Cybersecurity Trends

Edizione italiana, N. 3 / 2024

INTERVISTE VIP:

- PEPPINO ORTOLEVA
- VANNI CODELUPPI

Il regolamento DORA e la Cybersecurity

ISSN 2559 - 1797
ISSN-L 2559 - 1797

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

Ai nastri di partenza.

Autore: Nicola Sotira

Siamo al via della normativa Digital Operational Resilience Act (DORA) che rappresenta un passo significativo nel rafforzamento della resilienza operativa digitale delle istituzioni finanziarie nell'Unione Europea. L'obiettivo principale di questa normativa è garantire che il sistema finanziario dell'UE sia in grado di resistere, rispondere e riprendersi efficacemente da un'ampia gamma di minacce informatiche e di disastri tecnologici.

Continua il percorso della Commissione Europea nel migliorare la stabilità e la sicurezza del settore finanziario. In particolare, questa normativa mira a creare un quadro comune per la gestione del rischio informatico e per aumentare la resilienza operativa delle istituzioni finanziarie. Tra i principali obiettivi di DORA vi sono:

- Definire requisiti uniformi per la gestione del rischio ICT (Information and Communication Technology) per tutte le entità finanziarie.
- Stabilire un quadro di governance per garantire che le istituzioni dispongano di strutture adeguate alla gestione del rischio digitale.
- Rafforzare le capacità di supervisione e di controllo da parte delle autorità competenti.
- Migliorare la cooperazione tra le autorità nazionali e internazionali in materia di sicurezza informatica.

La direttiva richiede pertanto, una serie di requisiti tecnici e organizzativi alle istituzioni finanziarie per garantire la resilienza operativa. Tra i principali requisiti possiamo riassumere i seguenti:

- Implementazione di misure di sicurezza adeguate a proteggere i dati e i sistemi critici.
- Stabilire politiche e procedure per la gestione degli incidenti informatici, con particolare attenzione alla continuità operativa.
- Effettuare regolarmente valutazioni del rischio ICT e test di stress per identificare e mitigare le vulnerabilità potenziali.
- Mantenere registri dettagliati degli incidenti di sicurezza e delle misure adottate per risolverli.
- Garantire la formazione e la sensibilizzazione del personale in materia di sicurezza informatica.

L'implementazione avrà un impatto significativo su tutto il settore finanziario, come ad esempio:

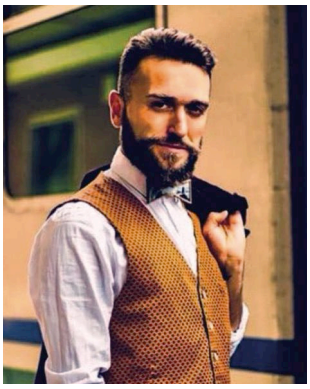
- Miglioramento della postura di sicurezza: maggiore capacità e resilienza nel prevenire e rispondere agli attacchi informatici.
- Competitività Rafforzata: La maggiore sicurezza e resilienza operativa contribuiranno a migliorare la fiducia degli investitori e dei clienti, rafforzando la competitività delle istituzioni finanziarie europee.
- Cooperazione Internazionale: la normativa promuove una maggiore cooperazione tra le autorità di vigilanza, facilitando la condivisione delle informazioni e il coordinamento delle risposte alle minacce.

Concludendo, la normativa DORA rappresenta un importante passo avanti verso la protezione del sistema finanziario dell'Unione Europea dalle minacce informatiche. Sebbene l'implementazione possa comportare probabilmente sfide iniziali, le opportunità sono significative per le istituzioni finanziarie. Le organizzazioni finanziarie dovranno investire in nuove tecnologie e formazione per conformarsi ai requisiti di DORA, il che potrebbe comportare un aumento dei costi operativi. Un punto che richiederà attente valutazioni negli investimenti così che i benefici a lungo termine, in termini di sicurezza e resilienza operativa, superino ampiamente tali costi. Sicuramente la normativa contribuirà a creare un ambiente finanziario più sicuro e stabile, promuovendo al contempo l'innovazione e la fiducia nel settore. Noi come sempre abbiamo voluto dare in questo numero il nostro modesto contributo. Buona lettura... ■

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.

Chamelyon: La crittografia per tutti per proteggere i dati nell'era del data trade.



Autore: Alboro Behluli

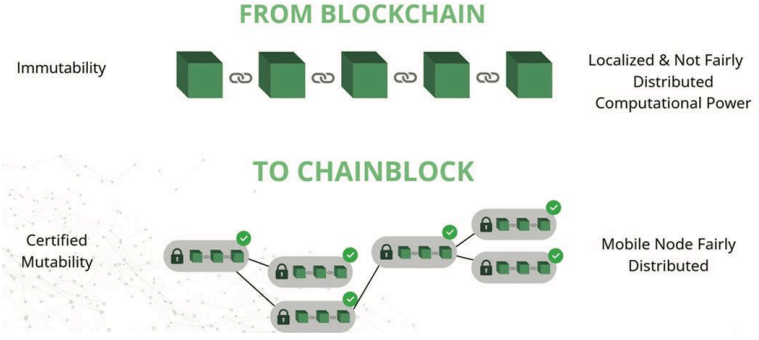
In un mondo in rapida evoluzione, i dati sono diventati la nuova moneta, il *data trade* a cui assistiamo oggi, con l'uso incontrollato e spesso improprio delle informazioni, richiede un cambiamento urgente. Tecnologie avanzate come il *crawling* tramite AI pongono nuove minacce, mettendo a rischio la privacy, il contenuto e il controllo individuale. È il momento di prendere in mano la situazione, proteggendo e dando valore ai dati direttamente nelle mani degli utenti. Chamelyon intende rispondere a queste sfide.

Il progetto Chamelyon è il risultato concreto di una sinergia tra esperienze nazionali e internazionali e competenze di alto livello nei settori IT e legale. Al cuore di Chamelyon c'è una solida amicizia, coltivata nel tempo, e la passione condivisa per la creazione di sistemi IT sicuri, la protezione dei dati personali e la scalabilità delle soluzioni tecnologiche. Il team ha messo in pratica un approccio interdisciplinare e la condivisione della conoscenza per sviluppare soluzioni innovative, sempre guidato da valori fondamentali come integrità, trasparenza e rispetto della privacy.

Chamelyon è stato guidato da cinque figure chiave:

- Due esperti in crittografia e cyber-sicurezza;
- Un sistemista e sviluppatore specializzato in tecnologie blockchain;
- Un giurista esperto nella gestione dell'identità digitale;
- Un manager con vasta esperienza in soluzioni di marketing digitale.

Questa combinazione di competenze ha permesso al team di affrontare e superare criticamente le attuali sfide nei sistemi blockchain, rispondendo in modo efficace ai bisogni di diversi mercati applicativi. L'obiettivo è stato raggiunto: migliorare la performance dei sistemi, valorizzare i dati e garantire l'autenticità dei contenuti digitali, tutto nel pieno rispetto dei

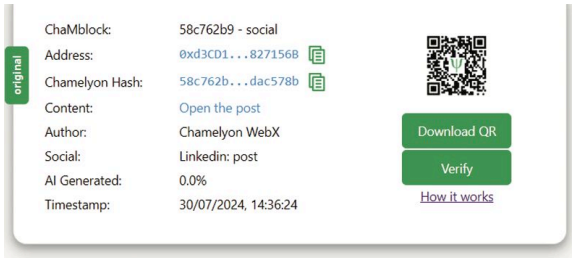


BIO

Alboro Behluli è un imprenditore appassionato di tecnologia e fondatore di Web Impact Agency, una realtà che combina competenze nei settori IT e legale. Alboro ha sviluppato Chamelyon, una tecnologia blockchain mutabile che mira a migliorare la sicurezza e la protezione dei dati. Con un forte interesse per i sistemi IT sicuri e una profonda attenzione alla trasparenza e alla privacy, lavora insieme a un team interdisciplinare per creare soluzioni innovative. Il suo approccio è fondato sulla collaborazione e la condivisione della conoscenza, sempre con l'obiettivo di portare un contributo positivo e responsabile nel mondo della tecnologia.

diritti dell'individuo e attraverso l'uso di una tecnologia sostenibile ed etica.

Chamelyon introduce il cambiamento del paradigma delle catene di blocchi (blockchain) a blocchi mutabili autocertificanti (chain-block), basati su modelli di crittografia evoluti.



Il cuore della tecnologia Chamelyon è il blocco mutabile, assimilabile ad un *fungible token*, che gli utenti possono gestire autonomamente e che viene rappresentato attraverso una scheda crittografica tale da semplificarne la comprensione e la gestione.

Il protocollo Chamelyon consente di effettuare operazioni fondamentali in un unico passaggio all'interno di un blocco mutabile, che può contenere transazioni, dati, e il nuovo concetto di data smart contract. Il data smart contract che introduce Chamelyon rappresenta un'evoluzione degli smart contract tradizionali, che automatizzano e verificano gli accordi basati su condizioni predefinite, integrando funzioni evolute per la gestione dei dati e della privacy direttamente all'interno del blocco stesso.

La tecnologia Chamelyon e le primitive crittografiche sviluppate rendono i blocchi autocertificanti, eliminando la necessità di meccanismi di consenso e rendendo tutte le operazioni di verifica più efficienti rispetto alle blockchain tradizionali.

