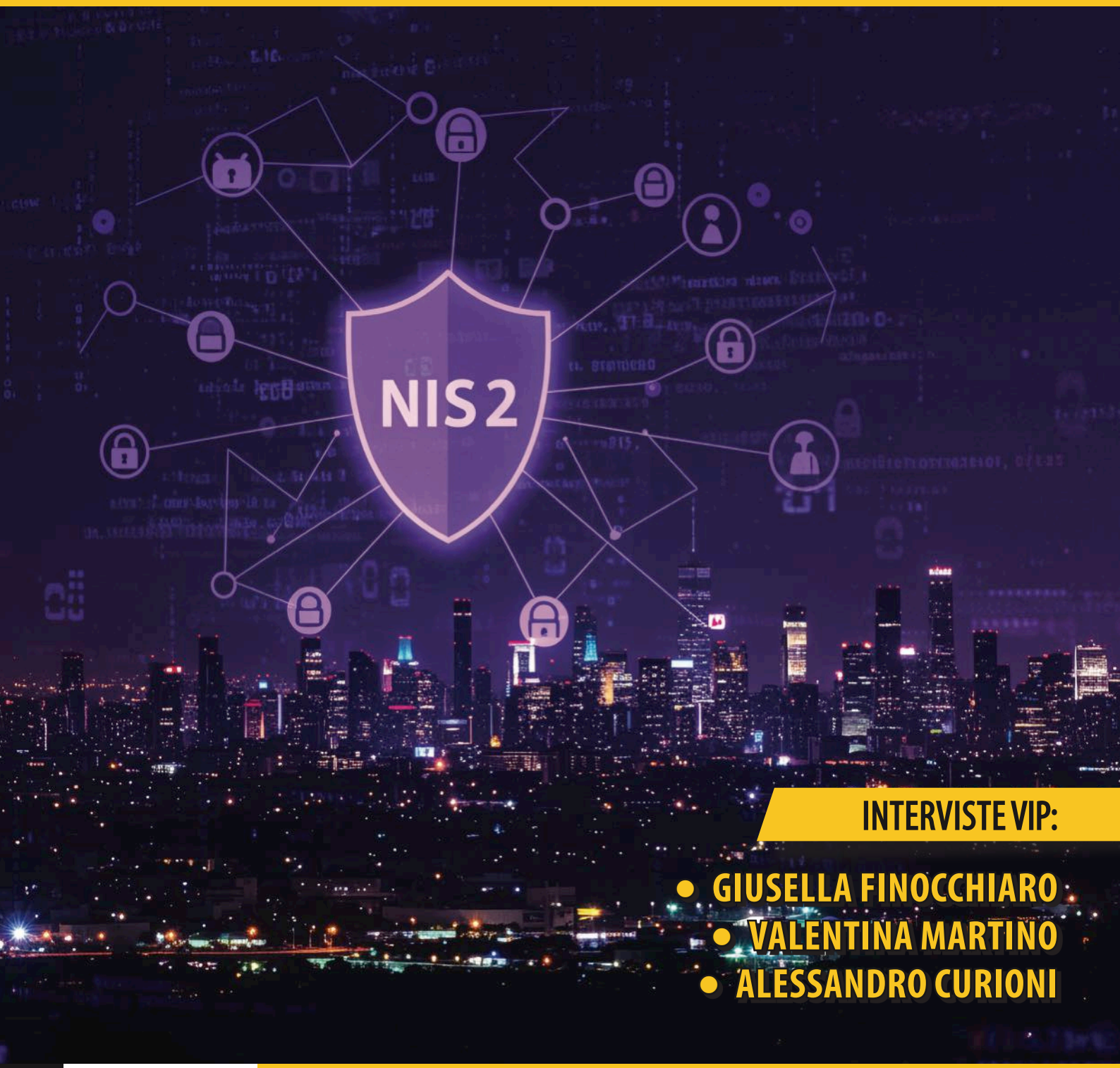
Cybersecurity Trends

Edizione italiana, N. 2 / 2025



INTERVISTE VIP:

- GIUSELLA FINOCCHIARO
- VALENTINA MARTINO
- ALESSANDRO CURIONI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale: NIS 2

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

NIS2 opportunità per aumentare la sicurezza.

Autore: Nicola Sotira

Network and Information Security 2, la direttiva che è stata varata dall'Unione Europea nel 2023, ha lo scopo di rafforzare la sicurezza informatica nei settori critici. Rispetto alla precedente direttiva NIS del 2016, la NIS2 amplia l'ambito di applicazione, impone requisiti più stringenti e introduce sanzioni più severe per le aziende. Le organizzazioni pubbliche e private che operano in settori essenziali (energia, sanità, trasporti, finanza, ecc.) e importanti (servizi digitali, produzione di tecnologie, fornitori IT, ecc.) devono adeguarsi. Ma cosa comporta concretamente la compliance?

Adeguarsi alla NIS2 significa rafforzare le difese contro gli attacchi informatici. La direttiva impone misure di gestione del rischio, protezione delle reti, risposta agli incidenti, continuità operativa e formazione del personale. Questo si traduce in organizzazioni più preparate, reattive e resilienti di fronte alle minacce cyber. Per il business, un'organizzazione che dimostra la conformità ai requisiti NIS2 trasmette un segnale chiaro a clienti, partner e stakeholder: l'azienda prende sul serio la cybersecurity. In un contesto in cui le violazioni di dati sono all'ordine del giorno, la fiducia è un vantaggio competitivo. Inoltre, la trasparenza nella gestione degli incidenti rafforza la credibilità. L'adeguamento spingerà, inoltre, le imprese a modernizzare sistemi IT, processi e policy. Questa spinta verso la trasformazione digitale può generare efficienze a lungo termine e migliorare la competitività. In questo contesto, si dovrà tenere conto che tutte le attività di audit, formazione, strumenti di sicurezza, aggiornamenti software e assunzione di personale qualificato comporteranno spese rilevanti, soprattutto per le PMI. La direttiva non distingue le imprese in base alla dimensione, ma solo in funzione dell'impatto settoriale. La compliance potrebbe anche portarsi dietro una certa complessità burocratica, richiedendo la creazione di processi strutturati per il risk management, la gestione degli incidenti, le comunicazioni verso le autorità e la documentazione. Questo può rallentare le operazioni, soprattutto nelle organizzazioni non abituate a normative stringenti. Altro tema da affrontare è quello della scarsità di risorse in ambito cybersecurity. La richiesta di esperti in cybersecurity, risk management e compliance è in forte crescita. Tuttavia, trovare personale qualificato è difficile. Questo rende la compliance un obiettivo difficile da raggiungere per molte aziende, creando disparità nel mercato. In ultimo, come vedremo nel nostro numero dedicato a questa tematica, abbiamo le due facce di questa medaglia: da un lato la direttiva aumenta la sicurezza, dall'altro impone obblighi molto rigidi, con sanzioni fino a 10 milioni di euro o il 2% del fatturato globale. La mancata o parziale conformità può avere conseguenze pesanti anche per errori non intenzionali.

La conformità alla direttiva NIS2 rappresenta un passo obbligato per molte imprese, con vantaggi strategici in termini di sicurezza, reputazione e conformità. Tuttavia, comporta anche costi, complessità e nuove responsabilità. La chiave è prepararsi in tempo, valutare i gap e costruire una roadmap sostenibile per trasformare questo obbligo in opportunità. ■

BIO

Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Il Decreto NIS nel framework della sicurezza Europea e Nazionale: dawn of a "new" CISO.

Autore: Alessandro Marzi

Introduzione

La sicurezza informatica rappresenta oggi uno dei pilastri strategici dell'Unione Europea, costituendo una leva fondamentale per la protezione dell'economia digitale, delle **infrastrutture critiche** e dei **diritti dei cittadini**.

In questo contesto, il decreto NIS, insieme alla **Direttiva NIS2**, costituisce un tassello essenziale del quadro normativo europeo e nazionale in materia di cybersecurity che, oltre a rappresentare un cambio di paradigma, nei suoi principi favorisce e sostiene la ridefinizione del ruolo del **Chief Information Security Officer** (CISO), quale garante della conformità normativa, ma anche e soprattutto guida per la trasformazione culturale e organizzativa della sicurezza in azienda, *conditio sine qua non* per affrontare le nuove sfide nel campo della sicurezza cibernetica.

In questo articolo, a partire dal posizionamento della direttiva NIS all'interno del contesto normativo dell'UE, analizzerò le sfide e le opportunità che il CISO "contemporaneo" potrà cogliere in questo nuovo scenario.

BIO

Alessandro Marzi è un esperto di cybersecurity con oltre 25 anni di esperienza. Ha lavorato in diverse industry, dalle telco alle energy & utilities, al gaming e digital payments, ricoprendo ruoli di crescente responsabilità nelle principali aziende e infrastrutture critiche nazionali e internazionali, guidando percorsi di trasformazione e consolidamento cyber. Alessandro contribuisce attivamente a community italiane ed estere, promuovendo la condivisione delle informazioni e la cultura della cybersecurity. Partecipa a convegni e seminari, condividendo la propria esperienza e conoscenza per diffondere l'importanza della sicurezza informatica e fornire una guida alle nuove generazioni.

Da NIS a NIS2: una visione evolutiva della sicurezza europea

L'Unione Europea ha intrapreso un **percorso ambizioso** verso la costruzione di un **cyberspazio sicuro, resiliente e affidabile**, necessario per sostenere l'**economia digitale**, l'integrazione dei servizi pubblici e la tutela dei **diritti fondamentali**.

Ricordiamo come il **primo significativo passo** nella regolamentazione della cybersecurity è stato compiuto con la Direttiva 2016/1148/UE, nota come **NIS**, volta a rafforzare la cibersicurezza delle reti e dei sistemi informativi per salvaguardare i servizi vitali per l'economia e la società dell'UE.

Per la prima volta, il tema della cybersecurity delle infrastrutture critiche è stato trattato in maniera organica, introducendo:

- l'obbligo di implementare **misure minime di sicurezza** e di **notifica degli incidenti**, per gli operatori di servizi essenziali (OSE) e alcuni fornitori di servizi digitali (DSP);
- il **principio della responsabilità nazionale**, con ogni Stato membro incaricato di designare autorità competenti e CSIRT nazionali;
- un **primo meccanismo di cooperazione** tra Stati membri.

L'esperienza di questi anni ha anche mostrato **limiti strutturali della NIS**: ambito troppo ristretto, disomogeneità tra i Paesi, mancanza di sanzioni efficaci, e assenza di supervisione armonizzata per non menzionare la **rapidissima evoluzione del panorama delle minacce**, favorita anche dalle tecnologie emergenti e l'**accelerazione della trasformazione digitale** tendenzialmente in un **tessuto organizzativo aziendale che non prevedeva la Sicurezza "by design"**.

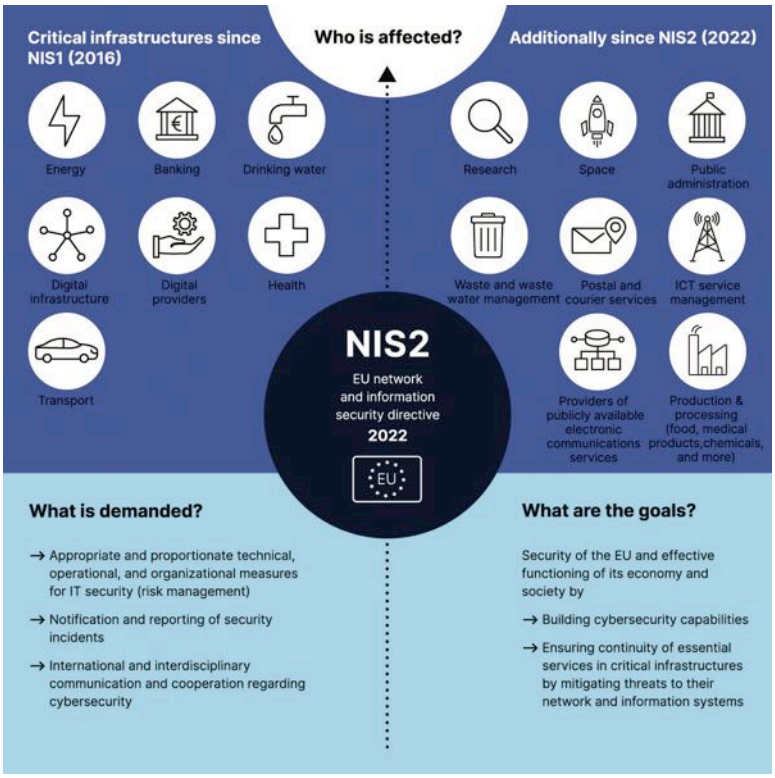
La Direttiva 2022/2555/UE, nota come NIS2, nasce proprio con l'ambizione di indirizzare e superare queste criticità. Recepita nell'ordinamento nazionale con **decreto legislativo 4 settembre 2024, n.138[1], la NIS2 amplia significativamente l'ambito soggettivo e oggettivo** della regolamentazione, rendendola più rigorosa, armonizzata e resiliente:

- ampliamento dell'**ambito soggettivo**: da alcune centinaia a decine di migliaia di entità coinvolte a livello europeo, includendo nuovi settori essenziali e importanti;
- introduzione di **obblighi di governance più stringenti con ruoli e responsabilità chiare, anche dei board**, piani di gestione del rischio, valutazioni e audit;
- **armonizzazione delle sanzioni** sulla falsariga del GDPR (fino al 2% del fatturato globale o 10 milioni di euro per i Soggetti Essenziali);
- **rafforzamento della cooperazione europea** con l'istituzione dell'European Cyber Crises Liaison Organisation Network (EU-CyCLONe) e potenziando i poteri dell'ENISA.

In sostanza, la NIS2 si propone di creare una vera e propria "baseline di cybersecurity" europea, definendo un insieme minimo e uniforme di misure di sicurezza a cui tutti i soggetti devono adeguarsi, secondo un approccio risk-based.

Il posizionamento della NIS2 nel quadro normativo dell'UE

Ma per comprenderne appieno il significato e l'impatto della nuova Direttiva, è necessario collocarla all'interno del **più ampio framework di regolamentazione della sicurezza digitale dell'UE**, in cui convivono e si integrano norme di natura preventiva e reattiva con requisiti sia organizzativi che tecnologici.



La NIS2 ha una valenza trasversale e settoriale, coinvolgendo soggetti pubblici e privati in 18 settori ritenuti essenziali o importanti – tra cui sanità, energia, trasporti, servizi digitali, gestione delle acque e amministrazioni pubbliche centrali e locali – non agisce in isolamento ma, al contrario, è complementare e interconnessa ad altri strumenti regolatori dell'UE:

- **Regolamento 2016/679** (GDPR - General Data Protection Regulation): riguarda la tutela dei dati personali e **come la NIS2 definisce obblighi per la notifica degli incidenti, la valutazione di rischio e la definizione di accountability chiare. CISO e DPO devono collaborare** per i presidi di sicurezza – spesso il primo aiuta il secondo in ambito tecnologico – e su incidenti congiunti (es. data breach derivante da attacco informatico);
- **Regolamento UE 2019/881** (Cybersecurity Act): riguarda la governance della cybersecurity a livello comunitario, rafforza l'Agenzia dell'UE per la cibersicurezza (ENISA) e istituisce un quadro di certificazione della cibersicurezza per prodotti e servizi. **La NIS2 potrà fare riferimento a certificazioni ENISA** per dimostrare conformità;
- **Direttiva 2022/2557 CER** (Critical Entities Resilience): si concentra sulla **resilienza fisica delle infrastrutture critiche, è complementare alla NIS2:** laddove NIS2 tutela il **dominio digitale**, la CER protegge quello fisico. **CISO e Physical Security Officer collaborano** per l'obiettivo comune della continuità operativa e della gestione delle crisi;
- **Regolamento DORA** (Digital Operational Resilience Act): dedicato alla **resilienza digitale degli operatori finanziari**, come la NIS2 determina obblighi di gestione dei rischi, verifiche tecniche e audit nonché gestione dei fornitori terzi in termini di sicurezza;
- **AI (Artificial Intelligence) Act:** per **stabilire regole per lo sviluppo e l'uso sicuro ed etico dell'intelligenza artificiale nell'UE**, anch'esso ha come base fondante la gestione del rischio e il **CISO si interrelaziona**

con stakeholder "noti" (DPO, Direzione Legal, Chief Data and Innovation Officer ecc.).

Ben si comprende che questo framework normativo, di cui la NIS2 è parte integrante, **non è solo tecnico, ma strategico** e rientra nella più ampia agenda di:

- **Sovranità digitale europea**;
- **Autonomia strategica nel cyberspazio**;
- **Protezione delle infrastrutture critiche in un contesto geopolitico instabile**.

Obblighi e impatti: cosa cambia per le organizzazioni

Il Decreto NIS, nella sua trasposizione italiana, è molto più che una direttiva settoriale: è la porta d'ingresso dell'Italia in una cybersecurity europea finalmente coerente, integrata e proiettata verso il futuro.

Il **cambio di paradigma normativo** per la cybersecurity in Italia si riflette nell'**ampliamento del perimetro dei soggetti regolati a cui applicare un approccio multirischio e garantire la notifica degli incidenti**. Non si parla più solo di operatori di servizi essenziali (OSE), ma di:

- **Soggetti essenziali:** operatori di servizi critici come energia, trasporti, sanità, acque, PA centrale, ecc.
- **Soggetti importanti:** settori ad alta rilevanza economica e sistemica, come produzione industriale, servizi postali, telecomunicazioni, ricerca, tecnologie digitali, gestione rifiuti, ecc.

Inoltre, a differenza del passato, dove spesso le responsabilità erano diluite o poco formalizzate, la NIS2 impone che:

- Il **management sia direttamente responsabile** dell'adozione delle misure di sicurezza.
- Le figure apicali ricevano **formazione specifica** sulla gestione del rischio cyber.
- Sia nominato un **Punto di Contatto**, con compiti di coordinamento e reportistica.

Le sfide della NIS2: tra risorse, cultura e tempo

In definitiva, il Decreto NIS cambia radicalmente il modo in cui la cybersecurity è percepita, gestita e governata nelle organizzazioni italiane. Non si tratta più di una scelta tecnica o discrezionale, ma di un obbligo normativo con effetti concreti sulla **governance, i processi e la reputazione aziendale**.

D'altra parte, se la NIS2 rappresenta un'opportunità strategica per aumentare la resilienza del tessuto digitale europeo, la sua **attuazione**

concreta non è però priva di difficoltà e, per molte organizzazioni, **il passaggio da un approccio reattivo a un modello strutturato e regolato di cybersecurity** si scontra con ostacoli di natura tecnica, organizzativa, culturale ed economica:

- Il fattore tempo e risorse: soprattutto le PMI non sono ancora pienamente consapevoli dei requisiti della NIS2, mentre il tempo per adeguarsi è breve e le risorse, anche e soprattutto in termini di competenze, sono scarse;
- Penuria di competenze: uno dei principali colli di bottiglia è la **disponibilità di figure professionali qualificate** per progettare, implementare e monitorare il sistema di sicurezza richiesto dalla NIS2. Il mercato italiano da tempo soffre di carenza di esperti di cybersecurity e molte aziende ricorreranno a consulenze, più o meno continuative, senza costruire una struttura interna competente e autonoma;
- **Integrazione con le altre compliance**: quando l'obiettivo è evitare ridondanze operative e creare una **strategia di cybersecurity omogenea e unitaria** in organizzazioni complesse, essere **soggetti a diverse normative di settore può rappresentare una sfida** con il rischio di creare **duplicazioni di attività** (es. audit multipli, reportistica diversa per ogni ente), generando inefficienze e overload burocratico;
- **Resistenza culturale**: L'adozione della sicurezza come parte del DNA aziendale richiede un cambiamento culturale profondo, che va oltre la tecnologia, richiedendo **formazione diffusa** multilivello, che includa il board e non solo i team tecnici, piuttosto che **KPI di sicurezza integrati nella performance aziendale**.

