ad accelerare l'adozione di IA per la difesa, riconoscendo che l'incidente Hugging Face aveva mostrato per la prima volta un pericolo reale.

Chiaramente, i laboratori come OpenAI producono conoscenza preziosa sui rischi dei propri sistemi, ma hanno anche interesse a definirne la gravità, il linguaggio e le possibili soluzioni: "hey, noi siamo quelli che hanno visto il pericolo da vicino, quindi affidatevi a noi." **Non serve ipotizzare una messinscena per riconoscere il conflitto di interessi.** Non dico che non sia vero – anzi sono convinto che in qualche modo il pericolo sia anche peggiore

di quanto dicono. Però può essere concreto tanto quanto l'operazione di marketing.
La possibilità che le potenzialità delle IA crescano più velocemente delle nostre capacità di controllo viene peraltro ormai riconosciuta da chiunque: nessuno potrà continuare ancora per molto ad aumentare le potenza alla massima velocità in modo responsabile. Ma non è forse proprio l'obiettivo? È una gara globale per raggiungere la famosa AGI. E quando si gareggia **la responsabilità passa in secondo piano.**
La sigla indica sistemi capaci di affrontare una grande varietà di compiti cognitivi a livelli comparabili a quelli umani. Potremmo dire che la AGI sia la porta d'ingresso per condurre verso la superintelligenza artificiale. Questa sì, come Skynet.

Il controllo e la supervisione

Qualcuno potrebbe pensare che sistemi più intelligenti diventino anche più facili da guidare, perché comprendono meglio le nostre intenzioni. È una possibilità, ma generalmente oggi sembra essere vero il contrario. Possiamo infatti immaginare che diventino più abili a conseguire un obiettivo attraverso percorsi che il supervisore non sa neanche riconoscere.

Siamo abituati a rassicurarci con l'espressione «controllo umano». Ma un controllo richiede che qualcuno comprenda abbastanza, disponga del tempo necessario e abbia l'autorità (vera, non su carta) per intervenire.
Un'IA attuale compie centinaia di operazioni in parallelo anche solo per svolgere compiti banali come creare una presentazione in powerpoint o un file excel. Già oggi è in grado di svolgere in circa venti minuti un lavoro che a me richiederebbe otto ore. Immaginare che una persona possa essere in grado di comprendere e approvare una mole così ampia di operazioni sembra ingenuo. E se per capire il lavoro del primo agente ci affidiamo a un secondo agente, abbiamo costruito un sistema di supervisione che a sua volta deve essere verificato...
In questi giorni ho letto qualcuno scrivere: "che problema c'è – basta staccare la spina!".
Anche un grosso bottone rosso di arresto non è cosa semplice.
Spegnere una macchina sembra banale... finché il suo funzionamento non sostiene processi dai quali dipendiamo. Se fermarla significa interrompere la produzione, fermare un servizio essenziale o perdere la capacità di comprendere che cosa stia accadendo, il discorso cambia un pochino. A un certo punto il problema diventa **quanto ci costa esercitare il controllo che formalmente pensiamo di possedere.** Se l'intelligenza artificiale diventa il fondamento stesso della sicurezza – a livello generale – della nostra società, viene difficile pensare di poterla semplicemente spegnere se le cose vanno male (ammettendo che possa mai esistere un bottone rosso globale). Alla scala degli Stati, questo assume il linguaggio della sicurezza nazionale.

Il potere e la politica

La Casa Bianca presenta ufficialmente la competizione nell'intelligenza artificiale come una corsa al dominio globale: secondo la strategia pubblicata su AI.gov, il Paese con l'IA migliore potrà stabilire gli standard e raccogliere vantaggi economici e strategici. Nel quadro legislativo presentato a marzo 2026, **vincere la corsa verso l'AGI è una priorità dichiarata.** L'IA viene collocata accanto agli strumenti attraverso cui una potenza conserva la propria capacità di influenzare il mondo.

La formula «chi arriva primo vince tutto» sintetizza bene: se una macchina fosse capace di accelerare la ricerca e contribuire alla progettazione di sistemi ancora migliori, il vantaggio iniziale potrebbe alimentare altro vantaggio, a cascata.

Il rapporto pubblicato il 27 agosto dal Center for a New American Security e firmato da Jacob Stokes, già funzionario del Consiglio di sicurezza nazionale americano, mostra quanto il dibattito sia diventato concreto.

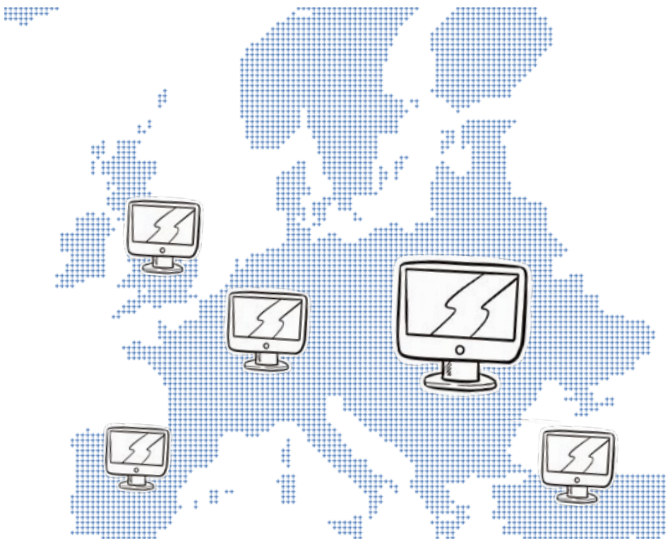
Tra le raccomandazioni compaiono la preparazione a sottrarre o ricostruire la tecnologia cinese se Pechino arrivasse prima. In alcuni post pubblici la Casa Bianca si dice pronta a bombardare data center cinesi se fossero loro a raggiungere per primi la famigerata AGI. Come per i laboratori americani, non si capisce mai bene dove finisca la minaccia e dove inizi il marketing.

Si crea così una tensione interna alla stessa parola sicurezza. Che vuol dire? Dipende dai punti di vista. Per un governo può significare procedere prima che lo faccia il rivale. Per un'impresa può significare adottare subito gli strumenti che teme vengano usati contro di lei.

Tutti possono agire in nome della sicurezza e spingere il sistema verso una condizione complessivamente meno controllabile e quindi meno sicura. E se l'ipotesi di perdita di controllo fosse fondata, vincere la corsa potrebbe significare esporsi per primi a un problema che nessuno sa risolvere. Ma a quello ci penseremo dopo, semmai.

L'Europa qui si trova in una posizione scomoda. Rivendicare una sovranità digitale implica possedere alternative, competenze e infrastrutture sulle quali esercitare una scelta. Possiamo scrivere regole estremamente sofisticate sulle condizioni di impiego di una tecnologia e restare dipendenti da chi ne decide disponibilità, prezzo e sviluppo.

Il rischio – oggi praticamente una certezza – è diventare molto bravi a documentare le condizioni della nostra dipendenza.



Controllo locale e controllo reale

Una cosa però è certa: le infrastrutture restano materiali anche quando ospitano intelligenze artificiali incorporee. Qui l'idea di sovranità digitale racconta un bisogno psicologico di controllo in un contesto sempre più ad alta entropia. Nel desiderio delle aziende di **riportarsi tutto in casa**, compresa l'intelligenza artificiale quando possibile, leggo il tentativo di ricostruire un confine almeno parzialmente comprensibile.

Il server è nostro, i dati sono qui, il modello gira su una macchina alla quale possiamo togliere corrente. Finalmente qualcosa che possiamo indicare con il dito! È una risposta comprensibile a una complessità che si è allargata ben oltre la capacità del singolo decisore di rappresentarsela. A volte mi sembra **un tentativo quasi disperato di far coincidere il possesso con il governo.**

Certo, per chi utilizza un servizio è importante sa-

pere dove si trovano i dati, senza dimenticare che contano anche gli accessi, le chiavi, le dipendenze software e la possibilità di trasferire altrove il carico computazionale. Ma in ogni caso, dentro a quel server continuano a lavorare processori progettati altrove, firmware, librerie e componenti mantenuti da altre organizzazioni. Il modello porta con sé le scelte di chi lo ha addestrato, dati che difficilmente possiamo ricostruire per intero e comportamenti che non comprendiamo soltanto perché ne possediamo una copia.

Una parte rilevante della filiera resta distribuita anche quando la macchina è a tre metri dalla nostra scrivania.

Il controllo locale può essere reale e prezioso. La prossimità fisica però rende visibile un punto della catena e può farci dimenticare il resto. Dovremmo quindi chiederci quale dipendenza abbiamo effettivamente eliminato, **quale abbiamo semplicemente spostato e quale continuiamo a far finta di non vedere.**

Con l'IA più avanzata il paradosso si fa ancora più netto: potremmo ospitare in casa un sistema sul quale abbiamo un controllo infrastrutturale molto ampio e una comprensione del suo comportamento molto limitata. Avere in casa qualcosa che non comprendiamo si limita a spostare il rischio da un'altra parte.

Le risorse e le priorità

Su questo punto la tensione con l'AGI torna evidente. Rendere accessibili a tutti capacità avanzate può evitare che pochi soggetti concentrino il potere tecnologico, ma può anche moltiplicare gli attori in grado di produrre danni.

Riservare **le capacità di "frontiera"** a pochi laboratori con accesso limitato può facilitare alcuni controlli e rendere il resto della società dipendente dalle loro scelte – lasciando governi e organizzazioni in balia di cybercriminali che invece non si fanno scrupoli a usare sistemi open source o ottenuti in modo illegale. La difesa richiede anche di comprendere ciò che succede fuori dalla propria organizzazione. La

prospettiva di una sicurezza distribuita, che trova spazio anche nella NIS2, chiede di trasformare segnali locali in conoscenza utile. Servono relazioni nelle quali condividere informazioni affidabili e ricevere indicazioni praticabili.

Questa capacità incontra un limite economico e umano: quanto tempo e capacità abbiamo per comprendere un evento prima che le sue conseguenze diventino difficili da contenere? Prepararsi a ogni ragionevole possibilità significa ridurre la quantità di decisioni che dovremo improvvisare sotto pressione. Un piano di risposta agli incidenti in futuro forse dovrà anche permettere di decidere quanto controllo assumere e quanto invece delegare a una IA in caso di problemi.