Attraverso Chamelyon, operazioni come verifica della ownership di un blocco mutabile, verifica della coerenza e della storia dei contenuti, incluse transazioni, e la garanzia della non ripudiabilità delle transazioni, risultano semplici dal punto di vista computazionale permettendo l'utilizzo nel network di nodi come smartphone o IoT, senza la necessità di investimenti importanti per l'attivazione o la creazione di data-center dedicati (i.e. *mobile phone as a node*).

Chamelyon offre una soluzione per proteggere e valorizzare i dati e i contenuti originali prodotti dalle persone anche contro l'utilizzo improprio dell'IA crawling. Garantisce così che ogni contributo umano sia riconoscibile (e distringuibile), sicuro e protetto. Chamelyon offre uno strumento per preservare l'autenticità e l'integrità delle informazioni in un ambiente digitale ove la creatività umana è incentivata.

Grazie all'uso di uno sharding DHT, all'implementazione di blocchi mutabili autocertificanti e alla possibilità di rendere le transazioni atomiche, localizzate e air-gapped, Chamelyon supporta un numero potenzialmente infinito di operazioni simultanee risolvendo i problemi di scalabilità e centralizzazione delle attuali blockchain.

Inoltre, la combinazione di protocolli proprietari con la crittografia avanzata di Chamelyon offrono sicurezza intrinseca e e permettono di rendere gli scambi digitali accessibili a tutti, anche gli utenti meno esperti, attraverso strumenti semplici e intuitivi che, di fatto, democratizzano il mercato digitale.

Bilanciando decentralizzazione ed efficienza con un nuovo modello di consenso ibrido, in contrasto ai meccanismi di proof of something, Chamelyon mantiene la rete sicura, performante e sostenibile. In linea con i regolamenti internazionali di protezione dei dati e rispetto dei principi di tutela dei diritti individuali associati, garantisce trasparenza e conformità tramite la gestione autonoma dei blocchi da parte degli utenti, incluso il diritto ad essere dimenticati.

L'orizzonte di applicabilità di Chamelyon è ampio: e-commerce, social media, certificazione di articoli e contenuti, gestione di contratti e sistemi di prenotazione e tracciamento, certificazione delle comunicazioni, certificazione dei documenti contabili, gaming, sistemi di voto digitali, *et al*.

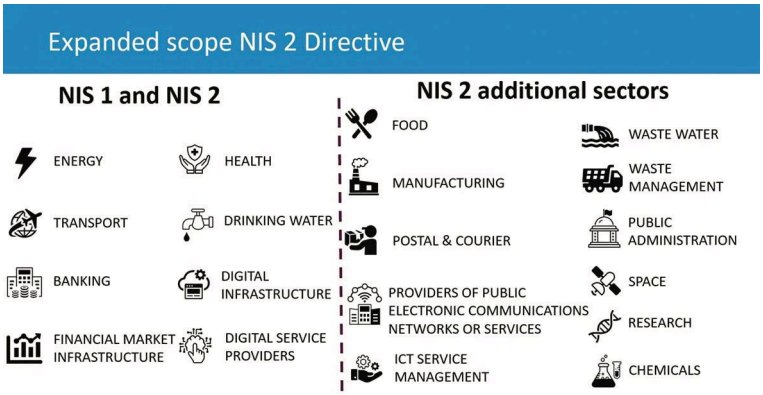
Dopo Web, Web 2, Web 3: benvenuti nell'era del Web X! ■

https://chamelyonscan.io/search/59e96b39
https://chamelyonscan.io/search/37b32562

Gestione delle terze parti, Direttiva NIS e regolamento DORA: i problemi irrisolti.

Autore: Francesco Corona

GENERALITÀ. 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** (Direttiva UE 2022/2555) 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.



Il Regolamento DORA (Digital Operational Resilience Act) si concentra specificamente sul settore finanziario. Esso richiede alle entità finanziarie di gestire i rischi derivanti dai fornitori di servizi ICT di terze parti in modo rigoroso. DORA stabilisce norme vincolanti per la gestione del rischio ICT, richiedendo una valutazione continua delle misure di sicurezza applicate dai fornitori. Di seguito i tre punti essenziali per una corretta gestione delle terze parti:

1. **Compliance Normativa.** Le aziende devono garantire che i loro fornitori rispettino le misure di sicurezza imposte da NIS2 e DORA. Questo implica un monitoraggio costante e la necessità di stabilire procedure di audit efficaci.
2. **Gestione del rischio cyber.** La dipendenza da fornitori esterni aumenta il rischio di attacchi informatici. Le normative richiedono una valutazione dettagliata dei rischi associati ai fornitori e una strategia per mitigare tali rischi.
3. **Integrazione delle Normative.** Le aziende devono affrontare la complessità derivante dalla necessità di conformarsi sia alla NIS2 che al DORA. Questo richiede un approccio integrato alla compliance

BIO

Francesco Corona è ricercatore e docente di Cyber Intelligence, già direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome; 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 capo dell'Intelligenza Artificiale e delle Reti Neurali per conto del CNR-IASI di Roma. Svolge attività di ricerca in svariati settori e in particolare in quello della Cybersecurity per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

normativa, evitando azioni disgiunte che potrebbero compromettere la sicurezza complessiva.

DORA impone alle entità finanziarie di effettuare una valutazione preventiva approfondita dei fornitori di servizi ICT, al fine di garantire la resilienza operativa e la sicurezza della supply chain. La valutazione preventiva dei fornitori richiesta da DORA presenta sfide significative che riguardano l'identificazione dei fornitori critici, la raccolta e gestione delle informazioni, il monitoraggio continuo, la definizione di contratti adeguati e la promozione di una cultura della sicurezza. Le entità finanziarie devono affrontare queste sfide con strategie ben pianificate per garantire la compliance normativa e la resilienza operativa. Di seguito riepiloghiamo in cinque punti ciò che la direttiva si prefigge di gestire nei confronti delle terze parti:

1. Identificazione e classificazione dei fornitori

- *Definizione di fornitori critici:* DORA richiede una chiara identificazione dei fornitori critici, i quali sono soggetti a requisiti di sicurezza più rigorosi. La classificazione accurata dei fornitori in base alla loro importanza e ai rischi associati è complessa e richiede un'analisi dettagliata delle loro operazioni e della loro interconnessione con l'entità finanziaria.
- *Valutazione dei subfornitori:* Non solo i fornitori diretti devono essere valutati, ma anche i subfornitori, il che complica ulteriormente il processo di audit e monitoraggio.

2. Raccolta e gestione delle informazioni

- *Richiesta di informazioni dettagliate:* DORA richiede una grande quantità di dati per la valutazione dei fornitori, inclusi aspetti tecnici, operativi e di sicurezza. La raccolta di queste informazioni può essere onerosa e richiede risorse significative.
- *Documentazione e reportistica:* Le entità devono mantenere registri dettagliati delle valutazioni effettuate, il che implica un sistema di gestione delle informazioni ben strutturato per garantire la trasparenza e la conformità ai requisiti normativi.

3. Monitoraggio continuo e audit

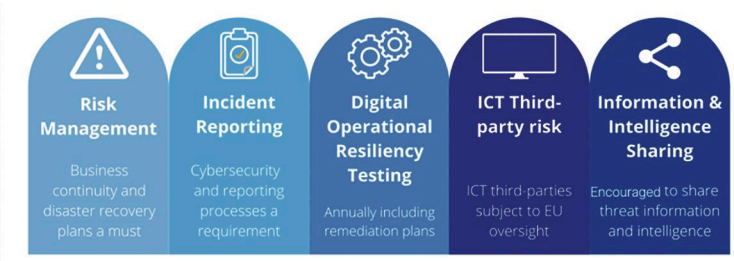
- *Necessità di audit regolari:* DORA prevede che le entità finanziarie non solo effettuino una valutazione iniziale, ma anche audit regolari per monitorare le performance di sicurezza dei fornitori nel tempo. Questo richiede un impegno costante e risorse dedicate.
- *Adattamento alle variazioni del rischio:* Con l'evoluzione delle minacce informatiche, le entità devono essere pronte a rivedere e aggiornare le proprie valutazioni in modo continuo, il che può risultare impegnativo.

4. Contratti e misure contrattuali

- *Definizione di clausole contrattuali adeguate:* DORA richiede che le entità stabiliscano contratti solidi con i fornitori, includendo clausole specifiche relative alla sicurezza informatica. La creazione di tali contratti può essere complessa, specialmente quando si tratta di bilanciare i requisiti normativi con le esigenze commerciali.
- *Gestione della responsabilità:* È fondamentale chiarire le responsabilità in caso di incidenti di sicurezza legati ai fornitori. Questo richiede una negoziazione attenta e una comprensione chiara delle implicazioni legali.

5. Cultura della sicurezza

- *Promozione della consapevolezza:* Le organizzazioni devono sviluppare una cultura della sicurezza che coinvolga non solo il personale interno ma anche i fornitori. Ciò implica formazione e sensibilizzazione sui rischi informatici.
- *Collaborazione tra parti interessate:* È essenziale stabilire relazioni collaborative con i fornitori per garantire che tutti siano allineati sugli standard di sicurezza richiesti da DORA.



