

Cyber Magazine

IN QUESTO NUMERO

10 anni di GDPR

Inserto speciale sul decennio
che ha cambiato il valore dei nostri dati

Conf
com



Assintel



CYBER
Think Tank
ASSINTEL



CYBER
Think Tank
ASSINTEL

COORDINATORE CYBER THINK TANK

ANTONIO ASSANDRI

COMITATO SCIENTIFICO

**ANTONIO ASSANDRI, GIANPIERO COZZOLINO,
PAOLO MONTALI, VITTORIO OREFICE, RANIERI RAZZANTE**

REDAZIONE

A CURA DI ASSINTEL

**SEGRETERIA@ASSINTEL.IT
WWW.ASSINTEL.IT**

7

10 ANNI DI GDPR

Inserto speciale sul decennio che ha cambiato il valore dei nostri dati

9

IL GDPR COMPIE DIECI ANNI E GUARDA ALLE SFIDE DEI PROSSIMI DIECI

A cura di Nicola Bernardi

10

SE IL GDPR FOSSE UN POEMA CAVALLERESCO

A cura di Andrea Chiozzi

11

BUON COMPLEANNO GDPR: DIECI ANNI DOPO, UNA PROMESSA ANCORA DA COMPIERE

A cura di Matteo Colombo

12

10 ANNI DI GDPR

A cura di Stefano Marzocchi

14

DIECI ANNI DI GDPR: DALLA PROTEZIONE DEI DATI ALLA PRODUZIONE DI VALORE

A cura di Rocco Panetta

16

**QUANDO IL CRIMINALE ASSUME
UN'INTELLIGENZA ARTIFICIALE**

A cura di Mohammed Bellala

19

**IL PASSAGGIO DALLA "COMPLIANCE SULLA CARTA"
ALLE PROVE REALI DI RESILIENZA**

A cura di Jim Biniyaz

22

**ARCHITETTURA DI RIFERIMENTO AGENTIC AI
PRONTA PER ISO/IEC 27001:2022**

A cura di Andrea Ceiner

26

**CAVI SOTTOMARINI, LA NUOVA FRONTIERA DELLA
SICUREZZA CYBER-FISICA**

A cura di Stefano da Empoli e Alessandro D'Amato

28

**EVOLUZIONE DELLE NORMATIVE EUROPEE
DELL'AREA DIGITALE**

A cura di Carlo Guastone

32 **L'ILLUSIONE DELL'INTELLIGENZA: PERCHÉ L'AI STA CAMBIANDO LA CYBERSECURITY PIÙ DEGLI HACKER**
A cura di Francesco Iarlori

35 **LA TECNOCRAZIA AMERICANA E LA NUOVA ERA GEOPOLITICA DELL'IA**
A cura di Sofia Scozzari

38 **SICUREZZA INDUSTRIALE, COME PREVENIRE LE CYBER-INTRUSIONI**
A cura di Francesco Tieghi

40 **VERSO LA FABBRICA COGNITIVA: UN NUOVO PARADIGMA PER L'OT SECURITY**
A cura di Elena Vaciago

43 **NIS2 E SUPPLY CHAIN: IL GRANDE EQUIVOCO DEI QUESTIONARI AI FORNITORI**
A cura di Enzo Veiluva



L'editoriale del Coordinatore del Cyber Think Tank Antonio Assandri

LUGLIO 2026

Carissimi lettori,

eccoci a voi con nuova edizione del Cyber Magazine che, visto il periodo dell'anno, confidiamo vi possa accompagnare nei vostri momenti di relax e di riposo.

Apriamo questo numero con un inserto speciale, dedicato ad un anniversario importante: i dieci anni del GDPR.

Gli anniversari possono essere un genere insidioso: occasioni per dedicarsi solo alla celebrazione, quando, invece, meriterebbero approfondimenti e bilanci. Ma non temete, il nostro inserto è in stile Cyber Think Tank, pratico e votato al confronto. Sono cinque articoli, più un editoriale, che affrontano il tema con voci diverse, anche in apparente disaccordo tra loro, perché il decennale merita onestà, più che retorica. C'è chi vede nel Regolamento una grande operazione di re-coding dei diritti fondamentali, chi ne misura con disincanto la distanza tra principi e pratica quotidiana, chi lo rilegge come infrastruttura di produzione di valore.

Da questo confronto emerge un filo comune, che attraversa l'intero numero e che va oltre l'inserto, dipanandosi attraverso gli altri articoli. Dieci anni fa l'Europa ha dettato quello che sarebbe divenuto un punto di riferimento globale in tema di protezione dei dati personali; oggi il quadro normativo, dal GDPR alla NIS2, da DORA all'AI Act, chiede di andare oltre: chiede di dimostrarle. Il passaggio dalla compliance "su carta" alla compliance dimostrabile è la vera cifra di questa stagione regolatoria. E' anche il punto in cui cadono le certezze di molte organizzazioni, che scoprono la distanza tra ciò che hanno scritto e ciò che sanno fare.

Su questo scenario si innesta l'intelligenza artificiale, presenza ormai fissa di tutti i numeri del nostro Magazine. In termini di cyber security l'AI ha abbattuto barriere su entrambi i fronti: aiuta chi ci attacca, rendendolo più veloce, più credibile e più economico, ma mette gli stessi strumenti nelle mani di chi difende. Non è la tecnologia a fare la differenza, è chi la governa e con quale consapevolezza. E' proprio su questo, insidioso, terreno che le norme costruite nel decennio scorso affrontano la loro prova di maturità: una regola invecchia bene se sa reggere davanti a ciò che non poteva prevedere.

C'è, infine, una dimensione che sta particolarmente a cuore ad Assintel ed al Cyber Think Tank: rendere questa maturità accessibile. Le grandi organizzazioni hanno uffici legali, budget e strutture dedicate; le PMI, ossatura portante del tessuto produttivo del nostro Paese e cuore della nostra associazione, hanno bisogno di strumenti, linguaggi e percorsi proporzionati. Una cultura della sicurezza appannaggio di pochi diventa una barriera. Il compito di una community come la nostra è proprio questo: aiutare a trasformare la complessità normativa e tecnologica in competenze diffuse e praticabili.

Il GDPR ci ha insegnato che i dati sono un'estensione della persona. Ora tocca dimostrare che anche la sicurezza lo è: non un documento, ma un comportamento.

Buona lettura e buona estate!



10 anni di GDPR

Inserto speciale sul decennio
che ha cambiato il valore dei nostri dati



L'editoriale del referente del Comitato Scientifico del Cyber Magazine Gianpiero Cozzolino

Scrivo questo editoriale nel maggio del 2026. Esattamente dieci anni fa, nel maggio 2016, il Regolamento Generale sulla Protezione dei Dati (GDPR) entrava ufficialmente in vigore, concedendo alle aziende e alle istituzioni un biennio di grazia prima della sua piena applicabilità. Il percorso che ci ha portato fin qui non è stato lineare, si è trattato, invece, di una faticosa scalata per rendere concreti principi troppo spesso percepiti come astratti, dove banner cookies e complessità hanno rischiato di trasformare un diritto fondamentale in un fastidio amministrativo.

Oggi non celebriamo la sopravvivenza di un apparato burocratico, ma la più grande operazione di *re-coding* dei diritti umani dell'era moderna: nel 1948 la Dichiarazione universale dei diritti umani sanciva il diritto alla vita privata, il GDPR ha avuto il merito storico di tradurre quella visione in un linguaggio compatibile con gli algoritmi. Dieci anni fa il dato personale era considerato il "nuovo petrolio": una materia prima da estrarre, raffinare e accumulare senza troppi scrupoli morali. Oggi, grazie al GDPR, quella metafora è naufragata. Il dato non è combustibile, è un'estensione della persona.

Il passaggio filosofico è stato radicale. Siamo passati da una cultura del "tutto è permesso finché non veniamo colti in flagrante" alla responsabilizzazione (accountability), integrando la privacy fin dalla progettazione (privacy by design): un requisito obbligatorio per ogni riga di codice.

E mentre i critici iniziali deridevano l'Unione Europea per la sua iper-regolamentazione – un museo destinato all'irrelevanza tecnologica –, il GDPR si trasformava silenziosamente nello standard globale. California, Brasile, India, Corea del Sud: le legislazioni sulla privacy nate nell'ultimo decennio portano tutte l'impronta genetica del regolamento europeo. L'Europa ha dimostrato che la sovranità si esercita anche con i confini normativi. Abbiamo esportato non software, ma valori.

Nel 2026 il GDPR affronta la sua prova di maturità definitiva: l'integrazione con l'AI Act. Se il Regolamento ci ha insegnato a proteggere i dati, fornendo le impalcature essenziali, le nuove sfide riguardano come questi vengono utilizzati per addestrare modelli che possono decidere del nostro credito, della nostra salute o della nostra occupabilità. La sua struttura flessibile e basata sul rischio ha permesso di arginare le derive più distopiche del capitalismo di sorveglianza, incanalando l'innovazione in un alveo antropocentrico.

Cosa resta di questi dieci anni? Una maggiore consapevolezza dei cittadini, un nuovo mercato - la "Trust Tech", dove la privacy è diventata vantaggio competitivo - e un enforcement ancora asimmetrico tra i vari Garanti nazionali, che resta però uno scudo a tutela dei diritti.

Nell'arena digitale, chi non siede al tavolo finisce sul menu. L'Europa ha scelto di stare al tavolo, convinta che la tecnologia debba servire l'umanità, e mai il contrario.

Buona lettura!



Il GDPR compie dieci anni e guarda alle sfide dei prossimi dieci

a cura di Nicola Bernardi

Il GDPR ha compiuto dieci anni, ma ne dimostra otto, perché se è vero che il Regolamento UE 679/2016 ha di recente festeggiato il decimo compleanno da quando è venuto alla luce, d'altra parte la sua effettiva applicazione è partita due anni più tardi, esattamente il 25 maggio 2018, quando ha iniziato a “vivere davvero” tra imprese, autorità e cittadini più o meno consapevoli.

Gli anni trascorsi sono sicuramente sufficienti per uscire da un'infanzia normativa fatta all'epoca di tanti buoni propositi, ma a quanto pare ad oggi il GDPR non è ancora abbastanza maturo da poterlo considerare un regolamento pienamente in grado di affrontare da solo le sfide di un futuro che si è complicato più del previsto rispetto a quando muoveva con entusiasmo i primi passi, tant'è che nel frattempo mamma UE gli ha dato pure altri fratellini per cercare di dargli una mano con svariati nuovi regolamenti come il Data Services Act, il Data Governance Act, il Data Act, il Digital Markets Act, e l'Artificial Intelligence Act.

La famiglia è diventata quindi decisamente numerosa, ma se in genere si dice che l'unione (l'UE in questo caso) fa la forza, strada facendo sono aumentate anche le criticità della privacy nella civiltà digitale, con tensioni geopolitiche, complessità della materia sia sotto il profilo giuridico che su quello informatico, e anche le difficoltà nel governare il fenomeno epocale dell'intelligenza artificiale, che nel 2016 era ancora una tecnologia promettente, ma ancora confinata a settori specialistici, mentre oggi fa ormai parte della realtà quotidiana di milioni di persone.

La vera domanda, non è tanto se il GDPR abbia funzionato nei suoi primi dieci anni di vita, quanto se sarà in grado di affrontare efficacemente i prossimi dieci. Le sfide che si profilano all'orizzonte sono infatti di portata tale da mettere alla prova alcuni dei principi fondamentali su cui si basa l'intero impianto della protezione dei dati personali.

Una delle questioni più delicate riguarda proprio il rapporto tra privacy e intelligenza artificiale. I modelli generativi vengono addestrati su quantità immense di dati, spesso raccolti da fonti molto eterogenee, e non sempre è semplice ricostruire con precisione l'origine delle informazioni utilizzate. In questo contesto, principi cardine come trasparenza, minimizzazione dei dati, limitazione delle finalità e diritto alla cancellazione rischiano di confrontarsi con difficoltà tecniche e operative senza precedenti. Accanto all'intelligenza artificiale, un'altra sfida sarà rappresentata dalla crescente concentrazione del potere digitale nelle mani di pochi grandi operatori globali. Sebbene il GDPR abbia contribuito a rafforzare la responsabilizzazione delle imprese, il confronto tra autorità nazionali e Big Tech continua a essere caratterizzato da evidenti asimmetrie economiche, tecnologiche e organizzative. Garantire un'applicazione uniforme ed efficace delle regole rimarrà quindi uno degli obiettivi più ardui da perseguire.

Non meno rilevante sarà il tema della sovranità digitale europea. Le tensioni geopolitiche degli ultimi anni hanno dimostrato come il controllo dei dati rappresenti ormai una leva strategica al pari delle infrastrutture energetiche o delle catene di approvvigionamento industriali. Vi è poi il rischio di una crescente contrapposizione tra tutela dei diritti e esigenze di competitività economica. In una fase storica in cui l'Europa cerca di recuperare terreno rispetto ad altre aree del mondo nella corsa all'innovazione digitale, aumenteranno probabilmente le pressioni per semplificare alcuni adempimenti o rendere più flessibili determinate regole. La sfida sarà evitare che l'obiettivo della crescita finisca per indebolire le garanzie costruite nel corso degli ultimi dieci anni.

Se il primo decennio è stato quello dell'affermazione dei principi, il secondo sarà probabilmente quello della loro tenuta di fronte alle trasformazioni più profonde che la società dell'informazione abbia mai conosciuto.



Se il GDPR fosse un poema cavalleresco

a cura di Andrea Chiozzi

Se il GDPR fosse un poema cavalleresco, ciò che ho letto sui social ultimamente somiglierebbe al suo canto celebrativo. Ho passato anni tra registri del trattamento spessi quanto l'Odissea e sanzioni, sono quasi commosso. Quasi. Perché c'è la teoria, la pratica e poi c'è il tasto "Accetta Tutto".

Si parla di dato-petrolio/dato-estensione della persona. Visionari! Nel mondo reale la gente tratta la propria *estensione della persona* come un volantino del supermercato: la getta nel primo cestino digitale, pur di leggere un articolo sui gatti o sbloccare uno sconto del 5%.

Si parla di dato che *non è più combustibile*, bellissima immagine dipinta da Cozzolino nel suo editoriale. Ma mentre noi filosofeggiamo, i data broker raffinano il prodotto meglio di prima. Non petrolio: essenza distillata di utente. Un mercato più florido che mai.

E la privacy by design è davvero un requisito obbligatorio *per ogni riga di codice*? Allora ogni automobilista rispetta rigorosamente i limiti di velocità! No, è *privacy by PowerPoint*: schemi per consulenti. Chi sviluppa continua a incollare codice da librerie terze per tracciare quante volte batti le palpebre.

Col GDPR "abbiamo esportato non software, ma valori"? Un capolavoro retorico per dire che, non avendo campioni tecnologici europei in grado di competere con i colossi USA e asiatici, siamo diventati i migliori arbitri del mondo in una partita che non stiamo giocando.

Vero, California e Brasile ci hanno copiato. Abbiamo creato il più grande prodotto da esportazione europeo dopo vino e moda: il modulo di consenso. Sono orgoglioso di questa sovranità normativa, ma i confini sono così invalicabili che neanche le nostre startup riescono ad attraversarli senza un team di tre avvocati e un esorcista. Ma ehi, i nostri valori sono al sicuro, anche se girano su server in Virginia.

