Cyber security

Come cambia il crimine online e l'attività di contrasto. Intervengono il generale Antonio Mancazzo, Massimo Chirivì e Paolo Spagnoletti

Ambiente Lavoro

Nuove tecnologie, simulazioni di rischio ed esperienze virtuose di wellbeing corporate in vetrina dal 26 al 30 maggio

REPORT SICUREZZA

Speciale Cyber Security

UNA VISIONE INTEGRATA

di **CG**

Wanda Ferro, sottosegretario di Stato al Ministero dell'Interno

Il tema della sicurezza è uno dei pilastri fondamentali dell'azione del Governo Meloni, perché rappresenta il presupposto della libertà, della coesione sociale e della fiducia dei cittadini nelle istituzioni. «Per troppo tempo alcuni fenomeni sono stati sottovalutati o affrontati con un approccio ideologico che ha finito per lasciare soli i territori e per indebolire la presenza dello Stato. Abbiamo dunque scelto- mette in evidenza il sottosegretario al Ministero dell'Interno Wanda Ferro- una linea diversa: concreta e pragmatica, fondata su investimenti, prevenzione e capacità di intervento». I numeri dimostrano che la direzione è quella giusta.

ALL'INTERNO

Le sfide della Farnesina
Al centro della nuova architettura, voluta dal ministro Tajani, è Alessandro De Pedys

MARINA CALDERONE
RAFFORZARE LA CRESCITA

In un mercato del lavoro che continua a registrare segnali positivi sul fronte dell'occupazione, il Governo punta ora a consolidare la crescita trasformandola in lavoro stabile, qualificato e meglio retribuito. Dal salario giusto agli incentivi per l'occupazione, passando per il rinnovo dei contratti e l'impatto dell'intelligenza artificiale sul mercato del lavoro: il Dl Lavoro rappresenta uno dei pilastri della strategia economica del Governo. Al centro del confronto anche il tema della sicurezza e della prevenzione, considerati elementi fondamentali per tutelare lavoratori e imprese. Ne parliamo con il ministro del Lavoro Marina Calderone, per capire quali siano le priorità dell'esecutivo e come cambierà il mondo del lavoro nei prossimi anni.

Ministro qual è oggi la priorità economica che guida l'impianto del Dl Lavoro e in che modo il Governo intende conciliare crescita, occupazione e tutela del potere d'acquisto?

«La priorità risiede nella volontà di rendere la crescita più solida, trasformandola in occupazione stabile e lavoro di qualità. Il Dl 1° maggio nasce nell'ambito di una fase oggettivamente positiva per l'occupazione italiana, che al momento non sembra rallentare. Sarebbe però un errore fermarsi ai numeri. Resta ancora il gap rispetto ad alcuni problemi strutturali che conosciamo bene: il potere d'acquisto dei salari, gli squilibri territoriali e una partecipazione al lavoro storicamente troppo bassa per giovani e donne. L'ulteriore intervento sul mondo del lavoro di questo provvedimento guarda in particolare all'inclusione lavorativa dei disoccupati di lunga durata, alle giuste retribuzioni e a un patto di responsabilità con le parti sociali per la qualificazione dell'occupazione in Italia. Abbiamo ribadito il nostro pensiero: la crescita non si difende comprimendo tutele e trasparenza. Un'economia competitiva ha bisogno di imprese forti, ma anche di lavoratori motivati, qualificati e ben retribuiti. In questa direzione vanno il sostegno del Governo alla contrattazione collettiva, gli incentivi per l'occupazione stabile e strumenti come la piattaforma SIISL, che mette finalmente in connessione competenze, imprese e opportunità».

Il Governo ha più volte ribadito la centralità del "salario giusto" e della contrattazione collettiva: come pensa che queste misure possano migliorare concretamente stipendi e qualità del lavoro senza penalizzare produttività e competitività delle imprese?

«Partiamo da un principio semplice: il lavoro non può essere valutato soltanto in relazione a una retribuzione oraria. Dall'integrale applicazione di un CCNL discendono diritti, tutele, welfare, sicurezza, formazione, progetti di vita. Per questo il decreto 1° maggio valorizza il TEC, il Trattamento Economico Complessivo previsto dai contratti sottoscritti dalle organizzazioni comparativamente più rappresentative.

INFINIDAT

AI-Ready, Cyber-Centric **Enterprise Storage**

- Reduce AI hallucinations with RAG workflows
- Easily create cyber-resilient storage environments
- Reduce threat windows with Automated Cyber Protection
- Identify compromised data using AI-based cyber detection
- Recover known good copies of data quickly
- Backed by InfiniSafe cyber storage guarantees

WWW.INFINIDAT.COM

GOLFARELLI EDITORE
INTERNATIONAL GROUP

Colophon

Sede
Tel. 051 228807 - Piazza Cavour 2
40124 - Bologna - www.golfarellieditore.it

Relazioni pubbliche
Via del Pozzetto, 1/5 - Roma

Supplemento a Dossier-Registrazione Tribunale di Bologna n. 7578/2004

La priorità è rafforzare la crescita

Dal Dl Lavoro agli incentivi per giovani e donne, fino all'impatto dell'intelligenza artificiale e alla sicurezza nei cantieri: il ministro Marina Calderone traccia la linea del Governo tra occupazione stabile, contrattazione collettiva e innovazione

In un mercato del lavoro che continua a registrare segnali positivi sul fronte dell'occupazione, il Governo punta ora a consolidare la crescita trasformandola in lavoro stabile, qualificato e meglio retribuito. Dal salario giusto agli incentivi per l'occupazione, passando per il rinnovo dei contratti e l'impatto dell'intelligenza artificiale sul mercato del lavoro: il Dl Lavoro rappresenta uno dei pilastri della strategia economica del Governo. Al centro del confronto anche il tema della sicurezza e della prevenzione, considerati elementi fondamentali per tutelare lavoratori e imprese. Ne parliamo con il ministro del Lavoro Marina Calderone, per capire quali siano le priorità dell'esecutivo e come cambierà il mondo del lavoro nei prossimi anni.

TUTTI GLI INDICATORI MOSTRANO CHE LADDOVE CRESCE L'OCCUPAZIONE FEMMINILE AUMENTANO COMPETITIVITÀ, PRODUTTIVITÀ E CAPACITÀ DI INNOVARE. NON È SOLTANTO UNA QUESTIONE DI EQUITÀ SOCIALE, MA DI CRESCITA ECONOMICA

Ministro qual è oggi la priorità economica che guida l'impianto del Dl Lavoro e in che modo il Governo intende conciliare crescita, occupazione e tutela del potere d'acquisto?

«La priorità risiede nella volontà di rendere la crescita più solida, trasformandola in occupazione stabile e lavoro di qualità. Il Dl 1° maggio nasce nell'ambito di una fase oggettivamente positiva per l'occupazione italiana, che al momento non sembra rallentare. Sarebbe però un errore fermarsi ai numeri. Resta ancora il gap rispetto ad alcuni problemi strutturali che conosciamo bene: il potere d'acquisto dei salari, gli squilibri territoriali e una partecipazione al lavoro storicamente troppo bassa per giovani e donne. L'ulteriore intervento sul mondo del lavoro di questo provvedimento guarda in particolare all'inclusione lavorativa dei disoccupati di lunga durata, alle giuste retribuzioni e a un patto di responsabilità con le parti sociali per la qualificazione dell'occupazione in Italia. Abbiamo ribadito il nostro pensiero: la crescita non si difende comprimendo tutele e trasparenza. Un'economia competitiva ha bisogno di imprese forti, ma anche di lavoratori motivati, qualificati e ben retribuiti. In questa direzione vanno il sostegno del Governo alla contrattazione collettiva, gli incentivi per l'occupazione stabile e strumenti come la piattaforma SIISL, che mette finalmente in connessione competenze, imprese e opportunità».

Il Governo ha più volte ribadito la centralità del "salario giusto" e della contrattazione collettiva: come pensa che queste misure possano migliorare concretamente stipendi e qualità del lavoro senza penalizzare produttività e competitività delle imprese?

«Partiamo da un principio semplice: il lavoro non può essere valutato soltanto in relazione a una retribuzione oraria. Dall'integrale applicazione di un CCNL discendono diritti, tutele, welfare, sicurezza, formazione, progetti di vita. Per questo il decreto 1° maggio valorizza il TEC, il Trattamento Economico Complessivo previsto dai contratti sottoscritti dalle organizzazioni comparativamente più rappresentative. Una scelta che valorizza la qualità della contrattazione collettiva italiana e che rifiuta l'idea che la competitività passi dalla compressione del costo del lavoro. Le economie più forti sono quelle che investono sulle competenze, sull'innovazione e sul capitale umano. Il compito del Governo è creare condizioni favorevoli a garantire questo equilibrio, sostenendo imprese e lavoratori facilitando il dialogo tra le parti sociali. Quando il lavoro cresce in qualità, cresce pure la forza dell'intero sistema produttivo».

Sul fronte dell'occupazione, quali incentivi ritiene più efficaci per favorire assunzioni stabili, soprattutto per giovani e donne, e quale ruolo avranno i rinnovi contrattuali nel rafforzare il mercato del lavoro?

«Gli incentivi funzionano davvero quando

aiutano a costruire lavoro stabile, correttamente retribuito, e sono capaci di intercettare le giuste platee di beneficiari. Proprio per questo, la revisione delle agevolazioni per le assunzioni nel Decreto 1° maggio avviene sulla base dei dati che i nostri sistemi informativi ci restituiscono. Sono oltre 165mila le assunzioni agevolate dai bonus del decreto Coesione, 84mila donne. Oggi, con un tasso di disoccupazione attorno al 5 per cento e la crescita dell'occupazione trainata dai contratti a tempo indeterminato, il focus deve spostarsi su chi non partecipa al mondo del lavoro. Il Dl 62/2026 sostiene l'assunzione di chi è disoccupato di lunga durata, superando il precedente vincolo del "mai assunto a tempo indeterminato", e vincola il bonus al riconoscimento del salario giusto. Gli esoneri contributivi per under 35 e per donne disoccupate di lungo periodo, che nelle aree Zes arrivano fino a 800 euro mensili, servono proprio a creare ulteriore occupazione stabile. Sostenere il lavoro femminile non è soltanto una questione di equità sociale, ma di crescita economica. Tutti gli indicatori mostrano che laddove cresce l'occupazione femminile aumentano competitività, produttività e capacità di innovare. Insieme agli incentivi, i rinnovi contrattuali restano decisivi per rafforzare il potere d'acquisto delle retribuzioni e accompagnare le trasformazioni del mercato del lavoro».

L'intelligenza artificiale sta trasformando rapidamente professioni e competenze: quali sono, secondo lei, i principali rischi e le opportunità dell'Ia nel mondo del lavoro e come il Ministero sta preparando lavoratori e imprese a questa transizione?

«L'intelligenza artificiale non è più una prospettiva lontana: è già dentro le fabbriche, gli uffici, i servizi, le piattaforme digitali. Cambia il lavoro, cambia la richiesta di competenze, cambia il modo stesso di organizzare la produzione. I rischi esistono e riguardano soprattutto l'obsolescenza delle competenze e l'uso distorto degli algoritmi nei rapporti di lavoro. Ma le opportunità sono enormi: maggiore produttività, più sicurezza, riduzione delle attività ripetitive e nuovi lavori ad alto valore aggiunto. La sfida vera è non subire la trasformazione. Per questo abbiamo scelto un approccio antropocentrico: la tecnologia deve restare uno strumento al servizio delle persone. Stiamo investendo sulla formazione digitale, sulla piattaforma SIISL, sui programmi di aggiornamento professionale e sull'Osservatorio sull'adozione dell'Ia nel lavoro, che ci permette di monitorare gli impatti concreti sul mercato occupazionale e costituisce una vera e propria cabina di regia. La tecnologia diventa pericolosa soltanto quando l'uomo rinuncia a governarla».

LA SICUREZZA NON DEVE ESSERE PERCEPITA COME UN VINCOLO BUROCRATICO, UN MERO ADEMPIMENTO, UN COSTO: È, INVECE, IL MODO PIÙ EFFICACE CON CUI UNA SOCIETÀ DIMOSTRA RISPETTO PER LE PERSONE E PER LA DIGNITÀ DEL LAVORO

Facendo riferimento ai dati sugli incidenti sul lavoro, quanto è centrale oggi il tema della prevenzione?

«La prevenzione è un pilastro della qualità del lavoro e della competitività del nostro sistema produttivo. Un'impresa che investe in sicurezza è un'impresa più forte, più efficiente e capace di crescere. Il tema della sicurezza non può essere affrontato solo dopo una tragedia: deve essere un impegno quotidiano, che considero parte integrante della mia responsabilità istituzionale e della mia storia professionale. Tra i molti interventi messi in campo, voglio ricordare l'istituzione della patente a crediti, introdotta sedici anni dopo la previsione di legge: uno strumento di qualificazione graduale delle imprese, adottato per l'edilizia, da estendere in altri settori e destinato a mostrare pienamente il suo valore nel tempo. Stiamo inoltre dando attuazione la previsione del decreto Sicurezza sul badge di cantiere, ancora una volta partendo da una sperimentazione e utilizzando l'area del Cratere Sisma 2016, il più grande cantiere d'Europa. Entrambe le misure hanno come obiettivo la promozione della legalità nel mondo del lavoro e la tutela della salute e della sicurezza. La prevenzione deve diventare parte della cultura d'impresa, dell'organizzazione del lavoro e della formazione quotidiana».

Ci sono interventi che ritiene prioritari per rafforzare la cultura della sicurezza nelle aziende italiane?

«In questi anni abbiamo potenziato l'attività ispettiva e concentrato i controlli nei settori più esposti al rischio, ma sappiamo che le ispezioni da sole non bastano. Abbiamo avviato l'assunzione di centinaia di ispettori dopo anni di blocco del turn over. Abbiamo promosso l'uso della tecnologia per migliorare vigilanza e prevenzione. E sia pure gradualmente, abbiamo riscontrato una generale diminuzione dei casi mortali: una preziosa inversione di tendenza. Nei prossimi mesi continueremo a intervenire in materia di sicurezza. Bisogna insistere lungo questa strada: investire nelle ispezioni, nella formazione continua, nell'innovazione organizzativa e nelle tecnologie che migliorano in concreto la sicurezza degli ambienti di lavoro. Bisogna investire in cultura diffusa della vita sicura. La sicurezza non deve essere percepita come un vincolo burocratico, un mero adempimento, un costo: è, invece, il modo più efficace con cui una società dimostra rispetto per le persone e per la dignità del lavoro». • **CG**

Marina Calderone, ministro del Lavoro

anas
GRUPPO FS ITALIANE

Con una rete di **32mila chilometri** di strade e autostrade uniamo il Paese, da più di 90 anni.

Siamo l'azienda del Gruppo Ferrovie dello Stato Italiane che gestisce le strade di interesse nazionale. Oggi siamo il **primo gestore della rete stradale in Europa** e forniamo un servizio fondamentale: sulle nostre strade circolano ogni giorno oltre 8 milioni di veicoli passeggeri e oltre 400mila veicoli merci. Lavoriamo per garantire una **mobilità più sostenibile, tecnologica e integrata**.

Siamo presenti sul mercato estero con servizi di ingegneria.

32.000 km
di strade e autostrade

38 sedi
sul territorio

1.300 km
di autostrade

2.157
gallerie

18.720
viadotti

8.000
persone

www.stradeanas.it

Una visione integrata

Dal Decreto Sicurezza al valore del riutilizzo dei beni confiscati come leva di legalità, sviluppo e presenza dello Stato nei territori più fragili. Il sottosegretario Wanda Ferro illustra le azioni messe in campo dal Governo

Il tema della sicurezza è uno dei pilastri fondamentali dell'azione del Governo Meloni, perché rappresenta il presupposto della libertà, della coesione sociale e della fiducia dei cittadini nelle istituzioni. «Per troppo tempo alcuni fenomeni sono stati sottovalutati o affrontati con un approccio ideologico che ha finito per lasciare soli i territori e per indebolire la presenza dello Stato. Abbiamo dunque scelto- mette in evidenza il sottosegretario al Ministero dell'Interno Wanda Ferro- una linea diversa: concreta e pragmatica, fondata su investimenti, prevenzione e capacità di intervento». I numeri dimostrano che la direzione è quella giusta. «Nel 2025 i delitti complessivi sono diminuiti del 2 per cento rispetto all'anno precedente. Abbiamo garantito il turnover al 100 per cento nelle Forze dell'Ordine, assunto oltre 42 mila unità e programmato ulteriori 27 mila ingressi entro la fine della legislatura. Sono stati stanziati oltre 1 miliardo e mezzo di euro per i rinnovi contrattuali, insieme al potenziamento di mezzi, tecnologie e sistemi di videosorveglianza».