È quindi chiaro che la piena attuazione della NIS2 richiede molto più di un aggiornamento tecnologico, serve **una trasformazione organizzativa e culturale profonda**, da costruire con visione, metodo e collaborazione.

È in questo contesto che il CISO gioca un ruolo cruciale nel superare queste sfide, agendo da **ponte tra la tecnica, il business e la normativa**, coinvolgendo tutte le funzioni aziendali per costruire un ecosistema di sicurezza **sostenibile, adattivo e allineato agli obiettivi strategici dell'organizzazione**.

Il ruolo del CISO nel nuovo scenario normativo

Nel contesto delineato dalla Direttiva NIS2 e dal Decreto NIS italiano, la figura del **Chief Information Security Officer** (CISO) assume una centralità completamente nuova. Se in passato era visto – e collocato – come una **costola tecnica del reparto IT**, oggi il CISO si trasforma in una **funzione autonoma e trasversale di governo, controllo e indirizzo strategico della sicurezza informatica** a cui le funzioni tecniche, sia in ambito Digitale che Industriale, devono far riferimento per implementare le direttive centrali in maniera coerente e omogenea.

Questa transizione si traduce in un profondo cambiamento nella **governance aziendale** della sicurezza. Per **governare la complessità attuale**, in cui la sicurezza non è più un problema tecnologico, ma **un rischio strategico aziendale**, giocoforza si passa **dal fare sicurezza al garantire che la sicurezza venga fatta in modo efficace, continuo e coerente con i rischi del business**.

Con la NIS2 e le nuove normative di resilienza digitale, il CISO consolida il proprio ruolo come **funzione di secondo livello**, analogamente al ruolo che il **risk manager** o il **compliance officer** già rivestono in altri ambiti:

PRIMA	DOPO LA NIS2
Parte dell'IT	Funzione autonoma
Focus tecnico	Focus sul rischio
Responsabile dell'implementazione	Responsabile dell'indirizzo, del monitoraggio, della supervisione e del controllo

Il CISO ha il compito essenziale di valutare, monitorare e garantire la conformità normativa del sistema di sicurezza aziendale, rappresentando i rischi in modo chiaro, oggettivo e misurabile al vertice dell'organizzazione.

Assumendo una visione trasversale e indipendente centrata sulla valutazione del rischio, il CISO funge da **"secondo occhio" sul sistema di sicurezza**, non coinvolgendosi direttamente nell'implementazione ma garantendone l'efficacia. Di conseguenza, l'indipendenza del CISO non è un lusso superfluo, ma una condizione imprescindibile per l'efficacia del sistema di sicurezza aziendale: chi gestisce operativamente la sicurezza non può essere l'unico responsabile della verifica della sua adeguatezza.

Per evitare che le normative restino un esercizio di stile su carta, il CISO assume anche un ruolo abilitante quando agisce come **agente del cambiamento culturale**. In un contesto in cui le relazioni e la *security as teamwork* sono centrali, e l'errore umano rappresenta la principale causa di attacchi riusciti, **il fattore umano diventa il primo livello di resilienza e difesa**.

La sicurezza non è una responsabilità esclusiva del CISO, ma un obiettivo condiviso. Il suo ruolo consiste nel facilitare questa trasformazione culturale, fungendo da catalizzatore tra le aree tecniche e i vertici aziendali.

In conclusione, nel mondo post-NIS2 il CISO esce dal perimetro tecnico-operativo per diventare un **attore chiave della governance d'impresa**. Non è più il "responsabile dei firewall", ma il **custode dell'equilibrio tra innovazione digitale, conformità normativa e gestione del rischio sistemico**. Una funzione autonoma, trasversale, con una visione strategica e integrata. ■

1 Gli Stati membri che avevano tempo fino al 17 ottobre 2024 per recepire la direttiva NIS2 nel diritto nazionale, la Direttiva NIS2 ha abrogato la NIS1 a decorrere dal 18 ottobre 2024

Formazione e consapevolezza: la miglior difesa contro la sfida della NIS2.

Autore: Italo Piroddi

La direttiva europea NIS2 è oggi più che mai un tema centrale nelle strategie aziendali di sicurezza informatica. Il panorama della cybersecurity richiede un approccio integrato e olistico, in cui la formazione e la consapevolezza rappresentano la prima e più efficace linea di difesa.

In Aruba, abbiamo scelto di trasformare la formazione interna da semplice strumento di compliance ad una vera opportunità strategica di crescita e maturazione per tutta l'organizzazione. La nostra Academy interna è diventata il fulcro di questo processo, promuovendo un percorso formativo innovativo, efficace e soprattutto coinvolgente.

Perché formare sulla NIS2

La direttiva NIS2 nasce dalla necessità di alzare il livello complessivo di resilienza cibernetica delle organizzazioni europee, allargando il perimetro rispetto alla precedente NIS e coinvolgendo un numero significativamente maggiore di settori e aziende. L'obiettivo è garantire una capacità di risposta uniforme, efficace e tempestiva contro le minacce cibernetiche.

Ma una normativa, per quanto ben concepita, non produce effetti significativi senza un investimento mirato sulla componente umana. Ed è qui che si inserisce il nostro intervento come Academy: formare le persone significa innanzitutto renderle consapevoli del proprio ruolo, delle proprie responsabilità e delle azioni concrete da intraprendere in caso di incidenti di sicurezza.

BIO

In un mondo in cui l'innovazione è all'ordine del giorno, c'è una persona che si distingue per la sua capacità di mantenere vive le competenze. Il suo nome è Italo Piroddi, l'HR Learning e Development Manager, del Gruppo Aruba, che sta ridefinendo le regole del gioco. Non è solo un manutentore di competenze, ma un vero e proprio custode della conoscenza. Dotato di una sete insaziabile di apprendimento, Italo è sempre alla ricerca di nuove sfide e nuovi orizzonti da esplorare. Ma non è tutto lavoro e niente gioco: quando il sole cala, Italo si rifugia nel suo mondo privato, un mondo costruito di parole e storie, un mondo che si apre ogni volta che apre un libro. La lettura è la sua passione, la sua fuga, il suo rifugio, così come la musica è la sua fonte d'ispirazione. Quando Italo non sta plasmando le menti di domani, si perde nelle melodie delle sue dieci chitarre, che danno vita ai suoi sogni. Italo, un manutentore di competenze, un apprendista perenne, un amante dei libri con la forza di un leader e il cuore di un musicista. Questo è il suo mondo. Questo è Italo.

Il nostro approccio alla formazione

In Aruba, la formazione su NIS2 non è interpretata come un semplice adempimento burocratico ma come un'opportunità strategica per:

- sviluppare consapevolezza individuale e collettiva sulla sicurezza informatica;
- creare una cultura aziendale orientata alla prevenzione e alla gestione proattiva degli incidenti;
- migliorare la capacità di reazione e resilienza dei team coinvolti.

Abbiamo costruito un percorso formativo modulare, flessibile e adattabile ai diversi ruoli aziendali, basato su quattro pilastri principali:

1 **Awareness e sensibilizzazione generale**
Ogni dipendente partecipa a moduli e-learning digitali periodici, progettati per illustrare in modo semplice e concreto le minacce più comuni, le tecniche di attacco e le best practice quotidiane per garantire una sicurezza digitale efficace.

2 **Formazione tecnica e specializzata**
I team tecnici e specialistici - come quelli IT, Sicurezza e Compliance - stanno seguendo un master avanzato focalizzato su strumenti specifici, analisi del rischio, gestione degli incidenti e procedure di recovery, fondamentali per affrontare le minacce più sofisticate.

3 **Simulazioni e Cyber Drill**
La formazione teorica viene completata da esercitazioni pratiche, attraverso simulazioni di incidenti informatici realistiche - i cosiddetti *cyber drill* - per testare concretamente capacità e prontezza operativa dei team coinvolti.

4 **Comunicazione e gestione della crisi**
I manager e i responsabili aziendali partecipano a sessioni dedicate alla comunicazione efficace e alla gestione della crisi, competenze fondamentali per limitare i danni reputazionali e assicurare un recupero rapido delle operazioni.

Digital Learning e innovazione didattica

Una delle caratteristiche distintive della nostra Academy è l'utilizzo intensivo di strumenti digitali innovativi e di metodologie didattiche avanzate.

Abbiamo introdotto:

- **Aruba4Learning, una Learning Experience Platform (LXP)** che consente un apprendimento personalizzato, adattivo e coinvolgente.
- **gamification**, per aumentare l'engagement e favorire una migliore assimilazione dei concetti.
- **AI e analytics**, che ci permettono di monitorare continuamente il livello di comprensione dei contenuti formativi e adattare i percorsi in tempo reale.

La centralità del fattore umano

Nonostante l'innovazione tecnologica, la componente umana resta centrale. La nostra strategia formativa pone infatti le persone al centro, considerandole non semplici destinatari della formazione, ma veri protagonisti del cambiamento organizzativo.

I risultati ottenuti e prossimi passi

Gli effetti di questa strategia sono stati evidenti e misurabili:

- incremento significativo nella capacità di rilevamento precoce e risposta agli incidenti;
- riduzione sensibile delle vulnerabilità causate da errori umani;
- maggiore coinvolgimento e motivazione del personale, che percepisce la cybersecurity come una responsabilità condivisa e non solo un obbligo.

Guardando al futuro, continueremo a sviluppare e migliorare i nostri programmi formativi, focalizzandoci su aspetti sempre più avanzati come la sicurezza predittiva, l'intelligenza artificiale applicata alla sicurezza, e la promozione di una mentalità sempre più proattiva e resiliente.

Conclusione

La direttiva NIS2, se interpretata e gestita correttamente, rappresenta una straordinaria occasione per rafforzare non solo le nostre difese informatiche ma anche - e soprattutto - la cultura organizzativa. Investire nelle persone, nelle loro competenze e nella loro consapevolezza è la strategia più efficace per affrontare con successo le sfide sempre più sofisticate poste dalla cybersecurity.

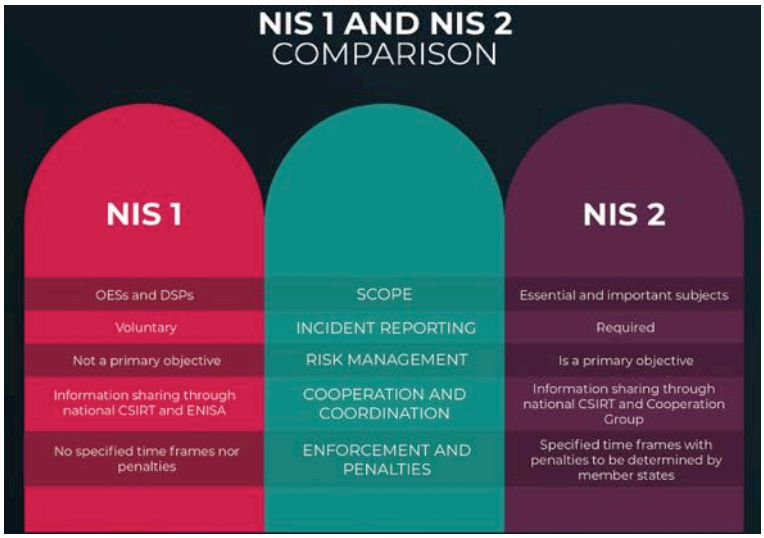
aruba.it ACADEMY

In Aruba, abbiamo già intrapreso questo cammino, consapevoli che una formazione continua, innovativa e umanocentrica sia la chiave per trasformare obblighi normativi in vantaggi competitivi reali e duraturi. ■

La NIS 2 nasce per definire in modo più chiaro il quadro disciplinare di una cybersecurity robusta e armonizzata a livello europeo.

Autore: Lucio G. Insinga

La NIS 2 è al centro dell'attenzione non solo degli addetti ai lavori, ma anche della pubblicistica che analizza l'evoluzione del delicato rapporto che esiste tra diritto e tecnologia. Un aspetto risulta subito evidente, anche all'osservatore più distratto: come mai una così forte attenzione non ha accompagnato l'approvazione della NIS 1, che pure aveva introdotto cambiamenti significativi nell'aggiornamento dei processi e delle soluzioni organizzative in tema di sicurezza aziendale? Una possibile risposta riguarda la creazione di un nuovo mercato per quei soggetti imprenditoriali che, non potendo permettersi i costi di gestione di certificazioni come la "ISO 27000", si trovano oggi obbligati - se vogliono continuare a interloquire e a collaborare con grandi player - ad adottare le misure di compliance previste dal nuovo strumento normativo. È quindi importante sottolineare le principali differenze tra la direttiva NIS 1 (2016) e la NIS 2 (2022), sua naturale evoluzione, che possono essere riassunte come segue:



1. Ambito di applicazione:

- NIS 1: si concentrava sugli "operatori di servizi essenziali" (OSE) in settori critici come energia, trasporti, finanza, sanità e infrastrutture digitali - e sui "fornitori di servizi digitali" (FSD) quali marketplace online, motori di ricerca e servizi di cloud computing.
- NIS 2: amplia significativamente il suo raggio d'azione, includendo un numero maggiore di settori e sottosettori definiti come "entità essenziali" e "entità importanti". Questi includono, ad esempio, la pubblica amministrazione, il settore spaziale, la produzione di prodotti critici (come quello farmaceutico e alimentare), i fornitori di reti e servizi pubblici di comunicazione elettronica, i servizi fiduciari digitali, i servizi di gestione dei

rifiuti, la produzione, la trasformazione e la distribuzione di alimenti, e molti altri. La distinzione tra OSE e FSD viene superata. Inoltre, la NIS 2 abbassa le soglie dimensionali, includendo anche medie e piccole imprese operanti in settori critici.

2. Obblighi di sicurezza:

- NIS 1: prevedeva obblighi di sicurezza generici, lasciando agli Stati membri una certa discrezionalità nella loro implementazione.
- NIS 2: introduce un elenco più dettagliato di requisiti minimi di sicurezza informatica che le entità devono implementare, seguendo un approccio basato sulla gestione del rischio. Tra questi rientrano: politiche di sicurezza delle informazioni, gestione degli incidenti, continuità operativa, sicurezza della catena di approvvigionamento, sicurezza della rete e dei sistemi informativi, controllo degli accessi e crittografia.

3. Notifica degli incidenti:

- NIS 1: richiedeva la notifica degli incidenti con un impatto significativo sulla continuità dei servizi essenziali, senza specificare tempistiche precise.
- NIS 2: rafforza gli obblighi di segnalazione, introducendo tempistiche più stringenti. Le entità devono inviare un "allarme rapido" entro 24 ore dalla scoperta di un incidente significativo, seguito da una notifica più dettagliata entro 72 ore e un rapporto finale entro un mese.

4. Supervisione e applicazione:

- NIS 1: la supervisione e l'applicazione variavano tra gli Stati membri.
- NIS 2: prevede una maggiore armonizzazione delle sanzioni a livello europeo, con la possibilità di imporre multe fino al 2% del fatturato globale per le entità essenziali e fino all'1,4% per le entità importanti in caso di non conformità. Introduce anche meccanismi di supervisione più rigorosi e poteri di intervento più ampi per le autorità competenti.

5. Responsabilità della dirigenza:

- NIS 2: introduce una maggiore responsabilità per gli organi di gestione delle entità, che devono supervisionare l'implementazione e il rispetto delle misure di cybersecurity.

6. Sicurezza della catena di approvvigionamento:

- NIS 2: introduce un focus specifico sulla sicurezza della catena di approvvigionamento, richiedendo alle entità di considerare i rischi derivanti dai loro fornitori e partner.

In sintesi, si può affermare che la NIS 2 rappresenta un'evoluzione significativa rispetto alla NIS 1, con *l'obiettivo di creare un quadro di cybersecurity più robusto e armonizzato a livello europeo, in risposta all'evoluzione delle minacce informatiche e alla crescente digitalizzazione della società e dell'economia.* La NIS 2 amplia la platea delle entità soggette, introduce obblighi di sicurezza più dettagliati e stringenti, rafforza i meccanismi di notifica e le sanzioni, e pone maggiore enfasi sulla responsabilità della dirigenza e sulla sicurezza della catena di approvvigionamento.

I numeri possono aiutare ad ampliare gli orizzonti. Il noto scienziato Albert Einstein amava affermare che *"La mente è come un paracadute. Funziona solo se si apre"*. Proviamo perciò a tessere un riepilogo dei dati relativi alle piccole e medie imprese (PMI) in Europa sulla base di alcuni dati di Confcommercio. In Europa esistono circa 19,6 milioni di PMI, che rappresentando il 99,8% del totale delle imprese, così suddivise:

- **Microimprese** (fino a 9 dipendenti): 18.035.000 unità (91,8%), occupano 37,5 milioni di persone (29,6%) e generano un valore aggiunto di 1.120 miliardi di euro (20,9%);
- **Piccole imprese** (10–49 dipendenti): 1.353.000 unità (6,9%), occupano 26,1 milioni di persone (20,6%) e generano un valore aggiunto di 1.011 miliardi di euro (18,9%);
- **Medie imprese** (50–249 dipendenti): 213.000 unità (1,1%), occupano 21,3 milioni di persone (16,8%) e generano un valore aggiunto di 954 miliardi di euro (17,8%);
- **Grandi imprese** (250 o più dipendenti): 41.000 unità (0,2%), occupano 41,7 milioni di persone (32,9%) e generano un valore aggiunto di 2.270 miliardi di euro (42,4%).

Concentrazione geografica

Le PMI sono distribuite in modo diffuso in tutta l'Unione Europea, sebbene con alcune differenze tra i vari Paesi. Ad esempio, in

Italia, Grecia e Portogallo, le PMI rappresentano oltre l'80% dell'occupazione totale, mentre in Germania e Regno Unito questa percentuale è inferiore al 55%.

Secondo i dati disponibili, in Europa sono circa **30.000 le organizzazioni certificate ISO/IEC 27001**, con un incremento del 25% rispetto all'anno precedente.

Tuttavia, non esistono statistiche ufficiali che indichino quante di queste siano effettivamente **piccole e medie imprese (PMI)**. Secondo un'indagine, circa il **50% delle organizzazioni certificate ISO 27001** ha meno di 200 dipendenti, il che suggerisce che una parte significativa delle PMI europee ha adottato questo standard.

La Commissione Europea stima che circa 160.000 entità saranno interessate dalla direttiva NIS 2, un incremento significativo rispetto alle 15.000 entità della NIS 1.