Intanto gli LLM avanzano. C'è l'AI Act che si interseca con il GDPR: il matrimonio tra il righello e il buio. L'integrazione tra i due è la *prova di maturità*? È il tentativo di spiegare a un'intelligenza artificiale generativa che non può mangiare i dati che ha già digerito tre anni fa: mentre noi costruiamo "impalcature essenziali" e "alvei antropocentrici", il resto del mondo costruisce modelli. Regoliamo l'innovazione degli altri, sperando che gli altri leggano il nostro manuale di istruzioni prima di renderci obsoleti.

Cosa resta davvero di questi dieci anni?

Consapevolezza (poca).

Trust Tech: paghiamo qualcuno per assicurarci di non essere multati. Enforcement asimmetrico tra i Garanti, mentre le PMI combattono una burocrazia pensata per chi fattura miliardi.

Nell'arena digitale siamo seduti al tavolo. Ma dopo dieci anni passati a discutere sulla forma delle posate, non ci siamo accorti che la cena si sta consumando in nostra assenza. Almeno abbiamo un banner che ci chiede se vogliamo accettare i cookie, proprio ora che i cookie stanno per morire di vecchiaia. Salute!



Buon compleanno GDPR: dieci anni dopo, una promessa ancora da compiere

a cura di Matteo Colombo

Dieci anni fa il GDPR non ha semplicemente introdotto nuove regole sulla protezione dei dati personali. Ha ridefinito il modo in cui cittadini, imprese, pubbliche amministrazioni e professionisti devono guardare alla compliance, alla tecnologia, all'organizzazione e alla responsabilità. Il Regolamento europeo sulla protezione dei dati è nato da una premessa chiara: la protezione dei dati personali non è un adempimento burocratico, ma un diritto fondamentale della persona, sancito dalla Carta dei diritti fondamentali dell'Unione Europea. In questi dieci anni abbiamo maturato la consapevolezza che i dati non sono solo "informazioni": sono identità, comportamenti, fragilità, relazioni, scelte di vita. Per questo il GDPR ha imposto un cambio di prospettiva: non basta più chiedersi se un trattamento sia tecnicamente possibile; occorre domandarsi se sia giuridicamente fondato, informato, proporzionato, trasparente e rispettoso della dignità degli interessati.

Il merito principale del GDPR è stato quello di portare nel linguaggio quotidiano delle organizzazioni principi come accountability, privacy by design, valutazione del rischio, minimizzazione, sicurezza, data breach, formazione degli incaricati, diritti degli interessati e ruolo del Data Protection Officer. Concetti che, prima del 2016, erano spesso confinati agli uffici legali o ai soli servizi IT e HR, oggi sono invece componenti strutturali dei modelli organizzativi più maturi.

Naturalmente, non tutto ha funzionato come avrebbe dovuto. In molte realtà il GDPR è stato vissuto come un insieme di documenti da predisporre, informative da aggiornare e registri da compilare. Ma la vera conformità non si misura dal numero delle policy archiviate. Si misura dalla capacità di trasformare quei principi in comportamenti, processi, controlli e cultura organizzativa. La privacy non è una pratica amministrativa: è un processo aziendale continuativo.

Il Data Protection Officer, in questo percorso, ha assunto una funzione sempre più centrale. Figura relativamente nuova nell'ordinamento italiano, non è semplicemente "quello della privacy" in senso esecutivo, né il soggetto chiamato a sostituirsi al titolare del trattamento. È, piuttosto, un presidio di garanzia — talvolta anche operativo: per l'organizzazione, perché aiuta a leggere e gestire correttamente il rischio; per gli interessati, perché mantiene viva l'attenzione sui loro diritti; per il sistema, perché contribuisce a rendere effettiva la protezione dei dati personali.

Oggi il GDPR si confronta con una nuova stagione regolatoria. Intelligenza artificiale, cybersicurezza, Data Act, Data Governance Act, NIS2 e nuove forme di sorveglianza digitale mostrano che la protezione dei dati non opera più in isolamento, ma innerva l'intero sistema. Il GDPR è diventato la base costituzionale dell'ecosistema digitale europeo: non esaurisce tutte le risposte, ma resta il punto di equilibrio irrinunciabile tra innovazione, mercato e tutela della persona.

La sfida dei prossimi dieci anni sarà evitare due errori opposti ma ugualmente pericolosi. Il primo: trasformare il GDPR in un adempimento burocratico privo di sostanza. Il secondo: rappresentarlo come un freno all'innovazione, anziché come una condizione per renderla sostenibile e affidabile. Al contrario, una buona governance dei dati è oggi una condizione necessaria per l'innovazione responsabile. Dove i dati sono governati male, anche l'intelligenza artificiale diventa opaca, fragile e potenzialmente discriminatoria. Dove i dati sono governati bene, tecnologia e diritti non solo possono coesistere: si rafforzano a vicenda. Buon compleanno, dunque, al GDPR. Ma senza autolellezze: la sua promessa non è ancora pienamente realizzata. Dopo dieci anni, la vera domanda non è se abbiamo imparato a redigere informative più accurate, ma se siamo riusciti a costruire organizzazioni più responsabili, tecnologie più trasparenti e processi decisionali davvero rispettosi delle persone. Ed è proprio qui che il GDPR continua a essere attuale: non come norma del passato da archiviare, ma come grammatica giuridica indispensabile per navigare il futuro digitale.



10 anni di GDPR

a cura di Stefano Marzocchi

A gennaio del 2016 mi trovavo al cinema multisala Utopolis di Lussemburgo, dove Viviane Reding e Jan Albrecht, madrina e padrino del Regolamento generale sulla protezione dei dati, ne celebravano l'imminente pubblicazione con la proiezione del docufilm Democracy. In meno di due ore si raccontavano gli oltre 4 anni di gestazione durante i quali la bozza del GDPR aveva collezionato oltre 4000 emendamenti, un record per la normazione unionale.

Quello sterminato carteggio ben mostrava le resistenze che il GDPR aveva e avrebbe incontrato, in quanto prima istanza di leadership europea del dato, un viatico che potesse sganciarci dalla pedissequa sequela dell'altra sponda dell'Atlantico. Quella che si stava disegnando era una nuova cultura della gestione delle informazioni, essenziale per la sopravvivenza dei valori europei nella data driven economy, che Cambridge Analytica e Snowden ci hanno mostrato essere ormai una data driven society.

L'Unione europea intendeva difendersi primeggiando, evitando di chiudersi a riccio in una lenta agonia, lanciandosi invece sulla scena globale come player primario, riflesso del suo essere la prima economia del mondo, egida dei propri valori e principi insindacabili. Beninteso, il GDPR non voleva solo tutelare il dato europeo, ma farlo circolare, sfruttarlo economicamente, nella consapevolezza che il suo valore deriva tutto dal suo utilizzo. Tutto questo però a patto che ciò avvenga lecitamente e in piena sicurezza.

I principi codificati dal GDPR li vediamo ora replicati in tutte le principali normative cyber che l'hanno seguito, le quali fanno tutte esplicito e molteplice riferimento al GDPR come imprescindibile normativa complementare. Pensiamo al concetto di by default e by design, o al pilastro dell'accountability che porta con sé l'approccio basato sul rischio.

Oggi, a distanza di un decennio, possiamo affermare che il GDPR è stato una delle più grandi innovazioni istituzionali europee dell'era digitale. Non soltanto una legge sulla privacy, ma un nuovo modello di governance del dato. Perché ridefinisce il rapporto tra tecnologia, mercato, democrazia e diritti fondamentali.

Introduce un'idea nuova e profondamente europea: che l'innovazione non debba svilupparsi in assenza di limiti, ma attraverso regole intelligenti, capaci di creare fiducia, responsabilità e sostenibilità. Difende l'idea che il progresso tecnologico non può essere separato dalla tutela della persona. Sostiene che la competitività non può fondarsi sull'asimmetria informativa o sull'estrazione incontrollata dei dati.

Il suo approccio anticipatorio è oggi il paradigma di riferimento di tutta la regolazione digitale europea. La governance tecnologica non può essere reattiva; deve essere preventiva, sistemica, *risk-based*. E il GDPR è stato il laboratorio di questa nuova stagione normativa.

Ma il suo valore innovativo non è stato soltanto giuridico. È stato anche economico e culturale. In questi dieci anni abbiamo compreso che la fiducia è una infrastruttura competitiva. Le organizzazioni che trattano i dati in modo trasparente e responsabile generano maggiore affidabilità, migliore reputazione, maggiore sostenibilità. In un'economia guidata dai dati, la fiducia è un asset strategico.

Il GDPR ha reso evidente che il dato non può essere governato esclusivamente secondo logiche di proprietà o di sfruttamento economico. Il dato implica relazioni, diritti, identità, libertà individuali.

Ecco perché il GDPR ha avuto un impatto globale, il GDPR ha esercitato una vera potenza normativa. Una capacità tipicamente europea: influenzare il mondo non attraverso la forza militare o il predominio tecnologico, ma attraverso la definizione di standard.

Ora che si accarezza l'idea della compliance integrata e della notifica unica, non dobbiamo però farci scoraggiare dagli innegabili, parziali fallimenti nella sua implementazione, o accarezzare l'idea di mettere in discussione quella che è la cellula totipotente della protezione del dato, che parla per principi perché i principi sopravvivono al tempo mentre le liste invecchiano.

Il futuro del GDPR dipenderà dalla nostra capacità di costruire una governance del dato che sia insieme efficace, proporzionata e abilitante, capace di sostenere l'innovazione senza rinunciare ai diritti.

Oggi questa sfida è ancora più urgente. Siamo entrati nell'era dell'intelligenza artificiale. I dati alimentano modelli sempre più potenti. Le decisioni automatizzate incidono sulla vita delle persone. Le infrastrutture digitali diventano sempre più pervasive.

In questo scenario, il GDPR mostra tutta la sua attualità. Perché i suoi principi fondamentali sono strumenti essenziali per governare il futuro. E forse il suo lascito più importante è proprio questo: aver introdotto una cultura del dato che rifiuta l'idea dell'inevitabilità tecnologica. Che ricorda che ogni architettura digitale incorpora sempre una scelta politica, etica e sociale.

E allora, celebrando questi dieci anni, non dovremmo limitarci a fare un bilancio normativo. Dovremmo riconoscere che il GDPR ha rappresentato una scelta di civiltà digitale. Ha affermato che i diritti fondamentali non sono incompatibili con l'innovazione. Che la tecnologia deve restare al servizio della persona. Che il mercato digitale ha bisogno di fiducia, responsabilità e trasparenza per essere sostenibile.

E soprattutto ha mostrato che l'Europa può ancora avere una visione, nella quale il governo del dato non coincide con il suo controllo assoluto, ma con la capacità di bilanciare libertà, innovazione e interesse collettivo.

Non esiste innovazione sostenibile senza governance. E il GDPR, con tutti i suoi limiti e i suoi aggiustamenti necessari, resta ancora oggi uno dei più avanzati tentativi al mondo di costruire una governance democratica del dato.

Per questo il suo anniversario non riguarda soltanto il diritto della privacy. Riguarda il futuro della nostra società digitale.

GDPR



Dieci anni di GDPR: dalla protezione dei dati alla produzione di valore

a cura di Rocco Panetta

Dieci anni di GDPR. Il Regolamento Generale sulla Protezione dei Dati, una normativa storica nella portata, ma tutt'altro che esaurita nei suoi effetti. Oggi, dopo un decennio di applicazione strategica e operativa, aziende, pubbliche amministrazioni e professionisti si confrontano tutti i giorni con una normativa sempre attuale e che è ancora in grado di guardare e guidare verso il futuro.

Non è un risultato scontato, anzi forse questa era la vera sfida sul tavolo del legislatore dieci anni fa: costruire una norma che potesse resistere al frenetico cambiamento di un mondo in cui il dato è sempre più nucleo e componente essenziale di ogni processo, di business come personale. Era così prima dell'avvento dell'intelligenza artificiale, lo è ancora di più adesso che gli algoritmi sono parte integrante nelle vite di aziende, enti pubblici e cittadini.

La perdurante attualità del GDPR non deve essere però associata a un fenomeno di immobilismo. In questi anni il testo del regolamento non è cambiato, ma è cambiato il valore di queste regole. Il GDPR è nato come una norma di protezione. E tuttavia, già dalla sua genesi, questa era solo una faccia della medaglia. Fin dalle prime bozze di questo regolamento ho sempre sostenuto che il GDPR fosse la nuova normativa in materia di circolazione e protezione dei dati personali. Circolazione e protezione come fondamenti della nuova disciplina europea sui dati. La protezione dei diritti e delle libertà fondamentali delle persone come faro e priorità di ogni intervento legislativo, diretta declinazione della tradizione costituzionale europea. La circolazione dei dati come apripista e abilitatore di quella che da lì a poco si è iniziata a chiamare data economy.

Arrivati al decimo anniversario di questa normativa, credo allora che il GDPR sia diventato adulto quando ha smesso di essere percepito solo come una disciplina della cosiddetta privacy ed è diventato, invece, infrastruttura per la generazione di valore fondato sui dati. Ecco che allora il GDPR non è più soltanto una norma di protezione, ma è anche – e oggi forse soprattutto – una norma di produzione.

Produzione di fiducia e affidabilità, di un vocabolario comune, di standard organizzativi e di governance, di qualità del dato. E quindi, in ultima analisi, di valore, efficienza e competitività per le organizzazioni.

Un cambio di paradigma giuridico ma prima ancora culturale, che tuttavia si deve saper cogliere.

Questa allora è la sfida del prossimo decennio. Di fronte agli inevitabili cambiamenti e alla crescente complessità nel mondo delle regole sui dati – dal Digital Omnibus alle intersezioni con le nuove normative in materia di intelligenza artificiale e cybersicurezza – società ed enti pubblici devono essere in grado di guardare al GDPR come nuova fonte di valore, anche economico. Per farlo servono presa di consapevolezza e formazione, al pari di adeguati investimenti. In questo cambio di passo, per non perdere un treno epocale, i Data Protection Officer possono e devono fare la differenza.

Questa funzione di controllo e consulenza è infatti la chiave strategica per trasformare la conformità normativa in un vero valore competitivo.

Quando il criminale assume un'intelligenza artificiale

A cura di Mohammed Bellala



Per anni il crimine informatico sofisticato è rimasto un'attività per pochi esperti. Servivano tempo, una buona padronanza delle lingue e competenze tecniche reali. Queste condizioni facevano da filtro: tenevano le operazioni più pericolose nelle mani di gruppi strutturati e ben finanziati, e relegavano il dilettante a danni di modesta entità. Quel filtro si è rotto. A romperlo è stata l'intelligenza artificiale, che oggi una parte consistente del crimine informatico utilizza come un normale strumento di lavoro.

È importante essere precisi su cosa sia cambiato, perché il punto sfugge a molti. L'AI non ha introdotto minacce inedite: il phishing, i deepfake, il malware esistevano già da tempo. A cambiare è stato **chi può permettersi di usarli, e su quale scala**. Operazioni che fino a poco fa richiedevano giorni di preparazione oggi si allestiscono in poche ore, con una qualità che prima era appannaggio dei professionisti.

Il meccanismo è questo: l'AI ha abbattuto le quattro barriere che proteggevano le organizzazioni dall'attaccante medio – il costo, la competenza, la lingua e la scala. Caduto quel muro, lo *script kiddie*, il dilettante che si limitava a copiare strumenti altrui senza comprenderli, è oggi in grado di condurre campagne con la sofisticazione e l'ampiezza che un tempo erano riservate a un gruppo organizzato, in alcuni casi persino a un attore sponsorizzato da uno Stato. È questa la trasformazione che ogni azienda dovrebbe avere chiara.