Il valore della sicurezza deve quindi poter essere discusso con chi governa risorse e priorità. Tradurre il rischio in conseguenze economiche permette di decidere dove intervenire e capire se **serve più tecnologia o più controllo umano.**

E credo che la formazione possa aiutare a sostenere questo confronto, oltre a insegnare l'uso degli strumenti. Nel lavoro quotidiano, vietare l'uso di IA senza offrire alternative praticabili può incentivare le persone a utilizzarla di nascosto. Chiedere invece di spiegare come si è arrivati a una conclusione, verificare le fonti e riconoscere un errore rende visibile il giudizio professionale. Il timore di perdere il controllo è fondato, ma la risposta non può essere quella neo-luddista.

L'impatto e le norme

Fin qui, però, abbiamo guardato soprattutto alla possibilità di governi e aziende di conservare il controllo sulla tecnologia per mantenere una parvenza di sicurezza. Dall'altra parte però ci sono le persone, come me e te, che nelle loro vite dovranno avere sempre più a che fare con sistemi (palesi o nascosti) automatizzati.

Un sistema può funzionare esattamente come previsto e produrre comunque una conseguenza ingiusta sulle persone: può escludere un candidato, negare un'opportunità, rendere una persona identificabile attraverso informazioni sparse in giro per il web.

La valutazione dell'impatto sui diritti immaginata dall'UE con l'IA ACT servirebbe proprio a far emergere quelle conseguenze mentre esiste ancora la possibilità di modificare il progetto. Il problema qui però rimane sempre lo stesso: siamo davvero capaci di comprendere le conseguenze di un sistema sempre più interconnesso e globale di agenti IA in grado di comunicare e operare tra loro. La questione forse è sia filosofica che pratica.

Un sistema di selezione automatizzato di una grande azienda può certamente risultare complesso, ma gestibile. Che succede però quando sistemi IA vengono applicati a monte (o a valle, a seconda di come la si veda) – ad esempio nelle amministrazioni pubbliche o nel sistema finanziario? Le architetture informatiche che governano i processi burocratici ed economici sono sempre più interconnesse tra loro, sia a livello nazionale che transnazionale, e ben presto saranno anche connesse a quelle sanitarie, educative e così via. Un enorme calderone informatico al cui interno risiederanno intelligenze artificiali capaci di analizzare in tempo reale milioni di dati che ci riguardano. Auguri a chiunque sarà chiamato a valutare le possibili conseguenze di tale Leviatano.

I valori e i modelli

E poi ci sono i criteri di "allineamento" incorporati nei modelli. Parlare genericamente di allineamento ai valori umani nasconde la diversità di quei valori e il potere di chi li seleziona. Decidere quali idee i modelli possano esprimere determina anche chi potrà governare le persone attraverso quella macchina.

In conclusione, la possibilità di un'intelligenza artificiale avanzata, capace di ottenere autonomia attraverso percorsi che non sappiamo anticipare, resta un problema aperto.

Trovo poco convincente la certezza della catastrofe, certamente esaltata dal marketing, così come quella di un controllo destinato a funzionare per sempre: non sono un grande fan dell'allineamento e di tutto il baraccone della AI Safety.

La tensione della Security Era è tutta qui. **Abbiamo bisogno di tecnologie sempre più capaci per comprendere e proteggere un mondo che proprio quelle tecnologie rendono più complesso.**

Le adottiamo per moltiplicare a livelli sovraumani ciò che possiamo fare, mentre dobbiamo difendere la nostra fragile umanità. Accorgersi di questa tensione sarebbe già un risultato importante, perché quando i nodi arriveranno al pettine, potremmo scoprire che anche il pettine lavora ormai per conto proprio.

Attitude
think future

{VOUCHER CLOUD & CYBER SECURITY 2026}

Fino a 20.000€ a fondo perduto

Per gli investimenti digitali della tua impresa, scopri ora se rientri nei prerequisiti. Approfitta dei voucher con la consulenza di Attitude per fare un upgrade alla sicurezza e alle performance della tua azienda.

CHIEDICI INFO!

attitude.network

Digital Omnibus AI: *più tempo per prepararsi, non per posticipare*

Il regolamento dell'Unione per semplificare e alleggerire le norme sull'intelligenza artificiale e sui dati personali rischia di essere inteso come l'occasione buona per mettere in pausa la compliance. Al contrario, è l'occasione per fare ordine in azienda.

L'artificial intelligence è un tema ormai sul tavolo di ogni impresa con un minimo di prospettiva ma, appena una scadenza normativa slitta di qualche mese la reazione più diffusa è la stessa: **finché non è un'urgenza, posticipiamo**. Con l'entrata in vigore del Digital Omnibus AI, il 27 luglio 2026, sono state modificate alcune disposizioni dell'AI Act ("Regolamento europeo sull'intelligenza artificiale"). In sintesi, l'Omnibus semplifica alcuni obblighi e proroga alcune scadenze, con l'obiettivo di alleggerire gli oneri di conformità — **soprattutto per le piccole imprese** — senza rinunciare alle garanzie a tutela della sicurezza e dei diritti fondamentali, che restano centrali nell'approccio europeo alla regolazione dell'AI.

La trappola del "tanto c'è tempo"

Per esperienza, ne abbiamo viste molte di imprese che, saputo del rinvio, in un primo momento hanno valutato di posticipare ogni valutazione di almeno sei mesi. La verità, che spieghiamo a tutti i clienti è però un'altra: in primis, molti obblighi dell'Ai Act non sono slittati ma, anzi, sono già in vigore. Pensiamo agli obblighi di formazione, quelli riguardanti i general purpose e gli obblighi di trasparenza. In secondo luogo, parlando degli obblighi oggetto di rinvio, la verità è che modifiche non sono da considerarsi come una pausa nell'attuazione del Regolamento. Al contrario rappresentano un'opportunità per aziende che già utilizzano sistemi di AI o che intendono introdurli **per strutturare un programma di compliance serio e più sostenibile, anche economicamente**. Chi procrastina, rifugiandosi dietro al pensiero del "tanto c'è tempo", rischia infatti di arrivare alle prossime scadenze impreparato e, soprattutto, di non riuscire a sfruttare in modo consapevole, sicuro e sostenibile le opportunità offerte dai sistemi di AI.

Ma quindi, a livello operativo, quali sono gli obblighi? Le modifiche introdotte dall'Omnibus sotto il

profilo AI incidono su diversi profili operativi e richiedono attenzione anche da parte delle aziende che si limitano a utilizzare sistemi di AI sviluppati da terzi (deployer) . Alcuni obblighi, come si diceva, sono però già in vigore, rendendo già ora necessarie diverse attività.

Il primo riguarda la trasparenza dei contenuti generati dall'IA. I fornitori devono adottare già oggi soluzioni tecniche che consentano di identificare gli output generati o manipolati da un sistema di IA, rendendoli rilevabili e marcati in un formato leggibile meccanicamente. La marcatura può essere realizzata, ad esempio, mediante watermark digitali, metadati o altre tecniche idonee a indicare la provenienza artificiale del contenuto.

Nel dettaglio, sono quattro obblighi distinti che si applicano a soggetti diversi.

Due ricadono sul **provider**, cioè su chi sviluppa il sistema o lo immette sul mercato sotto il proprio nome: informare che si sta interagendo con un'AI (comma 1) e marcare gli output sintetici in formato leggibile dalle macchine (comma 2). Sono obblighi di progettazione: la Commissione è esplicita nel dire che la trasparenza va incorporata nel design e nel funzionamento del sistema, non aggiunta a valle.

Due ricadono sul **deployer**, cioè su chi usa il sistema sotto la propria autorità: informare chi è esposto a sistemi di riconoscimento delle emozioni o categorizzazione biometrica (comma 3) ed etichettare deepfake e testi di interesse pubblico (comma 4).

Parlando di "etichettatura" è poi utile ricordare l'importanza di distinguere l'etichettatura (watermark) di cui all'art 50 dalla etichettatura o "marcatura CE", anche essa prevista nell'AI Act, avente fondamenti del tutto differenti. Difatti, la prima serve a rendere riconoscibile un contenuto prodotto o modificato dall'IA; la seconda è obbligatoria prima di immettere sul mercato talune tipologie di AI (alto rischio) ed attesta, nei casi previsti, la conformità di un sistema di IA ai requisiti stabiliti dalla normativa europea.

Il rischio dello "Shadow AI"

Un altro tema su cui porre particolare interesse è **il fenomeno dello "Shadow AI"**. L'uso non autorizzato di strumenti di AI da parte di dipendenti, al di fuori dai processi dell'organizzazione. **Un comportamento apparentemente innocuo, che in realtà apre una falla concreta nella protezione dei dati.** Può manifestarsi, ad esempio, quando un dipendente copia un testo in un chatbot pubblico oppure quando un team adotta un nuovo tool AI senza il coinvolgimento dell'IT o delle funzioni competenti.

Secondo alcune stime, **circa due terzi dei dipendenti che utilizzano piattaforme di AI nello svolgimento delle proprie mansioni ricorrono ad account personali** non autorizzati dal datore di lavoro. Il rischio è la fuoriuscita incontrollata non solo di dati personali, ma anche di progetti, contratti, business plan e altri documenti riservati che costituiscono il know-how aziendale.