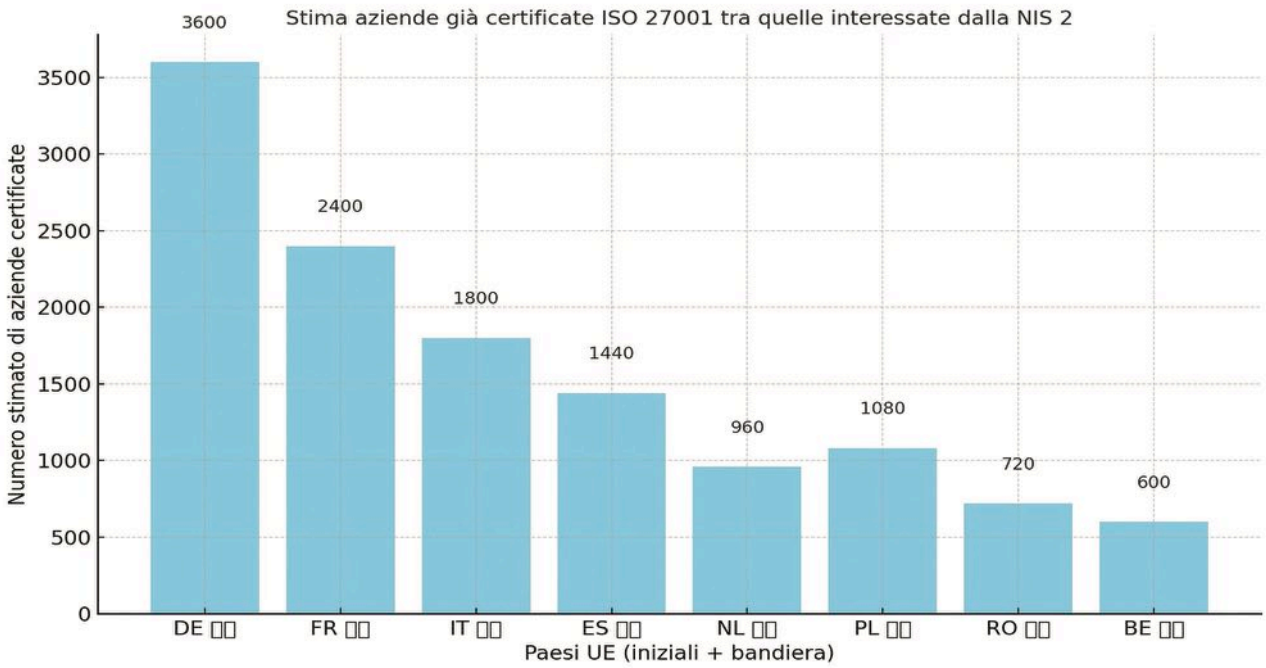
- Germania: circa 30.000
- Francia: circa 20.000
- Italia: circa 15.000
- Spagna: circa 12.000
- Paesi Bassi: circa 8.000
- Polonia: circa 9.000
- Romania: circa 6.000
- Belgio: circa 5.000
- Altri Stati UE: circa 55.000

Secondo stime basate su fonti ISO e dati ENISA, circa il 10–15% delle aziende interessate dalla NIS 2 sono già certificate ISO/IEC 27001. Questo equivale a circa 16.000 – 24.000 aziende in Europa.

Va ricordato che la certificazione ISO 27001 è nata prima della legge, cosa che non deve stupirci, in quanto il legislatore è chiamato a intervenire "quando l'interesse di natura privatistico assume una ricaduta e una valenza pubblica, divenendo pertanto materia di regolazione. L'interrogativo sulla necessità di normare ogni adempimento rimane aperto. Lascerei la questione come elemento di riflessione per i lettori di Cybersecurity Trends, con l'auspicio di aprire un confronto sulla stimolante dialettica che oggi si è aperta tra l'evoluzione rapidissima della tecnologia, e la possibilità di cucire un "vestito" normativo, più adatto possibile: non invasivo, snello e facilmente applicabile, che renda veramente più facile la vita delle aziende - le piccole soprattutto - che vivono il costante imperativo di reggere i ritmi della competitività, in un mercato globale sempre più difficile da affrontare, attraversato da una fitta rete di fenomeni sociali ed economici. ■

BIO

Lucio G. Insinga, coniuga l'attività di Dottore Commercialista e Revisore Contabile con quella di Business Angel e Advisor. La vocazione aziendalista gli consente di essere uno dei primi cinque Innovation Manager certificati da Cepas. È il primo in Italia ad effettuare un'operazione di aumento di capitale in Bitcoin. È autore di: La Responsabilità sociale. Le PMI alla prova del modello 231, per Plenum Editore (2017), Come finanziare l'impresa. Attori Strumenti e metodi per potenziare la crescita, pubblicato Salvatore Primiceri Editore (2019) . La compliance integrata Plenum Editore (2022). Di imminente pubblicazione il suo quarto testo "Dizionario Finanziario commentato".



NIS 2: Requisiti, Impatti e Strategie di Compliance.

Autore: Pierpaolo Romano

La **Direttiva NIS 2** (Network and Information Security Directive 2), entrata **in vigore il 17 gennaio 2023**, rappresenta per i Paesi membri dell'Unione Europea un aggiornamento della precedente direttiva NIS del 2016. Essa mira a rafforzare la sicurezza informatica e la resilienza delle infrastrutture critiche e dei servizi essenziali all'interno dell'UE, in risposta alle crescenti minacce cibernetiche. La direttiva impone obblighi di sicurezza più stringenti per un numero più ampio di settori. Inoltre, introduce meccanismi di coordinamento tra Stati membri per garantire una risposta uniforme alle minacce informatiche.

Uno dei principali cambiamenti introdotti dalla NIS 2 è l'ampliamento del perimetro di applicazione e la **classificazione degli enti soggetti alla normativa** in due categorie:

1. **Enti Essenziali:** organizzazioni che forniscono servizi fondamentali la cui interruzione avrebbe un impatto significativo sulla sicurezza, l'economia e la società. Tra questi settori rientrano: energia, trasporti, sanità, infrastrutture digitali, fornitura e distribuzione di acqua potabile, e servizi finanziari;
2. **Enti Importanti:** organizzazioni che, pur operando in settori considerati meno critici, svolgono un ruolo rilevante in ambiti strategici e il cui malfunzionamento potrebbe avere un impatto considerevole. Questi includono settori come il trattamento delle acque reflue, settore alimentare, fornitori di servizi digitali, produttori farmaceutici e chimici, sanità e fornitori di comunicazioni elettroniche.

Gli Enti Essenziali, come l'organizzazione di cui faccio parte, sono tenuti a rispettare requisiti di sicurezza informatica più rigorosi, che riguardano in particolare:

- l'adozione di misure tecniche e organizzative per la gestione dei rischi informatici;
- la gestione del rischio cyber nella supply chain, con particolare attenzione ai fornitori critici di tecnologia;
- la predisposizione di piani di continuità operativa e risposta agli incidenti informatici;

BIO

Pierpaolo Romano è laureato in Ingegneria Informatica presso l'Università degli Studi di Napoli "Federico II" e possiede una Licenza Professionale di Ingegnere più svariate Certificazioni di Sicurezza. Dopo circa 5 anni come Cybersecurity Engineer presso il SOC di una delle più importanti realtà aziendali italiane, ha continuato a sviluppare le proprie competenze affrontando nuove sfide in realtà aziendali diverse lavorando presso importanti società di consulenza, rafforzando così le competenze nel campo della Cyber Security. Nel 2019 entra a far parte del Cyber Security Team di Ferrovie dello Stato Italiane e ricopre il ruolo di Cyber Security Specialist. Nel 2023 assume la carica di Chief Information Security Officer (CISO) presso Italo con la responsabilità complessiva sul Programma di Cyber Security, sui processi e le attività ad essi collegati per la definizione e l'implementazione della strategia, dei processi, del budget, delle priorità e degli obiettivi di Cyber Security per supportare adeguatamente l'attività dell'azienda.

▸ la notifica tempestiva degli incidenti significativi entro le tempistiche previste dalla normativa.

Per avviare un percorso di maturità verso la compliance alla Direttiva NIS2, è stata condotta una gap analysis. L'ambito delle analisi ha riguardato le seguenti tipologie di requisiti:

1. **Requisiti organizzativi**, come la definizione di governance della sicurezza, l'implementazione di politiche di gestione del rischio e la formazione del personale.
2. **Requisiti tecnici e tecnologici**, che includono sistemi di protezione dei dati, rilevamento delle minacce e gestione degli incidenti.
3. **Requisiti operativi**, come la protezione della supply chain, i piani di continuità operativa e la collaborazione con le autorità competenti.

Partendo dal framework documentale, è stata avviata un'attività di aggiornamento delle procedure esistenti e di redazione di nuove, al fine di soddisfare i requisiti introdotti dalla normativa.

Tra le procedure oggetto di revisione vi è quella di Incident management, poiché la Direttiva impone di rivedere il processo di gestione degli incidenti informatici, fornendo indicazioni precise sulle tempistiche di notifica e introducendo il concetto di incidente significativo.

Per affrontare correttamente questo tema, si è partiti dalla definizione di incidente e di incidente significativo.

L'articolo 6, paragrafo 6, della Direttiva NIS2 definisce "incidente" come: "un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati memorizzati, trasmessi o trattati o dei servizi offerti da, o accessibili tramite, reti e sistemi informativi". Un incidente è considerato "significativo" ai sensi dell'articolo 23, paragrafo 3, se: (a) ha causato o è in grado di causare una grave interruzione operativa dei servizi o perdite finanziarie per l'entità interessata; oppure (b) ha colpito o è in grado di colpire altre persone fisiche o giuridiche causando danni materiali o immateriali considerevoli.

Nella di gestione degli incidenti è stata rivista la categorizzazione degli stessi, l'assegnazione di ruoli e responsabilità, le procedure per il rilevamento, l'analisi, la risposta, il contenimento, l'eradicazione, il ripristino, la documentazione e la segnalazione.

Qui di seguito si riportano le fasi tipiche del ciclo di vita della gestione degli incidenti e la loro corrispondenza con i requisiti della NIS2 sono le seguenti:

▸ **Preparazione:** Sviluppo di politiche, procedure e formazione del personale come previsto dall'articolo 21.

▸ **Rilevamento:** Implementazione di sistemi di monitoraggio e registrazione come richiesto dal regolamento di esecuzione e dall'allegato della direttiva.

▸ **Analisi:** Valutazione e classificazione degli eventi per determinare se si qualificano come incidenti significativi, ai sensi dell'articolo 23, paragrafo 3, e del regolamento di esecuzione.

▸ **Contenimento:** Adottare misure immediate per limitare la portata e l'impatto dell'incidente.

▸ **Eradicazione:** Rimozione della minaccia e risoluzione della causa principale dell'incidente.

▸ **Ripristino:** Ripristino dei sistemi e dei servizi interessati al normale funzionamento, come richiesto dalle misure di continuità operativa ai sensi dell'articolo 21, paragrafo 2, lettera c).

▸ **Attività Post-Incidente:** Documentazione dell'incidente e della risposta, segnalazione alle autorità entro le scadenze specificate (articolo 23) e conduzione di una revisione per migliorare la futura gestione degli incidenti.

Comprendere l'allineamento tra il ciclo di vita della gestione degli incidenti e gli articoli e i requisiti specifici della NIS2 consente di adottare un approccio strutturato, finalizzato a garantire una piena conformità normativa. Questa attività di mappatura delle fasi del ciclo di vita alle disposizioni della direttiva permette di identificare quali requisiti specifici si applicano a ciascuna fase della gestione degli incidenti.

Per rispettare le tempistiche previste dalla normativa, è fondamentale stabilire piani di comunicazione e di escalation che garantiscono una condivisione tempestiva e appropriata delle informazioni.

Per stabilire un solido piano di risposta agli incidenti (IRP) è fondamentale:

- Implementare un monitoraggio continuo e pratiche robuste di gestione dei log per consentire il rilevamento e l'analisi tempestivi di attività sospette.
- Stabilire procedure chiare per il contenimento degli incidenti al fine di prevenirne la diffusione ad altri sistemi.
- Definire le fasi per l'eradicazione al fine di rimuovere la causa principale dell'incidente e il ripristino per riportare i sistemi e i servizi interessati al normale funzionamento.
- Condurre approfondite revisioni post-incidente per identificare le lezioni apprese e migliorare l'IRP e la postura di sicurezza generale.
- Considerare e stabilire relazioni con le parti esterne pertinenti, come le forze dell'ordine, gli organismi di regolamentazione e le società terze specializzate nella risposta agli incidenti informatici.

L'enfasi posta dalla direttiva sulla segnalazione tempestiva, insieme al potenziale rischio di sanzioni significative in caso di non conformità, sottolinea la necessità critica di un piano di risposta agli incidenti IRP solido e collaudato.

Per sensibilizzate l'intera popolazione aziendale, è fondamentale condurre regolarmente programmi di awareness sulla cybersecurity, al fine di garantire che tutti siano in grado di identificare e segnalare potenziali incidenti. Inoltre, la normativa prevede che anche il top management sia consapevole delle tematiche legate alla gestione del rischio informatico aziendale. Questo obiettivo può essere raggiunto attraverso programmi specifici per gli executive come, ad esempio i tabletop excercises.

Gestione del Rischio di Terze Parti e della Sicurezza della Catena di Approvvigionamento ai Sensi della NIS2

La direttiva NIS2 pone una notevole enfasi sulla sicurezza delle catene di approvvigionamento e sulle relazioni con terze parti. Le entità sono tenute a considerare le vulnerabilità specifiche di ciascun fornitore diretto e prestatore di servizi, nonché la qualità complessiva dei loro prodotti e delle pratiche di cybersecurity, comprese le procedure di sviluppo sicuro.

È necessario stabilire politiche e procedure complete per gestire i rischi nelle proprie catene di approvvigionamento, coprendo aspetti quali la selezione, l'onboarding, il monitoraggio e l'offboarding dei fornitori. È importante includere misure di gestione del rischio informatico e chiari standard di sicurezza informatica negli accordi contrattuali con i fornitori, compresi i requisiti per audit regolari e segnalazione degli incidenti.

Le strategie chiave per l'implementazione di programmi efficaci di gestione del rischio dei fornitori (VRM) per conformarsi alla NIS2 includono:

- **Condurre Approfondite Valutazioni del Rischio dei Fornitori:** Eseguire una due diligence completa e analisi dei rischi per identificare le potenziali vulnerabilità introdotte da terze parti, valutando la loro criticità,

la postura di sicurezza, la conformità agli standard e le capacità di risposta agli incidenti.

- **Stabilire un Sistema di Tiering dei Fornitori:** Classificare i fornitori in base alla loro criticità per le operazioni aziendali e al potenziale impatto di un incidente di sicurezza che li coinvolge.
- **Implementare un Monitoraggio Continuo:** Monitorare costantemente la postura di sicurezza delle terze parti per rilevare anomalie o attività sospette, sfruttando feed di threat intelligence e avvisi automatizzati.
- **Condurre Audit di Sicurezza Regolari:** Eseguire audit e valutazioni periodiche dei fornitori per assicurarsi che rispettino gli standard di sicurezza concordati e gli obblighi contrattuali.
- **Applicare Obblighi Contrattuali:** Includere requisiti di sicurezza informatica chiari e applicabili, clausole di notifica delle violazioni e diritti di audit nei contratti con terze parti.

Un programma di gestione del rischio dei fornitori completo e proattivo, che comprenda valutazione, monitoraggio, audit e garanzie contrattuali, è essenziale affinché si riesca a gestire efficacemente i rischi di terze parti e si soddisfino i requisiti di conformità della NIS2.

Esempi Pratici e Best Practice per il Miglioramento della Sicurezza delle Terze Parti:

- Implementare un approccio Zero Trust all'accesso dei fornitori, garantendo che ogni utente e dispositivo sia verificato prima di concedere l'accesso alle risorse.
- Sfruttare soluzioni tecnologiche come strumenti automatizzati di valutazione del rischio, sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) e piattaforme di monitoraggio continuo per semplificare il processo di monitoraggio e audit dei rischi di terze parti.
- Fornire programmi di formazione e sensibilizzazione alla sicurezza informatica ai fornitori terzi per garantire che comprendano e rispettino le aspettative di sicurezza dell'organizzazione.
- Promuovere la collaborazione e la comunicazione con i fornitori sugli obiettivi di sicurezza e conformità, garantendo una comprensione condivisa dei rischi e delle responsabilità.
- Implementare solide procedure di gestione e segnalazione degli incidenti che si estendano agli incidenti di terze parti, garantendo il rilevamento, la risposta e la notifica tempestivi alle autorità competenti.

Il miglioramento della sicurezza delle terze parti richiede un approccio olistico che combini soluzioni tecnologiche, processi ben definiti e una comunicazione efficace con i fornitori, al fine di creare una catena di approvvigionamento resiliente e sicura. Fare affidamento su una singola misura di sicurezza o su un approccio puramente reattivo risulta insufficiente nel panorama complesso e interconnesso delle moderne catene di approvvigionamento.

La NIS2 attribuisce maggiore responsabilità al top management per la supervisione delle politiche di sicurezza informatica e per la garanzia della conformità, comprese quelle relative alla gestione del rischio di terze parti. Il top management può essere ritenuto personalmente responsabile della non conformità ai requisiti della

direttiva, inclusi i fallimenti nella gestione del rischio di terze parti. L'enfasi della direttiva sulla responsabilità del top management sottolinea la fondamentale importanza della gestione del rischio di terze parti e richiede che sia trattata come una priorità strategica ai massimi livelli dell'organizzazione. Il potenziale di responsabilità personale per il top management garantisce che il rischio legato alle terze parti non venga delegato esclusivamente ai team IT o di sicurezza, ma riceva attenzione e supervisione dalla leadership organizzativa.

Conclusioni e Raccomandazioni

In sintesi, la Direttiva NIS2 impone obblighi significativi e richiede l'adozione di best practice sia per la gestione degli incidenti che per la sicurezza delle terze parti, sottolineando la loro interconnessione nel raggiungimento della resilienza complessiva della sicurezza informatica. Per raggiungere la conformità, le organizzazioni dovrebbero intraprendere i seguenti passi:

- Valutare attentamente se rientrano nell'ambito di applicazione della Direttiva NIS2 e identificare le unità interessate.
- Condurre un'analisi approfondita delle lacune per identificare le aree in cui le misure di sicurezza informatica attuali devono essere migliorate per allinearsi ai requisiti della NIS2.
- Sviluppare e implementare solidi piani di risposta agli incidenti che soddisfino le rigorose tempistiche e i requisiti di segnalazione della NIS2.
- Stabilire e migliorare le politiche e le procedure di sicurezza della catena di approvvigionamento, incorporando approfondite valutazioni del rischio dei fornitori, monitoraggio continuo e garanzie contrattuali.
- Garantire un'efficace governance e responsabilità aziendale per la sicurezza informatica, con il coinvolgimento attivo del top management.
- Implementare misure di sicurezza tecniche e organizzative appropriate come previsto dall'articolo 21 e dal regolamento di esecuzione.
- Stabilire procedure chiare ed efficienti per la segnalazione degli incidenti di sicurezza alle autorità competenti entro le tempistiche richieste.
- Valutare e gestire regolarmente i rischi della catena di approvvigionamento, garantendo che anche i fornitori e i partner terzi rispettino gli standard della direttiva.
- Prepararsi a potenziali audit, ispezioni e azioni di esecuzione da parte delle autorità nazionali.