DORA, NIS2, GDPR: NORMATIVE A CONFRONTO. Le verifiche di conformità richieste dal DORA (Digital Operational Resilience Act) si differenziano significativamente da quelle imposte da altre normative, come il GDPR (General Data Protection Regulation) e la direttiva europea NIS2 (Network and Information Security 2). Queste differenze si manifestano in vari aspetti, tra cui l'ambito di applicazione, i requisiti specifici e le modalità di enforcement. In particolare avremo:

1. Ambito di Applicazione

- **DORA:** Si applica specificamente alle entità finanziarie, inclusi banche, compagnie assicurative e fornitori di servizi ICT. La normativa richiede che queste entità dimostrino resilienza operativa attraverso rigorosi test di sicurezza e audit regolari.
- **NIS2:** Questa direttiva ha un ambito più ampio, coprendo vari settori essenziali come energia, trasporti e salute. Le entità devono conformarsi a requisiti generali di sicurezza informatica, ma le specifiche possono variare a seconda della legislazione nazionale.

2. Requisiti di Verifica

- *DORA:* Impone test di resilienza annuali e test di penetrazione ogni tre anni per garantire che i sistemi siano in grado di resistere a attacchi informatici. Inoltre, richiede una gestione attenta dei rischi provenienti dai fornitori di servizi ICT.
- *GDPR:* Sebbene richieda anche misure di sicurezza, il focus è sulla protezione dei dati personali piuttosto che sulla resilienza operativa. Le verifiche si concentrano principalmente sulla gestione dei dati e sul rispetto dei diritti degli interessati.

3. Modalità di Enforcement

- *DORA:* È un regolamento direttamente applicabile in tutti gli Stati membri dell'UE, il che significa che non necessita di recepimento nazionale. Le autorità di vigilanza hanno un ruolo attivo nel monitorare la conformità e possono effettuare verifiche dirette sui fornitori critici.
- *NIS2:* Richiede il recepimento nelle legislazioni nazionali, il che può

portare a variazioni nei requisiti tra i diversi Stati membri. Le sanzioni per non conformità possono includere multe fino al 2% del fatturato globale annuo.

4. Gestione dei Rischi di Terze Parti

- *DORA:* Richiede alle entità finanziarie di gestire attivamente i rischi associati ai fornitori ICT attraverso *contratti solidi e monitoraggio continuo* delle loro prestazioni.
- *NIS2:* Sebbene affronti anche la sicurezza della catena di approvvigionamento, lo fa in un contesto più ampio e non sempre con lo stesso livello di dettaglio richiesto da DORA.

5. Sanzioni e Conseguenze

- *DORA:* Le sanzioni per non conformità possono includere multe significative (fino all'1% del fatturato globale medio giornaliero) e ordini di cessazione da parte delle autorità competenti.
- *GDPR:* Prevede sanzioni severe per violazioni, con multe fino al 4% del fatturato globale annuo o 20 milioni di euro, a seconda dell'importo maggiore.

6. Obblighi di Sicurezza

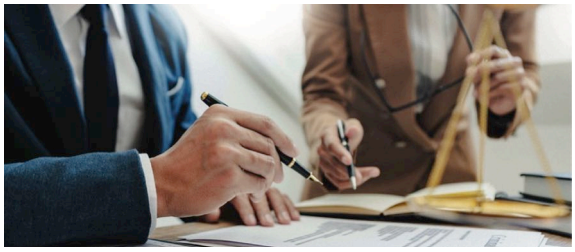
- NIS2 richiede una valutazione dei rischi informatici e l'implementazione di misure adeguate per mitigare tali rischi. Le aziende devono anche stabilire piani di comunicazione e audit regolari con i fornitori terzi.
- DORA stabilisce requisiti specifici per la resilienza operativa digitale, inclusa la gestione degli incidenti e la notifica alle autorità competenti in caso di violazioni della sicurezza.

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 specficity 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) slide 13

In sintesi, le verifiche di conformità richieste da DORA si caratterizzano per un focus specifico sulla resilienza operativa delle entità finanziarie, con requisiti rigorosi e modalità di enforcement dirette. Al contrario, altre normative come GDPR e NIS2 presentano ambiti più ampi o differenti focus tematici. Queste differenze evidenziano l'importanza per le organizzazioni di comprendere le specifiche esigenze normative in base al loro settore e alla loro operatività.

PROBLEMI 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. 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.



I clienti quindi si adoperano ad inviare ai fornitori tramite gli uffici legali le clausole inclusive di questionari, ma sta di fatto che ogni cliente invia questionari e regole contrattuali differenti. Ad esempio, ci si può trovare di fronte a documenti di clienti operanti in ambito telecomunicazioni (es. Vodafone, Tim, Wind, ecc.) nei quali si chiede di garantire costantemente i flussi giornalieri delle vulnerabilità (Information sharing), oppure di fissare le vulnerabilità critiche entro 48 ore, oppure di effettuare penetration test e audit oltre i limiti imposti dalle normative. Non esistendo ancora per il mercato europeo un Framework specifico dei controlli, queste richieste enucleate negli add-on contrattuali di cyber risk management, magari con tanto di manleva da parte del cliente per ogni tipo di problema che blocchi o introduca ritardi alla business continuity del fornitore, possono essere tutte riferite ad uno stesso ambito di gara con profili e richieste una diversa dall'altra. Il tutto si complica se questa variabilità di controlli contrattuali non tenesse adeguatamente conto dei seguenti punti:

1. **Diverse tipologie di aziende coinvolte.** (piccole, medie, grandi).
2. **Compliance e certificazioni.** Ci si interroga se potrà mai esserci la compliance a uno standard che risponde alle esigenze contrattuali senza necessità di questionari e clausole specifiche; ad esempio come già accennato la certificazione ISO 27001, sufficiente a garantire tutta una serie di controlli senza ulteriori obblighi previsti dal contratto. ISO 27001 può essere utilizzato per NIS 2: e

può soddisfare infatti la maggior parte dei requisiti di sicurezza informatica di NIS 2 spingendosi anche a DORA. Si aggiunga il fatto che NIS 2 e la stessa ENISA (European Union Agency for Cybersecurity) incoraggiano l'uso di standard di sicurezza informatica, ed è chiaro che ISO 27001 è una scelta sicura ed affidabile per la conformità a NIS2 (vedi Articoli 9, 10).

3. **Risoluzioni attraverso enti normativi.** Sarà compito del legislatore stabilire attraverso un nuovo **Framework** quali sono i controlli che un fornitore deve predisporre per i propri clienti/contratti.

4. **Disallineamenti** che possono determinarsi tra uffici legali, security manager e account manager.

5. **Aumento dei tempi e quindi dei costi** di gestione delle pratiche contrattuali e delle gare di appalto.

Sta di fatto che un fornitore di servizi ITC al quale verrà richiesto contrattualmente da un cliente di effettuare audit/penetration test con manleva per un ipotetico fermo del servizio in produzione non farà altro che stracciare il contratto proposto perché non perseguibile e contrario alle regole della Business Continuity aziendale.

RISOLUZIONI DELLE PROBLEMATICHE. 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) 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 (vedi precedente articolo 8), 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. (vedi B[008] Cybersecurity Supply Chain Risk Management (C-SCRM): un approccio dinamico - Rivista Cybersecurity Trends (cybertrends.it))

Bibliografia utile

[B001] A Complete Guide to DORA (Digital Operational Resilience Act) |Metomic (https://www.metomic.io/resource-centre/a-complete-guide-to-dora)

[B002] Directive - 2022/2555 - EN - EUR-Lex (https://eur-lex.europa.eu/eli/dir/2022/2555/oj)

[B003] NIS2 Directive what you need to know (https://tresorit.com/nis2?utm_term=NIS2+Penalties&msclkid=737612d5ca53114cfc4a743b47172b38&utm_content=NIS2)

[B004] Regolamento DORA e NIS2: necessario valutare misure di sicurezza applicate dai fornitori a protezione dei dati - Federprivacy (https://www.federprivacy.org/informazione/primo-piano/regolamento-dora-e-nis2-necessario-valutare-misure-di-sicurezza-applicate-dai-fornitori-a-protezione-dei-dati)

[B005] Obblighi cybersecurity, tra NIS 2, legge 90/24 e regolamento DORA | Namiral (https://focus.namirial.it/obblighi-cybersecurity-nis-2-legge-90-24-regolamento-dora/)

[B006] NIS 2: i rapporti con le altre normative in materia di resilienza e sicurezza informatica - Cyber Security 360 (https://www.cybersecurity360.it/legal/nis-2-i-rapporti-con-le-altre-normative-in-materia-di-resilienza-e-sicurezza-informatica/)

[B007] Primer di regolazione DORA | Comprendi il nuovo atto e come conformarti! (data-privacy.io) (https://data-privacy.io/dora-regulation-primer/)

[B008] Cybersecurity Supply Chain Risk Management (C-SCRM): un approccio dinamico - Rivista Cybersecurity Trends (cybertrends.it) (https://www.cybertrends.it/cybersecurity-supply-chain-risk-management-c-scrm-un-approccio-dinamico/)

[B009] NIS 2 vs. ISO 27001 mapping (advisera.com) (https://advisera.com/articles/nis-2-iso-27001-map/)

[B010] NIS2-Richtlinie: Mit ISO 27001 optimal auf EU-Sicherheit vorbereiten (dataguard.de) (https://www.dataguard.de/blog/nis2-richtlinie-iso-27001-vorbereitung-eu-sicherhei/) ■

Comprendere DORA: un Cambiamento di Paradigma per il Mondo della Cybersicurezza.