Oggi la sicurezza richiede soprattutto una visione integrata.

«Esattamente. Non esiste più una distinzione netta tra sicurezza urbana, infrastrutturale, economica o digitale. Pensiamo alle minacce cyber contro infrastrutture strategiche, ai fenomeni di degrado urbano che alimentano criminalità e violenza giovanile, oppure ai rischi legati alla sicurezza del trasporto pubblico e ferroviario. Per questo il Governo sta lavorando su una strategia complessiva che tiene insieme controllo del territorio, rigenerazione urbana, legalità e prevenzione sociale. In questo quadro si inseriscono anche operazioni come "Strade Sicure" e "Stazioni Sicure" e il modello Caivano, che considero uno degli esempi più efficaci di ritorno dello Stato nei territori più difficili: non soltanto repressione, ma recupero urbano, scuola, sport, servizi e restituzione degli spazi ai cittadini perbene».

Quali sono i pilastri principali del nuovo Decreto Sicurezza e quali obiettivi si pone nel breve e medio periodo?

«Il Decreto Sicurezza nasce per dare risposte concrete a problemi concreti, quelli che incidono direttamente sulla vita quotidiana delle persone. Parliamo di occupazioni abusive, borseggi, truffe agli anziani, spaccio diffuso, violenze contro le Forze dell'Ordine, blocchi stradali e ferroviari, fenomeni di degrado e criminalità urbana. Abbiamo introdotto strumenti più efficaci per prevenire e contrastare questi fenomeni, rafforzando allo stesso tempo le tutele per chi ogni giorno indossa una divisa e rappresenta lo Stato. Penso, ad esempio, alle norme contro le aggressioni agli operatori delle Forze dell'Ordine, al contrasto delle manifestazioni violente e dei blocchi illegali delle infrastrutture strategiche, oppure al rafforzamento dei controlli nelle aree più esposte al degrado».

IL DECRETO SICUREZZA CONTIENE NORME DI ASSOLUTO BUON SENSO. CONTRASTARE LO SPACCIO, LE OCCUPAZIONI ABUSIVE, I BLOCCHI ILLEGALI DELLE STRADE O LE AGGRESSIONI ALLE FORZE DELL'ORDINE SIGNIFICA TUTELARE I DIRITTI DELLA GRANDE MAGGIORANZA DEI CITTADINI CHE RISPETTANO LE REGOLE

Alcune forze di opposizione parlano di un rischio di compressione delle libertà individuali. Come risponde a queste critiche?

«Rispondo che difendere la legalità e garantire sicurezza ai cittadini non significa comprimere le libertà, ma renderle effettive. La vera limitazione della libertà è quando una persona ha paura di prendere un treno la sera, di uscire nel proprio quartiere o di mandare i figli a scuola serenamente. Il Decreto Sicurezza contiene norme di assoluto buon senso. Contrastare lo spaccio, le occupazioni abusive, i blocchi illegali delle strade o le aggressioni alle Forze dell'Ordine significa tutelare i diritti della grande maggioranza dei cittadini che rispettano le regole. Purtroppo ogni volta che si tratta di rafforzare la sicurezza, spesso ci troviamo davanti ad un'opposizione pregiudiziale. Si invoca più sicurezza a parole, ma poi si contestano tutte le misure concrete che servono a garantirla. Noi invece abbiamo scelto di stare dalla parte dei cittadini onesti, di chi chiede più presenza dello Stato, più legalità e più tutela. Poi il nostro approccio non è solo repressivo. Lo dimostra il modello Caivano e lo dimostrano gli investimenti sulla rigenerazione urbana, sulla scuola, sul recupero sociale e sui beni confiscati. La sicurezza si costruisce con il controllo del territorio, ma anche combattendo marginalità, degrado ed esclusione sociale».

Un capitolo particolarmente importante riguarda la violenza giovanile.

«Abbiamo introdotto norme più severe sul porto di coltelli e il divieto di vendita ai minori di strumenti che troppo spesso diventano armi nelle mani dei ragazzi. È una scelta di buon senso, necessaria davanti all'aumento di episodi di aggressione e baby gang. Fondamentale è anche il rafforzamento dei sistemi di

videosorveglianza, che svolgono una funzione non solo repressiva ma soprattutto deterrente. Una telecamera spesso evita che un reato venga commesso e aiuta a restituire sicurezza ai cittadini. Vogliamo aumentare la presenza dello Stato nei territori, rafforzare la percezione di sicurezza, prevenire il degrado e dare alle Forze dell'Ordine strumenti più adeguati per intervenire in modo tempestivo ed efficace».

Al Viminale è stata firmata un'intesa importante su riuso, legalità e rigenerazione urbana: che valore ha questo accordo per i territori coinvolti?

«Ha un valore strategico molto importante, perché dimostra che il contrasto alle mafie non si esaurisce nelle attività repressive, ma passa anche dalla capacità dello Stato di restituire ai cittadini ciò che la criminalità aveva sottratto. Mi riferisco innanzitutto al rinnovo dell'accordo tra l'Agenzia Nazionale per i beni confiscati e la Regione Calabria, un protocollo che consolida un modello di collaborazione istituzionale estremamente efficace. In Calabria gli immobili confiscati già destinati sono 3.869, di cui oltre 3.100 trasferiti ai Comuni. Parliamo di beni che diventano centri sociali, presidi di legalità, strutture contro le dipendenze, luoghi di inclusione e anche sedi delle Forze di Polizia. Questo modello ha già prodotto risultati concreti. Penso, ad esempio, alla demolizione dell'ecomostro "Palazzo Mangeruca" a Melissa, nel Crotonese, per realizzare un'area camper: un simbolo di rigenerazione urbana e restituzione del territorio alla collettività. L'esperienza è stata così positiva che accordi analoghi sono stati stipulati anche con Sicilia, Lombardia e Campania, mentre presto verrà coinvolto anche il Piemonte».

E per quanto riguarda la rigenerazione urbana?

«Dal Viminale sono stati destinati oltre 600 milioni di euro ai Comuni per progetti di riqualificazione urbana, messa in sicurezza degli edifici e recupero delle aree degradate. Una città è più sicura quando i cittadini sentono che lo Stato è presente e che i luoghi vengono curati, recuperati e protetti. Al contrario, il degrado urbano e l'abbandono degli spazi pubblici favoriscono insicurezza e illegalità. La cosiddetta teoria delle 'finestre rotte' mostra che dove lo Stato arretra, dove prevalgono incuria, vandalismo e marginalità, cresce più facilmente la criminalità diffusa. Per questo rigenerare un quartiere, recuperare un immobile confiscato, riqualificare una piazza o rafforzare un presidio di legalità non significa soltanto migliorare il decoro urbano e la vivibilità dei luoghi, ma prevenire fenomeni criminali e ricostruire fiducia tra cittadini e istituzioni».

Oltre 3.800 immobili sottratti alla criminalità organizzata verranno restituiti alla collettività: quale impatto concreto potrà avere questa operazione sul tessuto sociale ed economico?

«L'impatto può essere molto significativo, perché ogni bene confiscato restituito alla collettività rappresenta insieme una vittoria dello Stato e un'opportunità concreta di sviluppo e riscatto sociale. Parliamo di immobili che possono diventare scuole, centri di aggregazione, strutture sociali, sedi istituzionali o presidi delle Forze dell'Ordine, trasformando luoghi che erano simboli del potere mafioso in spazi di legalità, partecipazione e crescita civile. L'esempio più recente e significativo è stata la demolizione di Palazzo Fienga a Torre Annunziata, il cosiddetto "Fortapàsc" della camorra, storico simbolo del clan Gionta, da cui partì l'ordine di uccidere il giornalista Giancarlo Siani. In questi anni oltre 18 mila beni confiscati sono tornati nella disponibilità dei cittadini. Abbiamo rafforzato l'Agenzia nazionale, accelerato le procedure di destinazione e costruito una rete stabile con prefetture, procure, enti locali e privato sociale per trasformare questi patrimoni in strumenti di crescita e coesione. C'è poi un aspetto fondamentale: accompagnare le aziende confiscate che possono superare il cosiddetto "shock di legalità", restare sul mercato e continuare a produrre occupazione sana. Questo significa trasformare patrimoni criminali in occasioni di sviluppo e crescita per i territori».

UNA CITTÀ È PIÙ SICURA QUANDO I CITTADINI SENTONO CHE LO STATO È PRESENTE E CHE I LUOGHI VENGONO CURATI, RECUPERATI E PROTETTI. AL CONTRARIO, IL DEGRADO URBANO E L'ABBANDONO DEGLI SPAZI PUBBLICI FAVORISCONO INSICUREZZA E ILLEGALITÀ

Il riutilizzo dei beni confiscati può diventare anche uno strumento di prevenzione oltre che di contrasto alla criminalità: in che modo il Governo intende rafforzare questo approccio?

«Oggi il riutilizzo sociale dei beni confiscati è uno dei più efficaci strumenti di prevenzione antimafia, perché colpisce le organizzazioni criminali nel loro vero centro di potere: la capacità economica e il controllo del territorio. Le mafie moderne agiscono sempre più come sistemi economici e finanziari, infiltrandosi nell'economia legale e creando consenso sociale. Sequestrare e confiscare patrimoni mafiosi significa prevenire nuove infiltrazioni e indebolire le reti criminali prima ancora della repressione penale. Il modello italiano delle misure di prevenzione patrimoniale è oggi guardato con grande interesse anche dai nostri partner europei e internazionali. Non è un caso che la nuova direttiva europea sul recupero e la confisca dei beni si ispiri proprio all'esperienza italiana. Il Governo Meloni intende rafforzare ulteriormente questo approccio accelerando le procedure di destinazione, sostenendo gli enti locali e potenziando il coordinamento tra istituzioni, perché ogni bene restituito ai cittadini diventa un presidio concreto di legalità, inclusione e presenza dello Stato». • **CG**

Wanda Ferro, sottosegretario di Stato al Ministero dell'Interno

Con te, in Prima linea.

CENTRALINO NAZIONALE
ATTIVO H24
7 GIORNI SU 7

06 37 51 82 82

Dal 1988 sosteniamo le donne e i minori vittime di violenza, offrendo gratuitamente accoglienza, protezione, alloggi sicuri, consulenze legali, psicologiche e nutrizionali, percorsi mirati di fuoriuscita dalla violenza e appropriazione della propria autonomia.

TELEFONO ROSA

Più forti insieme.

telefonorosa.it

Una risposta forte alla crescente complessità che ci circonda

In un quadro di instabilità pervasiva globale, le attenzioni della Difesa sono concentrate su ogni latitudine geografica. Il sottosegretario di Stato Isabella Rauti descrive l'impegno dell'Italia su scala globale

La sicurezza nazionale e la libertà collettiva sono priorità del Governo e della Difesa. Dopo decenni di pace, percepita come garantita e data per scontata, il paradigma si è spezzato. «Da quattro anni, dopo l'aggressione russa all'Ucraina- spiega Isabella Rauti, sottosegretario di Stato alla Difesa- la guerra scuote il cuore dell'Europa. Nuovi conflitti nel Golfo Persico e in Medio Oriente generano instabilità alle porte del Mediterraneo- "un continente liquido", per citare le parole dello storico Fernand Braudel- condizionando gli equilibri globali. Siamo di fronte a nuove forme di guerra, combattute non soltanto "boots on the ground" ma ibride e non convenzionali, che si sviluppano in tutti i domini: nel dominio digitale e cibernetico, in quello spaziale, nell'ambito cognitivo e nella dimensione dell'underwater».

Quali sono le principali priorità della Difesa, in un contesto internazionale così sfidante?

«In questo quadro di instabilità pervasiva globale, le attenzioni della Difesa sono concentrate su ogni latitudine geografica; sul "Fianco Est" e sul "Fronte Sud" ma anche nel "Grande Nord". La Regione artica oggi rappresenta uno spazio strategico per la sicurezza euro-atlantica e per gli equilibri mondiali anche in relazione alla protezione delle infrastrutture critiche e delle linee energetiche che collegano scenari lontani ma interconnessi. Penso anche alle nuove tensioni geopolitiche che la guerra in Iran ha generato (Paesi arabi, Mar Rosso, Stretto di Hormuz) che ci ricordano quanto fragile sia l'equilibrio energetico globale e quanto siano interdipendenti ecosistemi distanti e diversi».

In che modo l'Italia sta bilanciando gli impegni nel quadro della cooperazione con la Nato e con altri partner internazionali, soprattutto nelle missioni all'estero?

«L'Italia è un alleato leale della Nato e un membro dell'Ue, di cui stiamo rafforzando le capacità di difesa come pilastro complementare della Nato; ovvero aumentando e investendo su un'industria con standard comuni by design. Oggi la guerra si combatte nel dominio cyber, nello spazio, nella dimensione subacquea e nell'ambito cognitivo. La risposta- come indicato nel "non paper" del ministro Crosetto- deve essere proattiva e integrata, puntando sulla deterrenza difensiva, sulla prevenzione, sulla resilienza e sulla cooperazione tra Stati. Da decenni siamo impegnati nelle missioni internazionali di pace e stabilità, nelle coalizioni multinazionali e con i nostri contingenti schierati siamo tra i maggiori contributori su scala globale. La presenza italiana nei teatri operativi è orientata non solo a garantire condizioni di sicurezza e di deterrenza delle minacce ma anche al supporto alla popolazione civile e alla cooperazione con le istituzioni locali. L'Italia è tra i Paesi più attivi nell'applicazione delle Risoluzioni delle Nazioni Unite su "Donne, pace e sicurezza" e sulle pari opportunità, nonché sull'impegno e nella ricostruzione post-conflict».

Come le politiche di Difesa possono contribuire alla promozione e tutela dei valori nazionali e al rafforzamento del ruolo dell'Italia nel mondo?

«La cultura della Difesa è un sistema di valori, "un patrimonio materiale e immateriale", come dichiarato anche di recente dal ministro Crosetto. Difesa significa tutela delle istituzioni della Repubblica, salvaguardia delle infrastrutture strategiche e delle reti essenziali per il funzionamento del Paese, insieme alla protezione del sistema industriale e tecnologico, del patrimonio storico e dell'identità nazionale. Non si tratta di una forma di militarizzazione ma della responsabilità di preservare le libertà individuali e collettive e di rafforzare la capacità di risposta nella crescente complessità che ci circonda. La partecipazione dell'Italia alle missioni internazionali è uno strumento di diplomazia strategica che rafforza il dialogo con i partner e consolida le relazioni bilaterali in aree di interesse geopolitico».

Quali opportunità vede per il made in Italy nei filoni di cooperazione industriale e tecnologica legati alla difesa e alla sicurezza internazionale?

«Il Governo lavora alla valorizzazione del tessuto produttivo nazionale, favorendo un circolo economico virtuoso; anche le spese per la difesa sono un investimento che produce lavoro e indotto occupazionale. In questa prospettiva, la cooperazione industriale e tecnologica rappresenta una leva strategica per rafforzare il posizionamento del made in Italy nei principali programmi internazionali; penso al Global Combat Air Programme (GCAP), un'iniziativa congiunta di Regno Unito, Italia e Giappone per sviluppare una nuova generazione di caccia multi ruolo avanzato di sesta generazione entro la metà degli anni 2030. E al programma Eurodrone, che segna un passaggio fondamentale nella costruzione di una capacità europea autonoma nel dominio dei sistemi a pilotaggio remoto, rafforzando al contempo il ruolo dell'industria nazionale nelle tecnologie avanzate per la sorveglianza, l'intelligence e la sicurezza».