È fondamentale un monitoraggio continuo, revisioni regolari delle politiche e delle procedure di sicurezza e un approccio proattivo per adattarsi al panorama delle minacce informatiche in evoluzione e garantire una conformità sostenuta alla Direttiva NIS2. ■

Gestione delle terze parti (Recall).

Autore: Francesco Corona

GENERALITA'. In un precedente articolo apparso sulla rivista Cybersecurity Trends [B001], si faceva notare che la gestione delle terze parti in ambito cybersecurity è diventato un tema cruciale, specialmente con l'introduzione della direttiva NIS2 e del regolamento DORA. Entrambi questi provvedimenti europei mirano a rafforzare la sicurezza informatica, ma presentano requisiti specifici e distinti per le organizzazioni, in particolare per quelle che operano nel settore finanziario e in settori critici. La **Direttiva NIS2** amplia il perimetro della cybersecurity includendo tutti i fornitori lungo la supply chain. Le aziende sono ora obbligate a rivedere i contratti con i fornitori di servizi ICT, integrando clausole di sicurezza informatica e prevedendo audit regolari per garantire la conformità. Questa direttiva si applica a un ampio numero di settori, tra cui energia, trasporti e servizi digitali, imponendo misure più severe rispetto alla precedente NIS1.

BIO

Francesco Corona è ricercatore e docente di Cyber Intelligence, già direttore del master di Hacking e Ingegneria della Sicurezza presso Link Campus University; è stato docente a contratto per 11 anni presso la Facoltà di Ingegneria Gestionale di Roma2 Tor Vergata, Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca nel campo dell'Intelligenza Artificiale e delle Reti Neurali per conto del CNR-IASI di Roma. Svolge attività di ricerca e sviluppo in svariati settori e in particolare in quello della Cybersecurity per conto di primari players nazionali e internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'Innovazione e il premio ICT Confindustria. f.corona@unilink.it

COMPLIANCE AREA	DORA	NIS2	GDPR
Legislative nature & scope.	Applies to EU FS firms & their ICT suppliers which must comply by Jan 17th 2025.	Applies to EU organizations considered vital to society. They must comply by 17th Oct 2024.	Applies to organizations processing EU personal data. In effect since 25th May 2018.
Technical & organizational measures.	Focuses on 3rd party risk, incident management, business continuity and regular testing.	Focuses on supply chain security based on an 'all hazards' approach to security.	Focuses on compliance with rules for data processing & security controls for personal data.
Notification Deadlines.	Incidents must be notified by the end of business day from discovery.	No deadlines specified.	72 hours from the time of a suspected data breach.
Enforcement & Compliance.	ICT suppliers face daily fines of up to 1% (for 6 months) of their prior years global turnover .	Each member state's supervisory authority determines appropriate fines.	Fines maybe imposed by data commissioners of up to €20m or 4% of global ann turnover.
Sector Specific Rules.	Focused on EU financial services and their ICT suppliers.	Focused on vital interest orgs know as essential and important entities.	EU extra-territorial scope covering any controller or proccessor of EU citizen personal data.
Alignment & Interaction.	DORA is similar to NIS but is mandatory and has more specifity than GDPR for FS firms.	NIS is a directive with more general security requirements than DORA or GDPR.	GDPR is more legalistic by nature with a focus on rights, notifications and data protection.

Fonte: DORA Introduction Presentation | Learn about the new rules quickly (data-privacy.io)

Un framework efficace per la gestione delle terze parti in ambito NIS2 e DORA deve integrare la gestione del rischio derivante da fornitori e terze parti ICT all'interno della strategia complessiva di risk management dell'organizzazione. Ecco gli elementi chiave di un tale framework, basati sulle normative e best practice europee:

- **Valutazione e gestione del rischio.** Il primo passo consiste nella valutazione approfondita dei rischi associati ai fornitori ICT, identificando vulnerabilità specifiche, qualità dei prodotti e delle pratiche di cybersecurity dei fornitori, incluse le loro procedure di sviluppo sicuro. Questa valutazione deve essere effettuata prima di instaurare o rinnovare contratti con terze parti e deve essere aggiornata durante tutto il rapporto contrattuale.
- **Integrazione nella strategia di risk management.** La gestione del rischio delle terze parti deve essere parte integrante della strategia complessiva di gestione del rischio dell'organizzazione, con obblighi specifici di registrazione, documentazione e monitoraggio continuo dei fornitori.
- **Contratti e clausole di sicurezza.** È fondamentale inserire clausole contrattuali che impongano ai fornitori il rispetto delle normative NIS2 e DORA, inclusi requisiti di sicurezza, audit regolari e obblighi di notifica in caso di incidenti di sicurezza. Questo permette di esercitare un potere contrattuale rilevante e garantire la conformità normativa.
- **Monitoraggio continuo e gestione degli incidenti.** Implementare un monitoraggio costante delle infrastrutture tecnologiche e delle terze parti per rilevare tempestivamente anomalie o minacce, affiancato da procedure specifiche per la gestione rapida ed efficace degli incidenti di sicurezza, con notifiche agli enti competenti come il CSIRT.
- **Piani di continuità operativa ICT.** Definire e testare periodicamente piani di continuità operativa che includano strategie di risposta e recupero

per mitigare l'impatto di eventuali incidenti o interruzioni causate da terze parti.

- **Formazione e sensibilizzazione.** Estendere le attività di formazione e sensibilizzazione sulla cybersecurity anche ai dirigenti e al management, per garantire una governance efficace della supply chain e responsabilità personali in caso di violazioni.

Per facilitare l'implementazione di questo framework, si possono adottare soluzioni software integrate che supportano la gestione dei processi di cybersecurity in conformità a NIS2, DORA, GDPR e standard internazionali come ISO 27001 e ISO 28000[B003], quest'ultimo focalizzato sulla sicurezza della supply chain.

In sintesi, un framework per la gestione delle terze parti in ambito NIS2 e DORA deve essere basato su una valutazione continua e integrata del rischio, contratti rigorosi con clausole di sicurezza, monitoraggio attivo, gestione degli incidenti, piani di continuità e formazione, il tutto supportato da strumenti e standard riconosciuti a livello europeo. Questo approccio garantisce una governance efficace della supply chain ICT e la conformità alle normative europee.

PROBLEMI ANCORA IRRISOLTI. La sinergia tra DORA e NIS2 offre un'opportunità per le aziende di sviluppare un approccio integrato alla cybersecurity. Tuttavia, la diversità degli ambiti e dei requisiti normativi può comportare sfide significative nella gestione della compliance. È essenziale che le organizzazioni adottino un modello di **"compliance integrata"** per navigare efficacemente tra le diverse normative e garantire una protezione robusta dei dati e delle operazioni. In sintesi, mentre DORA e NIS2 condividono obiettivi comuni in termini di sicurezza informatica, la loro integrazione richiede un'attenta considerazione delle specificità settoriali e delle misure richieste per ciascun ambito, tale integrazione potrebbe meglio esprimersi se le aziende fossero certificate ISO 27001 e/o ISO 28000. Come dicevamo, le attuali normative in ambito Cybersecurity prevedono che l'azienda fornitrice debba fare un controllo e una analisi rispetto alle proprie terze parti. Quindi, a valle di una gara, il fornitore deve includere clausole contrattuali richieste dai rispettivi uffici legali dei clienti in accordo con le loro strutture di Cybersecurity che prevedano la gestione del rischio cyber conforme alla propria postura aziendale.

POSSIBILI SOLUZIONI. Per affrontare la proliferazione di controlli e questionari in ambito cybersecurity, come evidenziato dalle normative NIS2 e DORA, è cruciale adottare un approccio integrato e standardizzato. Queste normative, pur fornendo indicazioni utili per i contratti di fornitura con terze parti, non stabiliscono formati uniformi per i controlli, il che può portare a inefficienze, duplicazioni e perdita di tempo nella gestione di una fornitura. Proponiamo a riguardo tre ipotesi risolutive:

- **Standardizzazione dei Controlli.** Una possibile soluzione consiste nell'implementare standard comuni per i controlli di sicurezza informatica. Questo potrebbe includere la creazione di un Framework di riferimento che tutte le aziende devono seguire, riducendo così la varietà di questionari e controlli richiesti dai diversi fornitori anche rispetto alle differenti tipologie di aziende.
- **Collaborazione tra Enti Regolatori.** È fondamentale che le autorità competenti collaborino per armonizzare le normative esistenti. Un'iniziativa congiunta tra NIS2, DORA e altre normative potrebbe facilitare l'integrazione dei requisiti e ridurre la complessità per le aziende.
- **Utilizzo di Framework già esistenti.** Adottare framework già esistenti, come il NIST (National Institute of Standard Technology) [B002] potrebbe offrire un modello utile. Il NIST ha già affrontato, diversi anni orsono, problematiche simili attraverso l'adozione di un approccio basato sulla gestione del rischio, incoraggiando le organizzazioni a valutare le proprie vulnerabilità e a implementare controlli proporzionati ai rischi identificati. In particolare incoraggia l'uso di pratiche di gestione del rischio che includono la valutazione continua delle terze parti e la revisione periodica dei contratti per garantire che i requisiti di sicurezza siano sempre aggiornati. Adottando queste strategie, è possibile migliorare l'efficacia della gestione della cybersecurity nelle relazioni con le terze parti, riducendo al contempo la complessità e il carico burocratico derivante dalla proliferazione di controlli. Nella pubblicazione SP 800-161r1, NIST offre una chiara ed efficace metodologia integrata globale di gestione del rischio cyber di una tipica Supply Chain operante nel settore della sicurezza informatica attraverso un modello organizzativo multilivello. La metodologia comprende le linee guida sullo sviluppo di piani di implementazione della strategia, le politiche, i piani e le valutazioni del rischio sui prodotti e servizi della Supply Chain.

La gestione dei rischi dinamici della sicurezza informatica lungo tutta la catena di fornitura è un'impresa complessa che richiede una necessaria trasformazione culturale e un approccio coordinato e multidisciplinare all'interno di un'impresa, nonché tecnologie avanzate di monitoraggio e controllo basate su ambienti di Cyber Threat Intelligence preferibilmente integrate con motori AI.

Bibliografia Utile

[B001] Gestione delle terze parti, Direttiva NIS e regolamento DORA: i problemi irrisolti - Rivista Cybersecurity Trends

[B002] Cybersecurity Supply Chain Risk Management (C-SCRM): un approccio dinamico - Rivista Cybersecurity Trends

[B003] ISO 28000:2022 - ISO 28000:2022 ■

Human Risk Management, psicologia del comportamento e Direttiva NIS2.

Autore: Veronica Patron

La Direttiva NIS2, approvata dall'Unione Europea nel 2022, ne prende atto in modo esplicito, ponendo l'attenzione sulla gestione dei rischi "di natura tecnica, operativa e umana". È qui che il concetto di *Human Risk Management* (HRM) incontra la psicologia comportamentale, offrendo alle organizzazioni un nuovo paradigma per costruire una cultura della sicurezza realmente efficace.

Perché le competenze cognitive sono il nuovo perimetro della sicurezza informatica

Nel panorama della cybersecurity, dove ogni giorno emergono nuove vulnerabilità tecniche, il rischio più subdolo resta quello legato al comportamento umano.

L'anello debole è prevedibile: comprendere l'errore umano

Nel lessico della sicurezza informatica, il "fattore umano" è spesso descritto come "l'anello debole della catena". Ma l'errore umano non è un evento casuale o sfortunato. È, molto più spesso, il risultato prevedibile di

BIO

Veronica Patron è psicologa specializzata in psicologia cognitiva e comportamentale, con una formazione accademica presso l'Università degli Studi di Padova, dove ha conseguito la laurea in Psicologia. Ha successivamente approfondito le tematiche di behavioral design, scienze decisionali e psicologia applicata alla cybersecurity, partecipando a corsi di alta formazione e programmi internazionali. Nel 2022 ha co-fondato Security Mind, piattaforma focalizzata sull'Human Risk Management in ambito cyber, dove ricopre il ruolo di Responsabile della Strategia Comportamentale. All'interno del team multidisciplinare, Veronica guida la progettazione di percorsi formativi basati su modelli scientifici, con l'obiettivo di trasformare i comportamenti a rischio in abitudini sicure e sostenibili. Partecipa regolarmente a conferenze e seminari sul tema del fattore umano nella sicurezza informatica, ed è autrice di articoli e contenuti divulgativi sul ruolo della psicologia nella prevenzione delle minacce digitali.

bias cognitivi, sovraccarico decisionale, automatismi e pressioni ambientali. In altre parole: non si tratta di ignoranza o disattenzione, ma di meccanismi psicologici naturali che, se ignorati, possono rendere inefficaci anche le difese tecnologiche più avanzate.

Un esempio emblematico è il phishing: anche dipendenti ben formati possono cliccare su link dannosi in condizioni di stress, urgenza o multitasking. Il problema non è la mancanza di conoscenze, ma l'incapacità del contesto lavorativo di supportare decisioni sicure in tempo reale.

La Direttiva NIS2: un cambio di paradigma anche per la formazione

La Direttiva NIS2 (Direttiva UE 2022/2555) impone agli Stati membri e alle organizzazioni "essenziali" e "importanti" nuovi obblighi in termini di governance del rischio. L'articolo 21, in particolare, richiede che le entità adottino misure tecniche, operative e organizzative adeguate alla gestione dei rischi, "inclusi quelli relativi al fattore umano".

Non è più sufficiente "fare formazione una tantum": la NIS2 apre la strada a un modello più maturo di gestione del rischio, che include la valutazione dei comportamenti, la modifica degli schemi decisionali e l'integrazione del fattore umano nei processi di sicurezza.

Human Risk Management: dalla formazione alla trasformazione comportamentale

Il concetto di *Human Risk Management* si fonda sull'idea che la sicurezza informatica non sia solo una questione tecnologica, ma un fenomeno socio-cognitivo. Non basta trasmettere nozioni; occorre trasformare abitudini, atteggiamenti, automatismi. E per farlo, serve un approccio mutuato dalle scienze comportamentali.

A differenza della formazione tradizionale, spesso teorica e poco memorabile, l'HRM si concentra su:

- **analisi comportamentale dei rischi umani** (es. risposta a phishing simulati, uso scorretto di dati e password);
- **interventi basati su principi psicologici**, come il *nudging*, il rinforzo positivo, la ripetizione distribuita e il contesto decisionale;
- **personalizzazione dei contenuti** in base a ruolo, rischio e stile cognitivo dell'utente;
- **integrazione tra security awareness**, cultura aziendale e processi decisionali quotidiani.

Psicologia comportamentale e sicurezza: una nuova alleanza

Le scienze comportamentali offrono strumenti preziosi per ridurre il rischio umano. Alcuni concetti chiave:

- **Bias cognitivi:** errori sistematici nel giudizio (es. effetto di familiarità, overconfidence) possono portare l'utente a sottovalutare segnali di pericolo.
- **Effetto framing:** la modalità con cui viene presentata un'informazione ne modifica la percezione (es. un alert "urgente" attiva risposte impulsive).
- **Nudging:** piccoli interventi che, senza imporre, "spingono dolcemente" verso scelte più sicure (es. impostazioni predefinite sicure, notifiche contestuali).
- **Habituation e memoria implicita:** contenuti ripetuti con varietà aumentano la memorizzazione rispetto a una singola sessione intensiva.

Integrare questi elementi nei percorsi di HRM significa passare da un approccio "comunicativo" a uno trasformativo.

Oltre il training: come misurare il rischio umano

Uno dei limiti storici della formazione alla sicurezza è la scarsa misurabilità. L'HRM propone invece una logica data-driven, dove il rischio umano diventa quantificabile attraverso indicatori specifici:

- **behavioral Risk Score** individuale o di gruppo;
- **tassi di risposta a campagne simulate** (es. clic su phishing);
- **livello di engagement nei contenuti formativi**;
- **prontezza nella risposta a incidenti simulati**;
- **miglioramento progressivo nel tempo** (riduzione dell'esposizione comportamentale).

Questi dati, aggregati e anonimizzati, consentono di costruire una mappa dinamica del rischio umano all'interno dell'organizzazione, utile sia per azioni correttive mirate sia per finalità di audit e conformità.

La sicurezza come comportamento collettivo

Uno degli aspetti più innovativi dell'approccio HRM è l'idea che la sicurezza sia un *comportamento collettivo*, non solo individuale. Cultura, leadership, comunicazione interna, ambienti digitali e pratiche di lavoro influenzano profondamente la sicurezza quotidiana.

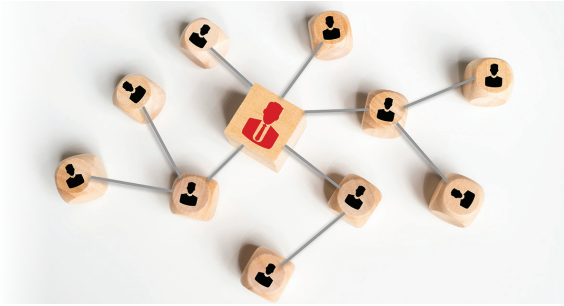
Promuovere la cultura della sicurezza significa:

- coinvolgere **tutti i livelli aziendali**, dal top management ai neoassunti;
- integrare la sicurezza nei **processi di onboarding, change management e gestione del personale**;
- valorizzare le **reti informali**, i modelli di ruolo interni e il feedback continuo.

Solo così si costruisce un contesto in cui comportarsi in modo sicuro diventa la norma, non l'eccezione.

Conclusione: un'opportunità culturale e normativa

La NIS2 non rappresenta solo un obbligo regolatorio, ma l'opportunità per ripensare il ruolo delle persone nella sicurezza informatica. L'*Human Risk Management*, fondato sulla psicologia comportamentale, offre gli strumenti per costruire non solo utenti "formati", ma persone capaci di agire responsabilmente in un contesto digitale complesso.



In un mondo dove il rischio non è più solo tecnologico ma umano-comportamentale, il vero perimetro della sicurezza è nella mente di chi ogni giorno prende decisioni. E il futuro della cybersecurity passa – inevitabilmente – dalla capacità di comprenderla, misurarla e trasformarla. ■

Procedure di gara: serve un esercizio di intelligenza condivisa.

Autore: Massimiliano Cannata

La **Fondazione ICSA** ha deciso di accendere i riflettori su un ambito particolarmente delicato, quale quello dell'impiego del denaro pubblico, promuovendo un dibattito sul tema: ***L'intelligenza artificiale nelle procedure di gara: rischi, opportunità e limiti per il comparto difesa e sicurezza*** che si è svolto a Roma lo scorso 18 agosto.

Tra le questioni esaminate dagli esperti figurano: l'ottimizzazione della gestione delle risorse pubbliche, la semplificazione delle procedure, la riduzione dei tempi di esecuzione delle gare, il miglioramento dei processi di verifica dei requisiti di partecipazione, nonché la riduzione degli errori di calcolo e di attribuzione dei punteggi. "Con l'IA – ha detto il **Presidente della Fondazione ICSA, il Generale Leonardo Tricarico** – si sta verificando quanto già successo con il fenomeno del cybercrimine: ne parlano tutti ma pochi hanno la consapevolezza del cambio di passo che comporterà nella vita di tutti i giorni. L'intelligenza generativa è la "Garlasco" della tecnologia - mi si passi l'immagine - perché sembra che ognuno abbia una ricetta, ma non emergono ancora delle pratiche attuative rigorose che offrano indicazioni chiare a chi opera nelle istituzioni e nelle imprese. Si tratta di un aspetto urgente, che siamo chiamati ad affrontare se vogliamo migliorare l'efficienza e la qualità dei sistemi produttivi e delle informazioni, che sono il petrolio della società digitale". Tricarico ha sottolineato la drammaticità di eventi come quelli che si stanno consumando sotto i nostri occhi a Gaza, spesso presentati attraverso racconti manipolati, che bisogna disinnescare se vogliamo almeno tentare di comprendere quello che sta accadendo.