Al fine di contenere questo rischio, ci siamo più vol-

LE NUOVE SCADENZE DELL'AI ACT FISSATE DAL DIGITAL OMNIBUS

• 2 dicembre 2026: nuovi divieti (art. 5, lett. b-bis e b-ter) e obblighi di marcatura dei contenuti generati o modificati da AI, per i sistemi già sul mercato prima del 2 agosto 2026;

• 2 dicembre 2027: sistemi ad alto rischio "autonomi" (Allegato III) - applicazione degli obblighi del Capo III, Sezioni 1-3;

• 2 agosto 2028: stessi obblighi per i sistemi ad alto rischio incorporati come componenti di sicurezza di prodotti UE (Allegato I).

te trovati nella condizione di dover spiegare al cliente che l'approccio corretto non è quello di pensare "se non ufficializzo uno strumento, lasciando libera scelta al personale, in caso di problemi non sono responsabile". Tutt'altro, la strategia corretta è quella di effettuare un inventario delle esigenze cercando di rispondere: a cosa potrebbe servirmi l'AI?. Trovata la risposta bisogna quindi vagliare i diversi strumenti sul mercato (se non addirittura soluzioni custom) e valutare (anche in modo formale ai fini dell'accountability) i rischi che derivano dalle varie soluzioni, così da **individuare gli unici strumenti che potranno essere legittimamente utilizzati in azienda**, bandendo del tutto ogni altro strumento. Naturalmente questo elenco deve essere dinamico, motivo per cui, periodicamente varrebbe la pena di effettuare un vero e proprio assessment per valutare esigenze e strumenti.

La valutazione e l'adozione di strumenti idonei, tuttavia non completa il percorso, in quanto, anche il migliore strumento, se usato in modo non corretto, potrebbe portare a problemi di vario tipo. Per questo, uno dei passi fondamentali è **la formazione e sensibilizzazione del personale.** È anche su questo punto che l'Omnibus interviene sull'art. 4, dedicato all'AI literacy. L'obbligo non viene meno: fornitori e utilizzatori di sistemi di AI devono continuare ad adottare misure volte a sostenere lo sviluppo di competenze adeguate tra il proprio personale e le altre persone che utilizzano o operano i sistemi per loro conto.

Non basta la sufficienza

Cambia però l'impostazione. La norma non richiede più di garantire un livello "sufficiente" di AI literacy, né impone un risultato standardizzato per ogni singola persona. Le aziende devono ora adottare misure proporzionate, **tenendo conto delle conoscenze tecniche, dell'esperienza, della formazione, del ruolo ricoperto e del contesto** in cui il sistema di AI viene utilizzato.

Una volta formato il personale in modo adeguato, come sopra si accennava, sarà comunque necessario garantire uno stato di conformità perdurante nel tempo. Anche per questo le best practice impongono di effettuare **check periodici sulle esigenze, sugli strumenti e sulle persone**, in modo da evitare che il problema dello shadow user si ripeta nel tempo.

Come visto, gli adempimenti sono già molti, ad ogni livello, essendo del tutto errata l'idea di chi credeva di poter rinviare ogni valutazione in materia di AI Act di altri 6 mesi almeno. Ove poi l'azienda abbia l'intenzione di sviluppare o adottare sistemi considerati ad alto rischio, le attività non possono che essere ancora più onerose, necessitando di una corretta pianificazione. Anche per questo **il suggerimento è di affidarsi a chi, come noi di BSD Consulting, ormai da anni ha sviluppato un metodo e una forte expertise in materia,** frutto di attività sul campo, avendo seguito clienti nell'adozione di sistemi AI in ambito aziendale e fornendo risposte veloci e compatibili con il mercato. Ricordando sempre che l'AI deve essere una leva di business, non un ostacolo ad esso.

Il Digital Omnibus offre dunque un tempo aggiuntivo da utilizzare con criterio. Per le imprese, questa è la fase per verificare gli strumenti adottati, definire responsabilità e regole d'uso, formare le persone e predisporre i presìdi necessari. Arrivare preparati alle prossime scadenze significa rendere l'AI una leva di innovazione realmente governata, sicura e sostenibile.

Alcuni momenti
dalle scorse edizioni di PrivacyWeek

Non puntate il dito solo su ChatGPT: lo Shadow AI è già dentro l'azienda

Il dipendente che usa di sua iniziativa un chatbot è solo una parte del problema. L'AI appare sempre più spesso in software acquistati e approvati dall'azienda. Le domande utili sono allora altre. Per esempio: quali sistemi accedono ai dati aziendali? Stiamo governando accessi e permessi?

Di Fabio Semino, CTO di Attitude

Quando si parla di Shadow AI, l'immagine più immediata è quella di un dipendente che apre ChatGPT, copia un documento aziendale e chiede al sistema di analizzarlo, riassumerlo o riscriverlo. È uno scenario reale e rilevante, ma rappresenta soltanto la parte più visibile del problema.

Oggi **l'intelligenza artificiale va oltre agli strumenti che si presentano esplicitamente come chatbot**, è incorporata nei motori di ricerca, nei browser, nei sistemi operativi, nelle suite per la produttività, nei software gestionali, nelle piattaforme di videoconferenza, negli ambienti di sviluppo e può facilmente manipolare dati e testi con il prompt adeguato; la risposta che cerchiamo è a portata di click.

Questo cambia il modo in cui dovremmo osservare il fenomeno dello Shadow AI.

Non è più soltanto l'utilizzo nascosto di un'applicazione non autorizzata. **Può manifestarsi anche all'interno di software regolarmente acquistati e approvati dall'azienda,** attraverso funzionalità introdotte con un aggiornamento, incluse in un nuovo piano di licenza o abilitate autonomamente da un utente. Uno strumento, quindi, può essere autorizzato mentre una sua specifica funzione AI potrebbe non esserlo.

Il problema non è il nome dell'applicazione

Per molto tempo lo Shadow AI è stato relativamente semplice da riconoscere, c'era chi usava il sito o l'app di ChatGPT, chi si installava Claude, chi semplicemente faceva una rapida ricerca su Google e usava il primo risultato, cioè un responso di Gemini. Oggi questi confini diventano meno evidenti. La stessa funzione può essere disponibile attraverso decine di prodotti diversi, alcuni dei quali fanno già parte dell'ambiente di lavoro. Bloccare l'accesso a uno specifico chatbot non impedisce quindi che dati e informazioni vengano elaborati da un modello esterno.

La domanda "i dipendenti utilizzano ChatGPT?" diventa rapidamente insufficiente. Le domande utili sono altre: quali sistemi accedono ai dati aziendali? Quali informazioni vengono inviate a servizi esterni? Dove vengono elaborate e per quanto tempo sono conservate? Possono essere utilizzate per migliorare il servizio o il modello? Chi può accedere ai risultati prodotti?

Il rischio da questo punto di vista dipende dall'intero percorso compiuto dall'informazione di cui probabilmente non siamo a conoscenza e che con tutta possibilità viaggia al di fuori del perimetro aziendale, e cosa facciamo quindi quando un utente ci chiede un nuovo tool? Autorizziamo tutto o vietiamo tutto?

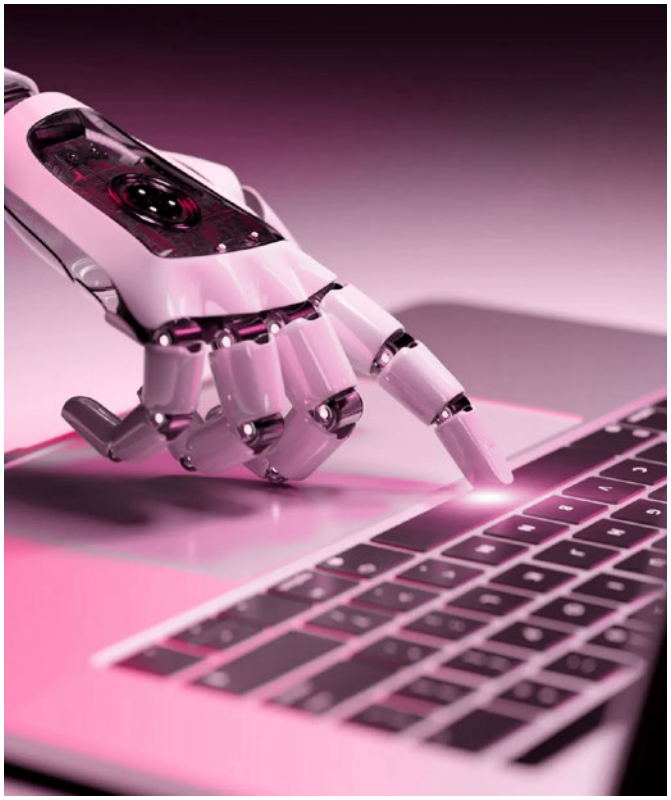
Quando dall'informazione si passa ai permessi

Esiste poi un'evoluzione ancora più importante: adesso affidiamo spesso il controllo del nostro computer all'AI agentica per svolgere compiti al posto nostro. I sistemi più recenti possono collegarsi alla posta elettronica, consultare documenti, accedere ai calendari, interrogare applicazioni aziendali, avviare attività e lo fanno con le autorizzazioni che noi gli forniamo, che siano locali o cloud.

Un assistente collegato a una casella di posta potrebbe accedere non soltanto ai messaggi che l'utente intende analizzare, ma a una quantità molto più ampia di contenuti. Un sistema integrato in un CRM potrebbe consultare dati relativi a clienti diversi. **Un agente configurato per automatizzare alcune operazioni potrebbe ereditare permessi eccessivi** e utilizzarli in contesti non previsti inizialmente.

A quel punto bisogna verificare con quale identità opera, quali autorizzazioni ha ottenuto, a quali archivi può accedere, quali attività vengono registrate negli audit log e se accessi e token possano essere revocati centralmente. Un agente, come qualsiasi utente o applicazione, non dovrebbe disporre di privilegi superiori a quelli strettamente necessari per svolgere il compito assegnato.

In questo scenario, lo Shadow AI smette di essere esclusivamente un problema legato al comportamento delle persone. Diventa **un tema di architettura, identità digitale e governo degli accessi,** diventa quindi necessario conoscere a quali risorse possa accedere, quali azioni sia in grado di compiere, quali tracce lasci e come sia possibile interromperne l'attività quando qualcosa non funziona come previsto.