Autore: Lisa Ventura

La cybersicurezza è una priorità importante per i governi, le aziende e i singoli individui di tutto il mondo. Le organizzazioni devono spesso districarsi tra una serie di normative, ma tra gli sviluppi normativi degli ultimi anni il più importante è l'introduzione del Digital Operational Resilience Act (DORA). Questo regolamento dell'Unione Europea, adottato nel dicembre 2022, è stato concepito per rafforzare la resilienza del settore finanziario contro le minacce informatiche. Tuttavia, le sue implicazioni vanno ben oltre il settore finanziario, indicando un cambiamento più profondo nelle modalità di gestione e regolamentazione della cybersicurezza in vari settori.

La Genesi di DORA

Il Digital Operational Resilience Act (DORA) è nato dal riconoscimento da parte dell'Unione Europea della crescente interdipendenza tra i sistemi finanziari e le tecnologie dell'informazione e della comunicazione (ICT). La crescente frequenza e sofisticazione degli attacchi informatici, unita alla dipendenza del settore finanziario dalle infrastrutture digitali, ha evidenziato la necessità di un quadro normativo completo che garantisca la resilienza operativa delle istituzioni finanziarie.

Prima dell'introduzione di DORA, le normative sulla cybersicurezza nell'UE erano frammentate, con diversi Paesi che adottavano standard e pratiche differenti. Questo approccio frammentario creava incoerenze e falle nelle difese di sicurezza informatica, rendendo difficile per le organizzazioni orientarsi nel panorama normativo e garantire la conformità. L'obiettivo generale dell'UE con DORA era quello di armonizzare questi standard, creando un quadro normativo unificato che avrebbe migliorato la postura complessiva del settore finanziario in materia di cybersicurezza.

Disposizioni Fondamentali di DORA

DORA è una normativa completa che affronta vari aspetti della cybersicurezza e della resilienza operativa. Le sue disposizioni principali possono essere classificate nelle seguenti aree:

1. Gestione del Rischio ICT

DORA richiede alle entità finanziarie di stabilire solidi framework di gestione del rischio ICT. Questi framework devono includere politiche, procedure e controlli progettati per identificare, valutare, monitorare e mitigare i rischi legati all'ICT. Ciò si estende a tutti gli aspetti delle operazioni

ICT risk management	• Set of key principles & requirements on ICT risk management framework	Chapter II Articles 5 to 16
ICT incident mgmt., classif. & reporting	• Harmonise & streamline reporting, extend reporting obligations to all financial entities & broaden the scope of incidents to be reported	Chapter III Articles 17 to 23
Digital operational resilience testing	• Subject financial entities to basic testing or advanced testing (e.g. TLPTs)	Chapter IV Articles 24 to 27
ICT third-party risk	• Principle-based rules for monitoring third-party risk, key contractual provisions & oversight framework for critical ICT TPPs (cTPPs)	Chapter V Articles 28 to 44
Information sharing	• Voluntary exchange of information & intelligence on cyber threats	Chapter VI Article 45

di un'organizzazione, compresa la protezione dei dati, lo sviluppo del software e i fornitori di servizi di terze parti.

2. Risposta agli Incidenti ICT e Reportistica

In base al regolamento DORA, le entità finanziarie sono obbligate a segnalare alle autorità competenti gli incidenti significativi legati alle ICT. La segnalazione deve avvenire entro tempi rigorosi, per garantire che le autorità di regolamentazione siano informate tempestivamente di qualsiasi evento che possa potenzialmente compromettere la stabilità finanziaria. Il regolamento sottolinea inoltre la necessità di monitoraggio e di valutazione continui degli incidenti, per consentire alle entità di rispondere rapidamente alle minacce emergenti.

3. Test di Resilienza Operativa Digitale

Uno degli aspetti più innovativi di DORA è l'obbligo di effettuare regolarmente test di resilienza operativa digitale (DORT). Si tratta di condurre test completi dei sistemi ICT di un'organizzazione, tra cui test di penetrazione guidati dalle minacce (TLPT), valutazioni delle vulnerabilità e test basati su scenari. L'obiettivo è simulare attacchi informatici reali e identificare i punti deboli prima che possano essere sfruttati da attori malintenzionati.

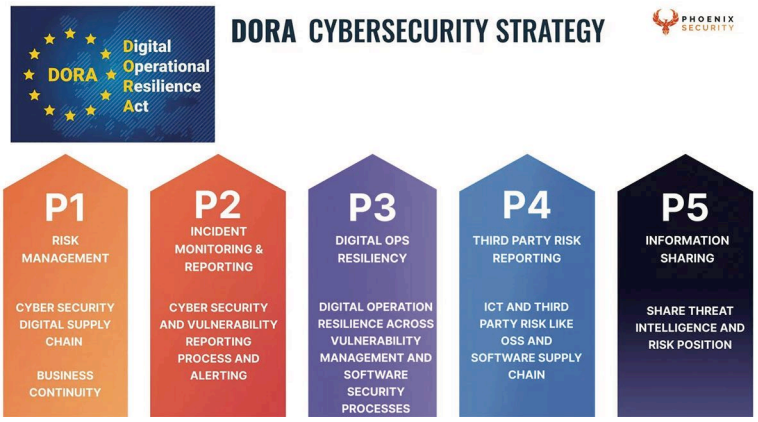
4. Gestione del Rischio delle Terze Parti

Il regolamento DORA pone un'enfasi significativa sulla gestione dei rischi associati ai fornitori di servizi di terzi parti. Data la dipendenza del settore finanziario dai servizi ICT esterni, la normativa richiede alle entità di condurre controlli di dovuta diligenza (due diligence) e un monitoraggio continuo dei loro fornitori terzi. Ciò include la garanzia che i fornitori aderiscano agli stessi standard di cybersicurezza e che gli accordi contrattuali includano disposizioni per la supervisione e la gestione dei rischi ICT.

5. Condivisione delle Informazioni

DORA incoraggia le entità finanziarie a impegnarsi nella condivisione di informazioni con altre organizzazioni e autorità. Condividendo le informazioni sulle minacce e sulle *best practices,* le entità possono migliorare collettivamente le loro difese di cybersicurezza. Questo approccio collaborativo mira a creare un ecosistema finanziario più resiliente, in cui le informazioni sulle minacce e sulle vulnerabilità vengono diffuse in modo rapido ed efficace.

Implicazioni per il Settore della Cybersicurezza



DORA rappresenta un grande cambiamento nell'approccio alla cybersicurezza, in particolare nel settore finanziario. Tuttavia, è probabile che la sua influenza si estenda anche al di fuori di questo settore, influenzando le pratiche e le normative di cybersicurezza in vari settori. Ecco come si prevede che DORA avrà un impatto sul più ampio panorama della cybersicurezza:

1. Migliorare gli Standard di Cybersicurezza

Uno degli effetti più immediati di DORA è l'innalzamento degli standard di cybersicurezza nel settore finanziario. Imponendo pratiche rigorose di gestione del rischio ICT, test regolari di resilienza e una rigorosa segnalazione degli incidenti, DORA stabilisce un livello elevato di cybersicurezza. È probabile che questo favorisca l'innovazione nelle soluzioni di sicurezza informatica, in quanto le organizzazioni cercano di soddisfare questi requisiti rigorosi.

Si prevede un aumento della domanda di tool e servizi avanzati per la cybersicurezza come piattaforme di threat intelligence, sistemi di risposta automatica agli incidenti e rilevamento delle minacce basato

sull'intelligenza artificiale. I fornitori di cybersicurezza dovranno innovare per soddisfare le crescenti esigenze delle entità finanziarie, portando allo sviluppo di soluzioni più sofisticate ed efficaci.

2. Promuovere una Postura di Cybersicurezza Proattiva

In genere, molte organizzazioni hanno adottato un approccio reattivo alla cybersicurezza, affrontando le minacce e le vulnerabilità non appena si presentano. Il regolamento DORA, invece, promuove un atteggiamento più proattivo, sottolineando l'importanza del monitoraggio continuo, dei test regolari e della preparazione agli incidenti.

Questo spostamento verso una postura proattiva della sicurezza informatica influenzerà probabilmente anche altri settori. Poiché le organizzazioni di vari settori riconoscendo i vantaggi di una migliore preparazione alle minacce informatiche, potrebbero adottare pratiche simili, anche se non sono direttamente soggette al regolamento DORA. Questo potrebbe portare a un cambiamento culturale più ampio nel modo in cui la cybersecurity viene percepita e gestita.

3. Favorire la Conformità Normativa

Sebbene il DORA sia un regolamento dell'UE, è probabile che i suoi effetti si estendano oltre i confini europei. Le istituzioni finanziarie che operano in più giurisdizioni dovranno garantire che le loro pratiche di sicurezza informatica siano conformi al DORA, oltre che ad altre normative pertinenti, come il Regolamento generale sulla protezione dei dati (GDPR) e la Direttiva sulle reti e i sistemi informativi (NIS2). Ciò potrebbe favorire la conformità normativa, in quanto altre nazioni potrebbero adottare standard simili per allinearsi al DORA.