Grandi inchieste come Ustica, da tempo oggetto di studio della Fondazione ICSA, se si "applicasse l'IA – ha commentato Tricarico - utilizzando milioni di dati che abbiamo a disposizione, probabilmente si arriverebbe a una conclusione; ma quella conclusione, senza la mediazione dell'uomo, sarebbe - possiamo dire con certezza - fuorviante".

La digitalizzazione della PA apre un nuovo orizzonte

È evidente che, se si prova a traslare gli esempi addotti a quanto avviene - e potrà avvenire - nella Pubblica Amministrazione, si apre un orizzonte nuovo, fatto di rischi ma anche di opportunità. Nel corso del convegno è stata offerta una panoramica dettagliata dei limiti e dei rischi potenziali legati alla automazione dei processi. "Garantire trasparenza e congruità delle gare è per noi prioritario – ha commentato in via generale - **Anna Maria Dominici presidente UNIV** (Unione Nazionale Imprese di Vigilanza e Servizi di Sicurezza, n.d.r.) – soprattutto in un ambito come quello della sicurezza, in

BIO

Massimiliano Cannata (Palermo, 1968), Filosofo, giornalista Professionista, autore televisivo, svolge attività di consulenza nell'ambito della comunicazione d'impresa. Membro del Comitato scientifico di "Anfione e Zeto",collabora con"TechnologyReview", "L'impresa", "Il Giornale di Sicilia", "Centonove Press".E' autore di numerosi saggi sui temi della social innovation, della formazione, dello sviluppo organizzativo e manageriale.

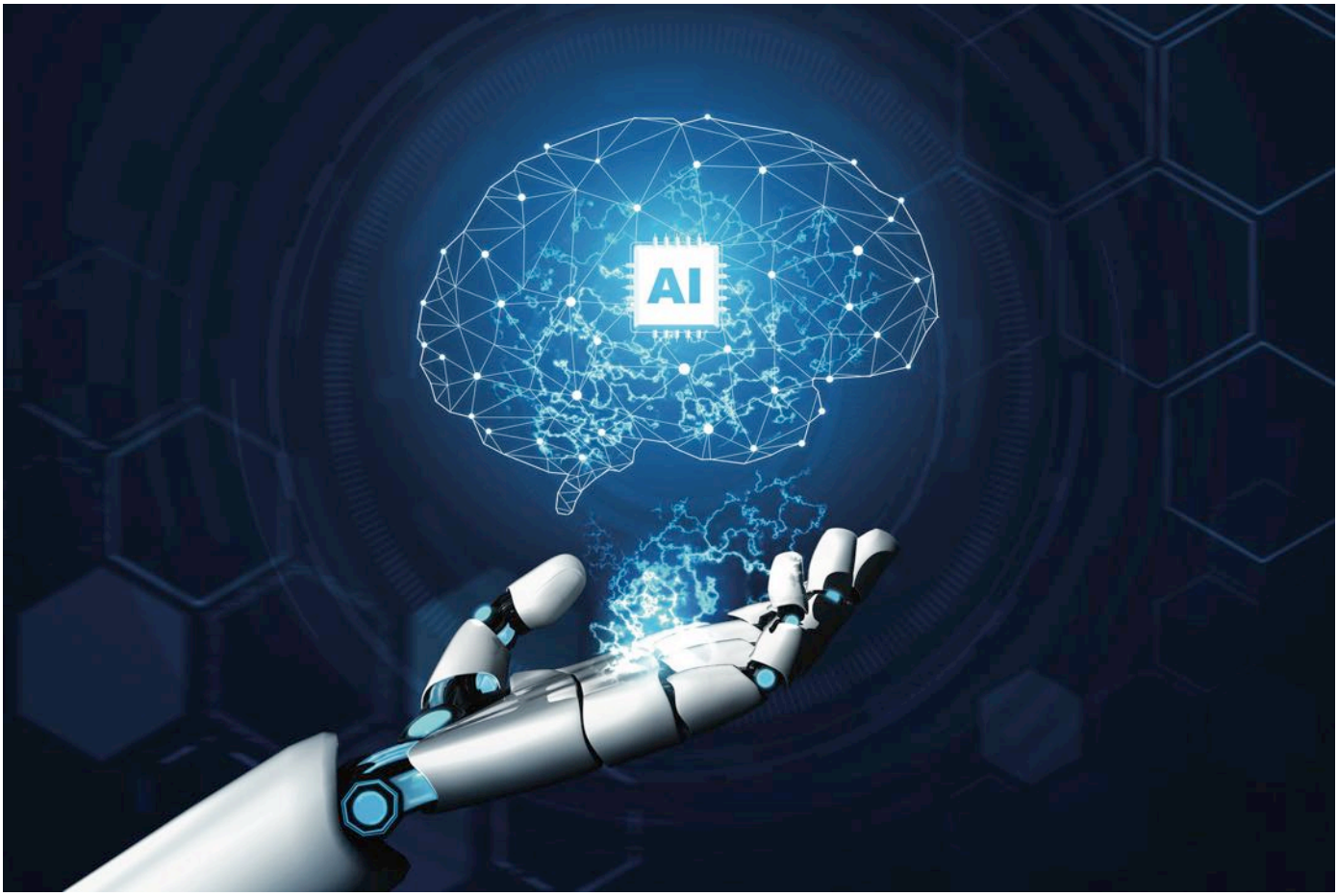
cui, come è noto, i servizi vengono affidati attraverso procedure di appalto pubblico e privato. La storia del settore – prosegue nell'analisi Dominici – ci ha mostrato capitolati mal scritti, talvolta persino viziati da illegittimità, e assegnazioni discutibili, quantomeno sotto il profilo dell'adeguatezza dell'offerta. Come UNIV guardiamo perciò con interesse a qualunque forma di automatizzazione che possa migliorare i processi di verifica e controllo che devono caratterizzarsi per equità nei trattamenti".

"Appare evidente - aspetto su cui tutti i relatori hanno trovato un punto di convergenza – che la IA non può essere la panacea. La supervisione umana e il lavoro dei funzionari non potrà essere sostituito né aggirato dalla macchina - ha puntualizzato **Italo Saverio Trento, Direttore della Fondazione ICSA**. Rimane centrale la capacità professionale di ogni singolo attore dell'organizzazione, così come la sovranità del giudice amministrativo, chiamato a disciplinare dal punto di vista dell'applicazione normativa, una materia che certo scotta".

La voce degli esperti

Per trattare il tema dell'**"IA al servizio della decisione amministrativa",** sono intervenuti il **Gen. B.A. Pietro Spagnoli**, Comandante Terza Divisione del Comando Logistico dell'Aeronautica Militare, il **Dott. Mario Nobile**, Direttore Generale Agenzia per l'Italia Digitale (AgID). Il tema **"Governance, etica ed applicazioni dell'IA: cooperazione uomo-macchina e riserva di umanità"** è stato affrontato dal **Prof. Nicola Lettieri**, Docente di Intelligenza Artificiale e Diritto, Università degli Studi del Sannio, dal **Dott. Paolino Madotto**, Consigliere scientifico ICSA e CEO Intelligentiae srl, dal **Dott. Maurizio Pulcini**, Management Advisor IFI srl, dall'Avv. Gaetana Natale, Avvocata dello Stato e dal **Gen. S.A. (r) Fernando Giancotti**, già Presidente Centro Alti Studi per la Difesa.

Ha moderato i lavori l'**Ing. Gianfranco Ciccarella**, Consigliere scientifico ICSA, mentre le conclusioni sono state affidate al **Sen. Francesco Paolo Sisto**. ■



Per regolare il prepotente sviluppo dell'IA, bisogna mettere a confronto culture giuridiche e sistemi-Paese.

Intervista VIP a Giusella Finocchiaro.

Autore: Massimiliano Cannata

Regolare lo sviluppo del digitale rappresenta un compito estremamente arduo per il legislatore, chiamato a sintonizzarsi con le dinamiche evolutive di un mondo che cambia a una velocità mai sperimentata prima. ***Giusella Finocchiaro***, professore ordinario di Diritto privato e di Diritto di Internet dell'Università di Bologna, da sempre impegnata a livello nazionale e internazionale su questa complessa frontiera. L'analisi contenuta nel suo ultimo saggio, *Diritto dell'intelligenza artificiale* (ed. Zanichelli), va oltre il complesso ambito della giurisprudenza di settore, affrontando la stretta correlazione che intercorre tra sviluppo tecnologico, equilibri geopolitici e crescita economica. Colpisce la sua capacità di visione interdisciplinare del governo del mondo.

Prof.ssa Finocchiaro, la tecnoscienza corre e trasforma le nostre vite, modificando comportamenti, relazioni e abitudini: siamo dentro un grande "cantiere" aperto. La legislazione europea sta rispondendo adeguatamente a queste sollecitazioni?

Il vecchio Continente ha deciso di rispondere costruendo una propria "sovranità digitale", partendo dalla consapevolezza che questo settore sarà decisivo per le future prospettive di crescita. Il processo di normazione può essere ricondotto alla "direttiva madre" sulla protezione dei dati personali del 1995 e alla normativa sulle firme elettroniche del 1999. Oggi, l'identità digitale è regolata con il Regolamento *e-IDAS 2*; la protezione e la valorizzazione dei dati personali dal *GDPR*, dal *Data Act*, dal *Data Governance Act* e dal Regolamento sullo Spazio europeo dei dati sanitari; l'ambito dei servizi digitali e del mercato digitale dal *Digital Services Act* e dal *Digital Markets Act*; infine, l'intelligenza artificiale è disciplinata dal recente *AI Act*.

Come si colloca l'Italia in questo quadro così articolato?

Siamo a uno stadio piuttosto evoluto. Il nostro Paese può infatti vantare una tradizione giuridico-normativa in ambito digitale che risale all'inizio degli anni Novanta, con un impegno costante confermato anche dall'agenda della Camera, attualmente al lavoro per licenziare un disegno di legge sull'intelligenza artificiale.

Le basi della Costituzione europea

In una recente intervista rilasciata alla nostra testata, Franco Pizzetti, a proposito dell'eccezionale sviluppo del digitale, ha commentato:

"Regolare il digitale significa porre le basi per la Costituzione europea". *Qual è il suo pensiero in merito?*

Nel contesto geopolitico globale, la strategia perseguita dall'Unione europea è quella di porsi come *leader* nella produzione normativa, per far sì che il modello continentale diventi un riferimento globale e possa essere adottato anche in altre regioni del mondo. Quella che si intende affermare, come accennavo prima, è una "sovranità digitale" sia esterna - rivolta agli altri attori globali, in particolare USA e Cina – sia interna, perché gli effetti delle misure legislative ricadono sugli Stati membri dell'unione. In questo processo emerge con chiarezza l'esigenza, del tutto comprensibile, di affermare un modello innovativo, evitando la frammentazione, che rappresenta sempre un pericolo incombente.

Guardando all'intelligenza artificiale, tema centrale del suo interessante saggio, quali indirizzi metodologici andrebbero seguiti e quali aspetti potrebbero essere oggetto di normazione in una materia così delicata?

Regolare l'IA non è un compito di poco conto, se si pensa all'estrema ampiezza dell'oggetto da disciplinare. Occorre innanzitutto chiedersi se sia opportuno, per il legislatore, adottare un approccio volto a regolamentare l'intelligenza artificiale nel suo complesso, oppure concentrarsi sulle applicazioni dell'intelligenza artificiale in specifici settori o ambiti tematici. La prima opzione è quella adottata dal Regolamento europeo sull'intelligenza artificiale, che presenta infatti un approccio normativo orizzontale. La seconda è quella auspicata da alcune organizzazioni internazionali, secondo cui si sarebbe preferibile regolamentare le applicazioni sull'intelligenza artificiale - o, più precisamente, i loro effetti – in specifici ambiti. La questione fondamentale sottesa alla scelta tra i due approcci riguarda lo scopo della regolazione. Le strade possibili sono due: da un lato, dettare regole nuove per un fenomeno inedito; dall'altro, limitare l'intervento normativo a quanto strettamente necessario per superare o rimuovere gli ostacoli giuridici all'utilizzo della tecnologia.

Per il giurista qual è la strada preferibile?

Non c'è una strada giusta in assoluto: bisogna considerare che gli ambiti del diritto che intersecano la regolazione dell'intelligenza artificiale sono molteplici - dalla protezione dei dati personali trattati da sistemi di intelligenza artificiale, al diritto d'autore, dalla responsabilità civile a quella penale. Si tratta di una materia estremamente articolata, che richiede una visione di insieme e una grande capacità di coerenza disciplinare. Con l'*AI Act*, il legislatore europeo ha inteso salvaguardare non soltanto i diritti fondamentali, ma anche i "valori" europei. Quest'ultimo aspetto è richiamato più volte nel Regolamento, a sottolineare che il modello elaborato non è solo normativo, ma anche culturale. Non si tratta soltanto di regole giuridiche, ma anche della cultura che esse esprimono.

BIO

Giusella Finocchiaro è Professoressa ordinaria di diritto di internet e di diritto privato nell'Università di Bologna e socio effettivo dell'Accademia delle Scienze dell'Istituto di Bologna. Vanta una pluridecennale esperienza professionale. Affianca alla carriera accademica numerose collaborazioni di carattere scientifico. Tra le altre, è stata membro dell'UNCITRAL (Commissione delle Nazioni Unite per il Diritto del Commercio Internazionale). Dal 2014 al 2022 è stata Presidente dell'UNCITRAL Working Group sul commercio elettronico, ove oggi è rappresentante italiana. È membro della Commissione intelligenza artificiale per l'informazione istituita dal Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei Ministri. È esperta legale presso la Banca Mondiale e UNIDROIT nel "Digital Assets and Private Law Project". È Consigliere indipendente nel Consiglio di Amministrazione di Unipol Assicurazioni S.p.A. È membro del Comitato di Direzione della rivista "Contratto e Impresa" e del Comitato Scientifico della rivista "DIMT". Dirige l'area "Soggetti e nuove tecnologie" della rivista "Giustizia civile". È membro del Comitato di Direzione della "Rivista di Diritto Sportivo" e del Comitato Scientifico della rivista "Diritto dell'Internet", della "Rivista italiana di informatica e diritto" e della "Rivista di diritto dei media". È autrice e curatrice di numerose pubblicazioni dell'informatica e di Internet.

La Privacy come fondamento della società dell'informazione

Lei segue da sempre i temi della privacy in un'ottica autenticamente globale. Molto è cambiato dalla fase che potremmo definire 'fondativa', tracciata da Stefano Rodotà, alla complessità dello scenario attuale. L'IA ha impresso un'ulteriore accelerazione, segnando un vero e proprio "salto quantico" nella rivoluzione in atto. Con quali conseguenze giuridiche?

L'intelligenza artificiale si basa sui dati e, pertanto, la protezione dei dati personali deve essere affrontata con rigore quando si tratta di questa materia. Le questioni in gioco sono molteplici. Il primo aspetto che emerge è il contrasto tra l'esigenza di disporre di un'ingente mole

di dati ai fini dello sviluppo di sistemi di intelligenza generativa e la necessità, opposta, di rispettare il principio di minimizzazione previsto dal GDPR, secondo cui il trattamento dovrebbe avere ad oggetto soltanto le informazioni strettamente necessarie e pertinenti in relazione alle finalità perseguite. Inoltre, poiché l'IA si nutre soprattutto di grandi masse di dati, la qualità di questi ultimi diventa un fattore essenziale. Da dati qualitativamente non corretti non possono, infatti, che derivare elaborazioni non corrette, secondo il noto principio *"garbage in, garbage out"*. Ma attenzione: i punti di frizione tra IA e la disciplina a tutela dei dati personali non si esauriscono a questi esempi presi in esame. Sarà infatti necessario un grande lavoro di coordinamento tra queste norme, che porterà - è facile prevederlo - a una revisione del GDPR.

Allarghiamo lo sguardo: diritto, cultura e tecnologia, in una delicata fase di trasformazione come quella che stiamo vivendo, in che rapporto dovrebbero stare?

Il diritto, come la cultura, è espressione del tempo storico in cui viviamo. La tecnologia va regolata, seguendo principi chiari e condivisi. Tuttavia, la pressione del quotidiano e le urgenze che connotano ogni nostra attività spingono all'adozione di immediate "istruzioni per l'uso". Se dovesse prevalere questa tendenza il rischio - molto serio - è quello che i giuristi definiscono *"over-regulation"*. Il giurista, però, non può cedere a questa tentazione, abdicando al proprio compito interpretativo e delegando tutto alla logica della compliance.

Il doppio legame tra diritto e geopolitica

Non si tratta di disquisizioni giuridiche astratte, quelli che Lei pone, se si considera la ricaduta che l'impianto giuridico–normativo avrà non solo sugli assetti del capitalismo - che sta mutando profilo - ma anche su quelli geopolitici, come dimostra la competizione innescata tra sistemi-Paese. Europa, Stati Uniti e Cina si muovono in uno scacchiere globale in cui si osserva una pericolosa commistione tra potere e tecnologia. Il fenomeno della tech right è emblematico sotto questo profilo. Riusciremo a trovare un punto di equilibrio tra la spinta ineludibile all'innovazione e i principi dello Stato di diritto, che sembrano vacillare in questa tormentata fase della storia?

Il mercato delle nuove tecnologie, e in particolare quello dell'intelligenza artificiale, è senza dubbio un mercato globale, privo di barriere geografiche, e appare sostanzialmente diviso in tre aree di influenza: quella europea, quella statunitense e quella cinese. Il modello adottato in Europa è di tipo regolatorio: l'obiettivo non solo normare e disciplinare i nuovi fenomeni, le tecnologie emergenti e i beni digitali, ma anche promuovere il cosiddetto "effetto Bruxelles", ovvero proporre il modello europeo come riferimento globale. Il modello adottato negli Stati Uniti, dovendo semplificare, è un modello co-regolatorio, basato principalmente sull'antitrust. Il modello cinese, invece, appare un modello dirigistico e basato sul capitalismo di Stato. Trovare un punto di incontro tra questi diversi approcci non è certo facile, ma è necessario. Diverse organizzazioni internazionali si stanno muovendo in questa direzione, a cominciare dall'UNCITRAL (la Commissione delle Nazioni Unite per il diritto del commercio internazionale, presso cui la professoressa Finocchiaro rappresenta l'Italia, n.d.r.), cui si è aggiunta di recente la Convenzione sull'IA stipulata dal Consiglio d'Europa.

United Nations
UNCITRAL

Di cultura del diritto abbiamo già ampiamente parlato. "Responsabilità" è l'altro termine critico. Che valenza assume questo concetto nella società digitale?