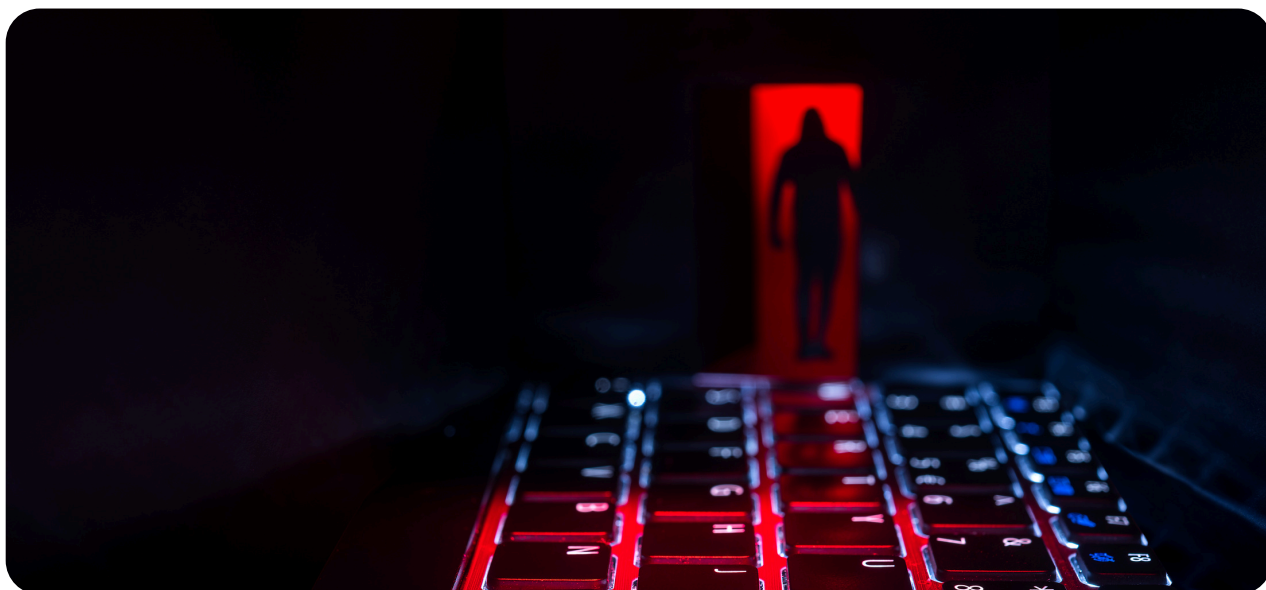
Non si tratta di allarmismo da convegno. L'Agenzia dell'Unione Europea per la Cybersicurezza, nel suo rapporto annuale, rileva che all'inizio del 2025 le campagne di social engineering supportate dall'AI rappresentavano oltre l'ottanta per cento dell'attività osservata nel settore a livello mondiale[1]. Non è una proiezione sul futuro. È la fotografia di ciò che accade già oggi.

Il falso senso di sicurezza del “non capiterà a noi”

C'è una convinzione che ricorre spesso nelle aziende, ed è sempre la stessa: “siamo troppo piccoli per interessare a qualcuno”, oppure “le nostre persone se ne accorgerebbero”. Era un ragionamento difendibile quando un attacco mirato costava tempo e fatica all'aggressore, che quindi sceglieva con cura le prede più grosse. Quella logica oggi non regge più.

Quando personalizzare un'email d'attacco non costa quasi nulla, non esistono più bersagli “troppo piccoli”. L'AI consente di raccogliere i dati pubblici di una persona – il profilo LinkedIn, i post, l'organigramma aziendale – e di confezionare un messaggio su misura per ciascun dipendente, in italiano impeccabile, con i riferimenti giusti al contesto. Il vecchio segnale d'allarme dell'errore grammaticale, quello su cui abbiamo costruito anni di formazione, è **semplicemente sparito**.

Il dato economico chiude il ragionamento: l'FBI ha



stimato per il 2025 perdite da crimine informatico vicine ai ventuno miliardi di dollari, e indica nei contenuti generati con l'AI uno dei fattori che rendono le frodi più difficili da riconoscere[2]. Chi pensa di essere fuori dal mirino, oggi, sta solo guardando dalla parte sbagliata.

Cinque mestieri che l'AI svolge per l'attaccante

Il modo più chiaro per capire cosa stia succedendo è smettere di ragionare in termini di "tecnologia" e iniziare a ragionare in termini di **ruoli**. Immaginiamo che un gruppo criminale abbia appena assunto un collaboratore artificiale. Quali mansioni gli affida? Almeno cinque, e le svolge tutte meglio, più in fretta e a un costo irrisorio rispetto a un complice umano.

1. Il Copywriter: il phishing che non sbaglia una parola

È il mestiere più maturo e quello con l'impatto più immediato. Secondo le analisi di settore, oltre l'ottanta per cento delle email di phishing è oggi generato con l'AI[3], e i tempi di confezionamento di una campagna si riducono drasticamente. Il modello linguistico scrive nella lingua del bersaglio, adatta il tono, conosce il gergo del settore. Sa fingersi l'ufficio risorse umane a gennaio, quando arrivano le comunicazioni sulle buste paga, o il corriere a dicembre. È instancabile e non lascia le tracce stilistiche – le sgrammaticature, le frasi tradotte male – su cui per vent'anni abbiamo addestrato le persone a insospettirsi.

2. L'attore: la voce e il volto del vostro amministratore delegato

Qui il salto è quello che spaventa di più, perché colpisce l'istinto più antico che abbiamo: fidarci di un volto e di una voce che riconosciamo. Bastano pochi secondi di audio – un video su YouTube, una vecchia intervista, un messaggio vocale – per clonare la voce di una persona. E la tecnologia è arrivata al video in tempo reale.

Il caso più noto è quello di una multinazionale dell'ingegneria, dove un dipendente del settore finance ha autorizzato un bonifico da circa venticinque milioni di dollari dopo aver partecipato a una videoconferenza con quello che credeva fosse il direttore finanziario e altri colleghi. Ogni volto su quello schermo era falso, ricostruito dall'AI a partire da materiale pubblico[4].

Non è un episodio isolato: nel solo secondo trimestre del 2025 i danni riconducibili a incidenti con deepfake hanno superato i trecentocinquanta milioni di dollari[5]. La vecchia frode del "falso CEO", che un tempo viaggiava su un'email maldestra, oggi vi telefona con la voce giusta.

3. Il ricognitore: ricognizione e scansione su scala industriale

Prima di colpire, un attaccante studia. Raccoglie informazioni sulla vittima, cerca i sistemi esposti, individua le falle non ancora corrette. È un lavoro che richiedeva pazienza e ore di setaccio manuale. L'AI lo automatizza e lo accelera: profila i dipendenti incrociando fonti pubbliche, cataloga le tecnologie in uso, e soprattutto aiuta a individuare e sfruttare vulnerabilità non corrette su larga scala. Dove prima passavano settimane tra la scoperta di una falla e il suo sfruttamento, oggi possono passare poche ore. Per chi difende, significa che la finestra utile per applicare una patch si è ristretta in modo brutale.

4. Lo sviluppatore: i "dark LLM" e il malware a noleggio

I modelli di AI commerciali hanno barriere etiche: se chiedete loro di scrivere un malware, rifiutano. Ma il mercato criminale ha risposto con versioni "liberate" da ogni vincolo – strumenti nati apposta per automatizzare l'ingegneria sociale e lo sviluppo di codice malevolo. L'ENISA documenta l'emergere di sistemi di AI malevoli autonomi e di finti strumenti di AI che, una volta scaricati, installano ransomware[6]. È importante essere onesti sulla portata del fenomeno: non siamo ancora di fronte a un crimine interamente automatizzato e autonomo. Quello che vediamo, oggi, sono operazioni *ibride*: l'essere umano dirige, l'AI esegue, accelera e amplifica. Che è esattamente ciò che rende il fenomeno scalabile.

5. L'industrializzatore: il crimine come servizio in abbonamento

L'ultimo mestiere è il più sottovalutato dai non addetti ai lavori, ma è quello che chiude il cerchio. L'AI ha reso possibile pacchettizzare l'intera catena d'attacco e venderla in abbonamento. Il phishing è ormai erogato "come servizio" – il cosiddetto *Phishing-as-a-Service* – con piattaforme pronte all'uso che permettono anche a chi non ha alcuna competenza di lanciare campagne sofisticate[7]. Stanno emergendo persino vettori d'attacco completamente nuovi legati a questo ecosistema, come l'avvelenamento dei file di configurazione degli strumenti di sviluppo o la registrazione di nomi di pacchetti software "allucinati" dai modelli stessi[8]. È qui che la barriera crolla del tutto: la competenza non è più un requisito. È un servizio che si compra.

Cosa cambia per chi decide

Messi in fila, questi cinque mestieri raccontano una storia sola: l'attaccante medio è diventato più bravo, più veloce e più economico. E lo ha fatto senza che la maggior parte delle aziende se ne accorgesse. La domanda, per un amministratore delegato o un

responsabile IT, non è più “verremo presi di mira?”, ma “quando succederà, le nostre difese saranno tarate sul vecchio attaccante o su quello nuovo?”.

Non servono rivoluzioni. Serve aggiornare alcuni presupposti che davamo per buoni:

- **La fiducia va verificata, sempre.** Una richiesta di bonifico o di credenziali non si valida più sulla voce o sul volto. Serve un secondo canale di conferma, una procedura concordata. Se vi chiamano “di corsa” e “in via riservata”, quello è il momento di insospettirsi, non di obbedire.
- **La formazione va riscritta.** Insegnare a cercare l'errore grammaticale oggi è inutile, anzi controproducente: dà un falso senso di sicurezza. Le persone vanno allenate sul contesto – l'urgenza ingiustificata, la segretezza richiesta, la pressione – non sulla forma del messaggio.
- **Il tempo di reazione è la nuova metrica.** Se l'attaccante sfrutta una falla in poche ore, applicare le patch “quando capita” non è più accettabile. La gestione delle vulnerabilità deve diventare rapida e, dove possibile, automatica.
- **L'identità resta il vero perimetro.** È il principio che vale più di ogni altro: autenticazione a più fattori ovunque, privilegi minimi, controllo continuo degli accessi. È l'ultima barriera che l'intelligenza artificiale non ha ancora abbattuto, e va presidiata di conseguenza.
- **Difendersi con l'AI, non solo dall'AI.** Lo stesso strumento che amplifica l'attacco amplifica la difesa: rilevamento comportamentale,



correlazione automatica degli eventi, threat hunting assistito. Chi rinuncia a usarlo combatte una guerra impari.

Conclusione: la barriera è caduta, la consapevolezza no

Il filo che lega tutto è uno solo. L'intelligenza artificiale non ha consegnato ai criminali un'arma che prima non esisteva. Ha fatto qualcosa di più sottile e, proprio per questo, più pericoloso: ha rimosso gli ostacoli che tenevano il crimine sofisticato nelle mani di pochi. Oggi quella sofisticazione è alla portata di chiunque disponga di una connessione e di una somma modesta da spendere nei canali giusti.

Per chi guida la trasformazione digitale – amministratori delegati, responsabili IT, responsabili della sicurezza – il messaggio è netto: l'avversario si è aggiornato. La buona notizia è che le contromisure esistono, sono note e in larga parte non richiedono investimenti proibitivi. Pretendono però una cosa che nessuna tecnologia può acquistare al posto dell'organizzazione, **la consapevolezza che la regola del gioco è cambiata.**

Il principio si può riassumere così: **se l'attacco è ormai alla portata di tutti, la difesa non può più restare un lusso di pochi.** Chi lo comprende per primo parte avvantaggiato. Chi aspetta di vederlo con i propri occhi lo vedrà comunque – ma sarà troppo tardi per dettarne i termini.

Note:

[1]ENISA, *Threat Landscape 2025* (ottobre 2025), basato sull'analisi di 4.875 incidenti registrati tra luglio 2024 e giugno 2025.

[2]FBI – Internet Crime Complaint Center (IC3), *Annual Report 2025*: perdite da crimine informatico segnalate pari a circa 21 miliardi di dollari.

[3]KnowBe4, *Phishing Trends Threat Report 2025*; dato ripreso da più fonti di settore (SlashNext, CrowdStrike).

[4]Caso Arup (febbraio 2024): un dipendente del settore finance della società di ingegneria trasferì circa 25 milioni di dollari dopo una videocall in cui tutti i partecipanti erano deepfake.

[5]Group-IB, *From Deepfakes to Dark LLMs* (settembre 2025): nel solo Q2 2025 i danni da incidenti con deepfake hanno raggiunto i 350 milioni di dollari (fonte Resemble.ai).

[6]ENISA, *Threat Landscape 2025*: emersione di sistemi di AI malevoli stand-alone (es. Xanthorox AI) e di siti che distribuiscono installer trojanizzati spacciati per strumenti di AI.

[7]ENISA, *Threat Landscape 2025*: il phishing resta il principale vettore di accesso iniziale (circa 60%), sempre più erogato come servizio (Phishing-as-a-Service).

[8]ENISA, *Threat Landscape 2025*: tra le nuove tecniche, il “Rules File Backdoor” (iniezione di istruzioni malevole nei file di configurazione degli assistenti di coding) e lo “slopsquatting” (registrazione di nomi di pacchetti “allucinati” dagli LLM).

Il passaggio dalla “Compliance sulla Carta” alle prove reali di Resilienza

A cura di Jim Biniyaz



Per anni molte organizzazioni hanno affrontato la cybersecurity e la compliance come un esercizio prevalentemente documentale: policy aggiornate, procedure approvate, registri compilati, questionari archiviati, contratti rivisti e report pronti per l'audit.

Tutti elementi importanti, ma non più sufficienti. In un contesto in cui incidenti cyber, interruzioni operative, attacchi alla supply chain e indisponibilità dei servizi possono generare impatti immediati sul business, la vera domanda non è più solo: “abbiamo la documentazione corretta?”. La domanda diventa: **siamo davvero in grado di resistere, rispondere e recuperare quando qualcosa va storto?**

È qui che avviene il passaggio dalla compliance sulla carta alle prove reali di resilienza: da un modello basato sulla dimostrazione formale dei controlli a un approccio fondato su test, evidenze operative, simulazioni e capacità misurabile di reazione.

Dal controllo documentale alla verifica operativa

La compliance tradizionale si è spesso concentrata sull'esistenza dei controlli: una policy di incident response, un piano di business continuity, una procedura di backup, una matrice dei rischi, un registro fornitori, un piano di formazione.

Il problema è che l'esistenza di un documento non garantisce la capacità reale di applicarlo. Un piano di continuità mai testato può fallire nel momento decisivo. Una procedura di escalation può risultare poco chiara durante un incidente. Un backup può essere formalmente previsto, ma non realmente ripristinabile nei tempi richiesti dal business.