Inoltre, le multinazionali potrebbero spingere per l'armonizzazione delle normative sulla cybersicurezza nelle loro operazioni globali, portando a un approccio più unificato alla sicurezza informatica a livello mondiale. Ciò potrebbe ridurre la complessità della conformità e migliorare i risultati complessivi della sicurezza informatica.

4. Migliorare la Gestione del Rischio di Terzi Parti

Il focus sulla gestione del rischio di terzi parti nel DORA evidenzia il ruolo critico che vendor e fornitori di servizi svolgono nella cybersicurezza di un'organizzazione. Poiché le entità finanziarie sono tenute a controllare più da vicino i loro rapporti con le terze parti, è probabile che gli standard di sicurezza informatica lungo la supply chain migliorino.

Questa enfasi sulla gestione del rischio da parte di terzi potrebbe portare allo sviluppo di nuovi framework e strumenti progettati per valutare e monitorare le pratiche di cybersicurezza dei fornitori. Inoltre, i fornitori potrebbero dover migliorare le proprie misure di sicurezza informatica per rimanere competitivi e soddisfare le aspettative dei loro clienti.

5. Promuovere la Resilienza della Cybersicurezza

L'attenzione del regolamento DORA per i test di resilienza e la segnalazione degli incidenti riflette una tendenza più ampia a promuovere la resilienza della cybersicurezza. Nel panorama attuale delle minacce, non è più sufficiente limitarsi a prevenire gli attacchi informatici; le organizzazioni devono anche essere in grado di contrastarli e di riprendersi da essi.

L'enfasi sulla resilienza probabilmente spingerà l'adozione di tecnologie avanzate come l'intelligenza artificiale, il machine learning e l'automazione nella cybersicurezza. Queste tecnologie possono aiutare le organizzazioni a rilevare e rispondere più rapidamente alle minacce, a ridurre al minimo l'impatto degli incidenti e a garantire la business continuity di fronte ai cyberattacchi.

BIO

Lisa Ventura MBE è una pluripremiata specialista di cybersicurezza, scrittrice/autrice pubblicata e relatrice di conferenze. È la fondatrice di Cybersicurezza Unity, un'organizzazione comunitaria globale che si dedica a riunire individui e organizzazioni che lavorano attivamente nel campo della cybersicurezza per contribuire a combattere la crescente minaccia informatica. Come consulente, Lisa lavora anche con i team di leadership della cybersicurezza per aiutarli a lavorare insieme in modo più efficace e fornisce formazione sulla consapevolezza e la cultura della cybersicurezza e sui vantaggi dell'assunzione di persone con disabilità neurologiche. Ha una conoscenza specialistica dei fattori umani della cybersicurezza, della cyberpsicologia, della neurodiversità e dell'IA nel cyber, ed è anche cofondatrice del International Imposter Syndrome Awareness Day. Ulteriori informazioni su Lisa sono disponibili su www.lisaventura.co.uk.
Lisa sui Social Media : X/Twitter - @cybergeekgirl ; LinkedIn - https://www.linkedin.com/in/lisasventura/ ; Facebook - https://www.facebook.com/lisasventurauk; Instagram - https://www.instagram.com/lsventurauk/ ; YouTube - https://www.youtube.com/@CyberSecurityLisa/

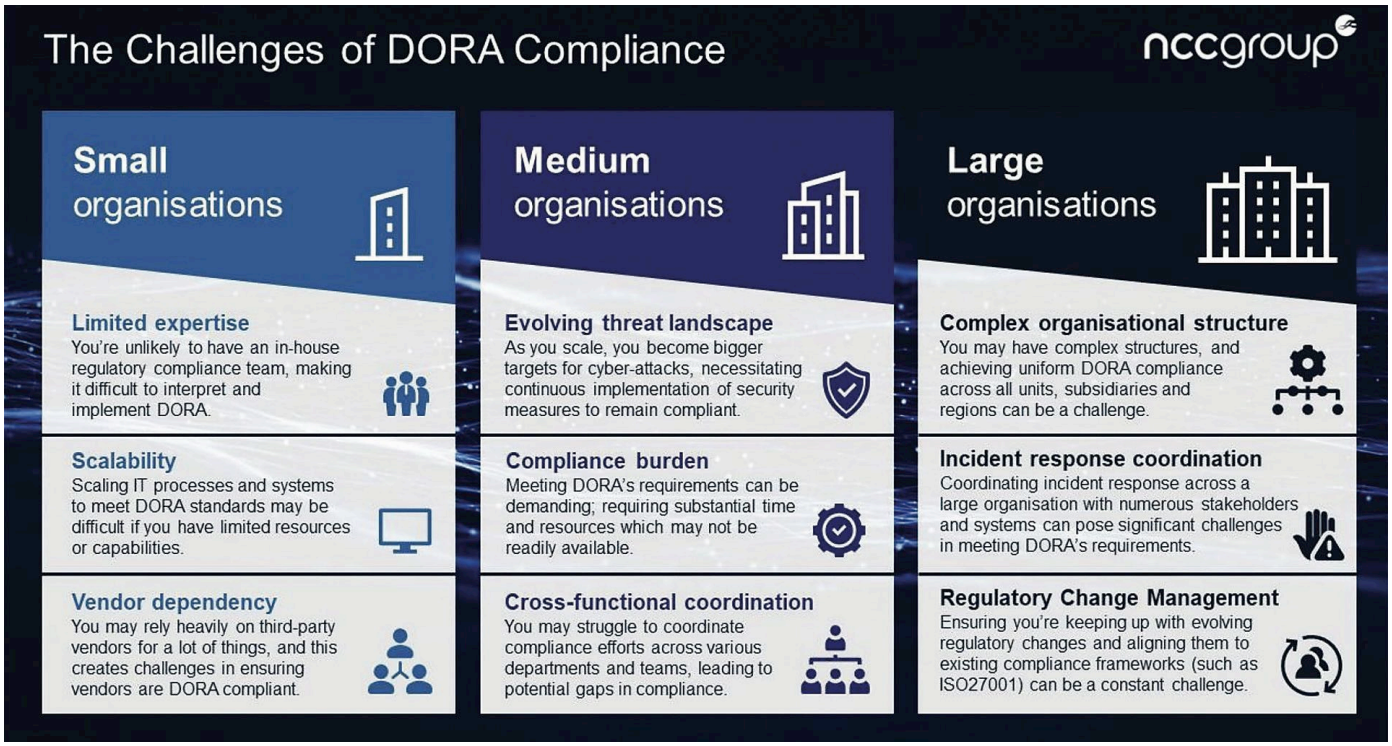
6. Incoraggiare la collaborazione e la condivisione delle informazioni

Le disposizioni di DORA per la condivisione delle informazioni tra entità finanziarie rappresentano un riconoscimento della natura collettiva della cybersicurezza. In un ecosistema digitale interconnesso, la sicurezza di un'organizzazione può avere un impatto sulla sicurezza di molte altre. Incoraggiando la collaborazione e la condivisione delle informazioni, DORA mira a creare un settore finanziario più resiliente.

Questo approccio collaborativo alla cybersicurezza potrebbe estendersi anche ad altri settori. Le organizzazioni di diversi settori potrebbero iniziare a vedere il valore della condivisione delle informazioni sulle minacce e delle best practice, portando a una comunità di cybersicurezza più collaborativa e interconnessa.

Sfide e Criticità del Regolamento DORA

Sebbene DORA rappresenti un significativo passo avanti nel rafforzamento della sicurezza informatica, non è privo di sfide e critiche. L'attuazione dei requisiti del regolamento richiederà un notevole dispendio di



risorse, soprattutto per gli istituti finanziari più piccoli che potrebbero non disporre delle competenze e delle tecnologie necessarie. Il costo della conformità potrebbe essere sostanziale e comportare potenzialmente un aumento dei costi operativi per queste entità.

Inoltre, vi sono preoccupazioni circa il potenziale di eccesso di regolamentazione. Alcune parti interessate del settore hanno sostenuto che i requisiti del regolamento DORA potrebbero essere troppo prescrittivi, limitando la flessibilità delle organizzazioni nell'adottare pratiche di cybersicurezza adatte alle loro specifiche esigenze e profili di rischio. Bilanciare l'esigenza di una solida cybersicurezza con la necessità di flessibilità e innovazione sarà una sfida cruciale sia per le autorità di regolamentazione che per il settore.

Il Futuro di Dora e il Suo Impatto sulla Cybersicurezza

Con l'attuazione del regolamento DORA in tutta l'UE, il suo impatto sul panorama della cybersicurezza continuerà a svilupparsi. È probabile che il regolamento serva da modello per altri settori e regioni, influenzando lo sviluppo di future normative sulla sicurezza informatica. Nel corso del tempo, potremmo assistere a una convergenza degli standard di cybersicurezza tra i vari settori e aree geografiche, che porterà a un ecosistema globale di cybersicurezza più unificato e resiliente.

Per il mondo della cybersicurezza, DORA rappresenta sia una sfida che un'opportunità. Si prevede che la domanda di soluzioni e servizi avanzati di cybersicurezza crescerà man mano che le organizzazioni si sforzeranno di soddisfare i requisiti della normativa. I fornitori di cybersicurezza e di servizi dovranno innovare e adattarsi per rimanere competitivi in questo panorama in evoluzione.