Per garantire sovranità, vantaggio competitivo e strategico cosa bisogna fare?

«Per garantire sovranità, vantaggio competitivo e strategico dobbiamo continuare a sviluppare le nuove tecnologie; governare l'intelligenza artificiale, utilizzare il quantum computing e la sensoristica avanzata, secondo un modello di difesa integrato e completo che coinvolga le industrie, le università, la società civile e il sistema Italia. In questo quadro, l'integrazione tra pubblico e privato e tra dimensione nazionale ed europea diventa determinante per sostenere l'innovazione e accrescere la resilienza industriale. La Difesa perciò deve continuare a muoversi in un'ottica di responsabilità nazionale: favorendo le relazioni industriali; abbattendo la lentezza procedurale cui ci vincola la burocrazia; investendo in cyberdifesa; in tecnologie dual-use; nella new space economy- decisiva per la sicurezza delle infrastrutture critiche e la resilienza delle reti- al pari della blue economy, sempre più centrale per la sicurezza delle rotte, la protezione delle infrastrutture sottomarine e la continuità energetica. Si tratta di due ambiti complementari che contribuiscono in modo crescente alla proiezione strategica e industriale dell'Italia». •LZ

OCCORRE MUOVERSI IN UN'OTTICA DI RESPONSABILITÀ NAZIONALE FAVORENDO LE RELAZIONI INDUSTRIALI, ABBATTENDO LA LENTEZZA PROCEDURALE CUI CI VINCOLA LA BUROCRAZIA, INVESTENDO IN CYBERDIFESA, IN TECNOLOGIE DUAL-USE, NELLA NEW SPACE ECONOMY E NELLA BLUE ECONOMY

Isabella Rauti, sottosegretario di Stato alla Difesa


Pomellato
MILANO 1967
NUDO COLLECTION
POMELLATO.COM

Ognuno è un ingranaggio consapevole

È la fiducia incondizionata, radicata nella conoscenza reciproca, nel rispetto e nella condivisione degli stessi valori, che nei momenti decisivi può fare la differenza. A guidare l'equipaggio nella riuscita delle loro missioni è il comandante Sara Vinci

Ogni comandante porta con sé un patrimonio unico fatto di esperienze, valori e tratti personali, ed è proprio l'unicità della persona, più che il genere, a riflettersi in modo determinante nel proprio stile di leadership. «Questa dimensione individuale, che si sovrappone a quella propria di ogni ufficiale di Marina- precisa Sara Vinci, comandante della Nave Alpino della Marina Militare- rappresenta una risorsa preziosa: la varietà dei vissuti e dei punti di vista arricchisce il modo in cui si affrontano le sfide quotidiane e si costruiscono le relazioni a bordo».

In che modo la leadership femminile può arricchire e influenzare la dinamica a bordo e la gestione dell'equipaggio?

«Nella mia esperienza, cerco di coltivare ogni giorno il senso di appartenenza dell'equipaggio e di mantenere alto il morale per garantire la massima efficacia operativa. Un equipaggio che si sente parte di un obiettivo comune, motivato e valorizzato nelle proprie individualità, è un equipaggio più coeso, reattivo e affidabile. In questo contesto, "remare all'unisono" non è soltanto un principio guida, ma una condizione imprescindibile per il successo di ogni missione. Significa costruire, giorno dopo giorno, una fiducia solida e autentica che nasce nel rapporto tra equipaggio e comandante, ma che si sviluppa anche in modo trasversale tra tutti i membri dell'equipaggio stesso».

Quali sono le principali responsabilità e sfide nel comando di una nave della Marina Militare come la Alpino?

«Il comandante ha come responsabilità primaria quella di garantire, in modo parimenti imprescindibile, la piena efficienza del mezzo e la prontezza operativa del personale, affinché l'unità sia sempre in grado di assolvere la missione assegnata. La nave rappresenta uno strumento tecnologicamente avanzato e complesso, ma è l'equipaggio, adeguatamente formato e addestrato, a renderlo realmente efficace e capace di esprimere tutte le sue potenzialità. Per questo motivo, accanto alla cura costante dell'efficienza della piattaforma e dei sistemi, che richiede attenzione continua, manutenzione accurata e gestione rigorosa delle risorse, riveste un ruolo centrale l'addestramento del personale per consolidarne prontezza, flessibilità e resilienza anche in contesti complessi e multidominio. La sfida principale consiste sicuramente nel garantire questo equilibrio in un contesto caratterizzato da una rapida e costante evoluzione. Le tecnologie si sviluppano con grande velocità e gli scenari operativi diventano sempre più dinamici e interconnessi, includendo nuove realtà come il dominio cibernetico e la dimensione cognitiva. Questo richiede non solo capacità di adattamento ma anche un aggiornamento continuo per integrare innovazione tecnologica e fattore umano in modo efficace».

IL COMANDANTE HA COME RESPONSABILITÀ PRIMARIA QUELLA DI GARANTIRE, IN MODO PARIMENTI IMPRESCINDIBILE, LA PIENA EFFICIENZA DEL MEZZO E LA PRONTEZZA OPERATIVA DEL PERSONALE, AFFINCHÉ L'UNITÀ SIA SEMPRE IN GRADO DI ASSOLVERE LA MISSIONE ASSEGNATA

Quali strumenti e percorsi formativi ritiene fondamentali per preparare ufficiali e marinai alle complesse operazioni militari e alle missioni internazionali?

«La Marina dispone di percorsi formativi ben delineati e strutturati, studiati per preparare al meglio il personale dei diversi ruoli ad affrontare la complessità delle operazioni militari e delle missioni internazionali. La formazione si costruisce su un sistema organico che integra preparazione di base, specializzazione e aggiornamento professionale, con contenuti sempre al passo con l'evoluzione degli scenari operativi e delle tecnologie. La formazione ci accompagna per tutta la carriera secondo un modello dinamico e circolare che favorisce il continuo sviluppo delle competenze indispensabili nei contesti complessi e multi-dominio. Particolare rilevanza assume l'addestramento secondo il principio del "train as you fight" preparando quotidianamente il personale ad operare in condizioni il più possibile aderenti agli attuali scenari internazionali».

Quanto conta la resilienza, la disciplina e la capacità di adattamento nella vita quotidiana a bordo e nelle missioni più complesse?

«La disciplina è la base di partenza, il punto fermo. Non è solo rispetto delle regole, ma è ciò che crea fiducia tra le persone, che rende ogni azione prevedibile, coordinata, affidabile. La resilienza, invece, è un fattore chiave per chi svolge il nostro lavoro. Significa non fermarsi alla difficoltà, ma attraversarla, mantenendo lucidità, equilibrio e capacità decisionale anche sotto pressione. Infine, la capacità di adattamento è ciò che permette di armonizzare la dimensione personale con quella collettiva: ognuno diventa un ingranaggio consapevole, capace di lavorare in sintonia con gli altri, contribuendo a un'unica azione coordinata ed efficace. Bisogna inoltre sapersi adattare al contesto che cambia continuamente perché cambia la missione o l'area geografica di gravitazione della nave».

Quali prospettive e opportunità vede per le donne nelle Forze Armate, e quale messaggio vorrebbe trasmettere alle giovani che aspirano a intraprendere una carriera militare?

«Sono entrata in Marina agli albori del reclutamento femminile e ho avuto il privilegio di vivere in prima persona un percorso di trasformazione profondo. Ho visto evolvere la Difesa italiana fino a diventare oggi una delle realtà più avanzate in termini di piena integrazione, fondata sul merito, sulle competenze e sul riconoscimento delle capacità individuali, indipendentemente dal genere. È vero, per una questione temporale il percorso non è ancora completamente maturo dal punto di vista numerico, ma la direzione è chiara. Proprio per questo guardo al futuro con fiducia e con l'aspettativa di vedere quanto questa integrazione continuerà a generare valore. Un'organizzazione più diversificata è, infatti, anche più solida, più pronta ad affrontare le sfide e, in definitiva, più resiliente. Alle giovani che oggi desiderano intraprendere questa strada direi che si tratta di una scelta certamente impegnativa, sia sul piano professionale che personale, ma anche straordinariamente arricchente. È un percorso che permette di acquisire competenze autentiche, vivere esperienze uniche e assumere responsabilità importanti fin da giovani. In Marina non si impara soltanto una professione, si cresce come persone in un contesto che si fonda su valori profondi e immutabili. Ed è proprio questo che dà un significato pieno e concreto alla nostra scelta di vita».

•Ginevra Cavalieri

Sara Vinci, comandante Nave Alpino Marina Militare


syngenta
DA QUI, IL FUTURO È MERAVIGLIOSO
Da 25 anni Syngenta guida l'innovazione in agricoltura, per scoprire dove è possibile fare la differenza e accompagnare le imprese di domani
Grazie all'impegno dei nostri ricercatori, agronomi e innovatori, abbiamo sviluppato tecnologie d'avanguardia per ottimizzare il lavoro degli agricoltori e garantire la sicurezza alimentare alle generazioni future. Dalle sementi di precisione a prodotti più sostenibili per la difesa delle colture, fino alle soluzioni digitali che stiamo mettendo a disposizione delle aziende agricole, il nostro lavoro ha già apportato cambiamenti che sono sotto gli occhi di tutti. Continueremo a investire in ricerca. Perché per Syngenta l'innovazione non è solo ciò che facciamo: è il nostro modo di vedere il mondo.

Dalla piazza fisica al terreno virtuale

In un'economia non solo globalizzata ma anche digitalizzata le organizzazioni criminali rinnovano strategie e tecniche per insinuarsi negli spazi anonimi della rete, così da compiere le stesse attività illecite perpetrate nel mondo reale. Il generale Antonio Mancazzo ci spiega come è cambiato il crimine online e l'attività di contrasto della Guardia di Finanza

La trasformazione digitale dell'economia ha aperto scenari senza precedenti per cittadini, imprese e mercati, ma allo stesso tempo ha ampliato il terreno d'azione della criminalità informatica. Oggi le frodi online non colpiscono più soltanto singoli utenti o sistemi isolati: coinvolgono infrastrutture strategiche, flussi finanziari globali e intere filiere produttive attraverso attacchi sempre più sofisticati e transnazionali. Dal furto d'identità digitale ai ransomware, fino all'utilizzo dell'intelligenza artificiale per costruire truffe credibili e difficili da individuare, il cybercrime rappresenta una delle principali sfide contemporanee per la sicurezza economico-finanziaria. In questo contesto il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza, guidato dal generale Antonio Mancazzo, svolge un ruolo centrale nel presidio investigativo della rete, operando anche negli spazi più opachi del deep e dark web.

Negli ultimi anni le frodi online sono diventate sempre più sofisticate: quali sono oggi le minacce economico-finanziarie più diffuse che colpiscono cittadini e imprese sulla rete?

«Mi sia consentita una doverosa premessa: oggi siamo di fronte a un'economia non solo globalizzata ma, grazie alle tecnologie, anche digitalizzata. A fronte degli indubbi vantaggi che tutto ciò comporta sia per i cittadini che per le imprese, non si può sottacere come, in tale scenario, anche le organizzazioni criminali, a diversi livelli, avvertono l'esigenza di rinnovare le proprie strategie e tecniche attraverso le quali potersi insinuare negli spazi anonimi della rete così da compiere le stesse attività illecite perpetrate nel mondo reale. Infatti, le attività investigative dimostrano proprio come negli ultimi tempi si stia assistendo ad uno spostamento dell'illecito dalla piazza fisica al terreno virtuale. L'utilizzo illecito delle nuove tecnologie ha portato, quindi, la Guardia di Finanza a rafforzare il dispositivo di contrasto che oggi è anche orientato al controllo economico del web attraverso il monitoraggio della rete telematica, soprattutto quella nascosta. Il riferimento è in particolare al deep e dark web dove si annidano le attività più perniciose portate avanti da soggetti dediti a delinquere e che hanno solide radici nel mondo reale. In tale ambito, il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche rappresenta, ad oggi, il Reparto del Corpo specializzato nel contrasto al cyber crime in ogni sua forma garantendo il costante presidio di polizia economico-finanziaria in rete».

I RANSOMWARE ATTACK, SE ATTIVATI, PRECLUDONO L'ACCESSO AI DATI UTILIZZANDO DELLE SOFISTICATE TECNICHE CRITTOGRAFICHE E ALIMENTANO COSÌ UN VERO E PROPRIO MERCATO CRIMINALE PARALLELO BASATO SUL PAGAMENTO DEI RISCATTI, SPESSO EFFETTUATI TRAMITE CRIPTOVALUTE PARTICOLARMENTE AMBITE DAI CYBERCRIMINALI PER LA LORO NATURA PSEUDO ANONIMA

Tornando alla mia domanda?

«Cercando di rispondere alla sua domanda, devo effettivamente sottolineare come purtroppo stiamo assistendo a un forte aumento delle frodi a monte delle quali, è bene sottolinearlo, c'è quasi sempre un furto d'identità digitale. Ecco perché bisogna prestare massima attenzione a non far circolare sul web, laddove non estremamente necessario, dati riferibili alla propria persona e/o che possano far risalire a posizioni di titolarità (come ad esempio quelle bancarie). In generale, si parla di minacce evolute attuate, ad esempio, attraverso i ransomware o attacchi alle infrastrutture critiche, spesso transnazionali, che sfruttano competenze e strumenti digitali avanzati, tecniche di ingegneria sociale, piattaforme online e persino sistemi basati sull'intelligenza artificiale per rendere le truffe più credibili

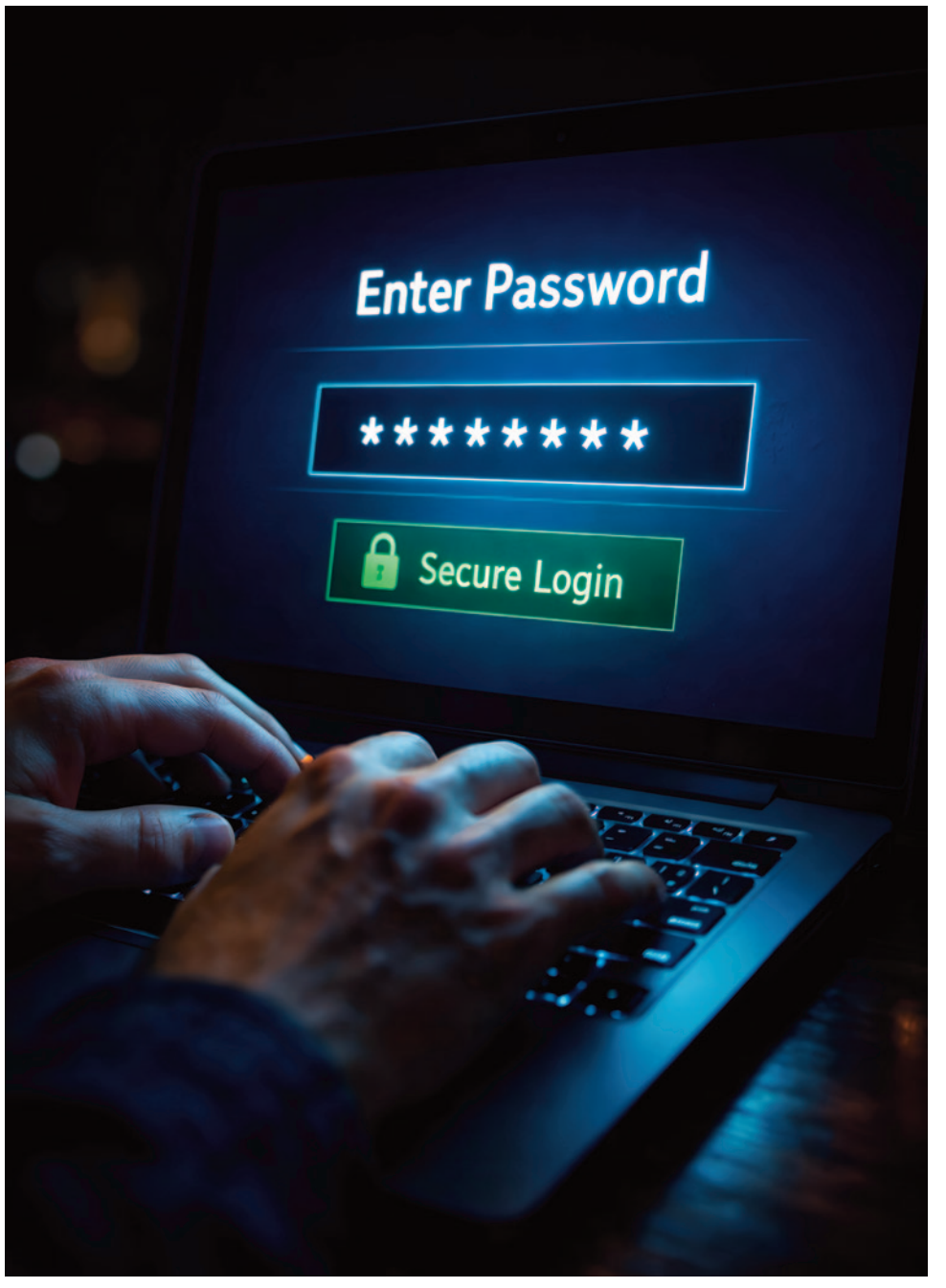
e difficili da individuare. I ransomware attack, se attivati, precludono l'accesso ai dati utilizzando delle sofisticate tecniche crittografiche e alimentano così un vero e proprio mercato criminale parallelo basato sul pagamento dei riscatti, spesso effettuati tramite criptovalute particolarmente ambite dai cybercriminali per la loro natura pseudo anonima».