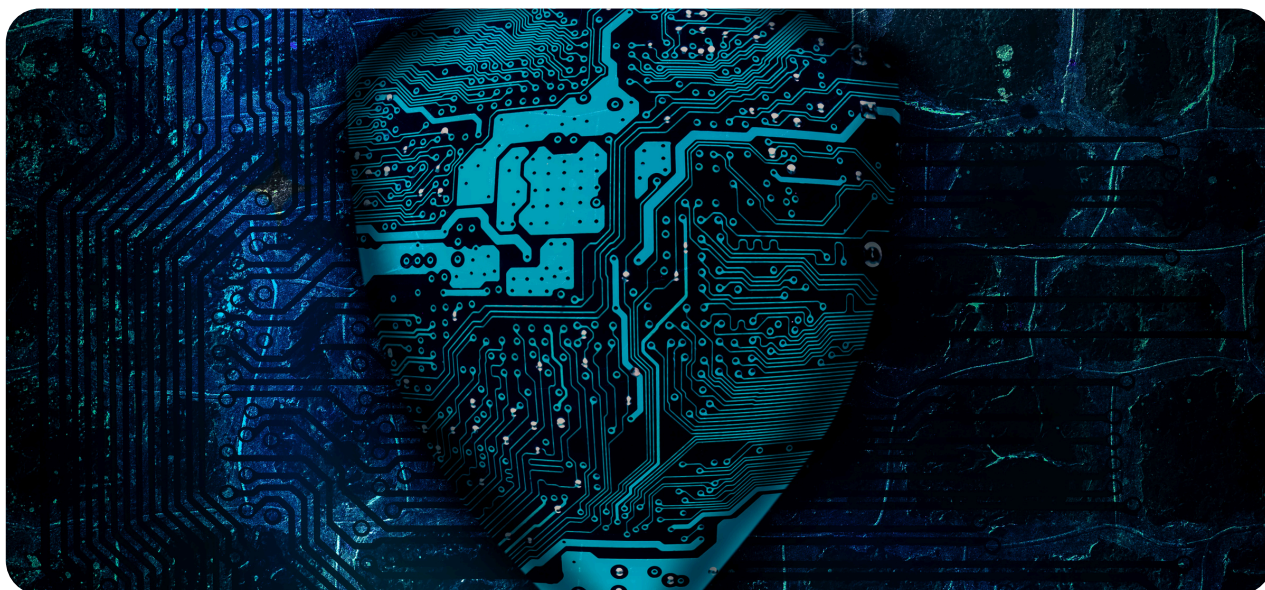
La resilienza, invece, richiede una verifica concreta. Non basta dichiarare che un controllo esiste: bisogna dimostrare che funziona, che è compreso dalle persone coinvolte e che produce risultati misurabili anche sotto pressione.

Che cosa significa provare la resilienza

Provare la resilienza significa sottoporre processi, sistemi, team e fornitori a scenari realistici, con l'obiettivo di misurare la capacità dell'organizzazione di prevenire, rilevare, rispondere e recuperare da un evento critico.

Le prove possono assumere forme diverse:

- simulazioni di incidente cyber;
- tabletop exercise con management, IT, security, legal e comunicazione;
- test di disaster recovery e business continuity;
- verifica dei tempi di ripristino dei backup;
- esercitazioni su ransomware, data breach o downtime;
- test di escalation interna;
- stress-test sui fornitori critici;



- analisi post-test con gap, remediation e lesson learned.

L'obiettivo non è dimostrare che tutto funziona perfettamente, ma far emergere in modo controllato le debolezze prima che diventino problemi reali.

Perché oggi è indispensabile

Il passaggio alle prove reali di resilienza è diventato indispensabile perché la complessità digitale è cresciuta. Le aziende dipendono da cloud provider, piattaforme SaaS (Software as a Service), software di terze parti, infrastrutture distribuite, dati condivisi, processi automatizzati e supply chain sempre più interconnesse.

In questo scenario, un incidente non colpisce solo un sistema tecnico: può bloccare processi operativi, interrompere servizi ai clienti, generare obblighi di notifica, esporre dati sensibili, danneggiare la reputazione e creare impatti economici rilevanti.

Anche il quadro normativo spinge in questa direzione. Regolamenti e direttive come DORA (Digital Operational Resilience Act), NIS2 (Network and Information Security Directive 2) e CRA (Cyber Resilience Act) chiedono alle organizzazioni di dimostrare una gestione del rischio più continua, concreta e verificabile. Non basta più avere procedure formalmente corrette: serve poter provare che le misure adottate sono efficaci, aggiornate e proporzionate al rischio.

I pilastri per passare dalla carta alla resilienza

Il primo passo è **identificare i processi critici**. Non tutto deve essere testato con la stessa intensità.

Bisogna partire da servizi essenziali, asset strategici, sistemi che trattano dati sensibili, fornitori critici e processi che, se interrotti, avrebbero un impatto diretto sul business.

Il secondo pilastro è **trasformare le procedure in scenari**. Una policy descrive cosa dovrebbe accadere; uno scenario verifica cosa accade davvero. Ad esempio: cosa succede se il sistema CRM resta indisponibile per 24 ore? Se un fornitore subisce un ransomware? Se un backup non è ripristinabile? Se il team chiave non è disponibile durante un incidente?

Il terzo elemento è **coinvolgere le funzioni giuste**. La resilienza non è solo un tema IT. Durante una crisi entrano in gioco security, legal, compliance, procurement, comunicazione, business owner e management. Testare la resilienza significa verificare anche ruoli, responsabilità, comunicazioni, escalation e capacità decisionale.

Il quarto pilastro è **misurare tempi e risultati**. Una prova senza metriche rischia di diventare una semplice esercitazione. È fondamentale misurare tempi di rilevamento, tempi di risposta, tempi di ripristino, qualità delle comunicazioni, disponibilità delle evidenze e capacità di rispettare gli obiettivi definiti.

Infine, serve **chiudere il ciclo con remediation concrete**. Ogni test deve produrre gap, priorità, owner, scadenze e azioni correttive. Senza remediation, la resilienza resta una simulazione. Con remediation tracciate e verificate, diventa un processo di miglioramento continuo.



Le metriche da monitorare

Per rendere la resilienza misurabile, servono KPI (Key Performance Indicators) chiari e comprensibili anche per il management.

Tra i più utili:

- tempo medio di rilevamento di un incidente;
- tempo medio di risposta;
- tempo medio di ripristino;
- rispetto di RTO (Recovery Time Objective) e RPO (Recovery Point Objective);
- percentuale di backup ripristinati con successo;
- numero di processi critici testati;
- numero di fornitori critici coinvolti in esercitazioni;
- remediation aperte e completate;
- gap ricorrenti emersi nei test;
- stato dei piani di business continuity;
- frequenza delle simulazioni;
- lesson learned effettivamente implementate.

Queste metriche permettono di trasformare la compliance da archivio documentale a sistema operativo di controllo, rendendo visibile il livello reale di preparazione dell'organizzazione.

Dalla compliance periodica alla resilienza continua

Il rischio principale è trattare le prove di resilienza come attività episodiche, organizzate solo in vista di audit, certificazioni o richieste regolatorie. Ma la resilienza non può essere testata una volta all'anno e poi dimenticata.

Serve un modello continuo, in cui test, evidenze,

remediation, aggiornamento dei rischi e reporting siano integrati nella governance aziendale. Ogni incidente simulato, ogni vulnerabilità critica, ogni cambiamento infrastrutturale e ogni nuovo fornitore dovrebbe alimentare una vista aggiornata della capacità di risposta dell'organizzazione.

In questo modo, la compliance smette di essere una fotografia statica e diventa un processo vivo, capace di adattarsi all'evoluzione delle minacce, dei sistemi e del business.

Dalla documentazione alla dimostrazione

La compliance sulla carta resta necessaria, ma non può più essere il punto di arrivo. Policy, procedure e registri servono solo se sono collegati a controlli reali, testati e migliorati nel tempo.

Le aziende più mature non si limiteranno a chiedersi se hanno tutti i documenti richiesti. Si chiederanno se quei documenti funzionano davvero quando l'organizzazione è sotto pressione.

Il passaggio decisivo è proprio questo: dalla documentazione alla dimostrazione, dalla dichiarazione di conformità alla prova concreta di resilienza.

In un mondo digitale sempre più interconnesso, non vince chi ha il fascicolo più ordinato, ma chi riesce a continuare a operare, reagire con lucidità e recuperare rapidamente quando un incidente mette alla prova l'intera organizzazione.



Architettura di riferimento Agentic AI pronta per ISO/IEC 27001:2022

A cura di Andrea Ceiner

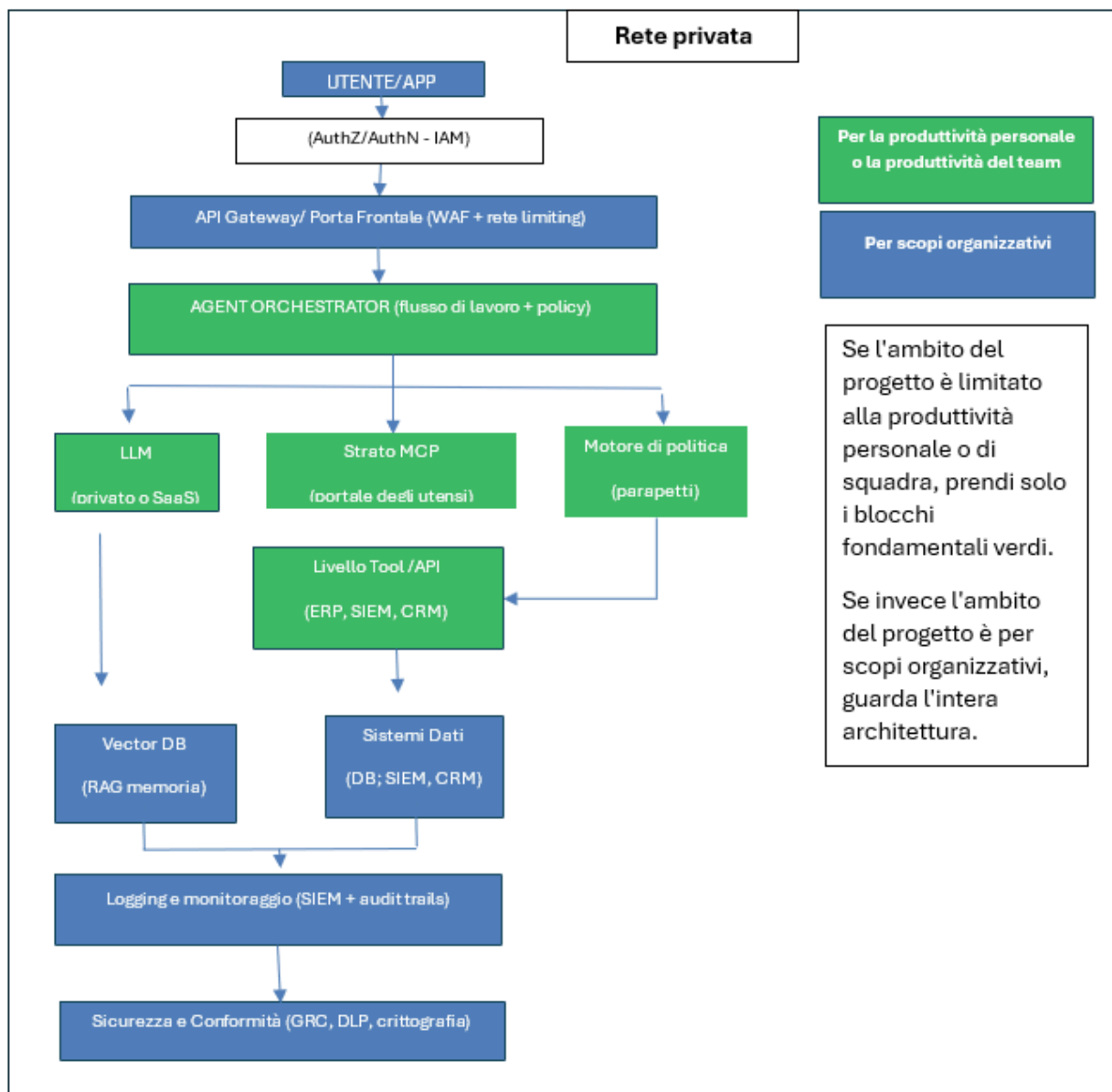


Man mano che le organizzazioni adottano rapidamente l'IA Agentic, un rischio diventa sempre più evidente: l'approccio "fai-da-te" non scala dal punto di vista della sicurezza e della conformità.

Costruire agenti assemblando componenti ad hoc - senza un'architettura strutturata - spesso porta a controlli incoerenti, responsabilità poco chiare e lacune critiche in aree come la gestione dell'identità, l'auditabilità e la protezione dei dati.

Un'architettura di riferimento fornisce una base condivisa e standardizzata per i team IT e DevOps. Garantisce che ogni implementazione segua gli stessi principi di progettazione, integri la sicurezza di default e rimanga allineata con framework come ISO/IEC 27001:2022.

In breve, invece di reinventare la ruota per ogni progetto, le organizzazioni possono **industrializzare l'adozione dell'IA Agente**, riducendo rischi,



migliorando la governance e accelerando la distribuzione. Nella pagina precedente trovate uno schema dell'architettura di riferimento raccomandata da implementare all'interno della tua rete privata.

Un sistema Agentic AI conforme a ISO 27001 distingue chiaramente:

- Cognizione (LLM)
- Memoria (DB/DB vettoriale)
- Azione (Strumento)
- Controllo (MCP + orchestratore) che fornisce sicurezza tramite IAM, logging e applicazione centralizzata delle politiche.

Componenti chiave

1. Gestione dell'Identità e degli Accessi (IAM): OBBLIGATORIO

- RBAC/ABAC per utenti e **agenti**
- Identità separata per ogni agente (senza account condiviso)
- MFA per l'accesso umano

Principio chiave: L'agente è un "utente privilegiato non umano"

2. API Gateway + WAF: FACOLTATIVO CONSIGLIATO

- Protezione dell'input (iniezione rapida, abuso)
- Limitazione del tasso
- TLS richiesto

Riduce:

- Attacchi di iniezione prompt LLM
- Esfiltrazione dei Dati

3. Agente Orchestratore (Nucleo di Controllo)

- Gestione del flusso di lavoro (pianificatore, esecutore, revisore)
- Controllo passo dopo passo (HITL opzionale)
- Timeout e ritentativi controllati

Deve garantire:

- **Determinismo operativo**
- Logging completo

4. Strato LLM (isolato)

- **Private** LLM / Azure OpenAI / tenant isolation
- Sanitizzazione tempestiva
- Nessun accesso diretto a dati sensibili

Pattern sicuro: LLM non accede mai direttamente ai database

5. Protocollo di Contesto del Modello (MCP) – PUNTO DI CONTROLLO CRITICO

- Unico gateway per: API, DB, strumenti

Funzioni:

- Autorizzazione per lo strumento
- Filtraggio in ingresso/uscita
- Revisione

IMPORTANTE: MCP = punto di controllo della sicurezza per l'agente

6. Livello Dati (DB + DB vettoriale)

- Classificazione dei dati
- Crittografia a riposo + in transito
- Separazione: RAG pubblico/ **interno** /sensibile

Questioni critiche:

- vettore DB = rischio di perdita semantica

Mitigazioni:

- Blocchi controllati
- Controllo degli accessi per l'incorporamento

7. Livello Strumento/API

- Accesso mediato solo tramite MCP
- Nessun accesso diretto da LLM

Migliori Pratiche:

- API a portata limitata
- Principio del minimo privilegio



8. Registrazione, Monitoraggio, SIEM

Registri richiesti:

- Prompt di input/output
- Azioni dell'agente
- Accesso ai dati
- Decisioni MCP

Deve permettere:

- Traccia completa di audit
- Analisi Forense

9. Livello di Sicurezza e Conformità

Include:

- DLP (evita perdite da prompt/risposta)
- Mascheramento dati
- Gestione delle chiavi (KMS)

Controlli specifici dell'"IA Agentica"

Controlli minimi per audit ISO 27001

1.Segregazione dei ruoli

- Agente ≠ Umano
- MCP ≠ logica aziendale

2.Traccia completa di audit

- Ogni decisione è stata tracciata

3.Controllo dell'accesso ai dati

- RAG filtrato per ruolo

4.Controllo degli utenti

- Strumento di Lista di Permessi per Agenti

5.L'essere umano nel ciclo (HITL)

- per azioni critiche (ad esempio modifica del sistema)

Architettura pronta per l'audit

Per essere conforme alla norma ISO 27001 devi dimostrare che:

- Agente controllato

- I dati sono protetti
- Le azioni sono tracciate
- L'accesso è limitato

10. Conclusioni

L'IA agentica introduce un nuovo paradigma in cui le entità software possono ragionare, agire e interagire autonomamente con i sistemi aziendali. Questo cambiamento ci costringe a ripensare la sicurezza: **gli agenti devono essere trattati come identità privilegiate non umane, governate con lo stesso rigore degli utenti** umani, se non di più.