Allo stesso tempo, l'enfasi posta da DORA sulla resilienza, sulla gestione proattiva del rischio e sulla collaborazione potrebbe portare a un cambiamento culturale nell'approccio delle organizzazioni alla cybersicurezza. DORA, dando priorità alla preparazione, alla resilienza e alla condivisione delle informazioni, ha il potenziale per creare un ambiente digitale più sicuro e resiliente per tutti.

Considerazioni finali

Il Digital Operational Resilience Act (DORA) segna una tappa significativa nell'evoluzione della normativa sulla cybersicurezza. Il suo approccio globale alla gestione del rischio ICT, alla segnalazione degli incidenti, ai test di resilienza, alla gestione del rischio da parte di terzi e alla condivisione delle informazioni stabilisce un nuovo standard per il settore finanziario e ha implicazioni più ampie per il settore della cybersicurezza nel suo complesso.

Sebbene l'attuazione del DORA presenti delle sfide, in particolare in termini di costi di conformità e di potenziale severità normativa, i suoi benefici nel migliorare la resilienza e la preparazione in materia di cybersicurezza sono sostanziali. Con la continua evoluzione del panorama della cybersicurezza, è probabile che il DORA svolga un ruolo centrale nel definire il futuro della regolamentazione della cybersicurezza, nel guidare l'innovazione e nel promuovere un ecosistema digitale più resiliente.

Per il mondo della cybersicurezza, il regolamento DORA rappresenta un'opportunità di innovazione e di leadership nello sviluppo di soluzioni che soddisfino le esigenze di un mondo più regolamentato e interconnesso. Poiché le organizzazioni di tutti i settori riconoscono il valore della resilienza e della gestione proattiva del rischio, i principi contenuti nel DORA potrebbero diventare le premesse di una nuova era della cybersicurezza. ■

Regolamento DORA e gestione degli incidenti connessi alle TIC.

Autore: Elena Mena Agresti

Chi nel mondo finanziario e assicurativo in Europa non ha sentito parlare del cosiddetto Regolamento "DORA" sulla resilienza operativa digitale? Penso veramente in pochi considerando che sta impegnando gli uffici di compliance, e non solo, di tutta Europa dediti a garantirne una completa conformità entro fine anno.

DORA, il Regolamento (UE) 2022/2554, si pone come obiettivo l'armonizzazione delle regole di ICT governance e gestione dei rischi ICT per le entità finanziarie nell'UE.

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, responsabile dell'Incident Prevention Management nel CERT di Poste Italiane. Esperta di compliance, standard internazionali, governance dell'information security, gestione dei rischi, security audit, formazione e awareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Orade Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

Stabilisce obblighi uniformi in materia di gestione dei rischi ICT, incidenti, test di resilienza operativa, condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche, misure relative alle terze parti, continuità operativa.

Si applica a tutte le istituzioni finanziarie che operano nell'UE e non parliamo solo di entità finanziarie tradizionali, ma anche di società di assicurazione e riassicurazione ed entità finanziarie emergenti quali ad esempio fornitori di servizi di crowdfunding e di criptovalute, i fornitori terzi di servizi ICT.

Interessando realtà molto differenti per settore, dimensioni, attività, il Regolamento prevede l'applicazione del principio di "proporzionalità" secondo il quale le Entità devono applicare la norma tenendo in considerazione le loro dimensioni e del profilo di rischio complessivo, nonché della natura, della portata e della complessità dei servizi, delle attività e della operatività. Tale principio, prevede dunque che l'Entità debba definire come applicare gli obblighi previsti in base alle proprie specificità che saranno prese in considerazione da parte delle autorità competenti in sede di eventuale riesame di conformità al Regolamento.

Uno dei temi più discussi è la gestione degli incidenti. Pur non essendo un argomento nuovo nel settore finanziario in EU, presenta diverse novità, dai nuovi criteri e soglie per la classificazione degli incidenti gravi connessi alle Tecnologie dell'Informazione e della Comunicazione, c.d. TIC, introducendo all'interno della classificazione anche il tema degli incidenti ricorrenti, al calcolo dei costi e delle perdite associate agli incidenti gravi e dell'identificazione delle minacce informatiche significative, prevedendo anche in questo caso dei criteri di classificazione.

Entriamo dunque nello specifico, da dove deve partire un'entità finanziaria per essere conforme al Regolamento in materia di gestione incidenti?

Di sicuro da un corretto monitoraggio degli eventi e da un processo di gestione degli incidenti connessi alle TIC, tale da eliminarne le cause di fondo e prevenirne il riverificarsi.

Il monitoraggio degli eventi di sicurezza deve essere basato su soglie di allarme, per consentire l'identificazione di attività e comportamenti anomali, e su criteri e meccanismi di allarme automatico per il personale incaricato della risposta agli incidenti, per avviare i processi di gestione e risposta agli incidenti.

Il processo di gestione degli incidenti deve essere ben definito e devono essere chiaramente assegnati ruoli e responsabilità. L'Entità finanziaria deve applicare procedure per identificare, tracciare, registrare, categorizzare e classificare gli incidenti connessi alle TIC in base alla loro priorità e gravità, stabilire procedure di risposta agli incidenti per attenuarne l'impatto e garantire tempestivamente l'operatività e la sicurezza dei servizi, analizzare le cause di fondo e attuare le azioni necessarie ad evitare il riverificarsi dell'incidente.

Il tema del miglioramento continuo e del prevenire il verificarsi di incidenti è molto sentito, al punto da introdurre il concetto di *incidenti ricorrenti* che possono indicare carenze e punti deboli significativi nelle procedure di gestione degli incidenti e dei rischi dell'organizzazione.

Il Regolamento richiede alle entità finanziare di verificare su base mensile la presenza di incidenti ricorrenti collegati da un'apparente causa di fondo simile. In particolare, prevede che gli incidenti ricorrenti che singolarmente non sono considerati incidenti gravi debbano essere considerati come un unico grave incidente se soddisfano tutte le condizioni seguenti:

a. si sono verificati almeno due volte nell'arco di sei mesi;

b. presentano la stessa apparente causa di fondo;

c. soddisfano collettivamente i criteri DORA per essere considerati un grave incidente.

Nel caso di identificazione di incidente grave dovuto a incidenti ricorrenti, questo dovrà essere gestito come qualsiasi altro incidente grave in tutti i suoi aspetti, inclusi quelli di notifica verso le autorità competenti.

È bene sottolineare che non è necessario che l'incidente ricorrente impatti sempre lo stesso servizio critico, ma solo che siano soddisfatte le tre condizioni succitate. Obiettivo del Regolamento è rendere consapevole l'Entità dei punti deboli associati a più incidenti quali processi non correttamente presidiati, carenze tecnologiche oppure organizzative per porne rimedio ed eliminare la causa.

La domanda a questo punto nasce spontanea, quali sono i criteri per classificare un incidente grave? La risposta non è semplice, i criteri sono diversi e in alcuni casi non facili da determinare in sede di incidente. Lo stesso Regolamento prevede che le entità finanziarie possano applicare delle stime per diversi criteri qualora non siano in grado di calcolarle.

Il prerequisito affinché un incidente possa essere considerato grave è che impatti un servizio critico e per farlo, le entità finanziarie valutano se l'incidente interessa o ha interessato servizi TIC o sistemi informatici e di rete a supporto di funzioni essenziali o importanti dell'entità finanziaria o servizi finanziari forniti dall'entità finanziaria che richiedono l'autorizzazione, la registrazione o che sono sottoposti a vigilanza da parte delle autorità competenti. Un incidente su un servizio non critico non può essere classificato come grave ai fini DORA.

Questo ci fa capire come per una corretta gestione e classificazione di un incidente sia indispensabile una identificazione dei servizi critici e delle catene tecnologiche ad essi associate per poterne comprendere immediatamente e a fondo gli impatti in caso di incidente.

La criticità del servizio interessato non è sufficiente affinché un incidente sia classificato grave. L'incidente TIC deve aver comportato anche accessi non autorizzati, dolosi e riusciti ai sistemi informatici e di rete, laddove tali accessi possono comportare perdite di dati[1], oppure soddisfare le soglie di materialità di almeno due dei sei seguenti criteri individuati dal Regolamento[2]:

- **clienti, controparti finanziarie e transazioni:** il criterio si attiva qualora l'incidente interessi: a) oltre 100.000 clienti o il 10% del numero dei clienti o clienti individuati come rilevanti; b) oltre il 10% del numero delle transazioni o il 10% della quantità delle transazioni; c) oltre il 30% di tutte le controparti finanziarie che svolgono attività connesse alla fornitura del servizio interessato dall'incidente oppure in generale controparti finanziarie individuate come rilevanti. Il Regolamento introduce infatti il tema dei clienti

e delle controparti rilevanti intese come quei soggetti (clienti o controparti) che se impattati dall'incidente potrebbero incidere sulla realizzazione degli obiettivi commerciali dell'Entità nonché sull'efficienza del mercato.