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche opera in un contesto in continua evoluzione: quanto conta oggi la collaborazione internazionale nel contrasto ai crimini digitali?

«Il contrasto ai crimini digitali è oggi, per definizione, una sfida globale: le infrastrutture informatiche, i servizi cloud, le piattaforme di pagamento e le reti criminali operano senza confini spazio temporali. Questo significa che le attività illecite possono essere pianificate in un Paese, essere eseguite attraverso server collocati in un altro e potenzialmente produrre effetti in più Stati contemporaneamente. In questo scenario, diventa fondamentale la collaborazione tra Forze di Polizia, autorità giudiziarie, organismi europei e internazionali per condividere informazioni, tracciare flussi finanziari, acquisire dati digitali e coordinare operazioni complesse in tempi che necessariamente devono essere compatibili con la rapidità dell'ambiente cyber».

Le criptovalute e i sistemi di pagamento digitali stanno cambiando il panorama finanziario: quali sono le principali difficoltà investigative nel tracciare flussi economici illeciti online?

«Sebbene la blockchain sia per natura pubblica, la vera sfida è identificare l'effettivo titolare di un wallet o di un'operazione registrata nella citata "catena di blocchi". E, qui, entrano in gioco le abilità dei nostri investigatori digitali che, attraverso il ricorso a tecniche specifiche di blockchain analysis e intelligence, cercano di anonimizzare i possessori di criptovalute. Attività che diventa ulteriormente complessa allorquando i cyber criminali ricorrono a exchange collocati in giurisdizioni poco collaborative, mixer e privacy coin. Un ulteriore aspetto riguarda la velocità con cui i proventi illeciti possono essere frammentati e trasferiti tra diversi strumenti finanziari digitali, rendendo più complessa la ricostruzione del percorso del denaro. Per questo motivo, le indagini economico-finanziarie in ambito cyber richiedono oggi un approccio multidisciplinare che integri competenze investigative, informatiche e di analisi finanziaria avanzata».



IL CONTRASTO AI CRIMINI DIGITALI È OGGI, PER DEFINIZIONE, UNA SFIDA GLOBALE: LE INFRASTRUTTURE INFORMATICHE, I SERVIZI CLOUD, LE PIATTAFORME DI PAGAMENTO E LE RETI CRIMINALI OPERANO SENZA CONFINI SPAZIO TEMPORALI

Sul fronte della prevenzione, quali comportamenti e strumenti ritiene fondamentali per aiutare cittadini e aziende a difendersi dalle frodi tecnologiche?

«La prevenzione rappresenta oggi la prima e più efficace linea di difesa contro le frodi tecnologiche, non a caso si parla di educazione finanziaria. Per i cittadini, questo deve tradursi nell'adozione di comportamenti semplici ma essenziali: utilizzo di password robuste e differenti, attivazione di sistemi di autenticazione a più fattori, aggiornamento costante dei dispositivi e software, verifica dell'identità di chi richiede dati sensibili o trasferimenti di denaro, attenzione a comunicazioni allarmistiche o troppo vantaggiose. Noi ribadiamo sempre un adagio del passato, oggi più cha mai attuale: "Se vi viene proposto qualcosa di troppo bello per essere vero, allora non è vero!!" È, altrettanto, importante segnalare tempestivamente tentativi di truffa alle autorità competenti, perché ogni segnalazione contribuisce a rafforzare la capacità di prevenzione collettiva. Per le imprese, soprattutto per le piccole e medie aziende che spesso dispongono di minori risorse dedicate alla sicurezza informatica, la prevenzione deve tradursi in investimenti concreti in cybersecurity, formazione del personale e protezione delle infrastrutture digitali. La sicurezza, pertanto non può essere percepita come un costo aggiuntivo, ma come un investimento strategico per la competitività e la continuità operativa».

L'intelligenza artificiale è sempre più presente anche nel mondo cyber: l'Ai può essere utilizzata per commettere illeciti, ma allo stesso tempo rappresenta una risorsa investigativa. Come sta cambiando il vostro lavoro e quali sono oggi le principali opportunità e incognite legate a questa tecnologia?

«Da un lato, l'intelligenza artificiale potrebbe rappresentare uno strumento sfruttato anche in modo illecito: pensiamo alla creazione di campagne di phishing sempre più credibili, ai deepfake, all'automazione delle frodi online o alla produzione massiva di contenuti ingannevoli. Dall'altro lato, la stessa tecnologia costituisce una risorsa strategica per le attività investigative che possono analizzare grandi quantità di dati, individuare anomalie, correlare eventi, supportare il monitoraggio delle minacce e accelerare le attività di analisi forense digitale. La sfida principale, tuttavia, consiste nel mantenere un equilibrio tra innovazione, sicurezza e garanzie democratiche, nel rispetto dei principi di legalità, proporzionalità, tutela dei diritti fondamentali e protezione dei dati personali».

•**Lucrezia Antinori**

Il generale Antonio Mancazzo, comandante Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza

Dal 1815 aiutiamo a spedire merci verso ogni destinazione

Quando il successo dipende dal commercio globale, sappiamo quanto è importante che le merci arrivino puntuali a destino. Ecco perchè DHL Global Forwarding promette di offrire sempre consegne affidabili, flessibili ed efficienti da e verso ogni Paese del mondo, in totale conformità con le normative locali.

infodgf.it@dhl.com

Excellence. Simply delivered.
dhl.com

La Farnesina è in prima linea

Su indicazione del ministro Antonio Tajani la struttura è stata incaricata di assicurare uno stretto raccordo tra la cybersicurezza del Ministero e delle sedi all'estero, da un lato, e l'azione di politica estera dell'Italia nei settori delle minacce ibride, della sicurezza cibernetica e delle tecnologie emergenti dall'altro. A guidarla è Alessandro De Pedys

La trasformazione digitale e l'accelerazione tecnologica stanno ridefinendo equilibri geopolitici, modelli economici e sistemi di difesa. Oggi il cyberspazio è diventato un terreno strategico nel quale si intrecciano sicurezza nazionale, tutela delle infrastrutture critiche, diplomazia e competizione internazionale. In questo scenario, l'Italia punta a rafforzare il proprio ruolo attraverso una strategia fondata su cooperazione multilaterale, resilienza tecnologica e governance condivisa. Ne parla Alessandro De Pedys, direttore generale per le questioni cibernetiche della Farnesina, al centro della nuova architettura voluta dal ministro Antonio Tajani per affrontare le sfide del dominio digitale e delle minacce ibride.

Com'è cambiata la missione della Direzione Generale dopo la riforma cyber e digitale promossa dal ministro Antonio Tajani e quali sono oggi le priorità strategiche dell'Italia nel cyberspazio?

«Il panorama internazionale è caratterizzato da una forte accelerazione del processo di innovazione tecnologica e, al tempo stesso, dalla progressiva digitalizzazione delle società avanzate. Le nostre società sono ormai rette da infrastrutture digitali tanto essenziali quanto vulnerabili e, in questo contesto, le dipendenze tecnologiche e le attività cibernetiche malevole sono alcune delle sfide che l'Italia è chiamata ad affrontare. Per questo la Farnesina si è dotata, su indicazione del ministro Tajani, di una struttura incaricata di assicurare uno stretto raccordo tra la cybersicurezza del Ministero e delle sedi all'estero, da un lato, e l'azione di politica estera dell'Italia nei settori delle minacce ibride, della sicurezza cibernetica e delle tecnologie emergenti dall'altro. D'altronde, quello digitale è un dominio nel quale l'interconnessione fra Paesi e aree del mondo è particolarmente evidente. Per questo motivo occorre adoperarsi attraverso molteplici iniziative di cooperazione internazionale per porre in essere misure volte a garantire la stabilità, la pace e la sicurezza, anche a tutela dei nostri interessi nazionali. In questo senso, la Farnesina collabora strettamente con tutte le Amministrazioni competenti per accrescere la propria postura di sicurezza cibernetica, definire una governance globale del cyberspazio, imperniata sulla cornice ONU di comportamento responsabile degli Stati, e contribuire alla costruzione di capacità informatiche nei Paesi in via di sviluppo».

LA FARNESINA COLLABORA CON TUTTE LE AMMINISTRAZIONI COMPETENTI PER ACCRESCERE LA PROPRIA POSTURA DI SICUREZZA CIBERNETICA, DEFINIRE UNA GOVERNANCE GLOBALE DEL CYBERSPAZIO, IMPERNIATA SULLA CORNICE ONU DI COMPORTAMENTO RESPONSABILE DEGLI STATI, E CONTRIBUIRE ALLA COSTRUZIONE DI CAPACITÀ INFORMATICHE NEI PAESI IN VIA DI SVILUPPO

Quali strumenti diplomatici e operativi ritiene oggi più efficaci per affrontare minacce sempre più ibride e globali, come attacchi alle infrastrutture critiche, interferenze nei processi democratici, campagne di disinformazione?

«Nell'attuale scenario globale, dove si afferma sempre di più un approccio competitivo- quando non di aperto confronto- tra Paesi o gruppi di Paesi portatori di interessi e valori diversi, è essenziale che alle strategie di deterrenza e difesa si sommino attività di preparazione e risposta sviluppate in maniera integrata, soprattutto a fronte del moltiplicarsi delle minacce di natura ibrida. Questo significa innanzitutto coinvolgere tutte le istituzioni a vario titolo interessate, sviluppando un approccio coordinato che permetta di fronteggiare sul serio tali sfide, in tutte le loro molteplici dimensioni».

Cos' altro occorre?

«È essenziale il coinvolgimento- oltre che delle istituzioni- del settore privato e industriale e, più in generale, della società civile, con l'obiettivo di garantire la stabilità della società e il suo sistema democratico, la continuità dei servizi essenziali per i cittadini, gli approvvigionamenti industriali,

il funzionamento delle infrastrutture critiche. Inoltre, le minacce ibride, per loro natura, sono caratterizzate da una dimensione transnazionale, che rende fondamentale il coordinamento internazionale e la cooperazione fra Paesi partner e alleati. L'Unione Europea, il G7, la NATO, le Nazioni Unite rimangono i principali punti di riferimento nell'ambito dei quali sviluppare strumenti adeguati. In primis, puntando ad alzare il "costo politico" di chi- attore statale o non statale- porta avanti campagne ibride. E farlo sempre insieme con i nostri partner, perché nella battaglia contro le minacce ibride la cooperazione internazionale ci offre strumenti dei quali da soli, altrimenti, non potremmo mai disporre. Su questo, la Farnesina è in prima linea».

Quanto è importante arrivare a regole internazionali condivise nel cyberspazio e quali sono i principali ostacoli alla costruzione di una governance digitale realmente globale?

«Delineare regole internazionali condivise nel cyberspazio è fondamentale per garantire la sicurezza nazionale e la tutela dei diritti umani, ma anche la stabilità economica, in un mondo in cui non c'è ambito dell'esperienza umana che sia rimasto estraneo alla digitalizzazione. Emerge, dunque, la necessità di trovare valori e standard condivisi per lo sviluppo di tecnologie umano-centriche. Sebbene si registrino importanti passi avanti multilaterali, la strada verso una governance realmente globale si scontra con ostacoli geopolitici, tecnici e ideologici».

Quali sono i più critici?

«Se sul fronte europeo e con i Paesi like-minded esiste un accordo di massima rispetto a tali principi di governance, occorre riconoscere che non tutti condividono la nostra visione. Agire senza essere vincolati da regole può consentire di guadagnare un vantaggio tecnologico, commerciale e strategico. Questo vale per tutte le nuove tecnologie dirompenti, dal cyber all'intelligenza artificiale al quantum. In breve, l'ostacolo principale alla costituzione di una governance globale è proprio la potenzialità di queste tecnologie, sono gli evidenti vantaggi comparati di cui godrà chi le dominerà per primo. Ciò detto, non bisogna essere troppo pessimisti: come si è riusciti a definire regole per l'uso dell'energia nucleare, creso sia possibile fare altrettanto anche per questi nuovi strumenti».

In uno scenario internazionale segnato da tensioni geopolitiche e competizione tecnologica, quale ruolo può giocare l'Italia nel promuovere un modello di cybersicurezza fondato su cooperazione, innovazione e tutela dei valori democratici?

«L'Italia è impegnata per promuovere uno spazio cibernetico aperto, libero, sicuro, accessibile. Convinti della forza del multilateralismo e del primato del diritto internazionale- anche in una fase in cui il rispetto del diritto sembra essere un dettaglio trascurabile- partecipiamo attivamente a molteplici iniziative di politica estera cibernetica, guardando non solo alle questioni di principio ma anche agli aspetti più concreti della collaborazione internazionale. Queste iniziative sono concepite per rispondere non solo alle sfide che minacciano la nostra sicurezza, ma anche all'esigenza di collaborazione fra Paesi dal comune sentire: penso, ad esempio, ai lavori in seno alla NATO, all'ONU, all'Unione Europea, all'OSCE, al G7 e ad altre coalizioni informali».

Tra queste iniziative qual è la più importante?

«Una di esse, che mi piace ricordare, è il Meccanismo di Tallinn: si tratta di una piattaforma internazionale per il coordinamento dei progetti di assistenza cyber civile all'Ucraina. L'Italia ne deterrà la presidenza da luglio a dicembre di quest'anno. Vista l'esperienza maturata in questo settore dagli Ucraini in questi anni, si tratta evidentemente di attività che consentono un arricchimento reciproco. Con lo stesso spirito sosteniamo, inoltre, progetti di costruzione delle capacità informatiche nei Paesi in via di sviluppo, in linea con l'approccio cooperativo promosso dal Piano Mattei. Quale che sia il fronte di impegno, è per noi prioritario stimolare il partenariato pubblico-privato, quale strumento vincente per lo scambio di informazioni, l'elaborazione di politiche settoriali e la realizzazione di progetti. Solo attraverso un gioco di squadra possiamo, infatti, posizionare in maniera efficace l'Italia quale attore di primo piano nel campo della cybersicurezza». •**Lucrezia Antinori**

LE MINACCE IBRIDE, PER LORO NATURA, SONO CARATTERIZZATE DA UNA DIMENSIONE TRANSNAZIONALE, CHE RENDE FONDAMENTALE IL COORDINAMENTO INTERNAZIONALE E LA COOPERAZIONE FRA PAESI PARTNER E ALLEATI

Alessandro De Pedys, a capo della Direzione Generale per le Questioni Cibernetiche, l'Informatica e l'Innovazione Tecnologica del Ministero degli Affari Esteri e della Cooperazione Internazionale

Nessuno si salva da solo

Il centro di competenza Cyber 4.0 svolge un ruolo decisivo: accompagnare le imprese nella comprensione dei propri bisogni, del proprio livello di maturità e dei rischi associati ai processi di trasformazione digitale. Interviene il presidente Paolo Spagnoletti

La sicurezza informatica non riguarda più soltanto la protezione dei dati, ma il funzionamento stesso di sistemi industriali, infrastrutture e tecnologie intelligenti sempre più interconnesse. L'avanzata di intelligenza artificiale, cloud e automazione sta infatti ampliando il perimetro dei rischi digitali, rendendo centrale la capacità di progettare ecosistemi tecnologici sicuri, affidabili e resilienti. «Oggi il problema- precisa il presidente di Cyber 4.0 Paolo Spagnoletti- non riguarda più soltanto la protezione del dato o delle infrastrutture It tradizionali. La trasformazione digitale sta portando intelligenza e connettività dentro oggetti fisici, processi industriali e catene di fornitura sempre più distribuite. Questo significa che ai rischi di security si aggiungono sempre più rischi di safety: una vulnerabilità non compromette solo informazioni, ma può influenzare il comportamento di sistemi autonomi, droni, robot o dispositivi intelligenti interconnessi. In questo scenario diventa essenziale governare l'intero ciclo di vita di prodotti e servizi digitali, perchè la sicurezza non riguarda più soltanto la protezione dei sistemi, ma la capacità di garantire comportamenti affidabili e controllabili di tecnologie sempre più autonome e interconnesse».