Un'architettura efficace non riguarda solo i livelli tecnologici, ma il controllo:

- controllo sull'accesso (IAM e privilegio minimo),
- controllo sulle decisioni (applicazione delle politiche e MCP),
- controllo sui dati (classificazione, DLP e isolamento),
- e controllo sulle azioni (auditabilità e monitoraggio).

La conclusione chiave è semplice: **senza un controllo strutturato, l'autonomia diventa rischio.**

Adottando un'architettura di riferimento standardizzata e pronta per l'audit, le organizzazioni possono:

- scalare in sicurezza l'IA Agentica tra casi d'uso,
- garantire tracciabilità e conformità,
- e trasformare l'innovazione in una capacità controllata e affidabile, piuttosto che in un esperimento non gestito.

L'IA agentica è potente, ma solo se è **progettata per essere sicura per costruzione.**

Rischi chiave (da gestire esplicitamente)

Rischio	Dove	Mitigazione
Iniezione immediata	LLM	Sanitizzazione + Motore di politiche
Perdita di dati	Vector DB	Controllo accesso + DLP
Azioni non autorizzate	MCP/Strumenti	RBAC + elenco dei permessi
Mancanza di audit	Orchestratore	Logging end-to-end
Agente sovraprivilegiato	IO	Minore privilegio

COME TI CREO UNA PASSWORD "INVIOLABILE"

www.assintel.it
info@assintel.it

Un giorno qualunque...

Ciao
DOC, hai qualche
indicazione su come
creare una
password?

Ma certo
Marky. Eccoti
qualche consiglio per
creare una password
sicura.

Usa una
frase, che ti
ricordi, che so di
una canzone.

Poi,
sostituisci alcune
lettere con numeri ed
inserisci caratteri
speciali...

...cerca
di non usare le
maiuscole all'inizio, o il
punto esclamativo
alla fine

Ecco
un esempio
pratico:
miF@St@r3B3ne

Carina
DOC

Un'altra cosa
che è bene
ricordarsi è
quella di non
usare dati
riconducibili a te
o ai tuoi cari...

Tipo?

Tipo: date di compleanno,
nomi di vie, nomi di
animali, nomi dei tuoi cari,
ecc. Dati facilmente
desumibili da quello che
pubblichiamo sui social.

E ricorda
di attivare sempre, o
quasi, almeno la verifica
a due fattori (2FA)

Ma
Doc, è
scomoda...

Nota: valutare anche la Multi Fattore (MFA)

In realtà no. Sui social
network, LinkedIn ad
esempio, una volta che
hai verificato il device,
se non ti disconnetti,
non te la richiede più...

E se qualcuno
prova ad
entrare con le
tue credenziali
non riesce e, in
alcuni casi,
ricevi un avviso.

Ah...non
lo sapevo!

Grazie
Doc per questi
consigli. Ci vediamo
presto!

Credits: NWN solutions

Cavi sottomarini, la nuova frontiera della sicurezza cyber-fisica

A cura di Stefano da Empoli e Alessandro D'Amato



La rete globale dei cavi sottomarini è una delle infrastrutture critiche dell'economia digitale: veicola la quota prevalente del traffico dati intercontinentale e connette mercati, piattaforme, centri finanziari e poli tecnologici. Per questo, la sua sicurezza non riguarda più soltanto la continuità delle telecomunicazioni, ma investe competitività, autonomia strategica e sicurezza nazionale, in una dimensione che è insieme fisica e cibernetica.

La resilienza di queste infrastrutture è divenuta oggetto di crescente attenzione. Secondo il Submarine Telecoms Forum, negli ultimi dieci anni si sono registrati circa 259 guasti sui cavi sottomarini: tra questi, l'International Cable Protection Committee attribuisce una quota rilevante ad attività di ancoraggio o pesca, cui si aggiungono eventi geologici, abrasione dei fondali marini e malfunzionamenti dell'impianto. Una parte consistente resta tuttavia non riconducibile a una causa specifica: questo non consente, di per sé, di attribuire automaticamente questi episodi ad azioni intenzionali, ma impone di considerare anche scenari di sabotaggio, interferenza o pressione geopolitica, soprattutto alla luce degli episodi verificatisi nel Nord Europa.

Sotto i riflettori, tuttavia, sono finiti quasi esclusivamente guasti – intenzionali o meno – che hanno riguardato la componente fisica dell'infrastruttura: questa prospettiva, pur fondamentale, rischia però di lasciare in secondo

piano la dimensione cibernetica. Tali infrastrutture, infatti, non sono meri condotti di trasmissione dati, ma sistemi complessi composti da apparati ottici, sistemi di alimentazione, *landing station*, centri operativi, piattaforme di supervisione e *network management systems*.

Le *landing station* rappresentano, in particolare, un nodo critico: qui il cavo emerge dal mare e si connette alle reti terrestri, ospitando apparati di alimentazione, supervisione, instradamento e gestione del traffico. Un attacco contro tali stazioni potrebbe assumere forme diverse: sabotaggio fisico, interruzione dell'alimentazione elettrica, compromissione dei sistemi di controllo, accesso non autorizzato agli apparati di gestione o interferenza con le procedure operative. A differenza dell'intercettazione diretta del cavo sul fondale, tecnicamente complessa e difficilmente realizzabile senza generare allarmi, la compromissione dei sistemi a terra o dei sistemi di gestione appare uno scenario più plausibile e, per certi versi, più rilevante dal punto di vista della cybersecurity.

La crescente digitalizzazione e remotizzazione della gestione dei cavi amplia ulteriormente il profilo di rischio: livelli software e sistemi di controllo connessi, se non adeguatamente protetti, possono ampliare la superficie d'attacco e consentire a un attore ostile di ottenere visibilità sui flussi di traffico, sulle configurazioni di rete e sulle vulnerabilità fisiche dell'infrastruttura.



A ciò si aggiungono i rischi legati a fornitori terzi, manutenzione da remoto, credenziali privilegiate e sistemi legacy, che in un ecosistema distribuito possono trasformare una vulnerabilità tecnica in un punto di accesso strategico. Come indicato dalla stessa ENISA (Agenzia dell'Unione europea per la cibersicurezza) nel report “*Subsea Cables - What Is At Stake?*”, in scenari più gravi un accesso illecito ai sistemi di gestione potrebbe permettere attività di monitoraggio, deviazione, degradazione o interruzione del traffico. Nella stessa direzione va anche il report UNDRR-ITU (UNDRR: Ufficio delle Nazioni Unite per la riduzione del rischio di catastrofi; ITU: Unione internazionale delle telecomunicazioni) “*When digital systems fail*”, che sottolinea come un'interruzione prolungata può propagarsi a pagamenti, logistica, servizi pubblici, sanità e capacità di risposta alle emergenze, soprattutto quando la riparazione dipende da poche navi specializzate e da procedure autorizzative complesse.

La risposta sul piano delle policy è già partita, sia a livello europeo che nazionale. Due anni fa è stata la volta della Raccomandazione 2024/779, che ha poi portato al Cable Security Action Plan del 2025, mentre lo scorso febbraio si è giunti al Cable Security Toolbox, contenente misure di mitigazione e progetti di interesse europeo. Dando attuazione all'Action Plan, la Commissione europea ha annunciato nel giugno 2026 l'assegnazione di 5,8 milioni di euro per i primi due Regional Cable Hubs, uno nel Mar Baltico e uno nel Mediterraneo, riconosciuti come gli ambiti più sensibili a minacce esterne. Mentre il primo sarà coordinato dalla Finlandia, il secondo, sostenuto con un finanziamento europeo di 3,3 milioni di euro, sarà coordinato dall'Italia con il supporto di Grecia, Cipro e Malta. L'hub mediterraneo combinerà procedure comuni, strutture decisionali condivise e una piattaforma tecnologica federata, con l'obiettivo di uno scambio di informazioni quasi in tempo reale, l'individuazione di anomalie e una risposta coordinata agli incidenti. A gestire la *call for proposals* e l'assegnazione dei finanziamenti sarà lo European Cybersecurity Competence Center, basato a Bucarest.

Rispetto alle politiche orizzontali, resta centrale il combinato disposto tra le direttive NIS2 e CER (Network and Information Security 2 / Critical Entities Resilience), già recepite in Italia, che incidono sul perimetro delle infrastrutture digitali e delle comunicazioni elettroniche, imponendo agli operatori interessati misure tecniche, operative e organizzative di gestione del rischio fisico e cibernetico, secondo l'ormai imprescindibile approccio *all-hazard*.

Sul versante nazionale, la legge 9/2026 compie un passo ulteriore nella dimensione subacquea, affidando alla nuova Agenzia per la sicurezza delle

attività subacquee (ASAS) compiti di monitoraggio, sorveglianza, piani di emergenza e procedure di manutenzione e riparazione per cavi e condotte. Proprio per le funzioni attribuitele, l'ASAS potrà svolgere un ruolo importante se opererà in stretto raccordo con ACN (Agenzia per la Cybersicurezza Nazionale), Difesa, autorità marittime e operatori privati. Il banco di prova sarà tradurre questo impianto in capacità operative, evitando duplicazioni e mettendo al centro il coordinamento interistituzionale e con gli attori industriali. In tema, si colloca anche la recente Strategia nazionale per la resilienza dei soggetti critici che cita espressamente i cavi sottomarini agli obiettivi 2.3 e 2.6.

Il punto non è soltanto proteggere il tracciato sottomarino, ma costruire un sistema di resilienza multilivello, capace di combinare sorveglianza marittima, sicurezza cyber, capacità satellitari e continuità operativa. In questa prospettiva, il paradigma Space and Blue, anche attraverso l'apposita convenzione tra Agenzia Spaziale Italiana (ASI) e Ministero delle Imprese e del Made in Italy (MIMIT), firmata lo scorso 24 dicembre e seguita da appositi bandi rivolti ai diversi attori della filiera, può valorizzare competenze nazionali in sensoristica, IA (Intelligenza Artificiale), cybersecurity, tecnologie quantistiche e *rerouting* satellitare.

Ne deriva che la resilienza dei cavi sottomarini deve essere interpretata nell'ottica di una più ampia e sistemica sicurezza cyber-fisica.

Il report ENISA NIS360 pubblicato a maggio colloca i servizi *digital-by-default* – incluse telecomunicazioni, cloud e data center – tra i settori più critici per l'economia e la società, con possibili effetti a cascata ben oltre il perimetro tecnico della rete. Per questo, la protezione dei cavi richiede non solo sorveglianza marittima, diversificazione delle rotte e rapidità nelle riparazioni, ma anche sicurezza dei sistemi di gestione, controllo degli accessi, monitoraggio continuo e procedure chiare e tempestive di *incident reporting*.

Il passaggio decisivo per l'Italia sarà tradurre il nuovo impianto regolatorio e istituzionale in una governance effettiva: ASAS, ASI, ACN, Difesa, autorità competenti per l'ambiente marittimo e subacqueo e operatori privati dovranno agire come parti di un'unica architettura composita, evitando che una vulnerabilità locale – fisica o digitale – produca effetti sistemici sulle funzioni essenziali a livello nazionale e regionale.

Evoluzione delle normative europee dell'area digitale

A cura di Carlo Guastone



Negli ultimi anni si è registrata in Europa e in Italia la pubblicazione di svariate normative che hanno reso sempre più complessa la compliance al quadro normativo nello svolgimento di processi digitali. Tali normative si sono proposte come snodi fondamentali per lo sviluppo economico e tecnologico dei mercati, nel rispetto dei diritti fondamentali delle persone e delle organizzazioni, introducendo, a volte, specifiche sanzioni per rinforzare il livello di ottemperanza richiesto. Il numero, la complessità e la interrelazione fra le singole norme sta determinando la percezione di una eccessiva frammentazione legislativa (si è parlato in più sedi di una «giungla»).

E' opportuno evidenziare, al riguardo, che sono in corso alcuni aggiornamenti del quadro normativo europeo dell'area digitale, motivati da esigenze di una maggior armonizzazione e semplificazione delle norme, e dalla necessità di governare l'evoluzione delle tecnologie considerando il crescente impatto delle stesse sul mercato e sui diritti delle persone. Ci riferiamo in particolare a tre proposte UE di aggiornamento-integrazione di alcune normative, proposte pubblicate fra novembre 2025 e gennaio 2026. Non è semplice ipotizzare i tempi necessari per la valutazione e approvazione delle proposte riportate nel seguito da parte delle autorità coinvolte (Commissione europea, Parlamento europeo e Consiglio dell'Unione europea), tuttavia è ragionevole ipotizzare che le proposte potranno entrare gradualmente in vigore nei prossimi anni.

Digital Omnibus - COM (2025) 837

La proposta, pubblicata il 19 novembre 2025, ha l'obiettivo di semplificare e razionalizzare l'intero quadro legislativo digitale dell'UE, riducendo sovrapposizioni normative e costi amministrativi per imprese e pubbliche amministrazioni. Le principali modifiche normative previste riguardano GDPR, Direttiva ePrivacy, Direttive NIS2 e CER (Cyber Entity Resilience Act), Data ACT con incorporazione del DGA (Data governance Act).

Il tema centrale e più controverso è la ridefinizione del concetto di dato personale: un dato sarebbe considerato personale solo se il titolare ha mezzi ragionevoli per identificare la persona. Si registra al riguardo una forte opposizione da parte di EDPB (Comitato europeo per la protezione dei dati) e EDPS (Garante europeo per la protezione dei dati), che ritengono che la ridefinizione del concetto di dato personale ridurrebbe in modo significativo le tutele dei dati personali.

Novità più significative della proposta COM 837:

- passaggio da 72 a 96 ore per notificare i data breaches, obbligo di notifica solo se vi è un rischio elevato per i diritti degli interessati;
- portale unico europeo per notificare incidenti di cybersicurezza (NIS 2), data breaches GDPR, incidenti DORA, futuri obblighi CER;
- consenso gestito direttamente nel browser, come preferenza unica applicata a tutti i siti;



- informative più brevi, semplificate, e standardizzate a livello europeo;
- chiarimenti definitivi su ruoli e responsabilità, semplificazioni per PMI e mid-cap;
- maggiore allineamento GDPR-AI Act-Data Act, con riduzione di oneri documentali per trattamenti a basso rischio;
- utilizzo di dati personali per training di modelli IA basato su legittimo interesse, con nuove garanzie e limiti.

Digital Omnibus on AI - proposta COM (2025) 836

La proposta, pubblicata il 19 novembre 2025, riguarda la semplificazione dell'attuazione delle regole sull'intelligenza artificiale, tramite la modifica dell'AI Act. La proposta nasce dalle prime difficoltà emerse nella fase di implementazione dell'AI Act e dalle consultazioni con imprese, autorità e PMI. L'obiettivo dichiarato è semplificare l'attuazione dell'AI Act, confermando l'approccio basato sul rischio, senza ridurre il livello di tutela dei diritti fondamentali, tramite una revisione mirata che incide su tempistiche, procedure e governance.