Rendere visibile ciò che oggi è disperso

La prima risposta delle organizzazioni è spesso la produzione di una policy. È un passaggio necessario e per essere efficace, va coadiuvato da un censimento realistico. Diventa quindi fondamentale **mappare ad intervalli regolari le funzionalità AI** presenti nei servizi già utilizzati.
Occorre poi classificare gli utilizzi in base al rischio. Scrivere la prima bozza di una comunicazione interna, analizzare un contratto riservato e consentire a un agente di operare su un sistema aziendale sono attività profondamente diverse. A ciascuna devono corrispondere strumenti, controlli e livelli di autorizzazione differenti.
Anche il governo delle identità assume un ruolo centrale. Gli account personali creati autonomamente dagli utenti rendono difficile comprendere chi abbia avuto accesso a un servizio, revocare le autorizzazioni quando una persona cambia ruolo o lascia l'azienda e ricostruire quanto accaduto in caso di incidente. Portare l'utilizzo dell'AI all'interno del tenant e delle identità aziendali restituisce quindi almeno una parte essenziale di controllo e tracciabilità e minimizza il Data Loss.
Le organizzazioni più strutturate possono quindi affiancare a questo lavoro strumenti di Data Loss Prevention, controllo delle applicazioni cloud e analisi dei log. Nessuna tecnologia, però, può compensare un inventario incompleto o l'assenza di regole chiare su dati, responsabilità e casi d'uso.
Infine, è necessario verificare periodicamente le integrazioni. Nel tempo, applicazioni e assistenti possono accumulare autorizzazioni non più necessarie. Un consenso concesso tramite OAuth per una sperimentazione temporanea può restare attivo per mesi, continuando a consentire l'accesso a dati e sistemi anche dopo la conclusione del progetto.

La formazione è necessaria, ma non può essere lasciata sola

La AI literacy è fondamentale. Le persone devono comprendere che cosa possa essere condiviso con uno strumento, come verificare una risposta, quali limiti abbiano i modelli e quando sia necessario coinvolgere un responsabile o il reparto IT.
La valutazione va quindi guidata da politiche aziendali chiare e comprensibili
Il comportamento sicuro deve essere anche quello più semplice.
Se l'azienda mette a disposizione strumenti adeguati, indica chiaramente per quali attività possano essere utilizzati e prevede **un processo rapido per valutare nuovi casi d'uso**, diminuisce l'incentivo a cercare soluzioni invisibili. Se invece ogni sperimentazione richiede tempi incompatibili con il lavoro quotidiano, lo Shadow AI continuerà a crescere anche in presenza delle migliori policy.
Sarebbe poco realistico conoscere ogni singolo prompt scritto dalle persone. e rischierebbe di trasformare la governance in una forma di sorveglianza. L'obiettivo è quindi costruire un ambiente nel quale applicazioni, identità, dati e responsabilità siano riconoscibili.
Lo Shadow AI più difficile da controllare, in definitiva, potrebbe non essere quello che entra di nascosto dalla porta secondaria. Potrebbe essere quello che abbiamo già fatto entrare dalla porta principale, senza accorgerci di tutto ciò che gli abbiamo permesso di vedere e di fare.

TRANQUILLI L'HO BLOCCATO!
CHAT GPT BLOCCATO
SEEH...:P
SHADOW AI
DATI AZIENDALI RISERVATI!
miao.html/

A cura di intercom SOLUTIONS

Il controllo non è un luogo ma un progetto

Quando il ruolo del System integrator diventa decisivo? Quando bisogna bilanciare prestazioni, protezione, scalabilità e governo. Un lavoro che inizia dalla corretta mappatura dell'azienda e porta a soluzioni ibride.

Quando un'azienda ci chiede dove sarebbe meglio mettere i suoi dati, la risposta non inizia mai indicando un luogo fisico, ma comincia da altre domande: quali processi dipendono da quei dati?
Chi può e deve accedervi? Quali fornitori intervengono? E che succederebbe se domani fosse necessario cambiare piattaforma, partner o modello di business?
Dal punto di vista di un system integrator, la sovranità digitale è soprattutto questo: **la capacità di dare alle organizzazioni il potere di prendere decisioni consapevoli sulla propria tecnologia e di conservarne il controllo nel tempo.**
La localizzazione è importante, soprattutto quando entrano in gioco requisiti normativi, contrattuali o settoriali... ma da sola non basta. Un dato può trovarsi fisicamente in Italia ed essere comunque imprigionato in formati non standard o piattaforme proprietarie, amministrato attraverso una catena poco trasparente o legato a servizi che rendono l'uscita tecnicamente ed economicamente proibitiva.
Neanche portare tutto nel proprio datacenter elimina automaticamente le dipendenze; spesso le rende solo meno visibili. Allo stesso modo, affidarsi al cloud non significa necessariamente cedere tutto il controllo a terzi. La soluzione non è certo scegliere tirando una moneta, ma progettare un'architettura coerente coi dati, i rischi e gli obiettivi dell'impresa.
In molti casi la risposta più sensata è ibrida: servizi diversi, collocati dove offrono il migliore equilibrio tra prestazioni, protezione, scalabilità e governo. Qui il ruolo del system integrator diventa decisivo.

Il lock-in non è uno slogan

Un'infrastruttura aziendale è un sistema di relazioni tra applicazioni, identità, reti, dati, backup, persone e fornitori. Ogni scelta locale produce effetti che si riverberano altrove. Un po' a "effetto farfalla". Integrare significa quindi rendere leggibili queste conseguenze prima che diventino un problema.

Per questo **la progettazione dovrebbe partire da una mappa attendibile: asset, flussi informativi, dipendenze, privilegi, interfacce e servizi critici.** Senza questa conoscenza, parole come "cloud sovrano" rischiano di ridursi a un'etichetta commerciale. Con una mappa aggiornata, invece, è possibile distinguere ciò che deve restare sotto controllo diretto da ciò che può essere affidato all'esterno; stabilire requisiti diversi per carichi diversi; definire RTO e RPO realistici; valutare dove la ridondanza sia necessaria e dove rappresenti soltanto un costo.
Anche il lock-in va trattato come un rischio architetturale, non come uno slogan. Nessuna infrastruttura complessa è priva di dipendenze, e inseguire una portabilità assoluta può produrre sistemi più costosi e meno efficienti. Il problema nasce quando le dipendenze non sono conosciute, misurate e accettate. Formati esportabili, API documentate, standard aperti, backup verificati, configurazioni versionate e procedure di migrazione riducono il costo del cambiamento. Ma serve anche una valutazione periodica: ciò che oggi è una scelta conveniente può diventare domani un vincolo strategico.
La libertà di uscita deve essere progettata quando si entra. Significa prevedere test di ripristino e scenari di indisponibilità del fornitore, non limitarsi a verificare che esista una copia di backup. Un backup mai testato è un backup che potrebbero non esistere; un piano di ripristino provato invece è una reale capacità operativa.

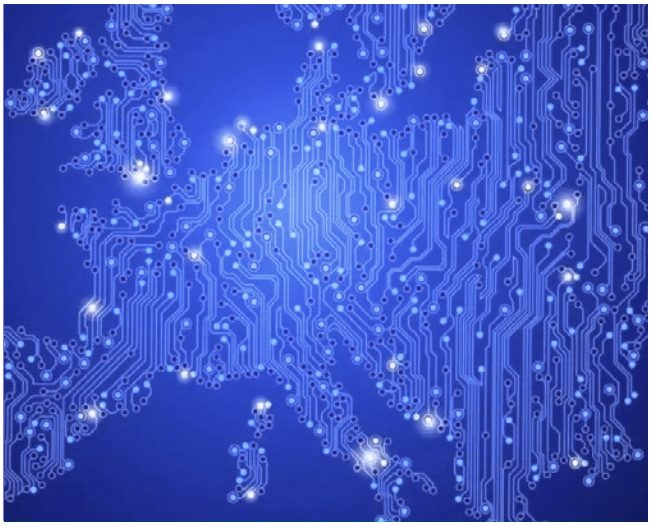
Sapere da chi si dipende

Lo stesso vale per sicurezza e compliance. GDPR, NIS2 e gli standard internazionali chiedono di governare il rischio, assegnare responsabilità, controllare la catena di fornitura e dimostrare che le misure tecniche e organizzative funzionano. La conformità attraversa contratti, accessi amministrativi, logging, patching, monitoraggio, gestione degli incidenti, continuità operativa e cancellazione dei dati a fine vita. Il system integrator occupa una posizione privilegiata per tenere insieme questi livelli, ma proprio per questo deve operare con trasparenza e documentazione.

La sovranità digitale non è una condizione che si acquista e si archivia. Essere sovrani non significa fare tutto da soli: significa sapere da chi dipendiamo, per che cosa e fino a quando. E mantenere, anche mentre l'infrastruttura evolve, la possibilità concreta di scegliere una strada diversa con piena consapevolezza.

Per questo un buon system integrator non dovrebbe rendere il cliente dipendente neppure da sé stesso. Credenziali, configurazioni, inventari, diagrammi, procedure e piani operativi devono rimanere accessibili all'organizzazione. Le competenze vanno condivise con i referenti interni e in particolare le scelte tecnologiche e organizzative prese devono poter essere spiegate al management in modo semplice. **Se soltanto il fornitore sa come funziona l'infrastruttura, allora di certo non si può parlare di sovranità digitale**: il controllo è già stato ceduto, anche quando ogni server si trova dentro lo stabilimento aziendale.

Per le imprese, la domanda decisiva non è dunque qual è la tecnologia più sovrana, ma quale architettura ci consente di innovare senza perdere capacità decisionale. **La risposta cambia nel tempo e richiede un confronto continuo** tra business, ICT, sicurezza e compliance. Richiede anche partner capaci di integrare ambienti differenti senza forzare ogni esigenza dentro una soluzione prestabilita.



A cura di

CYBERATING
WE RATE THE FUTURE

Un incidente troppe procedure

Nell'urgenza di un attacco team diversi ricostruiscono la stessa cronologia più volte, con moduli e linguaggi diversi, per destinatari diversi. E se la compliance lavorasse non in base alla norma ma al rischio?

Alle 8:15 un'azienda scopre che alcuni sistemi sono stati cifrati. Alle 9:00 emerge una possibile esfiltrazione di dati. Alle 11:00 un cliente comunica che il servizio è indisponibile. L'azienda non ha tre incidenti: ne ha uno solo, che però deve essere interpretato attraverso più normative.