In un contesto sempre più complesso e interconnesso, come si può costruire una digitalizzazione realmente sicura?

«Credo che il tema della security by design sia fondamentale, ma vada anche affrontato con grande concretezza. Abbiamo molto da imparare da settori come quello spaziale, dove progettare sistemi sicuri by design non è una scelta teorica ma una necessità: quando un satellite viene lanciato, intervenire successivamente è estremamente difficile. Per molti anni il digitale ha vissuto nell'idea implicita che fosse sempre possibile correggere dopo. Oggi non è più così, soprattutto quando il software controlla infrastrutture, mobilità, energia o sistemi autonomi. Una digitalizzazione realmente sicura richiede quindi capacità progettuali, simulazione, testing e una forte integrazione tra competenze tecnologiche, conoscenza dei processi operativi e capacità di progettare sistemi affidabili in contesti critici».

UNA DIGITALIZZAZIONE REALMENTE SICURA RICHIEDE CAPACITÀ PROGETTUALI, SIMULAZIONE, TESTING E UNA FORTE INTEGRAZIONE TRA COMPETENZE TECNOLOGICHE, CONOSCENZA DEI PROCESSI OPERATIVI E CAPACITÀ DI PROGETTARE SISTEMI AFFIDABILI IN CONTESTI CRITICI

Qual è il ruolo di Cyber 4.0 nel supportare le aziende italiane, in particolare le Pmi, nell'adozione di tecnologie sicure e nella crescita della resilienza digitale?

«Più che parlare di "adozione di tecnologie sicure", credo sia importante parlare della capacità di rendere sicure le tecnologie nei loro specifici contesti d'uso. È proprio qui che un centro di competenza come Cyber 4.0 può svolgere un ruolo decisivo: accompagnare le imprese nella comprensione dei propri bisogni, del proprio livello di maturità e dei rischi associati ai processi di trasformazione digitale. Questo significa trasferire conoscenza, facilitare l'accesso a competenze avanzate e creare connessioni tra università, imprese e territori. Per le Pmi, in particolare, è fondamentale poter contare su un ecosistema che le aiuti non solo a investire in innovazione, ma a farlo in modo sostenibile e sicuro».

Formazione e competenze rappresentano una delle grandi sfide del settore cyber. Come si può colmare il gap di professionalità specializzate e preparare le nuove generazioni ai lavori della sicurezza digitale?

«Oggi la sicurezza digitale non è più un tema riservato agli informatici. Le tecnologie intelligenti stanno trasformando il lavoro, le imprese e le istituzioni, e questo richiede competenze capaci di unire tecnologia, management, diritto e più in generale scienze sociali. Con la crescente automazione, il ruolo dell'uomo sarà sempre più legato alla supervisione, al controllo e alla gestione dei rischi associati ai sistemi digitali. Allo stesso tempo, le normative europee stanno introducendo responsabilità sempre più rilevanti per organizzazioni e professionisti. Per questo è fondamentale formare figure in grado non solo di usare le tecnologie, ma anche di comprenderne gli impatti economici, organizzativi e sociali e di governarle in modo responsabile».

Intelligenza artificiale, cloud e automazione stanno cambiando profondamente il panorama tecnologico: ritiene che queste innovazioni aumenteranno soprattutto le opportunità di difesa oppure i rischi legati agli attacchi informatici?

«Come spesso accade nelle grandi trasformazioni tecnologiche, aumenteranno entrambe le dimensioni. Le stesse tecnologie che possono rendere più sofisticati gli attacchi permettono anche di sviluppare capacità di prevenzione, rilevamento e risposta molto più avanzate. La vera sfida sarà la velocità con cui riusciremo a trasferire conoscenze e competenze tra settori diversi: tra ambito militare e civile, tra grandi imprese e Pmi, tra pubblico e privato. Oggi la sicurezza digitale dipende sempre più dalla capacità di mettere in relazione esperienze e competenze diverse, perché nessun attore può affrontare da solo la complessità dei nuovi scenari tecnologici». • **Linda Zorza**

Paolo Spagnoletti, docente alla Luiss e presidente Cyber 4.0


Dal 1919.
Passione Italiana.
Tratto Distintivo.
AURORA
Since 1919.
Italian Passion.
Sign of Distinction.
Nel cuore e nelle mani
degli italiani dal 1919.
AURORA
DAL 1919 FACCIAMO LE COSE ALLO STESSO MODO, CON LA STESSA
IMMUTATA PASSIONE. OGGETTI SENZA TEMPO, BELLI E CONCRETI,
COME SOLO NOI ITALIANI SAPPIAMO CREARE.
DA OLTRE 100 ANNI, NON SCENDIAMO MAI A COMPROMESSI,
SULLA QUALITÀ DEI MATERIALI E SULLE TECNICHE DI LAVORAZIONE.
ORGOGLIOSI DI CONTINUARE A SCRIVERE,
CON IL MEDESIMO CARATTERE AUTENTICO E APPASSIONATO,
LA STORIA DELLO STILE ITALIANO.
Aurora S.r.l - Strada Abbadia di Stura, 200 - 10156 Torino
aurorapenofficial
aurorapenofficial
www.aurorapen.it
aurorapen
#AuroraPen

Uscire dal cerchio ristretto degli specialisti

La cybersecurity sta diventando sempre più una professione di frontiera, dove tecnologia, diritto, economia e fattore umano si incontrano. Proprio per questo è, secondo Massimo Chirivì, una delle professioni più affascinanti e più necessarie per il futuro del nostro Paese

«La sicurezza informatica è una sfida centrale per il nostro tempo e il nostro impegno sarà quello di sostenere i professionisti del settore e promuovere una cultura della sicurezza digitale in tutta Italia». Ad assicurarlo è Massimo Chirivì, presidente AIPSI, Associazione Italiana Professionisti Sicurezza Informatica.

Quali sono oggi le priorità nella diffusione della cultura della sicurezza digitale nel Paese?

«La prima cosa da fare è cambiare proprio il modo in cui guardiamo alla sicurezza digitale. Per troppo tempo è stata considerata una faccenda tecnica, roba da informatici. Oggi non è più così: riguarda tutti, dal cittadino che usa lo smartphone al dirigente pubblico, dall'imprenditore al ragazzo delle scuole superiori. Le priorità concrete, dal mio punto di vista, sono tre. Anzitutto serve una formazione di base che arrivi davvero alle persone. La maggior parte degli attacchi che vanno a segno non sfruttano tecnologie sofisticate, ma la disattenzione di chi clicca su un link sbagliato o usa la stessa password ovunque. Phishing, credenziali deboli, leggerezza nella gestione dei dati personali: sono ancora questi i veri problemi».

E poi?

«Bisogna inserire la sicurezza digitale nei programmi scolastici e universitari in modo serio e strutturato, partendo già dalle medie e dalle superiori. C'è un equivoco da sfatare: il fatto che i ragazzi siano nati con uno smartphone in mano non significa affatto che sappiano usarlo in sicurezza. Anzi, spesso è vero il contrario. Su questo, come AIPSI, abbiamo voluto fare la nostra parte con un'iniziativa concreta: si chiama AIPSI School ed è un piano che mettiamo a disposizione di tutte le scuole italiane. In pratica, i nostri soci- che sono professionisti del settore- intervengono gratuitamente negli istituti per portare a studenti e insegnanti momenti di sensibilizzazione e formazione sulla sicurezza digitale. È il nostro modo di restituire al Paese una parte delle competenze che abbiamo, partendo da dove tutto comincia, cioè dai ragazzi. Infine, va rafforzata la collaborazione tra pubblico e privato. Quando ciascuno si difende da solo, perde. Servono scambio di informazioni sulle minacce, una regia nazionale chiara, e la consapevolezza che stiamo combattendo tutti la stessa battaglia».

Massimo Chirivì presidente AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

BISOGNA INSERIRE LA SICUREZZA DIGITALE NEI PROGRAMMI SCOLASTICI E UNIVERSITARI IN MODO SERIO E STRUTTURATO, PARTENDO GIÀ DALLE MEDIE E DALLE SUPERIORI

Quali sono gli obiettivi principali di AIPSI?

«AIPSI è nata per dare voce e rappresentanza ai professionisti della sicurezza dell'informazione qui in Italia. La missione sta in poche parole: competenza, etica del mestiere, cultura della sicurezza. Siamo il capitolo italiano di ISSA, e questo è un punto importante, perché ci consente di attingere a un patrimonio di esperienze che arriva da tutto il mondo e di calarlo nella nostra realtà, che ha caratteristiche sue, fatte di tante Pmi, di una pubblica amministrazione articolata, di un tessuto produttivo molto diversificato».

In che modo l'associazione intende supportare aziende, pubbliche amministrazioni e professionisti nel prossimo futuro?

«Per i prossimi anni stiamo lavorando su tre fronti. Il primo riguarda i professionisti del settore: vogliamo offrire loro spazi di aggiornamento, webinar, momenti di networking, occasioni in cui ci si possa parlare tra colleghi senza filtri commerciali. Sembra poco, ma in un mondo in cui ogni evento sembra finalizzato a vendere qualcosa, avere un luogo dove ci si confronta da pari a pari fa la differenza. Il secondo è il dialogo con le aziende e con la pubblica amministrazione. Abbiamo avviato diversi gruppi di lavoro tematici, dove i nostri soci mettono in comune competenze ed esperienze per produrre cose utili davvero; penso ad esempio a linee guida operative pensate per chi deve affrontare la sicurezza nella pratica di tutti i giorni. L'attenzione, in particolare, è verso quelle organizzazioni che non hanno al loro interno strutture di sicurezza articolate, e che spesso si trovano sole davanti a problemi complessi. Il terzo fronte è la divulgazione. Convegni, webinar, tavoli di lavoro: tutto ciò che serve a far uscire la sicurezza dal cerchio ristretto degli specialisti. La nostra ambizione è essere un riferimento credibile, indipendente e- questo lo sottolineo- non commerciale. Vogliamo poter parlare con la stessa serietà al ciso di una grande azienda e al piccolo imprenditore che gestisce una manciata di dipendenti. Sono mondi diversi, ma le domande di fondo, in fin dei conti, si somigliano molto».

In un contesto caratterizzato da attacchi cyber sempre più sofisticati, quanto è importante investire nella formazione continua dei professionisti della sicurezza informatica?

«È una cosa da cui non si può prescindere. La sicurezza informatica ha questa particolarità, che credo non abbia eguali in altri settori: ciò che si è imparato due anni fa, oggi rischia già di essere superato, almeno in parte. Le tecniche di attacco corrono a una velocità che fatichiamo a immaginare. Basta guardare cosa sta succedendo da quando

l'intelligenza artificiale generativa è diventata uno strumento alla portata di chiunque: campagne di phishing scritte in italiano perfetto, deepfake audio e video che ingannano anche persone preparate, malware che si auto-modificano per evitare i controlli. Cose che fino a poco tempo fa sembravano roba da film. In questo scenario, un professionista che smette di aggiornarsi non è semplicemente meno bravo: diventa, suo malgrado, un fattore di rischio per l'organizzazione in cui lavora. Per questo l'aggiornamento va vissuto come parte naturale del mestiere, non come qualcosa da ritagliare nei momenti liberi. Ed è qui che le associazioni come la nostra possono dare un contributo importante. Non tanto sostituendosi a chi fa formazione di mestiere, quanto creando comunità di pratica: ambienti dove i professionisti si parlano tra loro, raccontano cosa è successo davvero nelle proprie aziende, discutono di soluzioni che hanno funzionato e di altre che invece sono andate male. Spesso si impara molto di più da queste conversazioni che da un corso. Investire sulle persone resta l'investimento con il ritorno più alto in termini di sicurezza reale».

Le piccole e medie imprese italiane rappresentano spesso l'anello più vulnerabile dal punto di vista cyber. Quali consigli darebbe alle Pmi per migliorare la propria resilienza digitale senza affrontare costi insostenibili?

«Vorrei partire da un equivoco da chiarire subito: la sicurezza non è prima di tutto una questione di soldi, è una questione di metodo. Mi è capitato di vedere piccole aziende, con budget davvero modesti, proteggersi meglio di realtà molto più grandi e ben finanziate. Il motivo era semplice: avevano lavorato con ordine, definendo priorità chiare, invece di inseguire l'ultima novità presentata in fiera. Ai piccoli imprenditori darei quattro indicazioni pratiche».

Ovvero?

«La prima è capire cosa si possiede e cosa va davvero protetto. Dati dei clienti, know-how, sistemi gestionali, magari progetti che sono il cuore del valore aziendale. Sembra una banalità, ma molte Pmi questo esercizio non l'hanno mai fatto, e finiscono per difendere tutto allo stesso modo, cioè male. La seconda riguarda quella che chiamerei "igiene digitale". Sono comportamenti di base che, da soli, bloccano la stragrande maggioranza degli attacchi: tenere aggiornati sistemi e applicazioni, attivare l'autenticazione a più fattori dove è possibile, fare backup periodici e, soprattutto verificarli ogni tanto, perché un backup mai testato non è un backup, è una speranza. E poi gestire bene chi può accedere a cosa: non tutti devono poter fare tutto. La terza è formare le persone. In una piccola azienda ogni dipendente, dall'amministrativa al magazziniere, è di fatto un pezzo del sistema di difesa. Se non lo sa, è anche il primo punto debole da cui può entrare un attacco».

IN UNA PICCOLA AZIENDA OGNI DIPENDENTE, DALL'AMMINISTRATIVA AL MAGAZZINIERE, È DI FATTO UN PEZZO DEL SISTEMA DI DIFESA. SE NON LO SA, È ANCHE IL PRIMO PUNTO DEBOLE DA CUI PUÒ ENTRARE UN ATTACCO. PER QUESTO È NECESSARIA LA FORMAZIONE

Infine?

«La quarta è prepararsi a quando qualcosa andrà storto, perché purtroppo prima o poi succederà. Avere un piano minimo di risposta agli incidenti, sapere chi chiamare, dove sono i contatti utili, cosa fare nelle prime ore: la differenza tra un'azienda che reagisce con metodo e una che si fa prendere dal panico è enorme, anche in termini economici. Aggiungo una nota concreta. Oggi esistono strumenti messi a disposizione dall'ACN, l'Agenzia per la Cybersicurezza Nazionale, e da diverse iniziative europee, spesso gratuiti o a costi davvero contenuti. Le Pmi dovrebbero conoscerli meglio e utilizzarli di più. E quando serve un aiuto specifico, il mio consiglio è di rivolgersi a un consulente competente per un intervento mirato, piuttosto che spendere soldi in soluzioni complesse che poi nessuno sarà in grado di gestire davvero».