Il 30 giugno 2026 il Consiglio dell'UE ha approvato alcuni aggiornamenti della proposta COM 836, fra le quali il rinvio delle scadenze relative ai sistemi AI ad alto rischio: le nuove scadenze sono il 2 dicembre 2027 per i sistemi AI ad alto rischio autonomi, e il 2 agosto 2028 per i sistemi AI ad alto rischio integrati nei prodotti.

Novità più significative della proposta COM 836:

- snellimento della documentazione per i sistemi ad alto rischio;
- processi di valutazione della conformità per i sistemi ad alto rischio basati su linee guida ufficiali della Commissione;
- allineamento con altri schemi di certificazione UE (medical device regulation, machinery regulation, aviation regulation);
- presenza di un meccanismo di rinvio condizionato, gli obblighi high-risk non scatterebbero più a data fissa, ma sei o dodici mesi dopo la conferma di "misure adeguate a supporto della conformità" con date limite invalicabili;
- rafforzamento del ruolo dell'AI Office europeo, relativamente al coordinamento delle linee guida con la presenza di un punto unico di contatto (AI Act Service Desk);
- previsto il potenziamento dell'AI Service desk, tramite linee guida operative, template standard, webinar e soluzioni per ridurre costi e complessità per le imprese più piccole;
- non richiesta la registrazione per sistemi non considerati ad alto rischio dopo valutazione interna e documentazione alleggerita per le imprese più piccole.

Proposta Cybersecurity ACT 2

La Proposta del 26 gennaio 2026 punta a rafforzare la sovranità digitale europea e a rendere più assertiva la difesa informatica.

Novità più significative della proposta:

- rinforzo del ruolo operativo di ENISA (European Union Agency for Cybersecurity);
- introduzione di meccanismi per identificare ed eventualmente escludere fornitori ad "alto rischio" da settori critici;
- razionalizzazione della "giungla" legislativa per armonizzare il testo con la Direttiva NIS2 e il CRA (Cyber Resilience Act). E' opportuno precisare che il CRA richiede la marcatura CE obbligatoria per prodotti digitali hardware e software dotati di elementi digitali connessi direttamente o indirettamente a una rete o a un altro dispositivo, a decorrere dall'11 dicembre 2027, mentre gli obblighi di comunicazione all'ENISA e alle autorità competenti delle vulnerabilità e degli incidenti di sicurezza si applicheranno a decorrere dall'11 settembre 2026.
- accelerazione dei processi di certificazione definiti da ENISA per prodotti, servizi e processi ICT rendendoli più agili ed efficaci: a) EUCC (European Cybersecurity Certification Scheme on Common Criteria), già disponibile, per la certificazione di prodotti ICT (hardware, software e componenti come chip e smartcard).



b) EUCS (Cloud Services Scheme), già disponibile, per la certificazione dei Servizi di cloud computing (IaaS, PaaS, SaaS). c) EU5G (5G Cybersecurity Certification Scheme), in fase avanzata di finalizzazione, per la certificazione della Sicurezza delle infrastrutture e dei componenti delle reti mobili 5G. d) EUMSS (Managed security services Scheme), in fase di sviluppo dal giugno 2025, per la certificazione dei Servizi di sicurezza gestiti.

Tendenze di mercato e Impatti delle proposte per le aziende

Il concetto che accomuna le proposte è la volontà di definire un sistema comune di compliance dell'area digitale, evitando sovrapposizioni fra le singole norme e focalizzando l'attenzione su tre tematiche fondamentali: certificazione di sicurezza dei prodotti digitali, con i relativi impatti sul sistema competitivo dei prodotti digitali e sui diritti delle persone, sicurezza e rischi delle soluzioni di intelligenza artificiale, trasparenza e integrazione del risk assessment.

Proprio il risk assessment dell'area digitale sembra farla da padrone in ogni normativa che ormai, sull'onda di quanto previsto da NIS2, è una practice che esce dalla sfera tecnico-organizzativa per atterrare nella sfera manageriale con responsabilizzazione del Top management.

Quale lo scenario che le aziende dovranno pertanto affrontare? Il primo step è quello della comprensione della tematica e delle sue relazioni con il business. Le tre proposte considerate non determinano una rifondazione della compliance, quanto una manutenzione straordinaria dei sistemi di controllo. Questo fatto non semplifica il problema, perché richiede una profonda conoscenza dei processi di controllo nelle aziende e delle tecnologie adottate. Il secondo step, che probabilmente è il più complesso da realizzare, è la messa in campo di un approccio integrato al rischio che abbini i rischi delle applicazioni ICT, i rischi cyber, i rischi dei sistemi di intelligenza artificiale e i rischi dei trattamenti di dati personali, per limitarci solo ad alcune aree di rischio. Al riguardo non è secondario sottolineare che il management aziendale è sempre più coinvolto nella gestione di tutti rischi aziendali e che, di conseguenza, la gestione integrata del rischio assumerà sempre più rilevanza.



CYBER
Think Tank
ASSINTEL

Unisciti alla nostra
community!

Scrivi a segreteria@assintel.it
per avere maggiori info



Cos'è il phishing?



Una truffa online che cerca di carpire le tue informazioni personali (password, numeri di carta di credito, ecc.) fingendosi qualcuno di fidato (banca, social network, ecc.).

Come Funziona?



Email

Messaggi che sembrano provenire da enti affidabili, ma contengono link dannosi.



Siti Web falsi

Pagine che imitano perfettamente quelle originali per indurti a inserire i tuoi dati.



Messaggi

SMS o notifiche push che ti invitano a cliccare su link pericolosi.



Chiamata

furto di informazioni personali tramite telefono.

Perché lo fanno?

I cyber criminali utilizzano il phishing per:



Rubare informazioni personali.



Spiare le aziende.



Crittografare i dati e chiedere un riscatto.



Diffondere malware.

Cosa sfruttano?

Le loro armi sono:

La paura:

Ti minacciano di conseguenze negative.



L'avidità:

Ti promettono ricompense incredibili.



L'urgenza:

Ti spingono ad agire subito.

L'inganno:

Ti fanno credere di essere qualcuno di fidato.



Come difendersi?



Verifica l'indirizzo e-mail:

Controlla attentamente l'indirizzo del mittente.



Non cliccare su link sospetti:

Evita di cliccare su link presenti in e-mail o messaggi non richiesti.



Controlla l'URL:

Assicurati che l'indirizzo del sito web inizi con "https://" e abbia un certificato di sicurezza.

Non fornire mai informazioni personali:

Non comunicare mai password, codici di sicurezza o dati sensibili tramite e-mail o messaggi.



Utilizza un antivirus e un firewall:

Proteggi il tuo dispositivo con software di sicurezza aggiornati.



Tieniti aggiornato:

Informati sulle ultime truffe online.



L'illusione dell'intelligenza: perché l'AI sta cambiando la cybersecurity più degli hacker

A cura di Francesco Iarlori



Dalla sicurezza perimetrale alla sicurezza cognitiva: come l'Intelligenza Artificiale sta trasformando il concetto stesso di difesa digitale.

Per oltre quarant'anni la sicurezza informatica è stata una disciplina relativamente chiara. Esistevano sistemi da proteggere, reti da monitorare, vulnerabilità da correggere e aggressori da fermare. Le tecnologie cambiavano rapidamente, ma il paradigma rimaneva sostanzialmente invariato: difendere un perimetro digitale.

Oggi, con la diffusione dell'Intelligenza Artificiale generativa, stiamo assistendo a qualcosa di profondamente diverso. Non siamo di fronte a una semplice evoluzione tecnologica, ma a una trasformazione che coinvolge il modo stesso in cui le persone prendono decisioni, producono conoscenza e interagiscono con i sistemi informativi.

Dopo aver vissuto diverse rivoluzioni tecnologiche - dall'era Unix degli anni Ottanta all'esplosione di Internet, dalla telefonia mobile, satellitare ed ai pagamenti digitali - sono convinto che l'AI rappresenti una discontinuità ancora più profonda. Per la prima volta, infatti, non stiamo automatizzando soltanto attività operative, ma stiamo delegando parte dei nostri processi cognitivi.

Ed è proprio qui che emerge la nuova frontiera della cybersecurity.

Dalla protezione dei sistemi alla protezione delle decisioni

Storicamente, la sicurezza informatica si è focalizzata sulla protezione di asset chiaramente definiti, quali server, database, applicazioni, reti e dispositivi. Negli ultimi anni, in numerosi incontri con aziende dei settori Finanza e Telecomunicazioni, è emersa la crescente necessità di salvaguardare le proprie transazioni e gli asset trasmissivi, inclusi cavi sottomarini e satelliti.

Con l'AI generativa, il bersaglio si sposta progressivamente verso la conoscenza e i processi decisionali. Qui i settori sono trasversali, non solo le domande riguardano come introdurre nuove intelligenze in azienda in modo organico, ma anche come proteggerle.

Quando un professionista utilizza un Large Language Model per redigere un documento, sintetizzare un contratto o analizzare dati aziendali, il problema non è più soltanto proteggere il computer che utilizza. Occorre comprendere come vengono generate le informazioni, quali fonti vengono utilizzate, quali errori possono essere introdotti e quali conseguenze possono derivare da una fiducia eccessiva nei risultati prodotti dalla macchina.

La vulnerabilità non risiede più soltanto nel software, ma nel rapporto di fiducia che si instaura tra essere



umano e sistema intelligente.

L'evoluzione dell'attaccante

Anche il profilo dell'aggressore sta cambiando.

Per anni abbiamo associato l'hacker a competenze tecniche elevate: capacità di programmazione, conoscenza delle reti, studio delle vulnerabilità.

L'AI abbassa significativamente questa barriera.

Oggi strumenti avanzati consentono di generare codici, creare campagne di phishing estremamente convincenti, tradurre testi in molte lingue e simulare comunicazioni aziendali con una qualità che fino a pochi anni fa richiedeva competenze specialistiche. Ricordo che negli anni '90 le prime truffe erano abbastanza riconoscibili, mail e siti erano palesemente falsi, anche alla vista di un occhio poco esperto.

Il cybercriminale del futuro potrebbe non essere il miglior programmatore, ma il miglior orchestratore di strumenti intelligenti.

Questo fenomeno democratizza, purtroppo, la capacità offensiva e rende più difficile distinguere una comunicazione autentica da una manipolata.

Il problema della fiducia

Uno degli aspetti meno discussi riguarda il concetto di fiducia.

Nella sicurezza tradizionale il principio *trust but verify* ha sempre rappresentato una buona pratica. Con l'AI questo principio diventa essenziale.

I modelli generativi possono produrre contenuti corretti, plausibili e ben scritti anche quando le informazioni sottostanti sono errate. Possono inventare riferimenti bibliografici, generare dati inesistenti o formulare conclusioni apparentemente convincenti ma prive di fondamento.

La sfida non consiste soltanto nell'individuare contenuti malevoli, ma nel riconoscere quelli che appaiono credibili senza esserlo. Il problema diventa semantico.

Per questo motivo, ritengo che la cybersecurity del prossimo decennio dovrà integrare competenze provenienti da discipline diverse: psicologia cognitiva, comunicazione, gestione del rischio, governance dei dati e intelligenza artificiale.

Dalla sicurezza informatica alla sicurezza cognitiva

Le organizzazioni stanno progressivamente comprendendo che il patrimonio più importante non è rappresentato dall'infrastruttura tecnologica, ma dalla capacità delle persone di prendere decisioni corrette.

In questo contesto emerge il concetto di *sicurezza cognitiva*: l'insieme delle pratiche e delle tecnologie finalizzate a proteggere i processi mentali, informativi e decisionali da manipolazioni, errori e distorsioni.

Deepfake, contenuti sintetici, disinformazione automatizzata e sistemi conversazionali avanzati rappresentano esempi concreti di minacce che non colpiscono direttamente i sistemi, ma influenzano la percezione della realtà.

La domanda non è più soltanto *chi può entrare nei miei sistemi?*, ma *chi può influenzare le mie decisioni?* Sempre più i sistemi aiutano a decidere, ma spesso il poco tempo per decidere e le troppe decisioni da prendere favoriscono l'adozione di agenti che lavorano in autonomia. Da qui, il rischio della perdita di controllo, peraltro noto, che diventa sempre più alto.



Il ruolo della governance

L'errore più comune consiste nel considerare l'AI come una questione esclusivamente tecnica.

In realtà la sicurezza dell'Intelligenza Artificiale è prima di tutto un tema di governance: per questo, alla fine degli anni duemila frequentavo più spesso dipartimenti HR o strategici che dipartimenti tecnici.

Occorre definire regole di utilizzo, criteri di validazione, responsabilità decisionali e meccanismi di controllo. Le organizzazioni che adotteranno l'AI senza costruire adeguati modelli di governance rischiano di introdurre nuove vulnerabilità proprio mentre cercano di aumentare efficienza e produttività.

L'esperienza maturata negli anni nei grandi programmi di trasformazione digitale insegna che la tecnologia, da sola, non risolve i problemi organizzativi. Talvolta li amplifica.

Conclusioni

La cybersecurity sta entrando in una nuova fase storica.

Per decenni abbiamo protetto macchine, reti e applicazioni. Oggi dobbiamo iniziare a proteggere anche **conoscenza, fiducia** e, soprattutto, **capacità decisionale**.

L'Intelligenza Artificiale non sostituirà la sicurezza informatica tradizionale, ma ne estenderà il campo d'azione verso territori finora poco esplorati. Le organizzazioni che comprenderanno per prime questa evoluzione saranno meglio preparate ad affrontare un mondo in cui il principale bersaglio non sarà il computer, ma il pensiero umano.

La vera sfida dei prossimi anni non sarà costruire sistemi più intelligenti. Sarà garantire che l'intelligenza, umana e artificiale, rimanga affidabile, verificabile e governabile.



CYBER
Think Tank
ASSINTEL

Unisciti alla nostra
community!

Scrivi a segreteria@assintel.it
per avere maggiori info

La tecnocrazia americana e la nuova era geopolitica dell'IA

A cura di Sofia Scozzari



Di recente il governo americano ha intimato ad Anthropic di impedire l'accesso ai suoi due modelli più recenti, Claude Fable 5 e Mythos 5, per tutti i cittadini stranieri, sia all'interno che all'esterno degli Stati Uniti, compresi i dipendenti stranieri dell'azienda stessa, invocando un rischio di *sicurezza nazionale*.

Non essendo possibile applicare la normativa in modo selettivo ai propri utenti, Anthropic ha preferito per il momento disattivare i modelli per tutti gli utenti, sebbene Mythos 5 sia già oggetto di limitazione nell'ambito del Progetto Glasswing ed accessibile solo a circa 150 organizzazioni selezionate proprio per impedire che le sue capacità possano essere commercializzate.

Per anni, i controlli statunitensi sulle esportazioni nel campo dell'IA si sono concentrati sui chip e sugli strumenti di produzione. Questa è la prima volta che il governo americano interviene a livello di applicazione, indicando a un'azienda privata quali utenti, in base al passaporto, possano utilizzare il suo prodotto.

È anche la prima volta che un'azienda leader nel settore dell'IA si trova **costretta a disattivare un modello distribuito pubblicamente a causa di un ordine federale**.

Abbiamo dunque superato una soglia, oltre la quale **tecnologia per uso civile e geopolitica iniziano a**

convergere.