È un concetto essenziale. L'intelligenza artificiale è uno strumento estremamente utile e potente, ma è necessario che chi la utilizza lo faccia con responsabilità. Sul piano giuridico, la questione che si pone più frequentemente riguarda l'individuazione del soggetto responsabile in caso di danni cagionati da applicazioni di IA. In particolare, l'attenzione si concentra sui casi in cui l'esito dell'elaborazione generata da sistemi di intelligenza generativa non sia del tutto controllabile a priori, e presenti un certo grado di imprevedibilità. Mi riferisco ai quei casi in cui il processo non ha una natura prettamente deterministica, ma è caratterizzato da una certa autonomia elaborativa. In queste situazioni, chi è il responsabile? Il fornitore? Il distributore? L'utilizzatore? O il sistema di IA stesso?

Come si rivolve il dilemma?

Si può cercare di adottare regole già esistenti per disciplinare un fenomeno nuovo, oppure andare verso l'elaborazione di nuovo paradigma normativo. Inoltre, potrebbe rivelarsi opportuno adottare un modello di responsabilità fondato su un sistema puro di allocazione del rischio, prescindendo dalla ricerca dell'errore, e ripartendo i costi tra i soggetti coinvolti nell'operazione economica in modo collettivo. In quest'ottica, si potrebbe ipotizzare la costituzione di un fondo, ovvero la formulazione di meccanismi di assicurazione in carico ai soggetti che potrebbero essere chiamati a risarcire il danno. Come si può notare, la materia è molto ampia e complessa, e va affrontata con consapevolezza, equilibrio, competenza e nel rispetto della diversità delle culture giuridiche che si confrontano nel panorama internazionale. ■

La cultura, valore prezioso per l'impresa.

Intervista VIP a Valentina Martino.

Autore: Massimiliano Cannata

BiblHuB Sapienza, la biblioteca delle imprese e delle organizzazioni è una realtà unica e preziosa, che raccoglie il patrimonio editoriale che le aziende hanno prodotto segnando la storia degli ultimi due secoli. Valentina Martino, Professore Associato de La Sapienza, docente di Comunicazione Organizzativa e di Corporate, è responsabile del progetto.

Prof.ssa, le pubblicazioni di pregio custodite nella "sala rossa" dell'Ateneo più grande d'Europa sono ancora poco conosciute dal grande pubblico. Di recente avete organizzato un grande evento dedicato: con quali finalità?

La prima finalità ha una natura divulgativa. BiblHuB Sapienza dal 2018 raccoglie, conserva e valorizza, nelle sue molteplici espressioni, il patrimonio librario edito per iniziativa diretta di imprese e organizzazioni. Si tratta di testimonianze importanti, purtroppo ancora poco studiate e spesso effimere, attraverso cui è possibile leggere la storia industriale del Novecento. Stiamo cercando di rendere questo patrimonio fruibile a un pubblico di studenti, studiosi, addetti ai lavori e appassionati, che merita di essere consultato. Molte tesi di laurea hanno cominciato a utilizzare queste fonti, e credo che in futuro questa attenzione sia destinata a crescere.

In più occasioni Lei ha sottolineato l'inadeguata conoscenza di questi "giacimenti" per lo più inesplorati. Come si spiega questo "deficit"?

Dobbiamo pensare che molte delle pubblicazioni che il Dipartimento di Comunicazione e Ricerca Sociale de La Sapienza sta catalogando e conservando non erano destinati alle biblioteche, perché di prassi seguivano percorsi diversi. Alcuni volumi aziendali, come quelli a carattere celebrativo, non erano neanche catalogati con il codice universale identificativo (ISBN: *International Standard Book Number,* n.d.r.) che viene ufficialmente utilizzato in tutto il mondo per la registrazione degli scritti editi. Altri, come i cosiddetti "libri strenna", venivano donati alle grandi istituzioni e ai grandi clienti, altri ancora rientravano nei percorsi di comunicazione interna, e come tali non erano destinati alla fruizione del pubblico. Per queste ragioni il materiale che abbiamo recuperato era destinato all'oblio, mentre proprio la "Terza missione" ci spinge a intrecciare un rapporto sempre più forte con la cultura d'impresa al fine di rendere più completa l'offerta formativa dell'Ateneo.

L'esempio di Olivetti e l'insegnamento di Ferrarotti

Quello che sta prendendo corpo si può definire come "museo dinamico" della cultura di impresa", che vede coinvolte diverse aree geografiche e molteplici attori della ricerca e dell'imprenditoria?

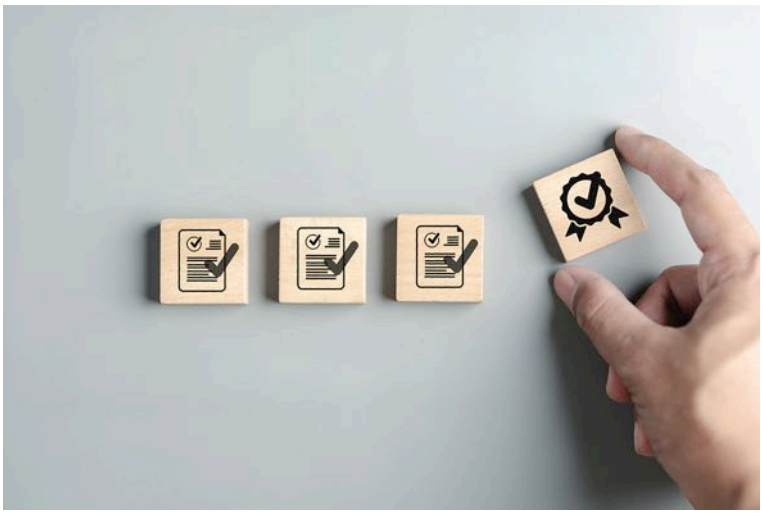
Il lavoro di ricognizione, catalogazione e raccolta, a cui facevo prima riferimento, non è fine a se stesso, perché di fatto sta spingendo le intelligenze imprenditoriali, da Nord a Sud, a confrontarsi e dialogare. Abbiamo in Italia testimonianze importanti di vita e cultura d'azienda che costituiscono delle best practices in grado di fare scuola. Franco Ferrarotti (padre della sociologia italiana scomparso il 13 novembre del 2024, n.d.r.) offre una testimonianza preziosa sul valore del libro nella società digitale, che esprime in maniera perfetta il DNA di BiblHuB.

BIO

Valentina Martino (Ph.D.) è Professoressa associata di Sociologia dei processi culturali e comunicativi al Dipartimento di Comunicazione e Ricerca Sociale della Sapienza Università di Roma, dove insegna Comunicazione Organizzativa e di Corporate. È responsabile scientifica di BiblHuB Sapienza, biblioteca specialistica di ricerca dedicata alla cultura e comunicazione d'impresa, e dell'omonima serie editoriale per Sapienza Università Editrice. È membro del Debiasing and Lay Informatics DaLI Lab, network scientifico internazionale sullo studio dei pubblici e del loro comportamento coordinato dall'University of Oklahoma – Center for Applied Social Research. I suoi lavori sono pubblicati su volumi e riviste internazionali. Tra le monografie più recenti: *Olivetti e il libro, storia di un'impresa che diventa cultura* (Sapienza Università Editrice, 2024), in collaborazione con l'Associazione Archivio Storico Olivetti (AASO); e *Dalle storie alla storia d'impresa. Memoria, comunicazione, heritage* (Bonanno, 2013). Ha curato, con Alessandro Lovari, la prima traduzione ed edizione italiana dell'opera di James E. Grunig nel volume *Public (&) Relations. Teorie e pratiche delle relazioni pubbliche in un mondo che cambia* (Franco Angeli, 2016).

Soffermiamoci su questo. Franco Ferrarotti quando scrive di sociologia industrial fa riferimento alla figura di Adriano Olivetti, per cui ha anche lavorato nei primi anni della sua lunga esperienza intellettuale e lavorativa. Nello scorso aprile è stata ricordato l'anniversario della nascita dell'imprenditore di Ivrea (era nato l'11 aprile 1901, n.d.r.) Era un innovatore autentico, che credeva nel lavoro come fonte di benessere e nella cultura come motore dell'economia. Una modernità stupefacente, che cosa rimane di quell'insegnamento?

Rimane tutto valido. Ferrarotti lo ha spiegato, con l'energia intellettuale unica e irripetibile che lo caratterizzava, in una video intervista che abbiamo realizzato insieme a Marco Stancati. "Personalità complessa, Olivetti viveva il rispetto per il libro e la venerazione per la scrittura. Credeva nella parola scritta, era un uomo biblico non solo dal punto di vista teorico, perché anche nella prassi riteneva che all'operaio non fosse sufficiente limitarsi a pagare lo stipendio, occorreva preoccuparsi della sua formazione e del suo sviluppo interiore", non saprei dirlo meglio di Ferrarotti, perché è



proprio questa la sensibilità che il management sia pubblico che privato deve acquisire ed esercitare, per affermare quello che Vittorio Foa definiva "la libertà dentro il lavoro".

Quando l'impresa si fa cultura

Nel suo saggio* "Olivetti e il libro, storia di un'impresa che diventa cultura" *emerge molto bene il nesso che deve legare etica ed economia. Siamo maturi per comprendere il significato reale di questo binomio inscindibile?

Non spetta a me esprimere valutazioni di merito. Mi limito a dire che il ricordo di grandi figure come quelle cui stiamo facendo riferimento in questa conversazione deve fare da stimolo concreto per investire nella cultura d'impresa. Olivetti operò in questa direzione, allarmando anche gli azionisti di riferimento, comprensibilmente preoccupati del valore dei dividendi, più che della cultura. Non è facile comprendere che il salario deve contenere una componente immateriale, dalla connotazione morale, intellettuale. Per questa ragione il sapere, e il libro in particolare, doveva essere consultabile da parte di tutti. A Ivrea, biblioteca e servizi sociali facevano parte delle strutture aziendali, cosa che dovrebbe succedere anche oggi, nella società che con molta enfasi definiamo della conoscenza.

Quelle sperimentate nel canavese, negli anni olivettiani, si possono considerare forme di welfare avanzato?

Certamente, e aggiungerei che **andrebbero bene anche nella contemporaneità**. Tornare alla logica del libro e della lettura, al silenzio, alla solitudine della concentrazione, riducendo il potere ipnotico dell'immagine che crea rumore, sarebbe utile a tutti noi. Ci aiuterebbe, e mi rifaccio ancora a Ferrarotti, a recuperare l'interesse per il passato, mentre viviamo in una sorta di eterno presente, schiacciati sull'attualità. Abbiamo perso il gusto per leggere gli antefatti, per capire la ragione profonda dei fenomeni; siamo portati ad esaltare quella che Emanuele Severino chiamava "la cieca volontà di Potenza della tecnica", dimenticando che il valore della tecnologia ha una natura strumentale. Il nostro impegno sarà quello di curare questa sorta di *Alzheimer* collettivo, che corriamo il rischio di contrarre.

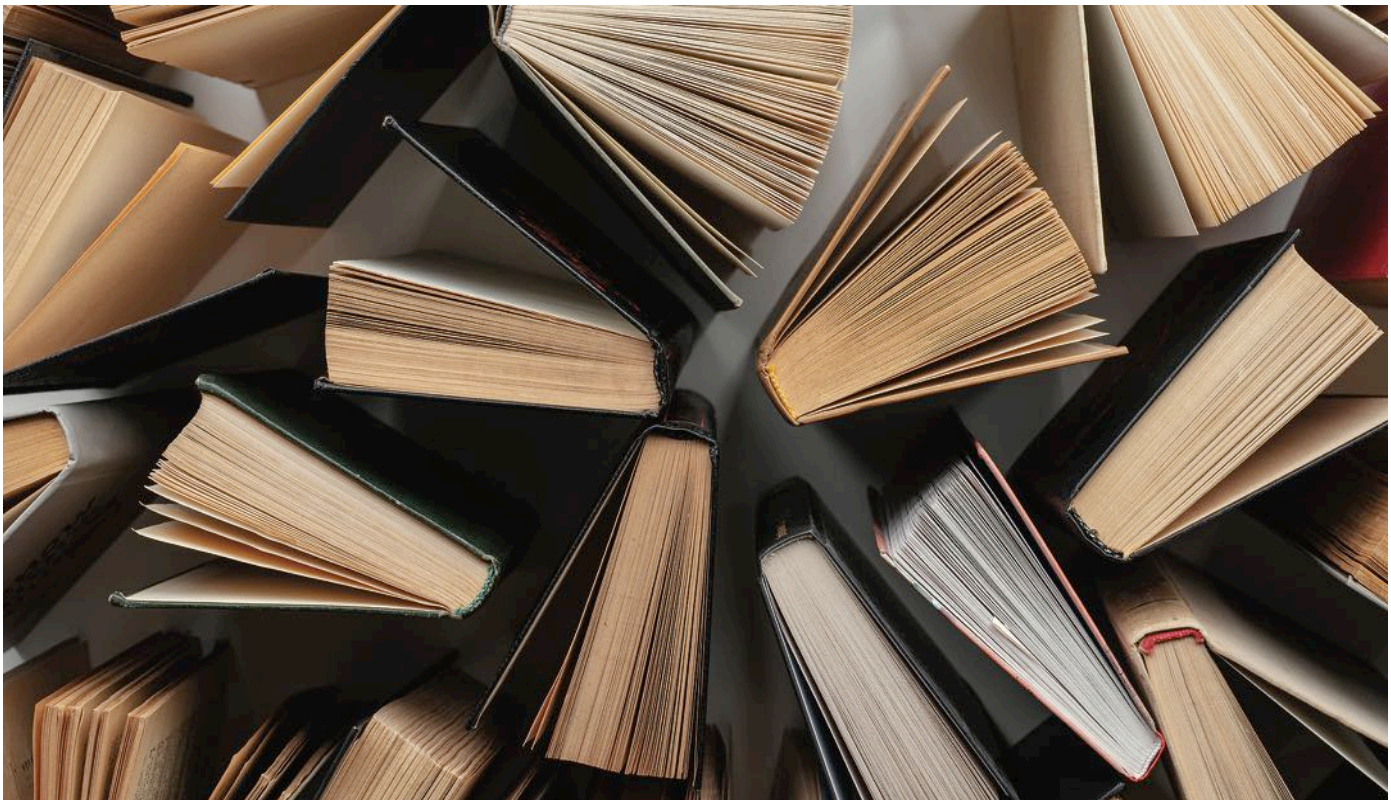
Lei è prorettrice con delega per la ricerca e innovazione, due termini-chiave ai quali non dedichiamo lo spazio che una civiltà evoluta dovrebbe assicurare. Quali sono le ragioni di una miopia difficilmente giustificabile?

Dobbiamo ricordarci che non siamo nulla senza memoria: ce lo hanno insegnato i grandi storici della scuola degli *Annales*, a partire della celebre affermazione di Fernand Braudel: "Essere stati è la condizione per essere". Olivetti si è mosso su quella scia, uomo della confluenza tra la tradizione ebraica salvifica messianica e quella valdese, protestante, fondata su un'etica vissuta e su una dirittura morale. Agire secondo questi principi vuol dire fare innovazione, perché senza memoria e cultura non siamo nulla, siamo destinati a non comprendere che l'uomo è un'impresa mai finita, un progetto in cui è l'altro, la circostanza, a chiamarci all'essere. La scrittura, parola sedimentata, segna il ritorno alla vita interiore. Torna ancora il libro, protagonista della nostra conversazione: un oggetto per nulla anacronistico, perché necessario a ritessere il dialogo tra le generazioni. Ricerca e innovazione devono trovare una spinta. Il libro dà una spinta "messianica" verso il cambiamento, perché trasporta i significati oltre il tempo effimero e rende perennemente vivo l'insegnamento degli spiriti magni, che da sempre tracciano la strada del nostro futuro.

Le chiedo, in conclusione: dove vuole arrivare BiblHuB?

Dopo tanti concetti vorrei dare un numero che li sintetizzi. Al momento sono circa 3600 le monografie aziendali, conferite alla Sapienza da più di 800 organizzazioni private, pubbliche e non profit di tutta

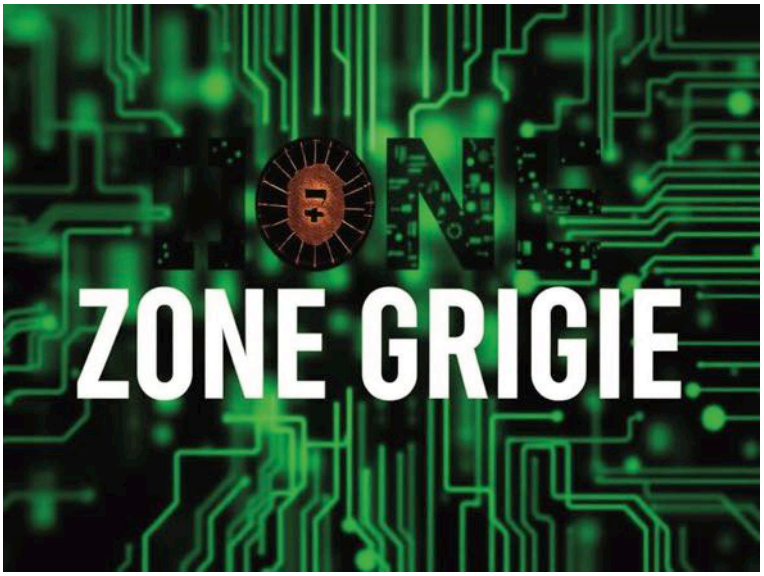
Italia. Non mancano alcune partecipazioni estere, che testimoniano un preciso impegno a internazionalizzare BiblHuB. Lo scorso anno abbiamo iniziato dalla Spagna. Come può vedere, la strada del futuro è già tracciata. ■



Cosa significa sicurezza oggi? "Zone grigie", la nuova collana di *Mimesis* lo spiegherà ai lettori.

Intervista VIP a Alessandro Curioni.

Autore: Massimiliano Cannata



"Percorsi di sicurezza digitale". Prof Curioni, con la sua guida tecno-scientifica nasce la collana "Zone Grigie" per l'editore Mimesis. Possiamo considerarla un'iniziativa in controtendenza, se pensiamo al declino della parola scritta, oggi evocato da più parti?

Sì, siamo in controtendenza e lo rivendichiamo con una certa convinzione. La collana *Zone Grigie* nasce proprio dalla consapevolezza che il digitale debba essere uno spazio capace di generare nuove ambiguità, tensioni e sfide culturali. In questo senso, la parola scritta — soprattutto quella riflessiva, argomentativa, problematizzante — non è superflua: è urgente. È ciò che consente di rallentare, comprendere, distinguere dove tutto tende a confondersi. In un mondo in cui la comunicazione è sempre più istantanea, performativa e guidata dagli algoritmi, *Zone Grigie* scommette sulla scrittura come forma di resistenza critica. Non si tratta di nostalgia per un passato cartaceo, ma di una scelta epistemologica: è nella scrittura che si sedimentano le domande complesse, che si esplora senza semplificare.

Possiamo enucleare gli obiettivi della collana che sta prendendo il via?

Primo: illuminare le zone d'ombra del digitale, dove la tecnica precede la norma, dove le decisioni non sono ancora codificate, dove i confini tra lecito e illecito, sicuro e vulnerabile, umano e automatizzato sono ancora mobili; secondo: colmare il divario tra sapere tecnico e consapevolezza culturale, offrendo contributi accessibili ma rigorosi che possano parlare al mondo accademico e professionale senza rinunciare a un orizzonte divulgativo; terzo: restituire alla scrittura la sua funzione generativa, come strumento per costruire pensiero, elaborare responsabilità e orientare scelte in un contesto che ci interpella tutti, quotidianamente. Non si tratta di essere contro "il presente", perché *Zone Grigie* cerca di leggerlo con più lucidità, per poterlo vivere con più libertà.