In futuro quali saranno le principali minacce informatiche emergenti e come dovrà evolversi il ruolo dei professionisti della cybersecurity in Italia?

«Ci sono diversi fronti aperti che mi preoccupano, e che meritano attenzione fin da oggi. Il primo è quello dell'intelligenza artificiale, che è davvero un'arma a doppio taglio. Da una parte ci sta dando strumenti potentissimi per difenderci meglio, dall'altra mette nelle mani degli attaccanti capacità che fino a poco fa erano riservate a pochissimi. Mi riferisco a campagne di phishing personalizzate, costruite su misura sul singolo destinatario; a deepfake che ingannano anche professionisti esperti; a malware che si adatta da solo al sistema che sta attaccando. Poi c'è il tema quantistico, che a molti sembra ancora fantascienza, ma non lo è del tutto. Quando i computer quantistici raggiungeranno una potenza concretamente utilizzabile, una parte importante della crittografia che usiamo oggi smetterà di essere sicura. Le organizzazioni dovrebbero iniziare a ragionarci adesso, perché certe transizioni richiedono anni di lavoro, non si improvvisano in poche settimane. Un terzo fronte critico è quello delle supply chain digitali. Sempre più spesso gli attaccanti non colpiscono direttamente l'obiettivo finale, ma arrivano attraverso un fornitore, un partner tecnologico, un software di terze parti che l'azienda utilizza ogni giorno senza pensarci. È un meccanismo subdolo, perrchè l'attacco entra da un canale che si considerava affidabile. E infine c'è il capitolo delle infrastrutture critiche e dei sistemi industriali. Qui un attacco non si traduce solo in dati rubati: può fermare una linea produttiva, bloccare un servizio essenziale, avere ricadute concrete sulla vita delle persone. Il livello di rischio è di un'altra natura».

Quali sono le sue conclusioni?

«In uno scenario del genere, il mestiere del professionista della cybersecurity sta cambiando in profondità. Le competenze tecniche restano importanti, ovviamente, ma da sole non bastano più. Servono persone che sappiano dialogare con il management, che riescano a tradurre il rischio in termini economici e normativi, che siano capaci di muoversi dentro la complessità crescente di normative come NIS2, Dora, AI Act. Serve insomma più visione d'insieme, più capacità di comunicare, più attitudine a stare in mezzo a discipline diverse. La cybersecurity sta diventando sempre più una professione di frontiera, dove tecnologia, diritto, economia e fattore umano si incontrano. E credo che proprio per questo sia oggi una delle professioni più affascinanti, e più necessarie, per il futuro del nostro Paese».

•**Gaia Santi**


Pineider
FIRENZE 1774
Pineider

Pronti per il bis

Tra intelligenza artificiale, semplificazione amministrativa e competenze digitali:
la visione del direttore generale dell'AgID Mario Nobile nel nuovo mandato che segna la sua conferma fino al 2029

La conferma di Mario Nobile alla guida dell'AgID fino al 2029 segna un passaggio inedito nella storia dell'innovazione pubblica italiana. Per la prima volta, il direttore generale dell'Agenzia viene confermato per un secondo mandato triennale, in un contesto in cui la trasformazione digitale della Pubblica amministrazione diventa sempre più centrale nell'agenda del Paese. Sotto la sua guida, e nel quadro della strategia digitale promossa dal governo con il supporto del sottosegretario all'Innovazione Alessio Butti, la Pa ha iniziato a sperimentare l'intelligenza artificiale come leva per migliorare servizi e processi. Restano però aperte sfide strutturali importanti: dalla complessità burocratica ai tempi ancora lunghi per procedure chiave come l'apertura di un'impresa.

La sua conferma fino al 2029 rappresenta un caso unico nella storia di AgID. Qual è la priorità assoluta del suo secondo mandato per accelerare davvero la trasformazione digitale dell'Italia?

«La priorità indicata dal sottosegretario Alessio Butti è chiara: in questi anni abbiamo realizzato e consolidato importanti infrastrutture come le piattaforme abilitanti (Spid, Cie, PagoPA, l'app Io, Anpr, Psn, Pdnd), la migrazione al cloud e l'interoperabilità tra i sistemi. Adesso bisogna evolvere creando un ecosistema in grado di farle funzionare insieme in modo coerente, assicurando la piena interoperabilità tra le banche dati, accelerando sull'adozione dell'IT Wallet, lavorando sulla qualità del dato come asset strategico e accompagnando le amministrazioni nella governance dell'intelligenza artificiale».

Sotto la sua guida e con la strategia promossa da Alessio Butti, la Pubblica amministrazione ha iniziato a sperimentare l'intelligenza artificiale. In quali ambiti concreti l'Ia può migliorare entro pochi anni la vita quotidiana di cittadini e imprese?

«Il primo e più immediato ambito è quello che riguarda l'assistenza e il supporto ai cittadini e alle imprese, e la semplificazione dei processi amministrativi. Oggi un cittadino- ma anche un'impresa- che vuole accedere a un servizio o completare un adempimento amministrativo si trova spesso di fronte a procedure che richiedono tempi lunghi e conoscenze burocratiche. Sistemi di Ia ben progettati possono fungere da intermediari intelligenti, guidando il cittadino anche in modo proattivo, traducendo il linguaggio burocratico in istruzioni comprensibili, riducendo gli errori nelle domande e quindi i tempi di lavorazione. Questo è già tecnicamente possibile e alcune amministrazioni stanno già sperimentando in questa direzione. Per non parlare della capacità di questi sistemi, ormai consolidata, di parlare tutte le lingue del mondo. Un altro ambito nel quale l'Ia può avere un forte impatto è quello della sanità pubblica: dall'analisi predittiva per la gestione delle liste d'attesa alla lettura assistita di immagini diagnostiche, l'Ia può alleviare il carico di lavoro del personale sanitario e amministrativo, distribuire in modo più efficiente le risorse disponibili e migliorare la tempestività delle diagnosi».

DALL'ANALISI PREDITTIVA PER LA GESTIONE DELLE LISTE D'ATTESA ALLA LETTURA ASSISTITA DI IMMAGINI DIAGNOSTICHE, L'IA PUÒ ALLEVIARE IL CARICO DI LAVORO DEL PERSONALE SANITARIO E AMMINISTRATIVO, DISTRIBUIRE IN MODO PIÙ EFFICIENTE LE RISORSE DISPONIBILI E MIGLIORARE LA TEMPESTIVITÀ DELLE DIAGNOSI

Molti imprenditori lamentano ancora tempi lunghi e procedure burocratiche complesse, ad esempio per l'apertura di una nuova impresa. Quali ostacoli frenano oggi la piena digitalizzazione della Pa e cosa serve per superarli definitivamente?

«Il problema principale è che spesso la digitalizzazione si ferma alla superficie: si è digitalizzato il punto di contatto con il cittadino o l'impresa, senza però mettere in discussione i processi interni alle amministrazioni. In realtà, digitalizzare significa prima di tutto semplificare i processi, eliminando passaggi inutili e riducendo la complessità, non limitarsi a trasferire online procedure pensate per il cartaceo. E questo è ancora più vero se applichiamo le tecnologie emergenti, come la Agentic AI. Il primo ostacolo è, quindi, culturale. Un altro ostacolo è rappresentato dalla frammentazione: l'Italia ha oltre 20.000 enti pubblici, ciascuno con i propri sistemi, i propri processi, spesso i propri applicativi sviluppati negli anni in modo disomogeneo. Raggiungere la piena interoperabilità in questo contesto è un lavoro enorme, che richiede non solo tecnologia ma anche capacità di coordinamento. Infine, c'è un problema di tipo normativo. Ci sono norme che impongono adempimenti ridondanti, vincoli procedurali pensati per un mondo cartaceo che sopravvivono nell'era digitale».

L'Italia ha spesso mostrato eccellenze tecnologiche ma difficoltà nell'esecuzione su larga scala. Come immagina il futuro digitale del Paese nel 2030 e quali risultati misurabili vorrebbe lasciare come eredità del suo mandato?

«I risultati che considero davvero importanti sono la riduzione dei tempi burocratici, la crescita dell'utilizzo dei servizi digitali, una maggiore interoperabilità tra amministrazioni, la diminuzione dei costi amministrativi per le imprese e un aumento delle competenze e della fiducia dei cittadini nei confronti dello Stato digitale. I risultati vanno misurati sui numeri della infrastruttura digitale pubblica, che crescono in maniera evidente: più di 40 milioni di identità digitali, più di 17 milioni di caselle Pec, più di 35 milioni di certificati di firma digitale».

La trasformazione digitale richiede non solo infrastrutture e piattaforme, ma anche competenze. Come può l'Italia colmare il divario digitale nella Pubblica Amministrazione e tra i cittadini, evitando che innovazioni come l'intelligenza artificiale aumentino le disuguaglianze?

«Nessuna trasformazione digitale può funzionare senza persone preparate ad accompagnare il cambiamento. In Italia, solo una persona su due ha competenze digitali di base e il numero di laureati in Ict è ancora troppo basso. L'intelligenza artificiale non aumenterà le disuguaglianze se sapremo costruire un ecosistema in cui tutti abbiano gli strumenti per parteciparvi. Non in modo eguale- non serve trasformare ogni dipendente in un programmatore- ma in modo equo: garantendo a ognuno una base di accesso, di comprensione, di tutela. Su questo abbiamo appena stipulato un accordo con la Crui, la Conferenza dei rettori delle Università italiane, proprio per dispiegare su tutto il territorio nazionale azioni di formazione e addestramento».• **Gloria Martini**

Mario Nobile, direttore generale AgID

Il Gruppo NSG è uno dei più grandi produttori mondiali di vetro e di sistemi di vetro in tre principali aree di business: Edilizia e Architettura, Autoveicoli e Tecnologie Creative. Nel 2006 ha acquisito il principale fornitore mondiale di vetro, Pilkington, e oggi il Gruppo NSG opera a livello globale con presenza commerciale in oltre 100 paesi.

In Italia, lo stabilimento di Venezia produce e fornisce vetro per il settore dell'edilizia, dell'architettura e dell'arredo, come anche altri settori, lo stabilimento di San Salvo (CH) produce prevalentemente vetro per il settore auto e comprende il vetro per il primo equipaggiamento auto (AOE) e i pezzi di ricambio originali (AGR).

Il Gruppo NSG è presente anche a Settimo Torinese (TO), con uno stabilimento di terze lavorazioni del settore auto, e a Melfi (PZ), con una cava di sabbia silicea.

PILKINGTON

NSG
GROUP


Un piccolo passo, una grande differenza
Pilkington **Mirai Øne**™
Da oggi è disponibile Pilkington **Mirai Øne**™: il nuovo vetro float a ridotta impronta di carbonio.
Prodotto in Italia, abbatte le emissioni lungo il suo ciclo di vita di oltre il 30% rispetto al nostro vetro standard*.
Un ulteriore passo verso una sostenibilità più accessibile, concreta e locale.
* Il valore del GWP deriva da calcoli interni, l'EPD è in preparazione.
PILKINGTON
NSG
GROUP

A Bologna si va sul sicuro

Le nuove tecnologie, simulazioni di rischio e le esperienze più virtuose di wellbeing corporate. Saranno in vetrina dal 26 al 28 maggio ad Ambiente Lavoro, fiera regina per gli operatori della sicurezza nei luoghi professionali

La salute e la sicurezza prima di tutto. È il messaggio ispirato alla costruzione di una cultura collettiva sulla prevenzione che intende rilanciare con forza Ambiente Lavoro, salone d'eccellenza per prodotti e servizi volti a minimizzare i rischi di incidenti e malattie professionali che tornerà in passerella a BolognaFiere dal prossimo 26 maggio fino al 28. Tre giornate che riuniranno all'ombra delle Due Torri operatori e aziende attive nel mondo della sicurezza, dell'ambiente, delle risorse umane e della sostenibilità, presentando le nuove tecnologie e le best practice per promuovere la salute professionale a 360 gradi- equilibrio psicologico e benessere organizzativo inclusi- e per aggiornarsi vicendevolmente sugli ultimi indirizzi normativi in materia.

DPI, IN MOSTRA LE GAMME PIÙ INNOVATIVE SUL MERCATO

In un collaudato scacchiere espositivo che anche nella passata edizione ha incassato il pollice alto di oltre 8 mila visitatori, in primo piano si confermerà Sicur Labor, il salone dedicato ai Dpi e all'abbigliamento professionale. Un'area espositiva che raccoglie le gamme più innovative del mercato, spaziando dalla protezione delle vie respiratorie ai sistemi anticaduta, fino alle nuove soluzioni per il benessere del piede. Uno sguardo speciale sarà rivolto agli aggiornamenti normativi Uni e al loro impatto sull'adozione e sull'utilizzo degli Apvr. Sicur Labor ospiterà inoltre iniziative dedicate alle nuove tendenze del workwear, valorizzandone sia la funzionalità sia l'estetica. Tanto da svelarne persino la dimensione spettacolare nell'ambito della DPI Fashion Week, in cui scarpe, tute, guanti, caschi e molto altro si prenderanno il palcoscenico grazie a sessioni di break dance, improvvisazione teatrale e Rock 'n' Roll acrobatico. Di grande interesse in termini di formazione pratica si preannuncia poi il Campo Prove allestito presso il padiglione 22, dove le aziende potranno mettere in funzione i propri prodotti inserendoli in una simulazione di rischio. Con un'area dedicata alla verifica e debriefing che affiancherà due zone dimostrative: una riservata alla "Movimentazione & Sicurezza Antitaglio", che includerà sistemi anticollisione, sensori intelligenti e dispositivi di assistenza per carrelli elevatori; l'altra ai "Lavori in Quota & Barriere di Sicurezza", che proporrà tra le altre cose simulazioni realistiche dedicate agli spazi confinati e alle procedure di primo soccorso, con stuntman professionisti e tecnici specializzati che metteranno in scena cadute dall'alto e casistiche di sovraccarico biomeccanico.

NELLA PRIMA EDIZIONE DEGLI OSCAR DELLA SICUREZZA VERRANNO PREMIATE ESPERIENZE DI SUCCESSO IN FATTO DI PREVENZIONE DI INCIDENTI E MALATTIE PROFESSIONALI, POLITICHE AMBIENTALI E ESG

DEBUTTA NEXT, LABORATORIO DI IDEE PER IL MONDO HSE

Sempre di stampo formativo saranno le iniziative messe a punto in partnership con Inail, Aias, fino al Ministero del Lavoro, mentre alla condivisione di buone pratiche si ispirerà il ciclo di workshop Safety Sensei, destinato alle migliori case history di grandi aziende in fatto di tematiche emergenti. Quest'anno, a finire sotto i riflettori saranno le novità per i datori di lavoro e i rischi derivanti dalle differenze di genere e generazionali, posti in risalto da Rspp e Hse manager di grandi realtà industriali che racconteranno le loro esperienze evidenziandone punti deboli e risvolti positivi. Sulla scia del gradimento riscosso nelle passate edizioni, ad Ambiente Lavoro si rinnoverà l'appuntamento con i percorsi di wellbeing corporate, un approccio strategico alla gestione delle risorse umane che mira a promuovere la salute e il benessere dei dipendenti in ufficio o in fabbrica. In questo senso, la Wellbeing Arena allestita nel quartiere fieristico di Bologna sarà il luogo prediletto in cui concedersi una pausa tra le molte attività proposte nelle 72 ore di palinsesto, approfondendo come si può migliorare il clima e il benessere aziendale. Per rafforzare il proprio ruolo di "place to be" culturale oltre che commerciale, quest'anno Ambiente Lavoro lancerà anche Next, il laboratorio di idee che costituirà il think tank della manifestazione. Una piattaforma di elaborazione permanente che coinvolgerà alcune tra le più autorevoli realtà associative e professionali del settore, con affondi sui temi oggi più rilevanti per il mondo Hse. Dal ruolo strategico del facility management nella gestione integrata degli ambienti di lavoro, focus di apertura della prima giornata, alla partecipazione attiva delle persone nei processi di prevenzione di cui si parlerà nell'ultimo incontro organizzato in collaborazione con Hse Excellence Sharing Team. Ancora sotto il cappello di Next, infine, annunciati altri due debutti importanti: Next Safety connection, format relazionale ideato per favorire lo scambio di competenze tra direzioni aziendali e professionisti Hse; la prima edizione degli Oscar della Sicurezza, che premieranno esperienze di successo in fatto di prevenzione di incidenti e malattie professionali, politiche ambientali e Esg. •**Gaetano Gemiti**

DOUBLE YOUR PERFORMANCE

PIQUADRO

GAGGIO MONTANO, ITALY
44°11'14.04"N 10°59'47.58"E

Un piano d'azione concreto

Dalla legge 198/2025, che premia le aziende virtuose, al ruolo della formazione, dei dati e dell'Ia, la strategia per rafforzare la cultura della sicurezza. L'analisi del presidente Inail Fabrizio D'Ascenzo

Il 28 aprile si è svolta la Giornata mondiale per la sicurezza e la salute sul lavoro. Un tema su cui l'Italia cerca una svolta, dopo anni di cronicizzazione del fenomeno. Per i primi tre mesi del 2026, calano le morti bianche, ma aumentano gli infortuni (le denunce nel 2025 sono state 416.900) e le malattie professionali. Entriamo nel dettaglio con il presidente dell'Inail, Fabrizio D'Ascenzo.