- **perdita di dati:** il criterio si attiva se si verifica un impatto sulla disponibilità, l'autenticità, l'integrità o la riservatezza dei dati.
- **impatto sulla reputazione:** nel valutare tale criterio le entità finanziarie tengono conto del livello di visibilità che l'incidente ha acquisito o potrebbe acquisire in relazione a diversi fattori quali la diffusione della notizia sui media con enfasi del relativo impatto, i reclami ripetuti dei clienti o controparti, la possibile incapacità di soddisfare i requisiti normativi, la possibile perdita di clienti o controparti finanziarie, con un impatto significativo sulla sua attività.
- **durata dell'incidente e il periodo di inattività del servizio:** il criterio si attiva se sono raggiunte rispettivamente le 24 ore (durata dell'incidente) e le 2 ore (inattività del servizio). La durata dell'incidente viene calcolata dal momento in cui si verifica (o è stato individuato) l'incidente fino al momento in cui lo stesso è risolto. Il periodo di inattività del servizio, invece, viene considerato dal momento in cui quest'ultimo è totalmente o parzialmente indisponibile per i clienti, le controparti finanziarie e/o altri utenti interni o esterni fino al momento in cui sono ripristinate le regolari attività o le operazioni al livello di servizio fornito prima dell'incidente.
- **estensione geografica:** riflette l'impatto transfrontaliero eventualmente avuto dell'incidente. Il criterio si attiva se è previsto l'impatto su almeno due stati membri.
- **impatto economico:** il criterio si attiva se i costi e le perdite sostenute dall'entità a seguito dell'incidente supera o potrebbe superare complessivamente i 100.000 euro. Il regolamento fornisce una lista di costi e perdite da prendere in considerazione quali ad esempio le perdite dovute ai mancati introiti, i costi del personale, di consulenza, di comunicazione, le spese per inosservanza di obblighi contrattuali, risarcimenti e indennizzi ai clienti.

Nella seguente immagine è presente lo schema proposto dalle Autorità Europee. Come rappresentato, un incidente non è grave se non interessa un servizio critico o quando impatta un servizio critico ma non ha comportato perdite di dati a seguito di accessi malevoli e non attiva almeno due criteri.

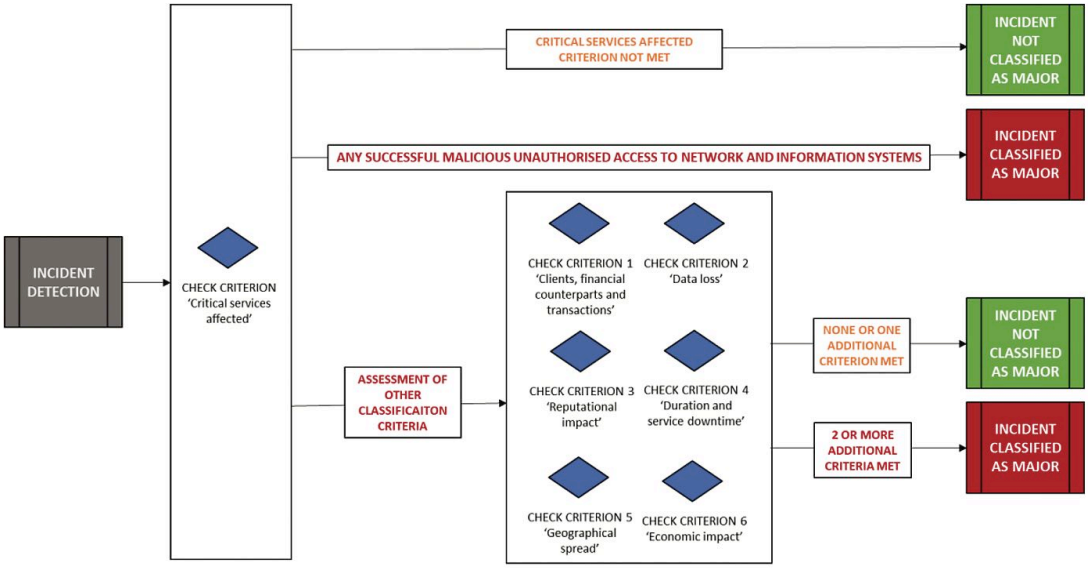
Analizzando i criteri è evidente quanto l'applicazione di una classificazione così complessa richieda l'adozione da parte dell'Entità di una metodologia specifica, del coinvolgimento di diverse funzioni aziendali e della raccolta di informazioni storiche necessarie ad una corretta stima dei criteri.

Il Regolamento prevede, ad esempio, che le entità determino i costi di risarcimenti e indennizzi ai clienti a seguito dell'incidente o che valutino la possibile di perdita di clienti o controparti finanziarie o i costi di consulenza. Come valorizzare in sede di incidente tali parametri? Le entità in sede di prima classificazione difficilmente saranno in grado di valutare la perdita di clienti con un impatto significativo sulle proprie attività così come i risarcimenti e indennizzi o i costi di consulenza che dovrà sostenere. Al contempo però tali valori potrebbero essere stimati prendendo in considerazione incidenti similari avvenuti in passato che possano essere considerati comparabili.

Questo cosa significa? Significa che le entità finanziarie devono arrivare preparate e strutturate per poter classificare un incidente.

L'esigenza di avere stime in base ad incidenti pregressi e l'eterogeneità stessa delle informazioni necessarie richiede il coinvolgimento di diverse funzioni per gli ambiti di competenza, sia per la stima che per il calcolo dei criteri. Tra queste oltre alla security e all'IT cito a titolo esemplificativo le funzioni di Privacy, Comunicazione, Business, Compliance, Risorse Umane, Marketing, Amministrazione Finanza e Controllo.

È bene precisare che le entità finanziarie dovranno valorizzare tutti i criteri per qualsiasi incidente che impatti servizi critici, non solo per la corretta classificazione del singolo incidente ma per identificare un incidente grave dovuto a incidenti ricorrenti e per consentire la stima



dei costi e delle perdite annuali aggregate sostenute a seguito di incidenti. Tranne le microimprese, tutte le entità finanziarie dovranno comunicare la suddetta stima alle autorità competenti in caso di richiesta.

Tale valutazione non dovrà considerare solo la somma dei costi e delle perdite sostenute dall'entità finanziaria a seguito di gravi incidenti TIC (criterio impatto economico) ma dovrà detrarre da essa gli eventuali recuperi finanziari associati all'incidente quali ad esempio risarcimenti da fornitori coinvolti nell'incidente o assicurativi, recuperi fiscali, recuperi di transazioni errate a seguito di malfunzionamenti.

Vi chiederete perché calcolare i costi e le perdite aggregate legate agli incidenti gravi se già viene calcolato l'impatto economico del singolo incidente grave? L'obiettivo è innalzare la consapevolezza delle entità finanziare. Il Regolamento mira, infatti, a potenziare la resilienza operativa digitale delle entità finanziarie anche aumentando la consapevolezza sui gravi incidenti TIC e le loro conseguenze e su quanto la mancanza di resilienza operativa possa compromettere la solidità dell'entità stessa. Una consapevolezza a tutti i livelli. È infatti previsto che le entità finanziarie segnalino agli alti dirigenti interessati almeno gli incidenti gravi connessi alle TIC e informino l'organo di gestione illustrandone l'impatto, la risposta e i controlli supplementari da introdurre.

La consapevolezza non deve essere alimentata solo post incidente ma anche e soprattutto prima che si verifichi un incidente. Per questo motivo le autorità europee richiedono che le entità finanziarie identifichino le cosiddette minacce informatiche significative, ovvero quelle minacce che hanno un'elevata probabilità di concretizzarsi e che in tal caso potrebbero impattare i servizi critici, comportare un incidente e attivare le soglie di rilevanza dei criteri DORA.

Per essere conformi al Regolamento, le entità finanziarie si devono dotate di una metodologia di classificazione delle minacce significative, censirle in un apposito registro e notificarle alle autorità competenti su base volontaria qualora ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti.

Sempre in tema di gestione incidenti, alle entità finanziare è richiesto di censire gli incidenti in apposito registro, conservare la documentazione inerente agli incidenti per un tempo congruo per le finalità previste e di notificare alle autorità competenti gli incidenti gravi connessi alle TIC e, su base volontaria, le minacce informatiche significative.

In conclusione, DORA introduce diverse novità sul tema gestione incidenti per rendere le entità finanziarie più resilienti e consapevoli dei rischi a cui sono soggette. Per una corretta attuazione del Regolamento in materia di gestione incidenti le entità dovranno recepire in primis le grandi novità di DORA aggiornando le proprie metodologie di classificazione adeguandole ai nuovi criteri e soglie introducendo tutti i processi necessari alla corretta stima/valorizzazione, introdurre verifiche almeno su base mensile per l'identificazione di incidenti gravi da incidenti ricorrenti, adottare delle metodologie per l'identificazione delle minacce significative, effettuare una stima dei costi e delle perdite aggregati annuali dovuti a gravi incidenti connessi alle TIC. Non da meno sarà necessario rivedere i propri processi di monitoraggio e gestione.

Infine, è bene ricordare che la conformità al Regolamento è soggetta a verifica da parte delle autorità competenti che hanno la facoltà di imporre sanzioni e richiedere l'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del Regolamento. In caso di verifica, tali autorità possono avere accesso a qualsiasi documento o dato considerato pertinente e svolgere ispezioni o indagini in loco. ■

1. Art.9, 5. B REGOLAMENTO (UE) 2022/2554
2. Art. 8 REGOLAMENTO DELEGATO (UE) 2024/1772 del 13 marzo 2024

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: https://www.itu-cop-guidelines.com/

www.itu.int/cop

Tecnologia e cultura sono inseparabili. Chi si occupa di cybersecurity farebbe bene a ricordarlo.