Il nuovo risvolto geopolitico della tecnologia

Gran parte della tecnologia software che utilizziamo quotidianamente è di origine americana: sistemi operativi di computer e smartphone, motori di ricerca, IA, applicazioni, cloud in cui risiedono i dati, ecc.

Fino ad ora è stato semplicemente **più conveniente affidarsi a tecnologie straniere già pronte**, con l'illusione che il pagamento della licenza di un prodotto ne definisse anche, se non la proprietà esclusiva, quantomeno la disponibilità.

L'Europa, d'altro canto, ha concentrato i propri sforzi nel regolamentare l'uso di queste tecnologie di terzi, piuttosto che investire in innovazione o per alternative comunitarie.

A seguito della direttiva americana, la Commissione Europea ha sottolineato la necessità per l'Europa di raggiungere una **sovranità tecnologica**, mentre il governo UK ha definito l'accesso alle funzionalità di IA una questione di **sicurezza nazionale**.

Il cambiamento geopolitico che si sta delineando intorno all'intelligenza artificiale, e che potrebbe estendersi anche ad altre tecnologie, sta chiaramente mettendo in luce quanto l'origine della tecnologia possa rivelarsi un dettaglio che non è più



possibile ignorare.

Un primo segnale di inversione è arrivato di recente: la Commissione europea ha lanciato la **Frontier AI Grand Challenge**, con l'obiettivo politico esplicito di **costruire una capacità autonoma nell'IA avanzata e ridurre la dipendenza dai fornitori extraeuropei**. La sfida è stata vinta dal consorzio Europa, guidato da Domyn, l'unicorno italiano che svilupperà la **prima vera IA sovrana europea** open-source, multilingua e addestrata su infrastrutture EuroHPC.

Le motivazioni politiche e commerciali dietro al ban

La problematica segnalata dal governo statunitense risiede nella capacità da parte dei modelli avanzati di Claude di individuare difetti software sfruttabili, un'abilità che, sebbene fornisca un notevole vantaggio agli aggressori, consente anche ai difensori di individuare e correggere eventuali vulnerabilità dei propri sistemi informatici.

Ma, sebbene sia stata invocata la sicurezza nazionale, apparentemente le ragioni alla base dell'embargo sui modelli Anthropic più avanzati hanno anche altre origini.

Innanzitutto, anche **altri modelli di IA (primo tra tutti GPT-5.5) sono soggetti alla stessa problematica**, ma OpenAI non ha ricevuto nessuna richiesta di disattivazione.

Inoltre, se la problematica principale fosse sicurezza nazionale, non sarebbe logico che il governo USA abbia imposto di limitare i modelli ai **solli utenti di nazionalità americana, e non a tutti**. Per una tecnologia dichiarata "pericolosa per la sicurezza nazionale", basare la discriminazione sul mero passaporto dell'utente e non su altri criteri (per esempio, particolari clearance di sicurezza, certificazioni, appartenenza a determinati uffici governativi), è un approccio maldestro e fondamentalmente inefficace.

D'altra parte, sono ben noti i precedenti dissidi tra il governo americano e Anthropic, e quanto i loro rapporti siano diventati tesi da quando l'azienda si è rifiutata di consentire al governo statunitense di utilizzare i propri modelli per la sorveglianza interna e per sviluppare armi completamente autonome.

Anthropic ha inoltre avviato la procedura per la quotazione in borsa, anticipando OpenAI: è chiaro che la rimozione dal mercato del suo modello di punta rappresenta da un lato **un vantaggio per il suo concorrente principale, e dall'altro, paradossalmente, una forma di "pubblicità" pre-IPO per Anthropic stessa**.

Un precedente pericoloso

L'episodio di "Fable 5" dimostra in modo esplicito che **il governo statunitense può privare in qualsiasi momento ogni soggetto non americano delle capacità di IA più avanzate (e potenzialmente, per estensione, di qualsiasi altra tecnologia)**, senza preavviso, senza una giustificazione tecnica trasparente e indipendentemente dalla localizzazione degli utenti.

Le **conseguenze pratiche per i soggetti non-americani (privati e governativi)** sono notevoli:

- **Il rischio di continuità legato all'IA non è più una questione di competenza solo dell'IT.** Una funzionalità core dell'azienda potrebbe essere disattivata, senza preavviso né possibilità di ricorso.
- **La diversificazione dei fornitori smette di essere una best practice e diventa un requisito imprescindibile.** Affidarsi a un unico fornitore, o a fornitori operanti in un'unica giurisdizione, concentra un rischio che ormai non è più solo teorico.
- **La sede legale delle risorse di calcolo e delle tecnologie è più importante di quanto non lo fosse una settimana fa.** I cloud regionali offrono una certa protezione, ma solo se il fornitore è in grado di continuare a erogare il servizio.
- **È arrivato il momento di rivalutare seriamente le tecnologie e i modelli IA in house.** Le tecnologie sotto controllo diretto non possono essere revocate da terzi: pur comportando costi differenti, il rischio di indisponibilità di strumenti fondamentali per il business deve rientrare nell'equazione.

Conclusioni

Mentre Anthropic si augura di ripristinare al più presto l'accesso ai modelli resi indisponibili dall'ordine federale, questo precedente non può essere ignorato.

Se per decenni software e applicativi sono stati adottati senza prestare attenzione alla loro giurisdizione di origine, oggi è evidente che l'interruttore non è (e non è mai stato) in mano all'utente finale.

Vale quindi la pena chiedersi se **il costo di investire in tecnologia europea proprietaria sia davvero superiore al rischio di affidarsi a soluzioni che possono essere disattivate**, in qualsiasi momento e per ragioni arbitrarie, dal governo che ne è il vero proprietario.



MARY HOLMES E LO STRANO CASO DEL PESCIOLINO ROSSO!

COME NON CADERE VITTIMA DEL PHISHING

www.assintel.it
info@assintel.it



Non cadere nei tranelli del phishing! Verifica sempre l'autenticità delle email e proteggiti i tuoi dati.
Credits: NWN solutions Bologna

Sicurezza industriale, come prevenire le cyber-intrusioni

A cura di Francesco Tieghi



IDS e IPS - acronimi di Intrusion Detection Systems e Intrusion Prevention Systems - sono sistemi di sicurezza industriale che permettono di rilevare le anomalie e intervenire rapidamente e in autonomia, migliorando così la sicurezza in ambito OT.

Proteggere le reti industriali è un compito impegnativo. Le infrastrutture critiche sono costantemente oggetto di potenziali attacchi dall'esterno. I **firewall**, da soli, non bastano. I team di sicurezza devono affrontare ogni giorno nuove sfide e hanno bisogno di strumenti in grado di automatizzare l'analisi del traffico e bloccare le azioni malevoli. Questi strumenti si chiamano, rispettivamente, IDS e ICS.

Che cosa fanno gli Intrusion Detection Systems

IDS è l'acronimo di **Intrusion Detection System**. Le piattaforme IDS sono sistemi di sicurezza industriale che rilevano le intrusioni **analizzando** in tempo reale il comportamento delle reti e **intercettando** potenziali segnali di azioni malevoli o non conformi alle policy di sicurezza. Nel momento in cui viene identificato un pericolo, viene generato un **allarme** che viene inviato al team che ha la responsabilità sulla sicurezza degli asset.

Il compito di un IDS è individuare in modo rapido anomalie e connessioni sospette all'interno dell'infrastruttura di rete. Gli IDS sono **applicazioni software** che vengono installate sugli endpoint, su

applicazioni cloud o su device hardware connessi alla rete. Vengono anche utilizzati come abilitatori e garanti della conformità, per assicurare il rispetto delle normative nazionali e internazionali che richiedono una vigilanza attiva sulla sicurezza degli asset.

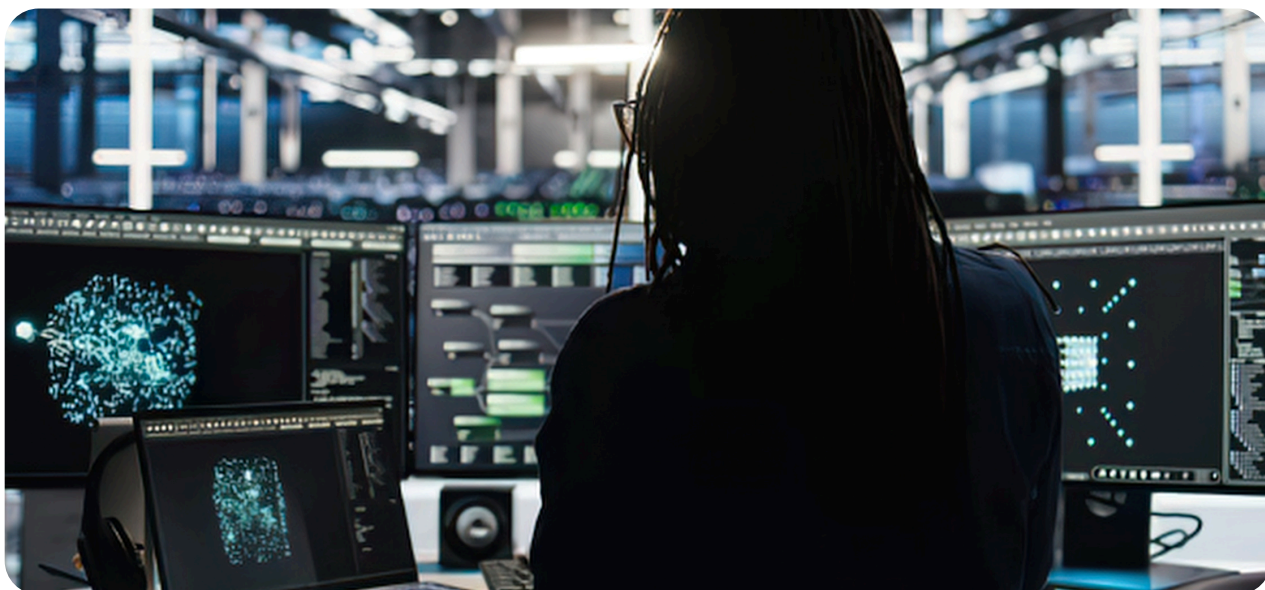
Gli IDS sono applicazioni di monitoraggio puro, per cui non intervengono direttamente sulle anomalie. In questa prospettiva, garantiscono un funzionamento continuativo senza interferire con l'erogazione dei servizi di rete e quindi con il funzionamento degli impianti.

La marcia in più degli Intrusion Prevention Systems

Gli **IPS** possono essere definiti un'evoluzione dei sistemi IDS. Si tratta di sistemi per la sicurezza industriale che permettono di prevenire le intrusioni - di qui il nome **Intrusion Prevention System** e l'acronimo IPS - analizzando il traffico di rete e intervenendo in automatico in caso di allarme.

Nel momento in cui vengono identificate delle anomalie, i sistemi IPS agiscono in **autonomia**, per esempio interrompendo le connessioni potenzialmente malevoli o eliminando contenuti pericolosi. Sono inoltre in grado di modificare in modo indipendente le **regole dei firewall** in caso di attacco.

Le caratteristiche proattive delle piattaforme IPS si



traducono in un intervento immediato contro i potenziali rischi, riducendo quindi sensibilmente il tempo di risposta. In questo modo, inoltre, si riduce l'intervento umano, alleggerendo così il carico di lavoro del team di sicurezza.

IDS e IPS: caratteristiche comuni

IDS e IPS sono sistemi di sicurezza industriale che hanno molti elementi in comune, a cominciare dalle metodologie di rilevamento delle minacce. Entrambi i sistemi si basano infatti su tre metodi principali:

- **Rilevamento della firma:** i sistemi analizzano i flussi di dati ricercando *firme* di attacchi, vale a dire sequenze di codice che possono essere associate a potenziali minacce. Ciò è reso possibile grazie all'adozione di algoritmi di machine learning.
- **Rilevamento delle anomalie:** i sistemi analizzano il traffico di rete evidenziando deviazioni rispetto a un modello di riferimento e intervenendo in caso di comportamento anomalo, ad esempio l'apertura di porte non programmata. Anche in questo caso vengono utilizzati modelli di apprendimento automatico.
- **Rilevamento basato sulle politiche:** in questo caso, i sistemi si attivano quando vengono rilevate attività o comportamenti che non sono in linea con le policy di cybersecurity dell'azienda.

IDS e IPS sono **strumenti complementari**, che rappresentano la pietra angolare di una strategia efficace di cybersecurity industriale.

I sistemi di rilevamento delle intrusioni permettono di analizzare costantemente le comunicazioni di rete, offrendo al team di sicurezza una panoramica in tempo di reale del comportamento dell'infrastruttura.

I sistemi di prevenzione delle intrusioni, in parallelo, neutralizzano in automatico potenziali minacce a software e hardware, migliorando così i tempi di risposta.

Oggi sono presenti sul mercato numerose **soluzioni** di sicurezza industriale che integrano sistemi IDS e IPS all'interno di un più ampio pacchetto di applicazioni per la sicurezza in ambito OT. Si tratta di **piattaforme** scalabili, facilmente integrabili all'interno dell'architettura di rete e adattabili ai diversi ambienti di produzione.

Questa tipologia di soluzioni è un alleato estremamente prezioso per **proteggere** le infrastrutture critiche e gli asset di produzione.



Verso la fabbrica cognitiva: un nuovo paradigma per l'OT Security

A cura di Elena Vaciago



La trasformazione dell'industria italiana verso lo Smart Manufacturing è avviata, ma incompleta: nonostante le realtà manifatturiere del Paese abbiano costruito solide basi tecnologiche, faticano ancora a tradurre gli investimenti in un reale vantaggio competitivo e in modelli decisionali evoluti. È quanto emerge dalla sesta edizione della "SMART MANUFACTURING SURVEY 2026" di TIG.

Svolta tra marzo e aprile 2026, l'indagine ha coinvolto un campione di 88 aziende manifatturiere italiane: i partecipanti ricoprono principalmente i ruoli IT (52%), direzione (15%) e progettazione / R&D (14%). I risultati mostrano che la digitalizzazione continua a essere considerata come un'opportunità per acquisire una maggiore efficienza produttiva (per il 47% delle aziende manifatturiere): solo una percentuale più limitata la associa alla trasformazione del modello industriale (28%) o alla differenziazione competitiva (22%).

Questo orientamento si riflette chiaramente nelle scelte di investimento: se negli ultimi anni le industrie italiane hanno concentrato gli sforzi su percorsi di automazione dei processi produttivi, acquisizione di infrastrutture IT, sensori e cybersecurity industriale, costruendo le fondamenta della fabbrica digitale, oggi l'attenzione si sta spostando verso una maggiore valorizzazione dei dati.

Le principali priorità per i prossimi anni saranno quindi l'intelligenza artificiale (52%), la condivisione del know-how (51%), lo sviluppo di competenze digitali (46%). Questo passaggio segna l'ingresso in una nuova fase della trasformazione, in cui il valore non deriva più principalmente dall'adozione di tecnologia, quanto piuttosto dalla capacità di utilizzarla in modo efficace.