Presidente, dove risiedono oggi le maggiori criticità del sistema italiano della prevenzione? La nuova Legge 198/2025 può contribuire positivamente?

«Il quadro normativo italiano in materia di salute e sicurezza sul lavoro è tra i più avanzati in ambito europeo. Ma questo purtroppo non basta. Permangono settori di attività- costruzioni, logistica, trasporto- che continuano a registrare un'elevata incidenza infortunistica, confermando la necessità di rafforzare ulteriormente le azioni di prevenzione per incidere sui contesti produttivi più esposti al rischio. Il provvedimento adottato a fine 2025, a cui l'Istituto ha lavorato attivamente per definirne i contenuti in sinergia con il ministero del Lavoro, ha riconosciuto all'Inail un ruolo determinante per contrastare gli infortuni sul lavoro, rafforzandone così la missione sociale. Era dal 2008 che mancavano passaggi legislativi così significativi sul tema della sicurezza».

Può evidenziare le novità più significative?

«Mi riferisco a temi emergenti come i near miss, l'importanza delle campagne formative e informative e la consultazione gratuita di alcune norme UNI rilevanti in materia di salute e sicurezza sul lavoro. In particolare, la nuova normativa si fonda su una logica premiale, che punta a incentivare le imprese virtuose attraverso il potenziamento del bonus per andamento infortunistico favorevole, con aliquote di riduzione del premio assicurativo. Inoltre, l'Inail, con l'oscillazione del tasso medio di tariffa per prevenzione, premia le aziende che eseguono interventi per il miglioramento delle condizioni di salute e sicurezza nei luoghi di lavoro ulteriori rispetto a quelli previsti dalla vigente normativa. La legge prevede, inoltre, la copertura assicurativa in itinere per gli studenti impegnati nei percorsi di formazione scuola-lavoro».

Quanto è importante rendere accessibile la formazione al più ampio numero di imprese possibile?

«La formazione è un pilastro centrale della strategia di prevenzione adottata dall'Istituto. Renderla accessibile al maggior numero di imprese, soprattutto alle Pmi, che rappresentano un segmento molto rilevante del tessuto produttivo italiano, è di fondamentale importanza. Con l'addendum all'accordo del 2023 tra l'Inail e la Conferenza delle Regioni e delle Province autonome, sottoscritto a dicembre 2025, si estende a tutto il 2026 l'opportunità per le imprese di accedere alla formazione finanziata in materia di salute e sicurezza attraverso i programmi formativi resi disponibili dalle Regioni e sostenuti dall'Istituto con oltre 10 milioni di euro».

La formazione è al centro anche dell'Accordo sottoscritto il 5 maggio scorso con Federmanager.

«Questa intesa nasce dalla convinzione che il management industriale possa contribuire alla diffusione della cultura della prevenzione, trasferendola lungo tutta la filiera produttiva e trasformandola in azioni concrete. Una leva che può fare la differenza nelle realtà più piccole, dove spesso mancano strutture dedicate e competenze specialistiche per tradurre gli obblighi normativi in pratiche efficaci».

Ha definito l'intelligenza artificiale un "alleato strategico" dell'Inail. In quali ambiti nello specifico?

«L'Ia è uno strumento prezioso in chiave prevenzionale, ma anche per lo sviluppo di protesi e strumenti riabilitativi; un ambito nel quale Inail collabora con enti di primo piano nel mondo scientifico e accademico. Sul fronte della prevenzione, sono stati avviati progetti per l'adozione di sistemi cognitivi per l'analisi dei dati relativi agli infortuni mortali, i "quasi incidenti" e gli infortuni su strada. L'Ia è stata trasversalmente integrata in tutte le linee di ricerca Inail: dispositivi di protezione individuale smart che integrano sensori e sistemi di controllo in Dpi tradizionali; oppure abiti intelligenti sensorizzati, realizzati con tessuti ingegnerizzati per monitorare sia i fattori ambientali, sia i parametri fisiologici del lavoratore. L'Ia può intervenire in alcune problematiche legate all'organizzazione del lavoro, rendendo le informazioni più accessibili e comprensibili. L'Inail sta sperimentando strumenti di comunicazione multilingua, anche attraverso scenari immersivi e avatar virtuali. Sul fronte dell'ambito protesico e riabilitativo, infine, numerose sono le applicazioni per rendere i movimenti delle persone con disabilità più intuitivi, naturali e personalizzati».

In base al Piano triennale della Prevenzione Inail 2025-2027, quali linee di intervento prioritario identifica?

«La Relazione annuale 2024 dell'Inail si chiudeva con una sfida per il futuro: contribuire alla definizione di una strategia nazionale di prevenzione e protezione, accompagnata da un piano d'azione concreto, basato su un approccio sistematico e a rete. In questa direzione, grazie alla fattiva collaborazione con il governo, sono stati compiuti importanti passi in avanti anche attraverso la Strategia nazionale in materia di salute e sicurezza nei luoghi di lavoro 2026-2030 e la legge 198/2025. Con un metodo di lavoro partecipato, l'Istituto intende rafforzare ulteriormente la cultura della sicurezza, sostenendo lavoratori e imprese e investendo nell'innovazione tecnologica e nell'analisi dei dati. Tra gli obiettivi prioritari, rientra il miglioramento delle condizioni di salute e sicurezza in un mondo caratterizzato da rischi nuovi ed emergenti, senza trascurare l'azione di mitigazione dei rischi tradizionalmente noti. In questa prospettiva, la circolarità tra ricerca e prevenzione, fondata su dati ed evidenze, potrà contribuire al miglioramento della qualità della vita dei lavoratori, con riflessi positivi in termini di sostenibilità».

•Francesca Druidi

LA FORMAZIONE È UN PILASTRO CENTRALE DELLA STRATEGIA DI PREVENZIONE ADOTTATA DALL'ISTITUTO. RENDERLA ACCESSIBILE AL MAGGIOR NUMERO DI IMPRESE, SOPRATTUTTO ALLE PMI, CHE RAPPRESENTANO UN SEGMENTO MOLTO RILEVANTE DEL TESSUTO PRODUTTIVO ITALIANO, È DI FONDAMENTALE IMPORTANZA

Fabrizio D'Ascenzo, presidente Inail

UN MONDO DI LUCE BEGHELLI

Illuminare razionalmente, limitando gli sprechi di energia

Un Mondo di Luce è il progetto Beghelli che prevede la **sostituzione "a costo zero" degli impianti di illuminazione presenti negli edifici con apparecchi di nuova generazione ad altissima efficienza**. Una soluzione "chiavi in mano" e "a costo zero" grazie al **risparmio energetico ottenuto, garantito contrattualmente**, con possibilità di ottenimento anche dei **Certificati Bianchi** e accesso agli **incentivi** legati al piano di **Transizione 5.0**.

Ad oggi sono stati realizzati oltre **6.750 impianti**, con **1.290.000 apparecchi installati**.

L'**efficientamento energetico** Beghelli è il risultato della combinazione di più variabili: sistemi di illuminazione con tecnologia elettronica all'avanguardia, fotosensori per compensazione con la luce naturale, comfort visivo, rilevazione presenza di persone, programmazione e gestione da remoto degli impianti.

Per industria, logistica, retail, GD, centri commerciali, uffici, ospedali, scuole, parcheggi e aree esterne.

- AUDIT ENERGETICO
- CALCOLO ILLUMINOTECNICO
- ANALISI COSTI-BENEFICI
- INSTALLAZIONE SENZA PENSIERI
- RISPARMIO ENERGETICO GARANTITO
- MANUTENZIONE INCLUSA

beghelli.it | numero verde **800 626 626**

Beghelli
IDEE PIENE DI VITA

Futuro in corso.

**Da oltre 140 anni,
siamo impegnati per il progresso
e la sicurezza energetica del Paese.
Anche adesso, anche qui.**

Puntiamo su fonti rinnovabili e tecnologie innovative
per garantire un sistema energetico stabile
e affidabile, al servizio delle generazioni future.

Impianto eolico Edison, provincia di Foggia.

EDISON | Diventiamo l’energia che cambia tutto.

Organizzazione e responsabilità

Le morti sul lavoro non sono frutto di mancanze individuali: «serve una cultura della sicurezza sostanziale, non solo burocratica». L'avvocato Rolando Dubini analizza riforme, criticità e prospettive della prevenzione

È ormai trascorso un anno dall'entrata in vigore dell'Accordo Stato-Regioni sulla formazione in materia di salute e sicurezza sul lavoro. Facciamo il punto con Rolando Dubini, avvocato penalista, cassazionista, docente e formatore esperto in queste materie, sulle principali novità legislative e sui nodi strutturali ancora da affrontare. «L'Accordo, pubblicato in Gazzetta Ufficiale il 24 maggio 2025, conclude il periodo transitorio il 24 maggio 2026. Da tale data, i corsi dovranno essere integralmente conformi alle nuove regole. Per i corsi avviati prima, secondo i previgenti Accordi, vale il principio tempus regit actum».

Quali sono gli elementi più innovativi introdotti dall'Accordo Stato-Regioni? E quali profili di criticità invece riscontra?

«Sono quattro le innovazioni principali. Innanzitutto, l'obbligo formativo per il datore di lavoro (16 ore), che colma un vuoto rilevante: prima del 2025, il datore non Rspp (Responsabile servizio prevenzione e protezione) non aveva un percorso definito, mentre ora deve acquisire "competenze organizzative, gestionali e giuridiche", superando "una visione formale della materia a favore di una visione sostanziale". Poi la verifica obbligatoria dell'apprendimento contest, colloqui e prove pratiche: non basta più la mera frequenza. Quindi la verifica di efficacia durante la prestazione lavorativa, con analisi infortunistica, questionari e check list, da riportare nella riunione periodica. Infine, il rafforzamento dei contenuti pratici: rapporto docente/discente massimo 1:6 e metodologie didattiche attive obbligatorie (lavori di gruppo, casi di studio, simulazioni, realtà virtuale). La criticità riguarda l'entrata in vigore: l'Accordo la fissa alla pubblicazione in G.U. (24 maggio), ma il Ministero ha diffuso indicazioni che la ancorano al 19 maggio. Cinque giorni di scarto possono incidere su scadenze e validità di atti, generando incertezza applicativa».

Rolando Dubini, avvocato penalista e cassazionista

Come valuta le novità della L. 198/2025 su formazione, tracciabilità e near miss, ossia mancati infortuni?

«La L. 198/2025 prosegue il rafforzamento avviato dalla L. 215/2021. Sul fronte tracciabilità, accelera il fascicolo elettronico ex art. 14D.Lgs. 150/2015, già richiamato dall'art. 37 comma 14 D.Lgs. 81/2008: gli organi di vigilanza verificano in tempo reale gli adempimenti formativi. La Cassazione (sentenza 16865/2024) ha chiarito che la formazione deve precedere l'adibizione alle mansioni e non può essere surrogata dal "Travaso di conoscenza tra lavoratori". Quando sarà operativa la tracciabilità digitale, renderà questo principio finalmente verificabile in modo oggettivo, impedendo regolarizzazioni retroattive. Sul near miss, la legge introduce un obbligo strutturato di rilevazione e analisi, sistematizzando quanto l'Accordo Stato Regioni 2025 già prevede includendo i "mancati infortuni" tra gli indicatori dell'analisi infortunistica aziendale. L'approccio è corretto: il near miss è il più potente predittore dell'infortunio. Resta il nodo culturale: se le segnalazioni non si traducono in azioni correttive, il sistema è inefficace. Serve una cultura organizzativa che valorizzi chi segnala».

Come si integrano D.Lgs. 81/2008 (Testo Unico Sicurezza sul lavoro) e la?

L'INTELLIGENZA ARTIFICIALE OFFRE GRANDI OPPORTUNITÀ: ANALISI PREDITTIVA DEI RISCHI INCROCIANDO DATI SU INFORTUNI E NEAR MISS; MONITORAGGIO REAL-TIME CON SENSORI IOT E ALERT AUTOMATICI; FORMAZIONE IMMERSIVA CON REALTÀ VIRTUALE, SENZA ESPOSIZIONE A RISCHI REALI; ASSISTENZA AI PREPOSTI NELLA VIGILANZA TRAMITE COMPUTER VISION

Quali sono i rischi e le opportunità nell'applicare questa tecnologia alla sicurezza sul lavoro?

«L'integrazione è governata dal Regolamento Ue 2024/1689 (Ai Act), che classifica ad alto rischio i sistemi di monitoraggio dei lavoratori, e dalla L.132/2025, che impone all'la di essere "sicura, affidabile, trasparente" e vieta che operi "in contrasto con la dignità umana". L'la offre grandi opportunità: analisi predittiva dei rischi incrociando dati su infortuni e near miss; monitoraggio real-time con sensori IoT e alert automatici; formazione immersiva con realtà virtuale, senza esposizione a rischi reali; assistenza ai preposti nella vigilanza tramite computer vision. Ma la posizione di garanzia è del datore (Cass. pen. 4361/2015: "è costituito garante dell'incolumità fisica dei prestatori di lavoro") e non è delegabile a un algoritmo. Chi si affida ciecamente all'la senza verificarne l'affidabilità risponde penalmente. Inoltre, sistemi di videosorveglianza pervasiva violano l'art. 4 dello Statuto Lavoratori se installati senza accordo sindacale o autorizzazione INL: la Cassazione (sent. 38882/2018) ha affermato che "il consenso del lavoratore, in qualsiasi forma prestato, non vale a scriminare la condotta del datore di lavoro". Serve dunque un bilanciamento: l'la è lecita se trasparente, proporzionata e accompagnata da supervisione umana».

Ha scritto che le morti bianche non sono frutto di disattenzioni individuali, sono conseguenza di disorganizzazione aziendale e di omissioni negli obblighi di legge. Quali restano le fragilità della cultura della sicurezza e della prevenzione nel nostro Paese?

«Le fragilità persistono. La sicurezza è ancora percepita come costo e non come investimento. Troppe aziende si fermano alla compliance cartolare: il Dvr (Documento Valutazione rischi) formalmente completo ma inattuato; formazione erogata ma non verificata; preposti nominati ma senza effettivi poteri di intervento. Le Pmi spesso non dispongono delle risorse per implementare sistemi di gestione adeguati e di segnalazione: in troppi contesti chi identifica un pericolo è percepito come elemento problematico».

In quale direzione attuare il necessario cambio di passo?