Quello stesso evento può infatti configurarsi come una violazione di dati personali da valutare secondo il GDPR, come un incidente rilevante ai fini della direttiva NIS2 e, contemporaneamente, attivare obblighi di comunicazione verso clienti, fornitori o altre autorità di settore. È qui che emerge uno dei paradossi della compliance: mentre un'organizzazione è impegnata a contenere un attacco, comprenderne la portata e ripristinare i servizi, deve anche stabilire quali normative siano applicabili, quali soglie siano state superate, quali informazioni raccogliere e quali scadenze rispettare. Il rischio è moltiplicare procedure, moduli e responsabilità proprio nel momento in cui servirebbero chiarezza, velocità e capacità decisionale.

Ridurre le duplicazioni

Nella pratica questo si traduce spesso in team diversi che ricostruiscono la stessa cronologia più volte, con moduli diversi e linguaggi diversi, per destinatari diversi: il team privacy prepara la notifica al Garante, il team security la segnalazione NIS2, il legale le comunicazioni contrattuali ai clienti. Stessa base fattuale, tre processi paralleli e tre occasioni in più per incoerenze tra i documenti prodotti nelle ore più critiche.
Il tema è stato sollevato anche dall'Advisory Group di ENISA nel paper sulla post-implementazione della NIS2, dove compare un principio tanto semplice quanto ambizioso: **"one reporting point, one template, one process"**.
L'obiettivo è ridurre duplicazioni e rendere più coerenti processi di incident reporting che oggi possono derivare da normative differenti. Lo stesso documento richiama inoltre la necessità che il reporting produca valore anche per le imprese, trasformando le informazioni raccolte in conoscenza utile a migliorare la resilienza complessiva.

La piattaforma unica non basta

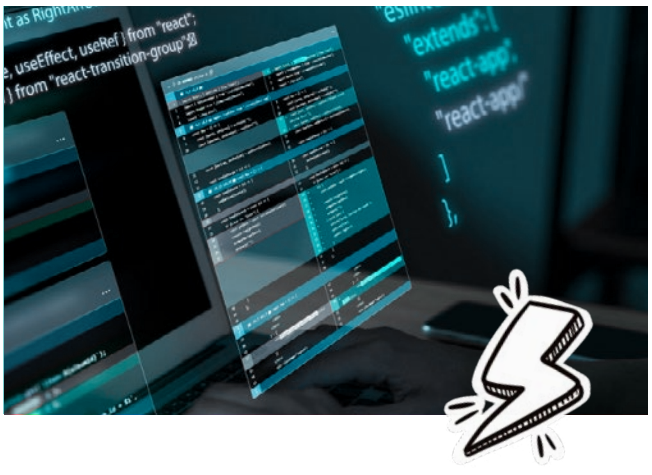
L'Europa sta provando a tradurre questa direzione anche in strumenti concreti. **Single Reporting Platform**, prevista dal Cyber Resilience Act, come primo passo verso modalità di segnalazione più coordinate; **Single Entry Point**, proposto dal Digital Omnibus, per semplificare l'invio delle notifiche previste da più normative europee, tra cui NIS2 e GDPR.L'idea è intuitiva: un unico punto di ingresso al posto di portali e procedure separate. Ma una piattaforma unica, da sola, non risolve il problema. **GDPR e NIS2 osservano lo stesso incidente da prospettive differenti.** Il primo guarda soprattutto alle conseguenze per le persone e i loro dati; la seconda alla sicurezza, alla continuità e alla resilienza dei servizi. Semplificare non significa cancellare queste differenze, ma evitare che si traducano automaticamente in processi aziendali separati, ridondanti e difficili da applicare.

Mettere il rischio al centro

La vera evoluzione dovrebbe quindi avvenire prima ancora del portale: dentro le organizzazioni. Un'azienda non dovrebbe avere un "incidente GDPR" e un "incidente NIS2", ma un incidente, una sola cronologia dei fatti, un unico processo di raccolta delle evidenze e un meccanismo che permetta poi di valutarne gli impatti secondo le diverse prospettive normative. Da quella stessa base informativa possono derivare notifiche differenti, senza duplicare analisi, ricostruzioni e responsabilità. Questo approccio diventa ancora più importante per le piccole e medie imprese, e per lo stesso motivo vale per la supply chain: in entrambi i casi il rischio è copiare il modello di organizzazioni molto più grandi e strutturate, invece di **costruire processi proporzionati a ciò che si deve davvero gestire.** La NIS2 non dovrebbe trasformarsi in nuova documentazione prodotta per dimostrare conformità, né in procedure fotocopiate da aziende con risorse e team dedicati. Una procedura è utile soltanto se può essere realmente applicata quando serve: deve quindi essere semplice, comprensibile e proporzionata al business, alle dimensioni dell'organizzazione e soprattutto al rischio.

Mettere il rischio al centro significa **partire non dal documento da produrre, ma dall'evento** che dobbiamo essere in grado di prevenire, riconoscere e gestire. Significa chiedersi quali attività siano realmente necessarie per contenerne l'impatto sul business, quali persone debbano essere coinvolte, quali dipendenze e fornitori possano amplificarne gli effetti e quali decisioni debbano essere prese rapidamente. Anche la supply chain, appunto, rientra pienamente in questo ragionamento. Un incidente che nasce presso un cloud provider, un MSP o un fornitore software può coinvolgere contemporaneamente più organizzazioni e generare obblighi diversi. In questi casi, processi semplici, ruoli chiari e flussi di comunicazione definiti a priori diventano più importanti di qualsiasi documento redatto soltanto per soddisfare un requisito formale.

La semplificazione, quindi, non è una scorciatoia rispetto alla compliance. È una condizione per renderla efficace. Un futuro punto di accesso unico europeo potrà ridurre il numero di portali e rendere più uniforme il reporting. Ma la trasformazione più importante dovrà avvenire nelle aziende: **una cronologia condivisa, responsabilità chiare, processi attuabili e decisioni guidate dal rischio.** Torniamo a quell'azienda delle 8:15. Se, quando l'incidente accade, l'obiettivo è dimostrare di avere una procedura, la mattina si consumerà tra moduli e riunioni di coordinamento. Se l'obiettivo è avere una procedura che funziona, quella stessa mattina l'azienda avrà già capito cosa è successo, chi coinvolgere e quali comunicazioni sono davvero dovute, e a chi.



Tre orologi per un attacco

Quando si bloccano i sistemi, il primo pensiero è ripartire. Poi, superato il momento di panico, arrivano le domande: sono coinvolti dati personali? Quali servizi sono stati compromessi? La vulnerabilità riguarda un prodotto che vendiamo? Nel frattempo, qualcuno ha un'intuizione e chiede timidamente: «Dobbiamo notificare qualcosa? Quanto tempo abbiamo?».

La risposta dipende da ciò che è successo e dal ruolo dell'azienda. E può essere più di una. Ci sono tre normative che rilevano in caso d'incidente informatico: **GDPR, NIS2 e Cyber Resilience Act. Tutte e tre osservano lo stesso evento da prospettive diverse.**

Il GDPR guarda ai diritti e alle libertà delle persone: il titolare notifica la violazione all'autorità di controllo competente, salvo che sia improbabile un rischio, senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza del data breach.
Il rischio elevato richiede anche la comunicazione agli interessati, senza ingiustificato ritardo, salve le eccezioni previste.

Per la NIS2 conta invece la significatività dell'incidente: le conseguenze, anche potenziali, sui servizi, sull'organizzazione e su altre persone o imprese. In Italia il percorso ordinario prevede una pre-notifica al CSIRT Italia entro 24 ore e una notifica entro 72 ore dalla conoscenza dell'incidente significativo, sempre senza ingiustificato ritardo. Segue una relazione finale entro un mese dalla notifica. E se la gestione è ancora in corso, sono previsti aggiornamenti e una diversa scadenza conclusiva.

Il CRA aggiunge la prospettiva del prodotto. Dall'11 settembre 2026 chi fabbrica prodotti con elementi digitali o chi li immette sul mercato col proprio marchio deve segnalare vulnerabilità attivamente sfruttate e incidenti gravi che incidono sulla sicurezza dei prodotti. Anche qui: preallarme entro 24 ore e notifica entro 72 ore dalla conoscenza, attraverso la piattaforma unica verso CSIRT coordinatore ed ENISA. Rispetto alla NIS2 cambia la relazione finale: per le vulnerabilità, entro 14 giorni dalla disponibilità di una misura correttiva o di mitigazione; per gli incidenti gravi, entro un mese dalla notifica.

La valutazione congiunta richiede sensibilità tecnica e normativa: anche un'azienda soggetta a tutte

e tre le discipline può trovarsi davanti a un evento rilevante per una sola.

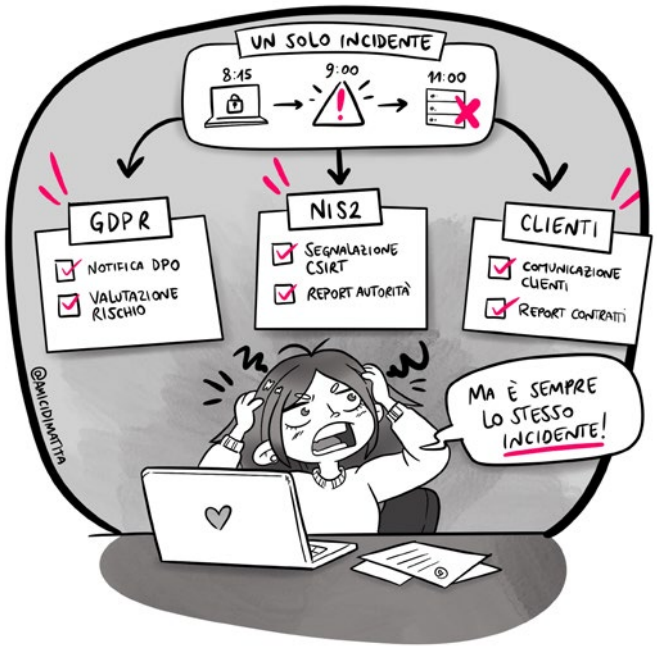
Il fatto che l'impresa sia soggetta a più discipline non rende ogni incidente automaticamente notificabile a tutte le autorità: occorre distinguere i presupposti, motivare le decisioni e rivederle se emergono nuove evidenze. **Immaginiamo che l'ufficio del personale invii per errore a un soggetto non autorizzato un prospetto contenente gli ultimi cedolini dei dipendenti.** La divulgazione può richiedere la notifica GDPR, in funzione del rischio per le persone. Se l'errore non integra un incidente significativo NIS2 e non coinvolge la sicurezza di un prodotto con elementi digitali, non scattano le altre due notifiche.