L'interdisciplinarietà appare come il "DNA" dell'iniziativa. Tecnologia, etica, società sono gli ambiti su cui insisterete. Qual è il* fil rouge *che consentirà di far convergere territori così complessi?

Il *fil rouge* è l'ambiguità stessa. O, meglio, l'ambizione di abitare l'ambiguità senza subirla. In *Zone Grigie* non cerchiamo di risolvere la complessità

riducendola a un solo linguaggio — tecnico, giuridico, filosofico — ma di attraversarla riconoscendo la legittimità e i limiti di ciascun punto di vista. La tecnologia è oggi il luogo in cui si decidono questioni profondamente umane: libertà, controllo, fiducia, identità, sicurezza. Non basta, dunque, parlarne "da dentro" l'informatica, né "da fuori" con uno sguardo etico o sociologico. Serve un approccio che sappia tradurre tra codici diversi, che sappia accogliere la frizione tra linguaggi come un'occasione generativa. Il *fil rouge* che ci guiderà sarà dunque la domanda: *"che cosa significa sicurezza oggi, per chi, contro chi e a quale prezzo?"*. È una domanda che ogni autore, qualunque sia la sua disciplina, è chiamato a declinare con strumenti propri ma in dialogo con gli altri.

La collana vuole essere uno spazio dove un giurista possa interrogare le zone d'ombra di un algoritmo, un ingegnere possa riflettere sulle implicazioni morali di una scelta architetturale, un filosofo possa misurarsi con la materialità del codice o della crittografia. Questo è possibile solo se si accetta che la sicurezza non è un fatto, ma un campo di forze: dinamico, conteso, attraversato da interessi, paure.

Il vero filo conduttore, allora, sarà cercare convergenza non nell'uniformità, ma nel confronto critico. *Zone Grigie* nasce per questo.

Nel comunicato stampa di presentazione si parla di uno "spazio di incertezza" - la zona grigia, appunto - che evoca, per molti aspetti, quella condizione culturale ed esistenziale connotata dal "pensiero debole" di Gianni Vattimo. Come ci si muove in queste aree sfumate, difficili da definire, entro cui spesso l'illecito prolifera?

Ci si muove con consapevolezza critica e con strumenti pluralistici, sapendo che le "zone grigie" non sono soltanto luoghi di indeterminatezza normativa o tecnica, ma sono, prima di tutto, luoghi interpretativi. In questo senso, sì, Vattimo ha ragione: la verità non è più univoca, ma debole e malleabile - nel senso che è sempre mediata, contestuale, soggetta a ridefinizione. In queste zone sfumate, la distinzione netta tra lecito e illecito, tra pubblico e privato, tra sicurezza e libertà, tra trasparenza e opacità, si fa porosa. Eppure, proprio per tale motivo, queste aree vanno indagate senza semplificazioni, né moralistiche né deterministiche. L'illecito non prolifera solo perché manca la legge, ma anche perché manca una comprensione adeguata dei contesti, delle tecnologie, delle intenzioni. Muoversi in queste zone non significa abbandonare ogni criterio, ma accettare che i criteri vanno continuamente ripensati. Significa riconoscere che non esiste un punto neutro da cui osservare il mondo digitale, ma che è necessario costruire spazi di confronto tra saperi diversi, tra pratiche diverse, tra visioni del mondo, anche conflittuali.

Quali sono le sfide della sicurezza in un contesto in cui il gioco (*the game*, per dirla con Alessandro Baricco) è mutato, ma è anche mutata la scacchiera entro cui business e potere si evolvono in un intreccio sempre più mediato dalla tecnologia?

La sfida è triplice, perché non è cambiato solo il gioco: è cambiato chi gioca, dove si gioca e secondo

BIO

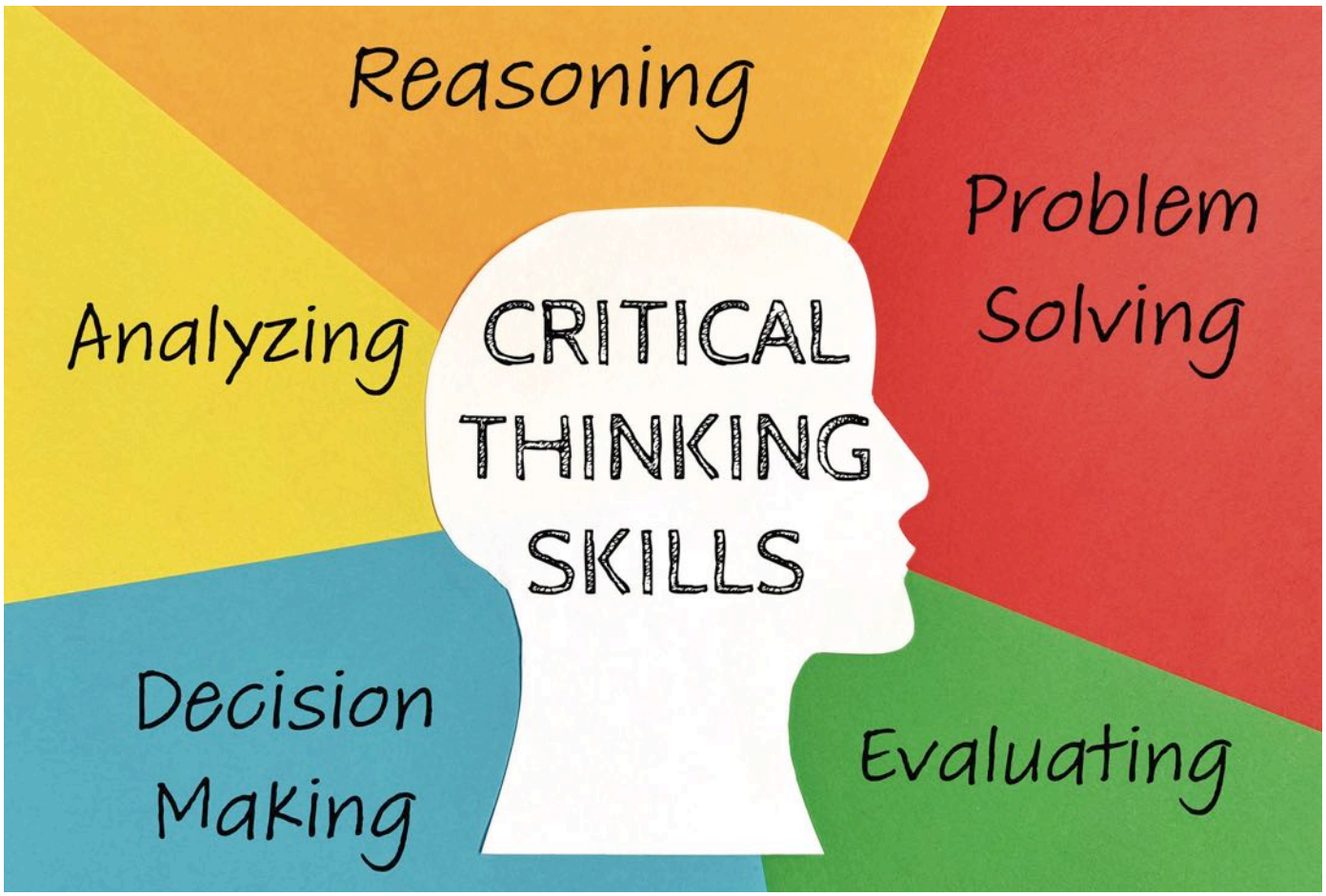
Dopo 15 anni di attività giornalistica, alla fine degli anni Novanta, Alessandro Curioni inizia a occuparsi di nuove tecnologie e nel 2001 si dedica a tempo pieno alle tematiche della sicurezza informatica. Nel 2003, dopo due anni di studio, pubblica per Jackson Libri il volume "Hacker@tack - Guida alla sicurezza informatica". Da questa esperienza nasce, in collaborazione con il Gruppi I.Net (in seguito British Telecom) un programma di corsi di formazione dedicati a quelle tematiche. All'attività di formatore affianca quella di consulente per i clienti del gruppo I.Net, attività che si protrae fino al 2008, anno in cui fonda DI.GI. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della sicurezza informatica, della quale è azionista e presidente. Negli ultimi quindici anni è stato consulente per primarie aziende nazionali e multinazionali tra le quali Edison S.p.A., Cardif Assicurazioni del Gruppo BNP Paribas, Vittoria Assicurazioni, Pepsico Italia, attività che alterna con quella di formatore (ENI, Poste Italiane, A2A, etc.) e conferenziere. Nel 2015 riprende la sua attività pubblicistica per diverse testate cartacee - tra cui "Il Sole 24 ore" (compresi gli allegati sul tema) - e on line e nel 2016 pubblica, con la casa editrice universitaria Mimesis, il libro "Come pesci nella rete – Guida per non essere le sardine di Internet" dedicato a problemi della sicurezza informatica personale, a cui seguono diversi altri pamphlet di successo ("La privacy vi salverà la vita", "Questa casa non è un hashtag", "CyberWar" etc) mentre con Chiarelettere ha pubblicato nel 2021 il suo primo giallo intitolato "Il giorno del Bianconiglio". Dal 2018 Curioni è anche docente a contratto nel corso di sicurezza dell'informazione per la Cattolica di Milano.

quali regole non scritte. La sicurezza, in questo nuovo ecosistema, non può più essere concepita come una muraglia statica, ma come una pratica adattiva, fluida e strategica, che tiene conto delle nuove forme di potere distribuito, invisibile, spesso non regolamentato. Le sfide si moltiplicano: comprendere le logiche delle piattaforme, prevenire la concentrazione di potere nelle mani di chi controlla l'infrastruttura, difendere i diritti delle persone in un contesto dove la raccolta dati è onnipresente, garantire resilienza senza ricadere nel mito della protezione totale. E tutto questo mentre la velocità con cui il "gioco" cambia rende obsolete, in pochi mesi, molte delle regole tradizionali. *Zone Grigie* nasce proprio per questo: per aiutare a leggere la nuova grammatica della sicurezza in un mondo in cui le parole chiave non sono più "confine" e "invasione", ma "interfaccia", "consenso", "automatismo", "asimmetria". Per giocare in questa scacchiera mutata serve, prima di tutto, uno sguardo critico, transdisciplinare e consapevole del fatto che il campo di battaglia è anche un campo semantico. Solo comprendendo questo mutamento si può, davvero, iniziare a pensare cosa significhi "sicurezza" oggi.

Si lamenta spesso l'assenza di pensiero critico. Come ha affermato lei, la collana vuole applicarlo al campo della sicurezza informatica. Quale sarà il primo passo editoriale che avremo modo di leggere?

Il pensiero critico, più che assente, oggi è spesso disinnescato: confinato ai margini, neutralizzato dal tecnicismo o banalizzato da un discorso pubblico che oscilla tra allarmismo e indifferenza. *Zone Grigie* nasce proprio per riattivarlo nel luogo dove è più urgente e meno applicato: la sicurezza digitale. Il primo volume sarà dedicato a un tema di drammatica attualità: le nuove guerre. Un conflitto che non si combatte più solo con le armi convenzionali, ma che si sviluppa nei circuiti, nelle narrazioni, nei codici normativi e nella percezione collettiva del rischio. Parleremo di guerre ibride, dove l'ambiguità è la prima tattica; di cyber warfare, che opera sotto soglie giuridiche e cognitive; di guerre narrative, dove l'informazione è arma e bersaglio; e di guerre normative, in cui la regolazione (o la sua assenza) diventa strumento geopolitico.

Sarà un primo passo editoriale che dimostrerà, nei fatti, cosa intendiamo per pensiero critico. ■



Bibliografia

Bruce Schneier
La mente del hacker
ed. Luiss University Press

Le metamorfosi dell'hacker nell'orizzonte dinamico della cybersecurity

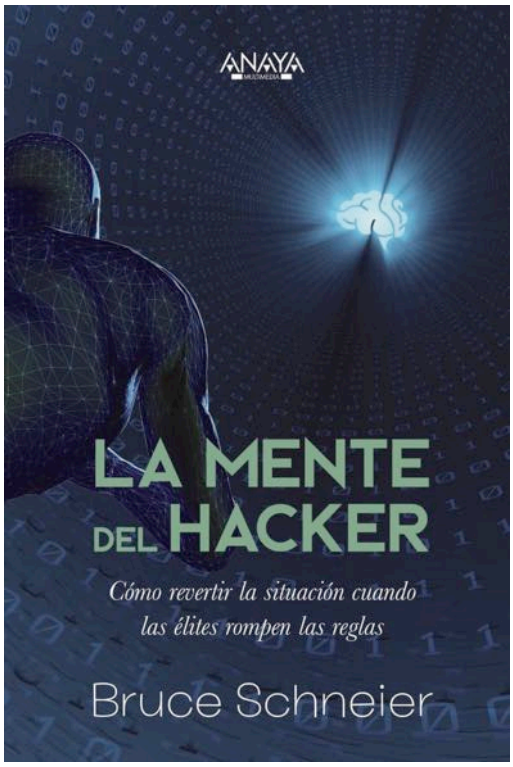
Autore: Massimiliano Cannata

La mente dell'hacker vive una metamorfosi simmetrica al cambiamento strutturale di reti e sistemi generato dalla rivoluzione digitale, che ha cambiato non solo il "gioco" del potere, ma anche, come ha rivelato molto bene Alessandro Baricco nel suo *The Game*, la stessa scacchiera entro cui quel gioco viene esercitato. Gli effetti delle trasformazioni sono in larga parte ancora tutti da misurare e comprendere. Sentiremo i loro effetti per lungo tempo, mentre cerchiamo di "trovare la falla…", per usare le parole di Bruce Schneier, considerato tra le personalità più influenti al mondo sui temi della *cyber security*.

L'attività hacking, dettata dalla continua ricerca delle falle, è ormai una vera e propria arte che si sta allargando a macchia d'olio, investendo l'economia, la finanza, la società. Non è più un affare per pochi smanettatori amanti del software. In coerenza con la necessità di allargare lo spettro, la trattazione del saggio tocca gli ambiti di pertinenza molto ampi: dal diritto alla politica, fino a investire i sistemi cognitivi e la frontiera dell'IA, che sarà il motore di sperimentazione per ulteriori metodi di hackeraggio da attuare in ogni angolo del pianeta. Per capire la portata del fenomeno dobbiamo considerare che siamo di fronte a dei "colletti bianchi" della tecnologia, che si muovono facendo squadra in tutti gli ambiti della vita sociale e produttiva. A ben guardare, la prospettiva di osservazione e di analisi scelta dall'autore non è quella individuale, legata alla visione di una mente sola, come il titolo potrebbe far pensare. Piuttosto, sono i meccanismi di funzionamento di una "mente collettiva" di cui bisogna osservare gli sviluppi, perché espressione di un paradigma destinato a connotare la società dell'informazione entro cui siamo tutti immersi.

Le falle del sistema

Potenzialmente, l'hacker è capace di fare anche del bene: la sua intelligenza nell'interpretare i fenomeni e il suo intuito, se ben indirizzati e guidati, possono essere utilizzati per finalità positive. Il velato ottimismo che si respira nelle ultime pagine nasce dalla natura ambivalente che ha da sempre avvolto di un "fascino" particolare questa figura, che ormai domina le pagine dei giornali e capace di influenzare il dibattito pubblico. Il punto nodale, su cui bisogna soffermarsi, sono le competenze, cioè la capacità di conoscere a fondo i meccanismi di funzionamento del digitale, che determinano la scelta oppositiva tra bene e male. È duplice, infatti, la strada da percorrere: investire tutte le capacità di cui si è capaci per rafforzare la resilienza del sistema oppure, al contrario, inserirsi nei "bug", cha si creano a ogni livello, in quegli interstizi "aperti" al



furto dei dati e delle informazioni, utili a impossessarsi del nuovo petrolio: le identità, con le storie professionali e biografiche che le caratterizzano. Impossessarsi del dato, divenuto un asset sociale, vuol dire arricchirsi a scapito delle imprese e dei cittadini, sottraendo ricchezza, limitando la sfera del bene comune, come sta avvenendo in "questa ultima fase del capitalismo". Potere e tecnologia tendono ad allearsi, facendo leva sulle crescenti diseguaglianze che rendono le élite del "finanzcapitalismo" più forti della democrazia e degli stessi poteri di controllo su cui si regge.

Si possono cogliere risvolti molto delicati andando a fondo della trattazione di Schneier, in cui si parla di valori come la fiducia - messa a dura prova dal crimine informatico che agisce su vasta scala – e si parla con preoccupazione di rischio esistenziale se consideriamo che tutto è hackerabile, lo dimostra il fatto che le reti produttive ma anche sociali si stanno trasformando in un campo di battaglia, sotto il perenne bersaglio di organizzazioni senza scrupoli.

La realtà aumentata e il "mondo 3" di Popper

Gli alert che giornalmente diffondono la Polizia Postale e l'Agenzia per la Cybersicurezza Nazionale ci parlano di attacchi DDoS, di campagne offensive rivolte alle istituzioni, di manomissione di conti correnti dei privati cittadini e di operazioni sempre più diffuse di *defacement* dei siti web. Il camuffamento di identità, che cambia faccia ai portali, è un'emblematica fenomenologia di trasformazione degli alfabeti della comunicazione: artefice di un mescolamento delle carte che altera il "game" di Baricco, citato all'inizio.

La realtà aumentata nelle sue molteplici definizioni ci porta a popolare "mondi virtuali" ancora poco leggibili. Chissà dove Karl Popper, teorizzatore dei "tre mondi", avrebbe collocato l'infosfera.

Forse la avrebbe considerata come una propaggine del suo "mondo 3", uno spazio di significato in cui verità e falsità convivono e fanno parte del nostro linguaggio, che esprime contenuti e saperi. Una dimensione che, oggi, la categoria del digitale proietta in una categoria nuova, ibrida, entro cui oggetti fisici e immateriali si fondono tutt'uno. La mente dell'hacker agisce in questi confini porosi, rafforzando costantemente le capacità cognitive di lettura dell'innovazione.

In questa dinamica, che vede l'innovazione come opportunità ma anche come rischio, anche la resilienza assume una connotazione mutante, come la mente: plastica, in virtù della sostanza neuronale che ne regola il funzionamento.

I ritmi dell'evoluzione proiettano ancora più avanti queste considerazioni. "Molto presto, infatti - scrive l'autore nell'introduzione – i sistemi di AI scopriranno nuovi hack, e tutto cambierà. Fino a oggi, l'hacking era stato un contesto umano, con hacker umani e hack soggetti ai limiti degli esseri umani. Questi limiti stanno per essere superati. La AI non hackererà solo i nostri computer, ma anche i nostri governi, i nostri mercati, o perfino le nostre menti. Le AI hackereranno i sistemi con velocità e abilità impensabili per gli hacker umani".

È bene soffermarsi su quest'ultimo passaggio: lo sviluppo della tecno-scienza impone risposte urgenti, siamo già oltre, non ci possono essere più intoppi nel percorso di crescita della conoscenza. ■

Edgar Morin, Mauro Ceruti
La nostra Europa
ed. Raffaello Cortina

La sicurezza, valore fondante della "nuova" Europa.