«Serve il passaggio dalla compliance formale a quella sostanziale, con controlli ispettivi che accertino l'effettività e non solo l'esistenza dei documenti; l'integrazione tra sicurezza e organizzazione aziendale; la promozione di una cultura della prevenzione che parta dalla formazione scolastica e accompagni il lavoratore per tutta la vita lavorativa, interiorizzando la sicurezza come valore e non come vincolo. La Cassazione (sent. 2084/2024) ha affermato che la tutela del lavoratore "non ammette sconti in ragione di fattori quali ineluttabilità, fatalità, fattibilità economica e produttiva". Le scelte organizzative devono essere valutate per il loro impatto prevenzionale» • **Francesca Druidi**

Una fase di estremo dinamismo

Grazie a tecnologie più avanzate e una spinta sul piano normativo verso una maggior resilienza aziendale, l'industria della sicurezza fisica e informatica degli edifici allunga la scia della crescita. Il punto di Andrea Monteleone

Con tassi di crescita che superano puntualmente il 10 per cento annuo, già da qualche tempo il mercato fire&security sta vivendo una fase di estremo dinamismo. Registrando un andamento che si può definire anticiclico rispetto alla situazione geopolitica attuale, e decisamente più maturo in termini di cultura aziendale. Specie alla luce dell'introduzione a livello europeo delle nuove normative NIS2, CER e CRA, che per la prima volta puntano a uniformare le regole e rafforzare la resilienza e la sicurezza informatica nei Paesi della Ue. «In questo scenario- sottolinea Andrea Monteleone, presidente di Anie Sicurezza- i settori dell'antincendio e della videosorveglianza risultano i più brillanti in termini di fatturato, grazie a dinamiche che si possono definire strutturali».

In virtù di quali fattori si stanno segnalando come locomotive dell'industria italiana della fire&security?

«Nel caso del fire, la crescita è determinata dall'evoluzione normativa e dalla ricerca sempre più spinta di soluzioni integrate e ad alta affidabilità; per quanto concerne invece la videosorveglianza, il trend positivo è legato alla transizione in atto da un approccio basato sulla "sicurezza" a quello basato sulla "resilienza", frutto anche qui di un nuovo assetto normativo».

Quali dispositivi dominano il panorama della videosorveglianza e in quali ambiti applicativi prevalenti?

«Il termine videosorveglianza, per certi versi, è diventato obsoleto per descrivere un mercato dove sensori termici, ottici, radar, sistemi di analisi automatici, metadati, intelligenza artificiale e computer vision concorrono a comporre sistemi sempre più pervasivi, evoluti e flessibili. Non mi soffermerei quindi su di uno specifico dispositivo, quanto piuttosto sul fatto che tecnologie più o meno consolidate vengano utilizzate con modalità, finalità e in ambiti differenti rispetto a quanto fatto finora con l'approccio di tipo tradizionale».

I SETTORI DELL'ANTINCENDIO E DELLA VIDEOSORVEGLIANZA RISULTANO I PIÙ BRILLANTI IN TERMINI DI FATTURATO, GRAZIE A DINAMICHE CHE SI POSSONO DEFINIRE STRUTTURALI

La direttiva europea NIS2 sta ridisegnando in modo radicale l'approccio con cui le imprese italiane devono fare e garantire la cybersecurity. Quali sono i nuovi comportamenti che prescrive?

«La NIS2 è uno dei tasselli fondamentali di un quadro normativo molto più ampio e articolato che la Comunità Europea ha introdotto per affrontare in modo coerente e coordinato la complessità all'interno della quale, volenti o nolenti, operiamo. L'approccio della NIS2 è di tipo risk-based e non si limita a definire una serie di prescrizioni tecniche minime da soddisfare, ma impone alle aziende una ridefinizione dei modelli di gestione interna, dell'assegnazione delle responsabilità, della formazione del personale e della scelta e gestione dei fornitori. Inoltre- e questo è un tema molto importante- impone tempi rapidi per la comunicazione di eventuali incidenti informatici alle Autorità preposte, in un'ottica di consapevolezza diffusa e massima collaborazione all'interno del "sistema Paese"».

In una cornice regolatoria così mutevole, la formazione dei professionisti è la chiave di volta per rimanere sulla cresta. Quali sono i principali focus tematici dei vostri attuali percorsi formativi?

«La formazione è diventata, se possibile, ancora più essenziale proprio in virtù della complessità richiamata in precedenza e di un contesto normativo sempre più articolato. Il nostro focus è indirizzato alla qualifica dei Tecnici Manutentori in ambito IRAI ed EVAC, alla formazione su CEI 79-3:2025 e DM 37/08 per il mondo dell'antintrusione così come alla divulgazione sulla corretta implementazione della UNI 11988:2025 per i sistemi di allarme vocale per scopi di emergenza. E questa è solo una parte delle attività, perché ci sono molti altri temi che richiedono approfondimenti sempre più mirati, sviluppati ed erogati secondo criteri di eccellenza».

Nel campo della protezione delle infrastrutture critiche, che sviluppi si prevedono in termini di convergenza tra sicurezza fisica e digitale?

«Qui il tema meriterebbe una trattazione a parte, data la sua ampiezza. Il concetto di convergenza tra sicurezza fisica e digitale si traduce, in concreto, nell'applicazione di due Direttive europee e dei relativi atti di recepimento nazionali: la NIS2, già citata, per la parte cyber e la meno nota, ma altrettanto rilevante, CER (Critical Entities Resilience Act), da non confondere con le comunità energetiche rinnovabili».

A quali traiettorie evolutive devono prepararsi le imprese?

«La traiettoria che si delinea è quella che porta a governare con consapevolezza i due contesti, mettendo a fattor comune tutte le professionalità disponibili, sia da parte delle entità critiche che da parte di tutte le loro filiere di fornitura, in uno sforzo congiunto e coordinato. Idea all'apparenza utopica, ma ai più attenti non sarà sfuggito che è proprio questo l'obiettivo fissato nei due testi normativi». •**Gaetano Gemiti**

Andrea Monteleone, presidente di Anie Sicurezza

DIGITAL ENTERPRISE

Accelera la tua trasformazione digitale

Diventa una vera Digital Enterprise, combinando perfettamente il mondo reale e quello digitale.

Raccogliere, comprendere e utilizzare l'enorme quantità di dati creati nell'Industrial Internet of Things (IIoT) è essenziale per diventare un'impresa ancora più sostenibile ed efficiente. La convergenza IT/OT offre la trasparenza necessaria - dal livello più alto al livello di campo - per un processo decisionale basato sull'analisi dei dati. L'integrazione di IT e software nell'automazione sta aprendo la strada per una produzione adattiva che abilita una maggiore flessibilità.

Con Siemens Xcelerator e con Industrial AI ti aiutiamo ad accelerare la tua trasformazione digitale e a diventare una vera Digital Enterprise!

siemens.it/digital-enterprise

SIEMENS

Una svolta necessaria

Vigilare sull'Accordo Stato-Regioni in materia di formazione. Rafforzare il coordinamento nazionale sulla prevenzione e creare uno standard europeo di sicurezza. Le priorità di AIAS indicate dal presidente Francesco Santi

AIAS (Associazione Italiana Ambiente e Sicurezza) è la prima e più importante associazione tecnico-scientifica costituita da professionisti della sicurezza, che nel 2025 ha festeggiato i suoi primi 50 anni e prosegue oggi la sua opera di valorizzazione delle competenze tecniche-professionali. In occasione della fiera Ambiente Lavoro di Bologna, «oltre agli eventi realizzati con i nostri partner su temi come l'Ai applicata alla sicurezza, Vision Zero e il nuovo quadro normativo, l'iniziativa di punta sarà il lancio del Comitato Nazionale di Controllo sull'applicazione dell'Accordo Stato-Regioni», anticipa il presidente Francesco Santi. «Vogliamo che sia un organismo indipendente promosso da AIAS per monitorare le Regioni nel recepimento della riforma della formazione obbligatoria, offrendo supporto tecnico-scientifico agli enti e garantendo che i contenuti innovativi dell'accordo non vengano dispersi nella frammentazione locale».

Tra le battaglie storiche di AIAS, ci sono l'approccio qualitativo alla formazione e la cultura della sicurezza nelle scuole dell'obbligo. Su quali obiettivi si concentra la vostra azione nel prossimo futuro?

«Le nostre priorità si sviluppano su tre assi. Il primo è rafforzare il ruolo di raccordo tra il mondo reale- cantieri, fabbriche, uffici- e le istituzioni, a livello sia regionale che nazionale. AIAS è nata cinquant'anni fa per dare voce tecnica a chi lavora ogni giorno sulla prevenzione, e questa missione è oggi più urgente che mai. Continueremo a organizzare eventi fisici e online per confrontarci su tutti i temi rilevanti. Il secondo asse è promuovere in Italia Vision Zero, la strategia internazionale ora adottata in Europa e in Italia per i prossimi tre anni: lavoriamo perché diventi cultura diffusa tra imprese, lavoratori e istituzioni. Il terzo asse riguarda il recepimento regionale dell'Accordo Stato-Regioni sulla formazione obbligatoria: dobbiamo monitorare le applicazioni regionali. La prima Regione ha legiferato e ha prodotto un testo che rischia di ridurre la formazione a mero adempimento documentale, vanificando le innovazioni dell'accordo. Se le venti Regioni procedessero ciascuna per conto proprio, ne deriverebbero uno spreco enorme di risorse pubbliche e costi insostenibili per le imprese. In questo momento storico, gli italiani non se lo meritano».

Francesco Santi, presidente AIAS

Lei presiede non solo AIAS, ma anche la Federazione delle Associazioni ENSHPO. Uno degli obiettivi è portare il Decalogo per la sicurezza, la Carta di Urbino, in Europa. Quali sfide individua a livello europeo?

«ENSHPO riunisce le associazioni professionali di sicurezza e salute sul lavoro di 17 paesi europei, rappresentando circa 50mila professionisti Hse (salute, sicurezza e ambiente). La sfida più grande è culturale prima ancora che normativa: convincere i Paesi membri che la standardizzazione non è una minaccia alle identità nazionali, ma un'opportunità per valorizzare il meglio di ogni esperienza. Purtroppo, ad esempio, i fenomeni sono già standardizzati: il plateau della prevenzione è, infatti, comune a tutti i paesi europei, così come la difficoltà con la prevenzione nelle Pmi. La Carta di Urbino è già un punto di riferimento riconosciuto in tutta Europa, così come l'approccio Vision Zero. Lavorare per la prevenzione in Europa significa lavorare per profili professionali riconosciuti in tutto il continente, percorsi formativi equivalenti e una raccolta dati armonizzata che consenta confronti affidabili tra paesi. Dobbiamo avere il coraggio di abbandonare i localismi e costruire uno standard europeo che unisca le migliori pratiche dei nostri Paesi. La direzione è quella giusta».

LA TECNOLOGIA OFFRE OPPORTUNITÀ STRAORDINARIE: DAI SISTEMI DI RILEVAMENTO PRECOCE DEI RISCHI FISICI E CHIMICI, AGLI ESOSCHELETRI CHE PROTEGGONO LA SCHIENA DEGLI OPERAI, AI SISTEMI DI RILEVAMENTO DI COMPORTAMENTI ERRATI, AGLI ALGORITMI CHE ANALIZZANO I DATI STORICI DEGLI INFORTUNI PER IDENTIFICARE PATTERN E PREVENIRLI

Per arginare morti e feriti sul lavoro ha indicato la necessità di sviluppare un coordinamento nazionale forte, basato su controlli uniformi ed efficaci, formazione standardizzata e raccolta dati integrata. Vede dei passi in avanti verso questa direzione?

«Dopo un anno, le direttrici restano le stesse. Sul fronte dei controlli: abbiamo in Italia decine di enti preposti alla vigilanza con risorse frammentate. Se in Italia ogni giorno muoiono mediamente due persone sul lavoro- una strage silenziosa- è anche perché i controlli non sono né sistematici né preventivi. Se questo fenomeno avesse le caratteristiche della lotta nazionale come fu per il terrorismo, avremmo già un coordinamento centrale. Serve un'agenzia nazionale che unifichi la vigilanza. Sulla formazione, il rischio concreto è che l'applicazione disomogenea dell'Accordo Stato-Regioni faccia sopravvivere gli "attestatifici"- chi rilascia certificazioni senza reale valore formativo- e mantenga viva la percezione della formazione come adempimento inutile, sprecando ingenti risorse. Sul fronte dei dati, qualche passo avanti c'è stato: oggi l'Inail dialoga con l'Inps. Ma bisogna accelerare nella costruzione di un completo sistema informativo nazionale integrato per la prevenzione. L'Inail potrebbe e dovrebbe essere il soggetto guida di questo percorso».

Quali sono i rischi e le opportunità che derivano dalle nuove tecnologie come l'intelligenza artificiale?

«L'intelligenza artificiale e le tecnologie connesse- IoT, wearable, sensori intelligenti- rappresentano una svolta epocale per la sicurezza sul lavoro. I rischi esistono, ma sono legati a un uso distorto: quando la tecnologia è impiegata unicamente per il controllo o la riduzione dei costi, a scapito della centralità e del rispetto delle persone. Le opportunità, invece, sono straordinarie. Penso ai sistemi di rilevamento precoce dei rischi fisici e chimici, agli esoscheletri che proteggono la schiena degli operai, ai sistemi di rilevamento di comportamenti errati, agli algoritmi che analizzano i dati storici degli infortuni per identificare pattern e prevenirli. L'Ai ben governata può trasformare la prevenzione da adempimento burocratico a sistema intelligente di tutela reale delle persone».

• **Francesca Druidi**

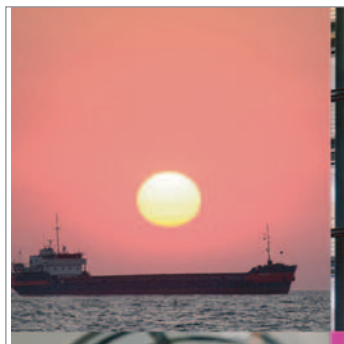
SUZUKI

S-CROSS HYBRID
NEXT LEVEL SUV

TUTTO DI SERIE, **SENZA SORPRESE.**

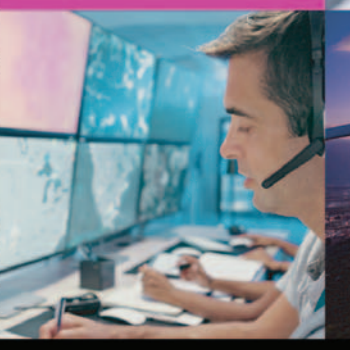
Suzuki S-CROSS Hybrid consumo ciclo combinato: da 5,4 a 6,1 l/100km (WLTP). Emissioni di CO_2: da 121 a 141 g/km. Tutti i dettagli sui vantaggi e le promozioni applicabili ai singoli modelli e la loro disponibilità sono disponibili presso le Concessionarie o sul sito suzuki.it. Le immagini delle vetture sono puramente indicative.

HYBRID ALLGRIP SUZUKI connect 3 PLUS SUZUKI Numero Verde 800-452625 SUZUKI finance MOTUL



NETWORK PROTECTION

EXPOSURE MANAGEMENT

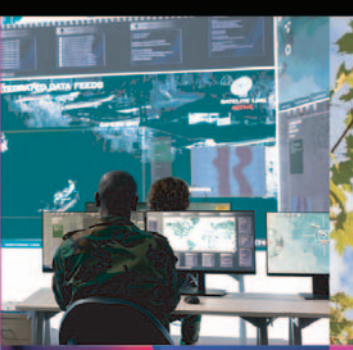


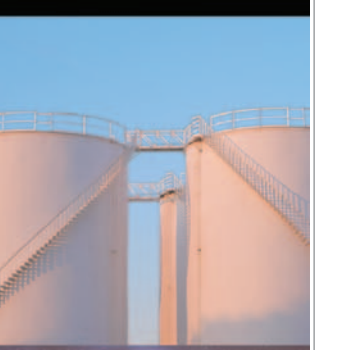
CLAROTY

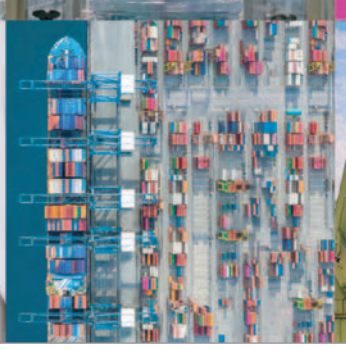
Life, uninterrupted.

Secure your mission-critical infrastructure.

SECURE ACCESS







THREAT DETECTION