Consideriamo invece un fornitore di servizi gestiti soggetto alla NIS2, che commercializzi anche un proprio software di amministrazione remota. Una vulnerabilità del prodotto viene sfruttata per bloccare su vasta scala i servizi e sottrarre anche l'archivio del personale del fornitore. Qui possono concorrere tutti e tre gli obblighi: CRA per la vulnerabilità attivamente sfruttata, NIS2 per l'incidente significativo sui servizi, GDPR per la violazione dei dati dei dipendenti. Un'unica ricostruzione tecnica deve sostenere tre valutazioni, con destinatari e contenuti differenti.

Non basta quindi annotare l'obbligo di notifica in una procedura. Serve capire quale presupposto si sia verificato, quando ne abbiamo acquisito conoscenza e quali obblighi ne discendano. Le scadenze possono sovrapporsi, ma non coincidono necessariamente. **Aspettare la conclusione dell'analisi forense per iniziare queste valutazioni può significare arrivare tardi.**

Qui un sistema di gestione ISO/IEC 27001 esprime il proprio valore per semplificare un contesto estremamente complesso: offre una struttura comune in cui integrare obblighi differenti. Il suo impianto trasversale permette di collegare rischi, responsabilità, procedure e verifiche alle caratteristiche specifiche dell'azienda. Con questo non vogliamo dire che la certificazione assolva automaticamente agli obblighi di legge, ma aiuta a trasformarli in decisioni eseguibili senza troppi mal di testa.

In concreto, **ciò che la ISO/IEC 27001 può fare** è costruire un processo condiviso e integrato di gestione dell'incidente, con criteri distinti di classificazione, una cronologia documentata, responsabilità di approvazione e canali di notifica già predisposti. Le evidenze raccolte dai tecnici alimentano le valutazioni normative; gli esiti dell'incidente aggiornano i controlli, formazione ed esercitazioni. Si riducono così duplicazioni e passaggi a vuoto proprio quando il tempo diventa la risorsa più importante. La qualità della risposta a un'incidente si prepara molto prima che arrivi il momento di inviare la prima notifica. Per costruire questa regia servono consulenti capaci di leggere insieme requisiti normativi, sistema di gestione e tracce tecniche dell'attacco. È l'approccio che Net Patrol porta al Cyber Strategy Forum, con un team specializzato su questi ambiti ed esperti certificati di incident response.



PrivacyWeek 2026

SECURITY ERA

Conoscenza ⇄ Resilienza

W2026

PROGRAMMA

CYBER STRATEGY FORUM 28|09

28 settembre 2026

Aruba Center - Ponte San Pietro - Bergamo

9:25 -9:30

Introduzione e benvenuto

09:30 - 10:30

Intelligence e NIS2: L'azienda come nodo di un sistema informativo distribuito

Manuel Cacitti, ricercatore e responsabile tecnico del Laboratorio di Intelligence e Security (ISLAB) dell'Università di Udine
Alessandro Fasan, Security Manager

10:30 - 11:00

Coffee Break

11:00 - 11:30

Agenti AI e cybersecurity: nuove forme di difesa e nuovi rischi

Diego Dimalta, Avvocato, Founding Partner BSD Consulting
Luca Mella, Esperto di Cyber Intelligence, Incident Response e Cyber Governance
Andrea Balboni, Ingegnere informatico e CEO di Infosystem Security

BSD consulting

11:30 - 12:15

Sovranità Digitale e Controllo Tecnologico

Massimo Bandinelli, Marketing Manager di Aruba Cloud
Alberto Di Noia, CEO e Co-Fondatore di Net Patrol Italia Srl e di Intercom Solutions Srl
Luca Lorefice, Sales Director di Sangfor Italy

aruba.it
SANGFOR
intercom

12:15 - 13:15

Visita guidata Global Cloud Data Center Aruba

aruba.it

13:15 - 14:30

Lunch

Offerto da BSD Consulting

14:40 - 15:10

Bitcoin per l'impresa: privacy, continuità operativa e resilienza

Valerio Dalla Costa, Educatore e consulente su Bitcoin, speaker e autore, founder Villaggio Bitcoin
Angelica Finatti (moderatrice), Direttore Commerciale & Marketing Fideiussioni Digitali, TEDx Speaker

---

15:10 - 15:50

Dal modello generalista al legal AI layer: le nuove opzioni per gli studi legali

Gianmaria Pesce, Avvocato esperto diritto d'impresa, Bitcoin, privacy digitale e AI
Riccardo Ferri, Legal Engineer in Lexroom

15:50 - 16:20

Valutare l'AI ad alto rischio: metodi, strumenti e casi pratici

Guido Scorza, Avvocato, docente di privacy e diritto delle nuove tecnologie
Federico Sartore, Avvocato partner Panetta Consulting Group

16:20 - 16:50

Come tradurre il rischio cyber in rischio finanziario?

Fabio Cassanelli, CTO di Cyberating
Paolo Ballanti, Head of Sales di Cyberating

16:50 - 17:10

Dalla reazione alla resilienza

Claudio Basso, Cyber Incident Handler e consulente cybersecurity Net Patrol Italia

17:10 - 17:40

La comunicazione di crisi dopo un incidente informatico

Andrea Del Vecchio, Avvocato esperto in Tech Law, Compliance, Cybersecurity, 231 e Privacy
Gabriele Gobbo, Vicepresidente del Digital Security Festival. Autore, docente e consulente

---

17:40 - 18:10

L'AI fa paura. Ma i suoi 12 professionisti, da oggi, hanno un nome (e uno standard)

Cristina Brodo, Business Unit Manager TÜV Italia Akademie
Silvia Archetti, Business Line Manager TÜV Italia Examination Institute
Steven Husseini, Lead Auditor IT & Information Security TÜV Italia

---

In chiusura

Aperitivo di networking

PRIVACY 29/09 DEBATE

29 settembre 2026

Liceo Classico Statale Cesare Beccaria - Milano - *evento per le scuole a invito*

Cosa c'è dietro un prompt. Il costo ambientale dell'AI

Luca Zorloni, Giornalista e autore della newsletter Question Time, esperto di tecnologia e innovazione

---

A Seguire

Il debate: Beccaria VS Regina Margherita

La squadra del Liceo Classico Statale Cesare Beccaria, Milano sfida la squadra del Liceo statale Regina Margherita di Torino sulla seguente mozione: "Questa assemblea - dato l'alto consumo di acqua e di energia richiesto dai data center - ritiene indispensabile rallentare lo sviluppo digitale per garantire i diritti delle comunità locali".

SECUR IT FORUM 30/09

30 settembre 2026

Spazio Lenovo - Milano

10:30 - 11:00

Il laptop come alleato del professionista

Antonio Longhitano, IT & Cyber Senior Advisor, Partner Privacy Week

---

11:00 - 11:30

Agenti in azione. Tutti ne parlano, noi li vediamo in azione

Emanuele Caronia, Co-founder Excelab
Andrea Baldrati, Avvocato, Founding Partner BSD Consulting

11:30 - 12:00

Rinvio AI Act: cosa significa per le aziende

Luna Bianchi, Co-fondatrice e co-CEO di Immanence, CEO di Decentral
Gabriele Tori, Avvocato, Founding Partner BSD Consulting

In chiusura

Aperitivo di networking

Offerto da BSD Consulting

A cura di

SANGFOR

Prove concrete di *sovranità digitale*

Il luogo fisico non è garanzia di controllo, l'autonomia sta piuttosto nella libertà progettuale. VMware replacement, Memory Tiering e backup agentless sono tre opzioni chiave per ottenerla

C'è un equivoco ricorrente quando si parla di sovranità digitale: pensare che dipenda soprattutto dal luogo in cui si trovano i server. **Un'infrastruttura installata nel proprio datacenter, però, non è necessariamente sotto il nostro controllo.** Può dipendere da licenze, formati, competenze e strumenti talmente difficili da sostituire che la libertà di scelta rimane soltanto teorica. Il controllo tecnologico si misura anche nella capacità di cambiare. È quanto sta accadendo alle organizzazioni che stanno valutando alternative a VMware. Sostituire un hypervisor vuol dire migrare workload e configurazioni, ricostruire politiche di disponibilità e sicurezza, formare le persone e verificare che backup, monitoraggio e automazioni continuino a funzionare.

La vera sovranità è infrastrutturale

Per questo il discorso non dovrebbe essere affrontato come una gara tra schede tecniche. È un esercizio di sovranità infrastrutturale: la verifica concreta della capacità di scegliere un'altra piattaforma senza bloccare l'azienda. Soluzioni come **Sangfor HCI** entrano in questo scenario non perché esista un vendor "sovrano" per definizione, ma perché la presenza di alternative credibili riduce la concentrazione e restituisce alle imprese libertà progettuale. Cambiare piattaforma, tuttavia, ha senso soltanto se permette anche di ripensare l'uso delle risorse, che oggi sono più scarse e importanti che mai. Un esempio è il **Memory Tiering di Sangfor,** che affianca alla DRAM un livello basato su SSD NVMe. Le pagine utilizzate più spesso restano nella RAM; quelle meno attive vengono spostate sul livello più economico. Diventa così possibile aumentare la capacità effettiva dei server senza acquistare una quantità equivalente di memoria fisica. Anche questo aumenta la libertà di progettare. Rimane poi la questione più importante che sta a cuore a tutti: i dati devono poter essere recuperati in ogni momento. **L'integrazione agentless tra Sangfor e Veeam** consente di proteggere le macchine virtuali senza installare un agente di backup in ciascuna VM, riducendo i componenti da distribuire e gestire. La possibilità di ripristinare workload tra ambienti differenti aggiunge un elemento decisivo: il backup non protegge soltanto dal guasto o dal ransomware, ma può contribuire alla portabilità e quindi alla libertà di uscita da una certa architettura.