PRIORITÀ DI INVESTIMENTO

TIG | THE INNOVATION GROUP

Macro-aree tecnologiche

Intelligenza artificiale Sicurezza informatica Dati / Know How Infrastrutture

PRIORITÀ DI INVESTIMENTO			PRIORITÀ DI INVESTIMENTO		
	Intelligenza artificiale per l'ottimizzazione dei processi	52%		Manutenzione predittiva	37%
	Digitalizzazione/ condivisione del know how interno	51%		Tracciabilità avanzata	36%
	Formazione e sviluppo delle competenze digitali	46%		Digitalizzazione della supply chain	35%
	Cybersecurity industriale (OT security)	41%		Infrastrutture IT, Edge computing per la produzione	31%
	Analisi avanzata dei dati	38%		Modello di servitizzazione (service-based)	27%

Fonte: Smart Manufacturing Survey 2026, TIG-The Innovation Group

Supported by:

contact
value



CSA

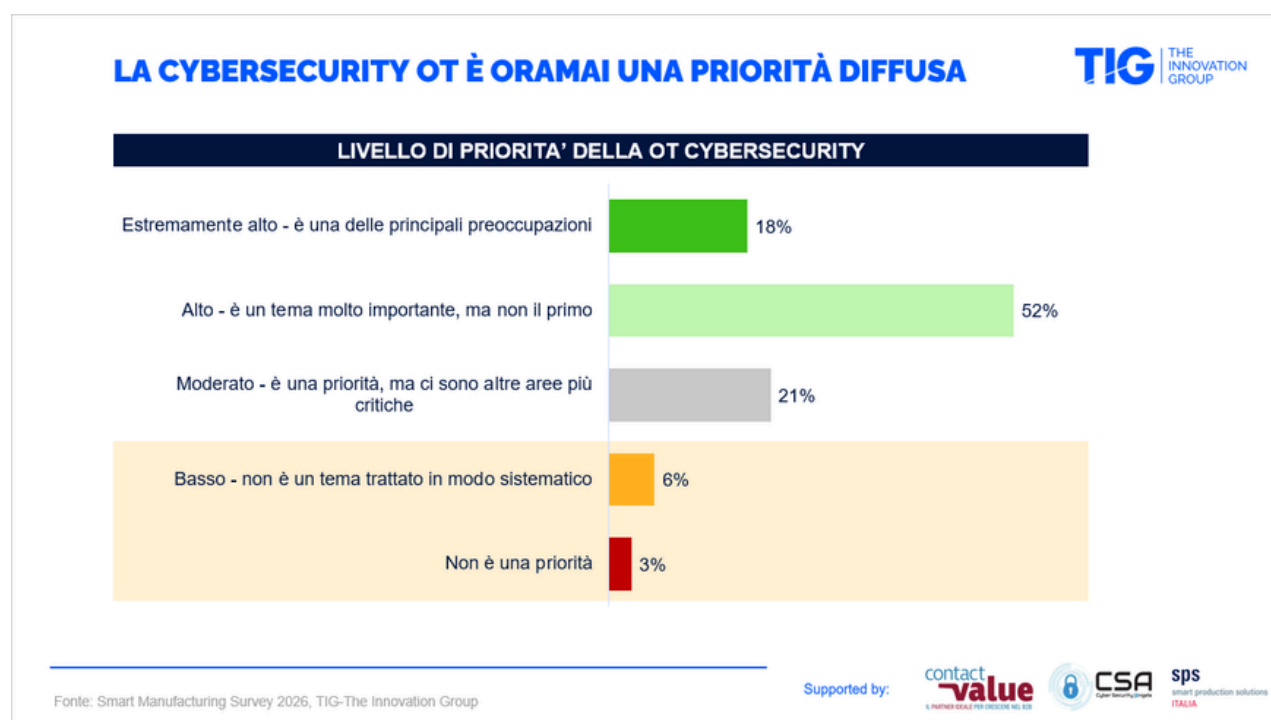
sps
smart production solutions
ITALIA

Cybersecurity industriale: verso una resilienza integrata

Il panorama della cybersecurity industriale (OT - Operational Technology) sta attraversando una fase di profonda trasformazione, spinto da una crescente consapevolezza dei rischi e da un'evoluzione normativa senza precedenti e, secondo i dati della survey, la cybersecurity OT è oggi una priorità "alta o estremamente alta" per il 70% del campione, segnando un netto incremento rispetto al 58% dell'anno precedente.

L'analisi evidenzia come la cybersecurity industriale sia oggi uscita definitivamente dal perimetro delle

opzioni tecniche per assurgere a imperativo strategico non negoziabile: la sicurezza non è più solo un onere tecnico ma una responsabilità aziendale integrata che coinvolge l'intera catena del valore e in particolar modo il fattore umano. In un panorama industriale dove l'interconnessione è la norma, la protezione degli asset produttivi rappresenta il cardine della continuità del business. Tuttavia, l'attuale fase di transizione evidenzia un divario profondo tra l'acquisizione di tecnologie difensive e la maturità organizzativa necessaria a gestirle: senza una governance solida, gli investimenti in Industria 4.0 rischiano di trasformarsi da asset a passività critiche.



Un nuovo paradigma per l'OT Security: disponibilità, safety e monitoraggio integrato

Nel mondo industriale, la gerarchia della sicurezza è invertita rispetto all'IT: in questo ambito al primo posto abbiamo la necessità di garantire la continuità produttiva (disponibilità). Poi c'è un tema di gestione sicura dei sistemi legacy, che hanno tipicamente una lunga durata del ciclo di vita. Infine, oggi va considerato l'impatto dirompente di nuove normative europee come la NIS 2 e il Cyber Resilience Act (CRA).

Va anche considerato che il paradigma della cybersecurity è molto cambiato negli ultimi anni, e questo ammodernamento andrebbe adottato nel mondo industriale: il passaggio da una difesa perimetrale a una resilienza attiva richiede un approccio diverso, molto più dinamico e orientato

all'analisi di comportamenti e anomalie. Poiché però obiettivi centrali della sicurezza OT sono la continuità dei processi industriali e la sicurezza fisica delle persone, il monitoraggio da preferire, rispetto alla scansione attiva, è quello passivo, così come vanno previsti dei risk assessment e vanno negoziate con l'area OT delle finestre di manutenzione per la security. In settori ad alta intensità, il costo del fermo macchina è stimato in decine di migliaia di euro l'ora: un dato che rende qualsiasi investimento in visibilità OT non solo una spesa di sicurezza, ma una polizza sulla produzione.

Impatti di NIS2, CRA e Regolamento Macchine

L'Europa sta ridisegnando le regole del gioco per garantire la sovranità tecnologica.

La direttiva NIS2 e il Cyber Resilience Act (CRA) non sono semplici adempimenti burocratici, ma driver di

standardizzazione che colpiscono l'intera catena del valore. Il CRA, in particolare, impone una trasformazione radicale agli Uffici Tecnici nel mondo industriale. Obiettivo del CRA è promuovere lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità e che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto. Le scadenze sono imminenti e stringenti:

1. Giugno 2026: obbligo di definizione dei processi per la notifica degli incidenti alle autorità (ACN).

2. Settembre 2026: operatività degli obblighi di segnalazione per vulnerabilità sfruttabili e incidenti per i fabbricanti di prodotti digitali.

3. Gennaio 2027: entrata in vigore del Regolamento Macchine, che si affianca al CRA per definire i requisiti di sicurezza essenziali dei prodotti.

4. Dicembre 2027: piena attuazione del CRA; ogni prodotto connesso dovrà garantire patch e gestione vulnerabilità per l'intero ciclo di vita (minimo 5 anni).

Mentre la NIS2 responsabilizza il cliente finale (l'operatore che utilizzerà la macchina e che è chiamato a controllare la sicurezza della sua supply chain), il CRA e il Regolamento Macchine spostano l'onere direttamente sul produttore. Nel complesso quello che si afferma è un concetto di "Responsabilità di Sistema": la novità è che il fornitore è obbligato a garantire che la macchina rimanga sicura nel tempo, pena l'esclusione dal mercato o l'inserimento in blacklist internazionali.

Sovranità contrattuale e gestione della supply chain

La catena di fornitura è diventata una superficie d'attacco privilegiata, e lo è ancora di più nel mondo industriale, che ha caratteristiche proprie. Il tempo dei fornitori "Black Box" - che consegnano macchinari senza trasparenza sui componenti digitali - è finito: le aziende devono oggi esercitare una vera "Sovranità Contrattuale".

Naturalmente permangono molte criticità, come il lock-in tecnologico e i contratti legacy che non avevano previsto clausole di cybersecurity. I sistemi non presidati sono estremamente vulnerabili, alla luce anche degli ultimi sviluppi AI (vedi Mythos di Anthropic).

Le principali raccomandazioni sono:

- Revisione dei contratti di manutenzione remota: limitare gli accessi "always-on" e imporre standard minimi di autenticazione.
- Sostituzione del lock-in con la trasparenza: richiedere la Software Bill of Materials (SBOM) per ogni apparato critico.
- Audit di maturità dei partner: valutare i fornitori non solo sulla performance, ma sulla loro capacità di Incident Response.



NIS2 e supply chain: il grande equivoco dei questionari ai fornitori

A cura di Enzo Veiluva



L'adeguamento alla NIS2 ed in particolare il presidio della supply stanno generando una reazione tanto diffusa quanto poco efficace: l'invio massivo ai fornitori di checklist lunghissime, spesso composte da centinaia di domande eterogenee, tratte dai più disparati framework.

Questo fenomeno nasce da un fraintendimento sostanziale, ovvero la confusione tra valutazione della fornitura e valutazione del fornitore.

La direttiva, infatti, distingue chiaramente i due piani: da un lato richiede di valutare i rischi della fornitura, cioè del bene o del servizio nel contesto specifico in cui viene utilizzato; dall'altro chiede di considerare l'affidabilità del fornitore, ma limitatamente ad alcuni aspetti rilevanti come: la qualità dei prodotti, la competenza, l'attuazione delle pratiche di sicurezza e la capacità di garantire continuità operativa nel tempo, etc. Non viene mai richiesto di svolgere una due diligence enciclopedica sul fornitore in quanto tale.

Il punto è che il rischio non risiede nel fornitore in astratto, ma nell'interazione tra ciò che fornisce e il contesto in cui quella fornitura è inserita. Tuttavia, molti soggetti NIS hanno interpretato il requisito come un obbligo di raccolta sistematica di informazioni, scaricando di fatto la compliance lungo la supply chain.

In questo modo, ciò che dovrebbe essere un processo interno di gestione del rischio diventa un esercizio documentale delegato ai fornitori. Anche i riferimenti ai framework, come il controllo GV.SC-01, sono spesso letti in modo improprio: tali requisiti non riguardano solamente ciò che il fornitore deve dimostrare, ma anche - ed in gran parte - ciò che il soggetto NIS deve definire in termini di strategia, politiche e processi di gestione del rischio della supply chain.

Molti degli elementi richiesti nei questionari - modalità di autenticazione, ruoli assegnati al fornitore, monitoraggio degli eventi, livelli di sicurezza desiderati - non sono caratteristiche intrinseche del fornitore, ma aspetti che devono essere stabiliti e governati nella relazione di fornitura. Non si tratta quindi di "chiedere informazioni", ma di definire requisiti, accordi e controlli coerenti con il rischio. L'approccio basato su checklist massive risulta così poco efficace: spesso produce risposte standardizzate, prive di reale valore informativo, ignora il principio di proporzionalità trattando allo stesso modo forniture critiche e marginali, e sovraccarica inutilmente i fornitori, compromettendo la qualità complessiva delle interazioni, oltre al fatto che nella maggior parte dei casi queste check list finiscono in un cassetto e non vengono utilizzate, ma rimangono a disposizione in attesa di qualche fatidico evento.



Il paradosso è evidente se si considera che molti fornitori sono a loro volta soggetti alla NIS2.

Continuare a richiedere le stesse informazioni attraverso questionari ridondanti non aumenta il livello di sicurezza, ma solo quello di burocrazia.

È importante chiarire a questo punto che quanto sopra riportato non intende affatto mettere in discussione l'utilità delle checklist come strumento operativo: se ben progettate, restano un mezzo valido e spesso indispensabile per raccogliere informazioni e supportare la valutazione del rischio.

Il problema non è lo strumento in sé, ma il suo utilizzo indiscriminato e standardizzato.

Un'applicazione coerente con lo spirito della Direttiva NIS2 richiede un cambio di paradigma: partire dalla fornitura, classificandola in base alla sua criticità in termini di impatto su operatività, sicurezza e continuità, e solo successivamente calibrare il livello di approfondimento richiesto al fornitore.

Ne deriva la necessità di adottare valutazioni mirate e proporzionate, evitando di sottoporre tutti i fornitori allo stesso livello di analisi, soprattutto quando la fornitura è a basso rischio.

In questo contesto, la qualità delle domande diventa più rilevante della quantità: poche domande, ma strettamente connesse ai rischi specifici della fornitura (come la gestione delle vulnerabilità o i tempi di aggiornamento), risultano molto più efficaci di lunghe liste generiche.

Allo stesso modo, è fondamentale valorizzare le evidenze già esistenti, come certificazioni quali ISO/IEC 27001 o audit indipendenti, evitando di duplicare inutilmente richieste informative.

Infine, la valutazione dell'affidabilità non dovrebbe essere un esercizio una tantum, ma un processo continuo nel tempo: monitorare e aggiornare le informazioni è spesso più utile che raccoglierne una grande quantità in un singolo momento.

La sicurezza della supply chain non si costruisce accumulando risposte, ma esercitando controllo consapevole sulle proprie scelte e sulle relazioni che ne derivano e creando un rapporto di fiducia e costruttivo di miglioramento efficace con il proprio fornitore.



Disclaimer

Gentile lettore,

ti informiamo che il contenuto pubblicato su questo magazine è fornito a scopo puramente informativo e di intrattenimento. Tutte le opinioni, idee e punti di vista espressi negli articoli sono esclusivamente quelli degli autori e non riflettono necessariamente l'opinione di Assintel o dei suoi redattori.

Tutte le informazioni fornite sono basate sulle conoscenze e le fonti disponibili al momento della pubblicazione. Tuttavia, non possiamo garantire l'accuratezza, l'integralità o l'aggiornamento delle informazioni fornite. Pertanto, l'utilizzo delle informazioni presenti su questo magazine avviene a proprio rischio e discrezione.

Si prega di tenere presente che il contenuto potrebbe evolvere nel tempo e potrebbe non essere più aggiornato o rilevante al momento della lettura. Pertanto, consigliamo di verificare sempre l'attualità delle informazioni fornite e di consultare professionisti qualificati per eventuali questioni specifiche o decisioni importanti.

Inoltre, il Cyber Think Tank di Assintel declina ogni responsabilità per eventuali errori, omissioni o danni derivanti dall'uso delle informazioni contenute nel presente magazine. Non siamo responsabili per qualsiasi rivendicazione, perdita o danno di qualsiasi tipo che possa sorgere direttamente o indirettamente dall'utilizzo delle informazioni qui presentate.

Ti invitiamo a fare affidamento su più fonti di informazione per ottenere una visione più completa e a considerare che i punti di vista espressi possono variare in base all'esperienza e alle opinioni personali degli autori.

Infine, vorremmo sottolineare che il magazine non fornisce consulenza legale, finanziaria, medica o professionale di alcun genere. Si consiglia di consultare sempre un professionista qualificato per risolvere eventuali questioni specifiche che riguardano la tua situazione personale.

Cordialmente

La redazione



Assintel è l'associazione nazionale delle imprese ICT e rappresenta le aziende dell'ecosistema tecnologico e digitale italiano. Aderisce a Confcommercio – Imprese per l'Italia, entro cui è punto di riferimento per la valorizzazione del Digitale, sia a livello di mercato sia di politiche istituzionali. L'associazione è un vero business network per l'ecosistema ICT, capace di creare relazioni, sinergie e opportunità concrete per le aziende socie su tutto il territorio nazionale, negli ambiti tecnologici più innovativi e nei diversi settori economici, dagli operatori globali alle PMI e alle startup.

**Conf
com**



Assintel



**CYBER
Think Tank
ASSINTEL**