Autore: Massimiliano Cannata

La sicurezza sarà un valore centrale per comprendere il destino dell'Europa. L'affermazione non proviene, come sarebbe facile pensare, dagli ambienti militari e strategici, né da quelli ingegneristici, oggi sempre più coinvolti nella delicata della difesa degli asset digitali, ma da un brillante pamphlet scritto da "due maestri del nostri tempo". Edgar Morin, sociologo francese che ha superato con straordinaria lucidità la soglia dei cento anni, massimo teorico della complessità, e Mauro Ceruti, Professore Emerito di Filosofia della Scienza, Direttore del CRiSiCo (Centro di Ricerca sui Sistemi Complessi dell'Università IULM, di Milano) Premio Nonino.

Le debolezze dell'Europa sono da "curare", scrivono gli autori, l'aggressività del fronte sovranista, la necessità di un nuovo paradigma indirizzato a governare la potenza tecnologica, va messa a punto se si vuole dare un futuro al continente che sta sperimentando il tremendo ritorno della guerra. Il saggio scritto con uno slancio e una passione inusuale – i cui autori sono europeisti per sensibilità e per cultura – mostra con chiarezza la profonda metamorfosi del concetto

di sicurezza, un valore che non può essere affidato unicamente alla efficienza degli eserciti, reali o virtuali. È qualcosa di più: un termine polisemico, che assume mille volti e che dobbiamo saper coltivare, rilanciando il dialogo tra i popoli nella cornice di una nuova visione del potere e dei rapporti tra gli Stati. È la percezione del "comune destino" - insistono gli studiosi - che deve cambiare il modo di pensare l'Europa e la sicurezza come asset valoriale imprescindibile. Il destino non una parola che si rivolge al passato, ma deve partire dal futuro, segnando una profonda inversione di marcia.

Dall'età del ferro alla civiltà digitale

Nella ***Nostra Europa si parla*** di un'età età del ferro planetaria attraversata da tante crisi cicliche. La più grave è la crisi del pensiero, della civiltà, dei suoi valori e delle sue credenze, che stiamo vivendo. Serve un progetto per rinascere: altrimenti si rischia una catastrofe autodistruttiva. L'umanità deve porsi nella condizione di offrire, anche nel pericolo, gli esiti preziosi del suo umanesimo.

"Dove cresce il pericolo, cresce ciò che salva": la citazione del poeta tedesco Friedrich Holderlin, nella tessitura di un testo che si concede anche dei passaggi lirici, anche se sempre funzionali alla costruzione di una visione pragmatica di una Europa politica, fa percepire quanto importante sia la governance di un rischio che mette tutti nella stessa condizione di incertezza, quando non di precarietà esistenziale prima che economica e professionale." Tocca a noi – spiega Ceruti - salvare l'Europa, sentendoci europei, ricordiamolo proprio a chi malamente governa le sue istituzioni, stringendoci nel sentimento di una comune appartenenza alla civiltà del diritto, della democrazia, della solidarietà, della sicurezza, della pace. "Cambiare o perire… L'improbabile è sempre possibile" mette in guardia lo studioso. Oggi quell'improbabile appare necessario se vogliamo avere "un futuro". La riflessione sulla maturazione giuridica, al centro degli ultimi numeri della nostra rivista (in questo numero il focus è dedicato alla NIS2) si innesta - come fa notare molto bene Giusella Finocchiaro nella intervista che pubblichiamo - "in un contesto geopolitico globale perseguito dall'Unione europea che vuole porsi come leader nella produzione normativa, per far sì che il modello continentale divenga un riferimento globale e possa essere adottato nelle altre regioni del mondo". È possibile che si voglia affermare una "sovranità digitale", tema affrontato da Roberto Baldoni in un saggio recentemente pubblicato da Il Mulino. In ogni caso, sono passi importanti verso la costruzione

della nuova Europa vagheggiata: non più debole e afona, preda delle paure del passato, iscritte nella memoria dei drammi di cui si è stata protagonista. Le guerre mondiali e l'olocausto sono tragici ricordi che ci appartengono. Perché, anche se viviamo nell'epoca degli imperialismi, della demagogia populista - fenomeni aggravati dalla recente, pericolosa riemersione del virus del nazionalismo - c'è un mondo che sta reagendo, che ha ripreso le sue lotte per l'emancipazione, per ritrovare quello equilibrio tra libertà, giustizia e sicurezza su cui si fonda la democrazia autentica.

Sicurezza e nuovi equilibri geopolitici

Perseguire la sicurezza nel dosaggio armonico di tutte queste componenti che abbiamo ricordato, significa fare un salto verso il superamento metanazionale, che realizzi pienamente il principio costitutivo dell'unità nella diversità. Unitas Multiplex, Edgar Morin non si stanca di ripeterlo quasi come un mantra, mentre si sofferma sui contenuti del libro, che vuol dire concepire le frontiere tra razze, popoli ed etnie, non come muri divisori, ma come argini porosi che ammettono, anzi si nutrono del dialogo, che accresce la sicurezza perché è la migliore valvola di sfogo di ogni tensione.

Vista nell'ottica prismatica della complessità, che non è solo un indirizzo filosofico ed epistemologico, ma un fattore genetico che racconta come la vecchia Europa sia nata proprio dal conflitto, dalla eterogeneità, dalla sovrapposizione di fatti ed eventi drammatici, da cui è comunque scaturita la pagina radiosa dell'umanesimo e dell'illuminismo europeo, che ha gettato le basi dei diritti universali dell'individuo: frontiera mobile da difendere e definire ogni giorno.

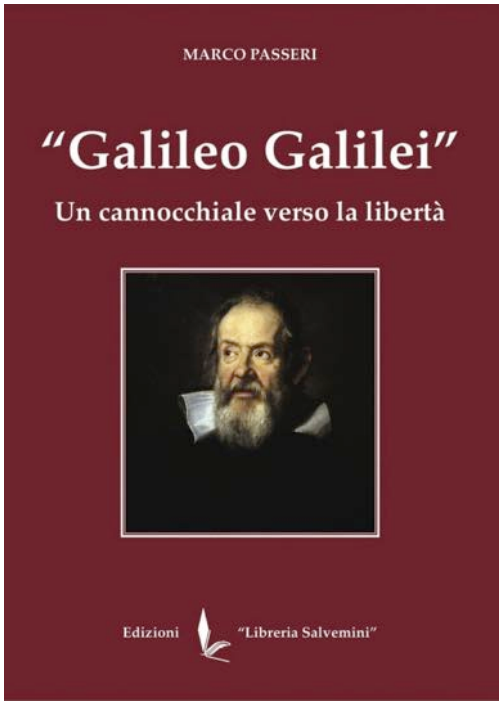
Alla luce di una disamina sulla contemporaneità densa di stimoli storici, letterari e filosofici c'è da chiedersi: il *"tecno-umanesimo" da più parti invocato come ponte di collegamento tra le "due culture"*, può essere interpretato come una missione civile, un progetto politico che può salvarci dai tanti rischi imminenti - crisi ecologica, guerre economiche e militari, tentazioni autocratiche, modelli di finanzcapitalismo - che rendono ancora più instabile e insicuro il quadro geopolitico? La sfida va affrontata senza sottrarsi, ed è quella di riconoscere, di ritrovare e di riannodare le vecchie funi sommerse, come le chiamava Predrag Matvejevic (intellettuale di Mostar grande conoscitore della Grecia classica e dell'Occidente autore di Mediterraneo n.d.r.), spesso rotte o strappate dall'intolleranza o dall'ignoranza o dai virulenti conflitti etnico-religiosi. Si stanno facendo strada i sovranismi, emergono fenomeni *ibridi* come la *tech right* fondata sullo stretto connubio tra ipertecnologia e iperprofitti che schiaccia le libertà dello stato di diritto, in questo contesto il deficit di democrazia va affrontato come un'autentica emergenza. Ripensare a un'adeguata governance della sicurezza implica un'azione strategica tesa a innovare anche le istituzioni. Per realizzare questa non facile prospettiva, le classi dirigenti dovranno dimostrare di saper guardare oltre la dimensione economica e quantitativa nella lettura dei fenomeni, per disporsi ad affrontare con coraggio problemi e bisogni reali della comunità planetaria. ■

Marco Passeri Galileo Galilei ed. "Libreria Salvemini"

Autore: Marco Passeri

Un cannocchiale verso la libertà

Il saggio di Marco Passeri, in un'epoca dominata dal prepotente sviluppo della tecno-scienza fa riflettere. Parlare di Galilei significa parlare della libertà della scienza e dei difficili rapporti che la ricerca e il sapere intrattiene con il potere. Pubblichiamo la prefazione di Passeri che presenta dei tratti di grande interesse per chi si occupa di sicurezza a tutti i livelli, soprattutto nella parte conclusiva dove si fa riferimento alle nuove minacce globali e alla necessità di una sostenibilità del rischio, aspetto cruciale per il management della sicurezza, che non è più un ambito per cultori della materia, ma una leva strategica per la governance economica e politica degli stati.



Eric Hobsbawm ha scritto che il progresso della Scienza nel corso dei secoli è avvenuto *"sullo sfondo di un bagliore di sospetto e paure"*, un bagliore che in particolari momenti storici si è acceso in vere e proprie *"vampate di odio e di rifiuto della ragione" (Il secolo breve*, Rizzoli, Milano, 1995). Queste affermazioni sono più che mai vere se consideriamo le vicende biografiche di Galileo Galilei, fondatore della Scienza moderna che, in pieno clima controriformistico, è stato vittima dell'oscurantismo religioso, subendo un lungo processo, conclusosi con l'abiura e l'isolamento.

La "colpa" di Galilei – agli occhi della Chiesa cattolica e degli scienziati tolemaici – era stata quella di aver messo in discussione il principio di autorità (l'*ipse dixit* aristotelico) e di aver abbracciato una teoria scientifica "rivoluzionaria" (l'eliocentrismo copernicano) in contrasto con i principi delle Sacre Scritture. Naturalmente lo

scienziato non ebbe mai l'intenzione di entrare in contrasto con la Chiesa cattolica e di mettere in discussione l'autorità dei testi sacri; in più occasioni Galilei ribadì la fondamentale distinzione tra la teologia (che si basa sulla "verità rivelata" e ha la funzione di guidare moralmente e spiritualmente gli uomini) e la scienza che si occupa dello studio della natura: il "grandissimo libro dell'Universo" creato da Dio e scritto in caratteri matematici e figure geometriche.

Se Dio ha donato agli uomini l'intelletto è per consentire loro di comprendere i principi che governano la natura. Quindi, attraverso l'osservazione, il ragionamento e la sperimentazione (i fondamenti del "metodo" galileiano), l'uomo può pervenire alla conoscenza delle leggi (matematiche) che regolano l'Universo. Per Galilei non esiste una verità scientifica in contrasto con la verità delle Scritture, la verità è una sola, ciò che cambia è il linguaggio con cui è espressa: quello della Bibbia (allegorico) non può essere utilizzato nell'ambito della scienza che necessita di grande esattezza. È con argomentazioni di tal genere che Galilei tentò di evitare lo scontro diretto con la Chiesa di Roma, tuttavia la condanna da parte del Sant'Uffizio, nel 1633, fu inevitabile e l'abiura fu l'unica possibilità di salvarsi e di evitare il carcere a vita.

La vicenda di Galilei è diventata, dunque, l'emblema della difficile conciliazione tra scienza e fede e il simbolo delle difficoltà e dei pregiudizi che spesso gli scienziati, anche quelli attuali, devono affrontare per affermare la loro libertà di pensiero e di ricerca. Come disse **Rita Levi Montalcini** in un discorso a Montecitorio nel febbraio del 2001: *"La libertà di ricerca è quello che distingue l'Homo Sapiens da tutte le altre specie"* e dunque deve essere difesa sempre e a qualunque costo.

Naturalmente condividiamo le dichiarazioni della Senatrice Montalcini e riteniamo indispensabile difendere l'autonomia della ricerca scientifica dalla religione e dalla politica; d'altro canto, la Storia dimostra che è impossibile arrestare il progresso scientifico: gli uomini possono essere fermati (vedi il "caso Galilei"), ma le idee, quando sono valide, vanno avanti comunque.

Inoltre, va detto che ostacolare, bloccare un ricercatore alle prese con una scoperta importante o una teoria da confermare è un'impresa vana; gli scienziati sono sempre "innamorati" delle proprie ricerche e farebbero di tutto per difenderle e per vederne l'applicazione pratica, a prescindere da eventuali ripercussioni biologiche, etiche, politiche, ecc. È appunto quanto racconta **Heisenberg** a proposito di un incontro con Enrico Fermi: quest'ultimo considerava la sperimentazione della prima bomba all'idrogeno nel Pacifico un "bello esperimento", sorvolando sulle conseguenze terrificanti che tale esperimento avrebbe comportato. *"Lo scienziato" – scrive Heisenberg – "ha bisogno di sentirsi confermare da un giudice imparziale, dalla natura stessa, di aver compreso la sua struttura. E vorrebbe verificare direttamente l'effetto dei suoi sforzi".* (W. Heisenberg, *La tradizione della scienza*, Garzanti, Milano, 1982).

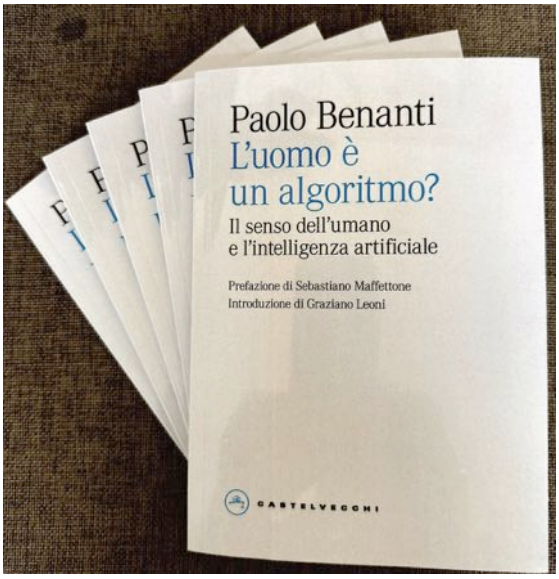
Proprio il riferimento alla bomba all'idrogeno e alla sperimentazione sulle armi termonucleari dovrebbe farci riflettere, però, su un altro aspetto (politico) della questione, che oggi appare più che mai attuale. Ci riferiamo alla necessità di vigilare sugli sviluppi della ricerca scientifica e tecnologica, sull'importanza di dettare delle condizioni e anche di imporre dei limiti affinché il progresso sia "sostenibile"; occorre aprire gli occhi sui rischi di una ricerca scientifica fuori controllo giacché in ballo non vi sono più questioni di ordine morale o religioso (come al tempo di Galilei) ma la nostra stessa sopravvivenza sul pianeta. ■

Paolo Benanti L'uomo è un algoritmo? Il senso dell'umano e l'intelligenza artificiale ed. Castelvecchi

Autore: Massimiliano Cannata

Ulisse e Prometeo, sete di sapere e algoretica devono camminare insieme

Il mito di Ulisse ci insegna che la ricerca umana di senso è guidata dall'intelligenza, nelle sue due declinazioni: νοῦς e μῆτις, intuizione e pratica. Dalla sinergia di queste facoltà sono nate le grandi invenzioni che segnano la nostra specie, a partire dalla «grande invenzione del linguaggio».



Oggi, però, il linguaggio non sembra più una prerogativa esclusivamente umana: l'Intelligenza Artificiale, nelle vesti di ChatGPT e dei Large Language Models (LLM), ha introdotto una lingua computazionale che riconfigura in modo nuovo parola e pensiero.

Paolo Benanti ci accompagna in una breve e suggestiva riflessione etica sul paradosso della tecnica, pur riconoscendone le potenzialità: questa estensione della nostra «naturalità artificiale» sembra infatti sempre meno orientata a mappare la realtà e sempre più propensa a confonderci.

Muovendosi tra informatica, filosofia e spiritualità – da Turing a Searle, da Scheler a Jonas – Benanti avanza una proposta semplice ma dirompente, capace di restituire centralità alla dimensione

umana. Recuperare oggi un «pregiudizio umanista» non significa infatti ripudiare il progresso, ma riaffermarne la sfida più autentica: vivere una vita buona e consapevole.

L'intelligenza algoritmica deve tornare a essere uno strumento nelle nostre mani, al servizio della piena dignità umana. È alle università, oggi, che spetta il compito fondamentale di creare nuovi «paesaggi culturali», dove ritrovare il senso delle nostre creazioni e delle nostre vite.

Affrontare la svolta radicale che abbiamo di fronte rimane l'interrogativo di fondo cui la mente lucida di Benanti certo non si sottrae:

"Le trasformazioni in atto – mi ha spiegato nel corso dell'intervista – non sono arrestabili. Come tali, non sono né da temere né da accogliere in maniera acritica. Non si può, infatti, nutrire la vana pretesa di fermare il vento con le mani. Quello che possiamo esercitare, da esseri dotati di intelligenza e ragione, è una forma di equilibrato discernimento che ci consenta di afferrare tutte le opportunità che possono aprirsi in un universo in rapido divenire. Quando, settantamila anni fa, ci siamo spostati dall'Africa e abbiamo abitato diverse latitudini della Terra, il nostro comportamento è stato molto diverso da quello di molti animali. Se un mammut si fosse spostato dalle steppe siberiane per andare in Africa e in Asia, prima di affrontare questa nuova avventura della sua storia evolutiva avrebbe dovuto aspettare i tempi evolutivi di una discendenza che avrebbe portato alla nascita di esemplari privi della folta pelliccia. L'uomo non ha osservato nessuna attesa, perché fin dall'inizio si è attrezzato di strumenti adeguati per preparare il suo lungo viaggio verso il progresso. Detto in altri termini: quello che per altri esseri viventi è rigidamente confinato nel DNA, per noi è qualche cosa di aperto, che ha a che fare con l'uso sapiente di artefatti tecnologici. L'artefatto tecnologico è la nostra "traccia" che serve ad abitare il mondo, o, se preferisce, è una modalità importante per manifestare la nostra umanità".

La novità sta nel fatto che la traccia di cui parla Benanti dialoga con la struttura profonda del nostro essere, riuscendo a mimare anche le facoltà superiori.

Il salto ontologico dagli oggetti alle "non-cose"

Dobbiamo fare i conti con questo salto ontologico, tematizzato dal teologo, che richiama gli ultimi scritti di Byung-Chul Han, filosofo di Seul, pensatore tra i più influenti del Pianeta, che definisce il mondo che abitiamo come il "regno delle non-cose", raccontando, in un recente saggio pubblicato da Einaudi, come abbiamo smesso di vivere il reale.

È questo il territorio entro cui ci muoviamo. Se ormai l'"anima del mondo" è data dal software, il tesoro che muove economia e società è rappresentato dai dati e dalle informazioni.

L'algoretica, invocata da Benanti e da Sebastiano Maffettone, filosofo della politica, docente emerito della LUISS, che ha curato la prefazione del saggio, può essere una strada verso la "sostenibilità digitale", che vuol dire indirizzare la ricerca della tecno-scienza in una direzione coerente rispetto ai bisogni della famiglia umana, intesa nella sua accezione più alta e universale. ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
https://www.cybertrends.it/supportaci/