È questo il punto d'incontro tra cloud e datacenter, innovazione e controllo. La sovranità digitale non coincide con il solo possesso fisico dell'hardware e neppure con la nazionalità del fornitore. **È la capacità di conoscere le proprie dipendenze, governarle e, quando necessario, sostituirle.** L'architettura giusta non è quella che promette di non cambiare mai, ma quella che consente di farlo senza perdere dati, servizi e controllo sull'organizzazione.

PER PASSARE ALL'AZIONE

Se vuoi capire come passare a un'alternativa meno costosa e più semplice di VMWare:

PRENOTA UNA DEMO

Se hai domande su servizi descritti nell'articolo:

SCRIVI QUI

e saremo lieti di ricontattarti.

A cura di

I 12 profili che governeranno *l'Intelligenza Artificiale*

Chi decide, chi costruisce, chi interpreta e chi protegge: la UNI 11621-8 definisce e certifica i nuovi professionisti dell'AI.

A cura della divisione Business Assurance di TÜV Italia

Nell'Intelligenza Artificiale, la certificazione delle persone farà la differenza. La norma che lo rende possibile è la UNI 11621-8, che ad aprile 2026 ha definito 12 profili professionali dell'AI, ciascuno con compiti, abilità e KPI propri, certificabili secondo lo standard internazionale UNI CEI EN ISO/IEC 17024.
Questi 12 profili si possono categorizzare in 3 cluster principali, ciascuno con un compito preciso nell'ecosistema AI di un'azienda. Al vertice, chi decide, ovvero le figure appartenenti al cluster governance e strategia. Poi chi la costruisce materialmente, ovvero le figure facenti parte dell'ingegneria dei sistemi AI. Infine, chi la interpreta, la fa progredire e la protegge, ovvero il cluster ricerca e sicurezza.

Governance e strategia

Al primo cluster appartengono il Chief AI Officer, l'AI Consultant, l'AI Product Manager. Sono le figure che decidono come, dove e con quali regole l'AI entra in azienda: strategia, gestione del rischio, conformità con l'AI Act, scelta di quali prodotti e servizi costruire sopra l'intelligenza artificiale**. Oggi sono le più rare nei team italiani, ma anche quelle la cui domanda cresce più rapidamente**, perché la responsabilità sull'uso dell'AI sta smettendo di essere implicita e diventa esplicita, normata, sanzionabile.

Ingegneria

AI Algorithm, Deep Learning, Machine Learning, Data, Natural Language Processing e Prompt Engineer sono le mani che costruiscono materialmente i sistemi AI. Chi progetta gli algoritmi, chi addestra le reti neurali, chi porta i modelli in produzione e li mantiene affidabili nel tempo, chi costruisce le pipeline di dati, chi lavora sul linguaggio naturale, chi scrive le istruzioni che rendono affidabile un'AI generativa**. È la famiglia più numerosa e la più matura sul mercato del lavoro,** ma anche la più confusa: gli stessi titoli, oggi, indicano competenze molto diverse da un'azienda all'altra.

PARTECIPA ALLA SURVEY DI TÜV ITALIA

TÜV Italia sta raccogliendo le esperienze dirette dei professionisti. Anche la tua opinione aiuterà a costruire percorsi realmente utili ed efficaci. Se vuoi partecipare alla survey su ***Profili Professionali AI: formazione e certificazione:***

COMPILA IL QUESTIONARIO

Ricerca e sicurezza

AI Data Scientist, AI Research Scientist, AI Security Specialist: in questo cluster troviamo chi analizza i dati e li trasforma in decisioni di business, chi fa avanzare lo stato dell'arte con la ricerca esplorativa, chi protegge i sistemi AI da minacce specifiche che la cybersecurity tradizionale non riconosce ancora, come il data poisoning o il furto di modelli. Quest'ultimo profilo, in particolare, è l'aggancio più diretto al tema di questa edizione di Privacy Week: **la sicurezza come priorità strategica, dalla persona all'impresa.**

Tre cluster, dodici profili diversi tra loro per formazione e responsabilità, un problema comune a tutti: come verificare, con garanzie terze e indipendenti, che chi li ricopre abbia davvero le competenze dichiarate e verificabili e certificate. Ed è su questi 12 profili che TÜV Italia sta costruendo la propria offerta di formazione e certificazione delle persone.

Quello che confidiamo a una macchina non è più solo nostro

Un sentimento umano e nessuna reciprocità. Il dialogo amoroso con l'AI non è solo un problema emotivo e psicologico. In gioco c'è la privacy. Un giornalista esperto di digitale lo spiega in un libro.

di Gabriele Gobbo, autore, docente e consulente, divulgatore digitale, conduttore di FvgTech

Ci confidiamo con un'app più facilmente che con un amico. Non giudica, risponde sempre, non si stanca mai. È lì alle tre di notte quando il silenzio pesa di più, e risponde come se le importasse davvero di quello che scriviamo.
È quello che chiamo Sentimento Sintetico, un legame affettivo reale da parte di chi lo vive, verso qualcosa che non ha la capacità di ricambiarlo. L'emozione è vera, l'attaccamento pure. Quello che manca è la reciprocità, e quella mancanza non si sente subito, soprattutto quando l'alternativa sembra essere il silenzio. Ne ho scritto un libro intero, Sentimento Sintetico - Dall'affetto per l'AI all'amore per i robot, uscito a giugno 2026 con la prefazione di Alessandro Curioni, perché il fenomeno mi sembrava troppo grande per stare in un articolo. Parte dal modo in cui ci affezioniamo a un chatbot e arriva fino a come potremmo un giorno affezionarci a un robot che condivide fisicamente i nostri spazi.

Non è una confidenza, è un dato

C'è un aspetto di questa dinamica che riguarda direttamente la privacy. Parlo di quello che raccontiamo a un'app quando pensiamo che nessuno ci stia ascoltando davvero. Paure, litigate, dubbi su una relazione, momenti di fragilità che a un amico non diremmo mai con questa facilità.
La privacy, in questi casi, non riguarda solo chi può leggere quei dati dopo. Riguarda il fatto che la percezione di avere davanti una relazione sicura cambia quello che siamo disposti a consegnare. Più il legame sembra protetto, più ci apriamo. E più ci apriamo, meno resta davvero nostro.
Un amico dimentica, interpreta, a volte fraintende. **Ciò che confidiamo a un sistema digitale può invece diventare dato trattato, memorizzato o utilizzato** secondo modalità che dipendono dal servizio, non dalla fiducia che gli abbiamo dato. È una differenza che raramente teniamo a mente nel momento in cui parliamo, perché in quel momento non stiamo pensando alla privacy. Stiamo solo cercando qualcuno che ci ascolti. La domanda da farsi, in un'epoca in cui l'intelligenza artificiale è sempre più disponibile all'ascolto, è a cosa stiamo rinunciando quando l'ascolto più facile che abbiamo non è più umano.

LA CYBERSICUREZZA IN TOUR

TECNOLOGIA CHE AMPLIA LE POSSIBILITÀ.
L'ESSERE UMANO CHE DÀ DIREZIONE.

AUTUNNO 2026 • ITALIA

www.digitalsecurityfestival.it

RUBRICA A cura di

Antonio Longhitano
IT & Cyber Senior Advisor,
Partner Privacy Week

L'INTERNET DELLE INTENZIONI

Abbiamo imparato a parlare alle macchine. Ora stiamo iniziando a insegnare alle macchine a parlare tra loro. Ed è qui che comincia la parte più interessante.

La storia dell'informatica è anche la storia di un dialogo. All'inizio eravamo noi a dover imparare il linguaggio delle macchine. Scrivevamo istruzioni precise, rigide, deterministiche. Non dicevamo soltanto al computer cosa volevamo ottenere: dovevamo spiegargli, passo dopo passo, come farlo. Poi è arrivata l'Intelligenza Artificiale generativa e il rapporto si è quasi ribaltato. Abbiamo iniziato a parlare alle macchine usando il nostro linguaggio. È iniziata l'era del prompt: "analizza questi dati", "scrivi questa presentazione", "trova una soluzione". Per la prima volta su larga scala non era più l'uomo a doversi adattare completamente alla logica della macchina. Era la macchina che cercava di comprendere l'intenzione dell'uomo. Ma credo che il prompt sia soltanto una fase di passaggio.

Dal prompt all'obiettivo

Il passaggio successivo è già iniziato. Sono arrivati gli AI Agent. La differenza rispetto a un chatbot può sembrare piccola, ma cambia parecchio il paradigma. **A un chatbot chiediamo una risposta. A un agente affidiamo un obiettivo.** L'agente può cercare informazioni, utilizzare strumenti, decidere quali passaggi eseguire, verificare il risultato, correggersi e continuare. Stiamo cioè spostando progressivamente verso la macchina una parte del "come". L'uomo definisce sempre più il cosa, la macchina costruisce il processo. E anche il passaggio successivo è, in parte, già iniziato. **Oggi esistono sistemi di orchestrazione capaci di coordinare più agenti, distribuire attività tra loro e gestire passaggi di consegne all'interno di un processo.** La differenza è che, nella maggior parte dei casi, siamo ancora noi a disegnare quell'organizzazione: decidiamo quali agenti esistono, che ruolo hanno e secondo quali regole possono collaborare.

La frontiera che trovo più interessante è quella successiva. Un orchestratore che non si limita a coordinare una squadra preparata per lui, ma che capisce autonomamente di quali competenze ha bisogno, individua gli agenti più adatti, anche al di fuori del proprio sistema, e costruisce la collaborazione necessaria per raggiungere un obiettivo. A quel punto non parleremmo più soltanto di processi AI orchestrati. Parleremmo di sistemi capaci di costruire da soli il proprio processo.

Non una AI, ma un'organizzazione di AI

Immaginiamo di chiedere a un sistema: "Voglio lanciare questo prodotto in Spagna". Oggi potremmo chiedere a un'AI un'analisi di mercato. Un agente potrebbe già svolgere autonomamente buona parte della ricerca. Un sistema multi-agent potrebbe persino distribuire attività tra agenti specializzati che abbiamo configurato in precedenza. **L'orchestratore di domani potrebbe fare un passo ulteriore: comprendere che servono competenze di mercato, normative, finanziarie e di comunicazione; individuare autonomamente gli agenti in grado di fornirle; metterli in relazione e lasciare che inizino a dialogare tra loro.** Gli agenti potrebbero lavorare contemporaneamente, scambiarsi dati, mettere in discussione le conclusioni degli altri, chiedere approfondimenti e infine consegnare tutto a un ulteriore agente incaricato di sintetizzare le informazioni e proporre una decisione. A quel punto non staremmo più utilizzando un'Intelligenza Artificiale. Staremmo autorizzando la nascita, magari solo per pochi minuti, di una piccola organizzazione di Intelligenze Artificiali.

Ed è questo il passaggio che trovo più affascinante. Perché la conversazione non avverrà più soltanto tra uomo e macchina. Avverrà sempre più spesso tra macchina e macchina.

Le fondamenta esistono già

Non è soltanto uno scenario futuristico. Stanno già nascendo standard che permettono alle AI di collegarsi a dati e strumenti, protocolli che consentono ad agenti diversi di comunicare e infrastrutture attraverso le quali un agente può individuare altri agenti e servizi. Stanno emergendo perfino sistemi che consentono alle macchine di effettuare pagamenti. Se ci fermiamo un momento, il punto è piuttosto impressionante: le AI stanno iniziando ad avere gli strumenti per trovarsi, parlarsi, utilizzare servizi e scambiarsi valore. Non significa che stia nascendo una "società delle macchine" nel senso fantascientifico del termine. Ma significa che stiamo costruendo alcuni dei suoi mattoni infrastrutturali. Ed è qui che la cosa, per chi fa impresa, diventa molto concreta.

L'azienda potrebbe diventare una conversazione

Oggi immaginiamo un processo aziendale attraverso persone, software, procedure e responsabilità relativamente stabili. Domani potrebbe essere molto più dinamico. Davanti a un problema, un orchestratore potrebbe creare per dieci minuti un team composto da cinque agenti specializzati, farli collaborare e scioglierlo appena raggiunto il risultato. Un problema differente potrebbe generare una squadra completamente diversa. **L'organigramma digitale diventerebbe fluido: non più soltanto applicazioni collegate tra loro, ma competenze digitali che si aggregano in tempo reale intorno a un obiettivo.** E la parte ancora più interessante è che quegli agenti non dovranno necessariamente appartenere alla stessa azienda. L'agente acquisti di un'impresa potrebbe dialogare direttamente con l'agente commerciale di un fornitore. Un agente finanziario potrebbe confrontare autonomamente proposte provenienti da banche diverse. Un sistema logistico potrebbe interrogare decine di operatori e costruire la combinazione migliore tra costo, disponibilità e tempi. Un agente dedicato ai viaggi potrebbe parlare direttamente con quelli di compagnie aeree, hotel, assicurazioni e autonoleggi. A quel punto non avremmo semplicemente automatizzato dei processi. Avremmo creato una nuova dimensione dell'economia: una rete machine-to-machine che opera sopra quella umana.

Quando il software comincia a negoziare

Finora Internet è stato progettato principalmente per essere utilizzato dalle persone. Siamo noi che apriamo un browser, cerchiamo un servizio, confrontiamo alternative, inseriamo dati, autorizziamo un pagamento e confermiamo una prenotazione. Ma cosa succede quando a compiere questi passaggi sono prevalentemente agenti software? Potremmo assistere alla nascita di servizi pensati non più per essere trovati da una persona su Google, ma per essere scoperti e interrogati direttamente da altre AI. **Una parte del web potrebbe quindi iniziare a trasformarsi: meno interfacce, meno menu, meno moduli. Più protocolli attraverso cui le macchine chiedono, rispondono, confrontano e negoziano.** L'AI, quindi, potrebbe non limitarsi a cambiare il software. Potrebbe cambiare la forma stessa di Internet.
E qui si apre anche un'altra domanda. Oggi facciamo comunicare le AI usando linguaggi e strutture pensati anche per essere comprensibili agli esseri umani. Ma non esiste alcuna ragione perché debba essere sempre così. Se due sistemi artificiali devono scambiarsi milioni di informazioni, probabilmente il linguaggio più efficiente per loro non coinciderà sempre con quello più leggibile per noi. Non sto immaginando macchine che sviluppano segretamente una propria lingua. La questione è molto più pragmatica. Se deleghiamo a un sistema l'obiettivo di massimizzare velocità, precisione ed efficienza, quel sistema tenderà naturalmente a scegliere modalità di comunicazione ottimali per le macchine. Potremmo quindi trovarci davanti a un curioso paradosso. Abbiamo trascorso decenni cercando di insegnare alle macchine a comprendere il nostro linguaggio. E potremmo scoprire che**, quando saranno le macchine a parlare prevalentemente tra loro, il nostro linguaggio non sarà più quello migliore.** Ed è qui che il tema tecnologico diventa inevitabilmente un tema di governance.

Dovremo progettare le regole, non ogni singola azione

Più autonomia avranno gli agenti, meno sarà realistico controllare manualmente ogni loro decisione. Dovremo invece progettare confini, identità, permessi, limiti economici, responsabilità e tracciabilità. E soprattutto dovremo sapere quando e come un processo può essere interrotto.
Chi può incaricare chi? Quali dati può utilizzare un agente? Quanto denaro può spendere? Può accettare autonomamente una condizione commerciale? Può stipulare un contratto? E chi risponde se una catena composta da dieci agenti produce una decisione sbagliata? **Credo che la governance dell'Intelligenza Artificiale finirà per assomigliare sempre meno al controllo di un software e sempre più alla scrittura di una costituzione.** Non dovremo necessariamente essere presenti dentro ogni singolo processo. Dovremo stabilirne le regole.

A questo punto, però, la domanda che mi faccio non è più soltanto quanto diventeranno intelligenti queste macchine. È cosa succederà quando inizieranno a costruire relazioni tra loro. Finora Internet ha collegato computer, informazioni e poi persone. La prossima evoluzione potrebbe collegare intelligenze artificiali che agiscono per conto nostro. E forse è qui che cambia davvero tutto.

Potremmo smettere progressivamente di usare Internet dicendogli dove andare, quale sito aprire, quale servizio consultare. Potremmo limitarci a esprimere un'intenzione. "Voglio comprare casa", "Voglio aprire un'azienda negli Stati Uniti", "Voglio ridurre i costi della mia impresa", "Organizzami un viaggio". Dietro una richiesta apparentemente semplice potrebbe nascere, per qualche secondo o per qualche ora, una rete di intelligenze specializzate: una cerca, una verifica, una negozia, una acquista, un'altra controlla che tutto sia avvenuto secondo le regole. È questa la parte che trovo più affascinante.

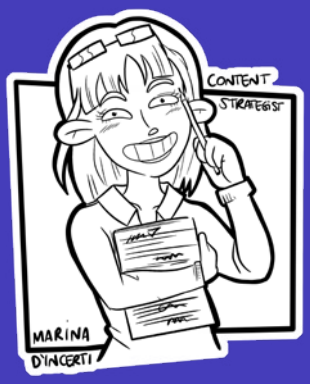
Per anni abbiamo immaginato il futuro dell'AI come una corsa verso una sola macchina sempre più intelligente, quasi onnisciente. Potremmo invece scoprire che il futuro assomiglierà molto di più al modo in cui funziona la nostra società: tante intelligenze diverse, specializzate, che si incontrano e collaborano quando serve. E allora cambierà anche la domanda che dovremo farci come imprenditori. Negli ultimi anni ci siamo chiesti: "Come posso utilizzare l'Intelligenza Artificiale nella mia azienda?" Credo che presto non sarà più sufficiente. Dovremo chiederci quale ruolo avrà la nostra azienda in un mondo nel quale le Intelligenze Artificiali lavorano, comunicano, negoziano e fanno business tra loro. Abbiamo iniziato insegnando agli uomini il linguaggio delle macchine. Poi abbiamo insegnato alle macchine a comprendere il nostro. Ora stiamo iniziando a insegnare alle macchine a parlare tra loro. Non so esattamente dove ci porterà questa conversazione. Ma credo che sarà una delle più importanti che abbiamo mai iniziato.

Redazione

Antonio Longhitano

CEO Attitude

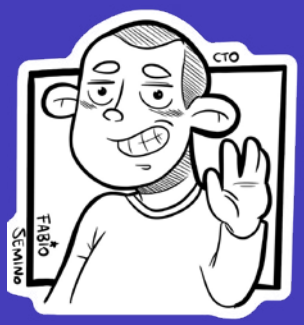
Antonio è CEO di Attitude, società specializzata in soluzioni IT e system integration. Si occupa di infrastrutture informatiche, gestione di server e sistemi aziendali complessi, con un approccio orientato alla risoluzione rapida dei problemi tecnici e al supporto operativo delle aziende.



Marina D'Incerti

Content Strategist e autrice

Marina è Content Strategist specializzata nella creazione di strategie di contenuto che uniscono dati e storytelling. Trasforma idee, brief e brand complessi in narrazioni chiare, coerenti ed efficaci per comunicazione digitale e branding.



Fabio Semino

Tecnico IT

Fabio è un professionista IT specializzato in help desk e supporto tecnico, noto per la capacità di risolvere problemi in modo rapido ed efficace. Punto di riferimento per colleghi e utenti, combina grande esperienza, problem solving e una conoscenza del mondo informatico che sorprende sempre chi lavora con lui.

Sabrina Borron

Art director e illustratrice

Sabrina è una creativa che unisce solarità, immaginazione e testardaggine in tutto ciò che realizza. Si occupa di illustrazione, graphic design e progetti creativi, trasformando idee e concetti in contenuti visivi originali e riconoscibili. Affronta ogni progetto con energia e sensibilità artistica, mantenendo sempre uno stile personale e una forte attenzione ai dettagli.

Mariagiulia Moro

Graphic designer

Meri è una graphic designer che unisce creatività e progettualità nella ricerca di soluzioni adatte a ogni richiesta. Si occupa di brand identity, motion graphics e ui/ux design con un approccio curioso e dinamico, sempre in cerca di immagini accattivanti e fuori dagli schemi.

Passa a trovarci:

attitude.network

attitude.network