Intervista VIP a Peppino Ortoleva.

Autore: Massimiliano Cannata

Peppino Ortoleva, professore di storia e teoria della comunicazione, curatore di musei e mostre sulle fenomenologie del cambiamento sociale e tecnologico, editorialista per i quotidiani del Nord Est, è autore di molti saggi di successo. "Miti a bassa intensità", "Sulla viltà", "La comunicazione imperfetta" con Gabriele Balbi, sono solo alcuni dei titoli più recenti. In questa intervista analizza, per la rivista Cybersecurity Trends, la fragilità, i punti di debolezza ma anche le potenzialità di sviluppo della Rete. Il suo è un invito a riflettere su come rendere più efficaci le norme a garanzia dei navigatori - utenti, che spesso si ritrovano nel mare aperto di Internet traditi nelle aspettative di libertà e di crescita della conoscenza che li avevano animati lungo il percorso, scoprendo di essere invece esposti a pericoli invisibili, molto difficili da prevedere e governare.

BIO

Peppino Ortoleva, già professore di storia e teoria della comunicazione, curatore di musei e mostre sulla società, la cultura, le tecnologie del mondo contemporaneo, ha pubblicato tra l'altro "I movimenti del 68 in Europa e in America", "Il secolo dei media", "Dal sesso al gioco", "Miti a bassa intensità", "La comunicazione imperfetta" con Gabriele Balbi.

Professore, il popolo dei cybernauti ha superato i 5 miliardi, viviamo la connettività in una dimensione omeopatica. Potenza e fragilità si toccano. Il sociologo Vanni Codeluppi ha scritto recentemente un saggio sui tradimenti del digitale, che la dice lunga sullo stato di incertezza e di paura che stiamo vivendo. Comincerei col chiederle: siamo a un nuovo, delicato capitolo della "Società del rischio", per usare la celebre definizione di Ulrich Beck?

Tutte le società si possono definire del rischio, nel senso che nessun corpo collettivo può esistere compatto, granitico sotto ogni profilo. Va comunque precisato che nella società dove ci troviamo a vivere vi sono alcuni rischi particolarmente evidenti, che giustificano la definizione dello studioso tedesco. Oltre il rischio ecologico, viviamo da ottanta anni con la guerra atomica sopra la testa, una spada di Damocle, un pericolo per l'umanità tutta. È in questo fragile ecosistema globale che si innestano tutti i pericoli connessi alla rete.

Possiamo prenderli in esame?

Innanzi tutto, va detto che la rete, a differenza di molti altri aspetti della società, appare sregolata proprio in virtù del carattere globale che la

connota. Intendo dire che al di là di tutte le buone intenzioni, le norme, che certamente esistono, sono tali perché ci sono Stati che le varano e le fanno applicare. Il nostro Pianeta è ancora dominato dalle entità statali, il "leviatano" non è scomparso come molti hanno sostenuto, infatuati dal fenomeno della globalizzazione. Insomma, le leggi esistono solo in virtù degli Stati che le fanno osservare, e possono farlo solo all'interno di territori ben definiti.

L'"ubiquità" della rete mette a nudo la difficoltà di governarla

Ci eravamo battuti per un pianeta senza confini, dove la libera circolazione di persone e merci avrebbe dovuto garantire crescita e progresso. Siamo degli illusi?

La realtà è lontana da tanta superficiale retorica. Non voglio negare l'esistenza di un corpus normativo sovrannazionale, che giustifica l'attività di soggetti come l'Unione Europea, il punto su cui vorrei insistere è, però, la centralità degli Stati nel recepimento delle normative continentali. Il risultato di questo dualismo tra regole transnazionali e diritto nazionale è che non abbiamo, a fronte della "ubiquità" della Rete, nessuna entità di dimensioni tali da poterla realmente governare.

Non pensa che qualcosa si stia facendo, se pensiamo al GDPR e all'IA Act che hanno regolamentato le problematiche inerenti alla privacy e all'uso delle macchine intelligenti?

Quello che siamo riusciti a fare riguarda alcuni grossi player economici. Penso alla recente presa di posizione di un giudice federale degli USA che ha sanzionato Google per monopolio applicando una legge fondamentale del sistema statunitense che è quella contro i trust. Un passo avanti importante che si può verificare in culture giuridiche come quelle degli USA o dell'Europa ma altrove, mi chiedo: il fenomeno Internet ha proporzioni gigantesche che rendono poco adeguate le misure di *governance* fin qui esperite. Si è ormai creato un netto spartiacque che spiega molte delle contraddizioni che ci ingabbiano.

A che cosa si riferisce?

Alla dicotomia, che segna anche l'attuale orizzonte geopolitico: da un lato le autocrazie, dove vigono sistemi di governo illiberale che cercano di tenere la rete sotto uno stretto controllo, l'"esempio più importante e conosciuto è quello della Cina; cui si contrappongono i sistemi liberaldemocratici che lasciano alle Authority di settore la possibilità di verificare l'applicazione delle norme vigenti. In questa dinamica accade che nel nostro Occidente si concreta il rischio di una gestione selvaggia del web, a causa della latitanza di qualsiasi intervento di disciplina e controllo.

Alla luce della sua analisi verrebbe da dire che l'idea coltivata da Stefano Rodotà sulla possibile edificazione della "Costituzione di Internet" è destinata a rimanere nel regno delle utopie. È un'analisi corretta?

Per il momento siamo costretti a riconoscere che questa grande intuizione non ha trovato il soggetto

istituzionale che la possa rendere "realtà effettuale" per dirla con linguaggio machiavellico. Alla base di ogni costituzione, diceva un grande teorico come Kelsen, ci deve essere una legge fondamentale che ne certifichi la possibilità di farla valere; serve, scriveva lo studioso nella *"Teoria generale del diritto"* una *Grundnorm*, una sorta di nocciolo duro perché si possa attuare la costituzione stessa, e che dice: "questo sistema normativo è capace di farsi rispettare". Quello che invece vediamo è da un lato l'esercizio dell'autoritarismo nei governi dittatoriali, senza alcuna garanzia per utenti e cittadini, senza costituzioni valide e rispettate, dall'altro l'impotenza, in molti campi, delle democrazie che definiamo occidentali per semplicità. Ma c'è un ulteriore rischio, di natura politica (parlerò dopo degli aspetti legati alla comunicazione), che deve allarmarci: che la Rete diventi uno strumento di guerra.

Quando la Rete diventa strumento di guerra

Come si fa a limitare questa possibilità, che si sta manifestando in questi ultimi mesi, con esiti drammatici?

Quello che sta succedendo adesso fa capire che la rete è un pezzo delle guerre che si combattono nel pianeta. La guerra ibrida, che la Russia sta portando avanti in Ucraina servendosi della rete, può essere efficace perché

è evidente che vi sono partner alleati che la stanno aiutando.

Venendo agli aspetti comunicativi, dobbiamo dedurre che i social hanno una "malattia intrinseca" che ne favorisce l'uso distorto?

È innegabile che i social presentano per loro natura alcune problematiche non trascurabili. A partire dal fatto che si sostanziano di una forma di comunicazione intermedia, che si colloca tra oralità e scrittura. Questo fa sì che riescono a coniugare la dimensione irresponsabile dell'oralità con la permanenza nel tempo e l'autorevolezza della scrittura. Un mix pericoloso. Anche le voci dei bar fanno opinione se diffuse sui social. Come regolare tutto questo?

Ritorna il tema centrale della nostra conversazione. Se interpreto bene il suo pensiero, regimentare i social è un esercizio impossibile oltre che vano. Non ci resta che la resa senza condizioni?

La velocità della divulgazione che corre sui binari social è spaventosa, per altro questi strumenti possono essere completamente gestiti da algoritmi, con la possibilità di diffondere miliardi di messaggi da un'unica fonte, senza alcuna responsabilità legale per quello che viene scritto. Si potrebbe dire che le norme sulla diffamazione possono essere applicate sui social, nel senso che se diffondo la diffamazione contro una persona possono farmi causa, ma solo nel caso in cui sottoscrivo le mie affermazioni. Ma come sappiamo l'anonimato la fa da padrone insieme all'uso degli pseudonimi nei documenti in rete. Mentre nella carta stampata esiste una responsabilità del giornalista, del direttore e dell'editore a seconda dei regimi ordinamentali che vigono nei diversi paesi, on line l'anonimo la può fare franca. Così di fatto risulta impossibile controllare il contenuto di tutte le conversazioni che attraversano *Facebook o X*. Non mi pare sia più sostenibile un simile assetto.

Non pensa che proporre un sistema sofisticato di verifica delle fonti e dei contenuti non finirebbe col rivoluzionare l'universo dei social?

Rispondo utilizzando la sua stessa domanda: perché non rivoluzionarlo? La libertà di pensiero e anche di stampa non è assoluta in nessun sistema né cultura giuridica. Soffermiamoci su chi si occupa di sicurezza, focus di questa rivista: per la cyber security è un problema decisivo sapere e capire da dove arrivano i messaggi offensivi, lesivi della dignità che minano reti e sistemi. Perché non concordare con delle convenzioni internazionali una punizione degli autori di messaggi malevoli, che generano rischi sul fronte delicato della sicurezza della collettività? Il problema non è di facile soluzione, ma dobbiamo metterci nell'ottica di affrontarlo.

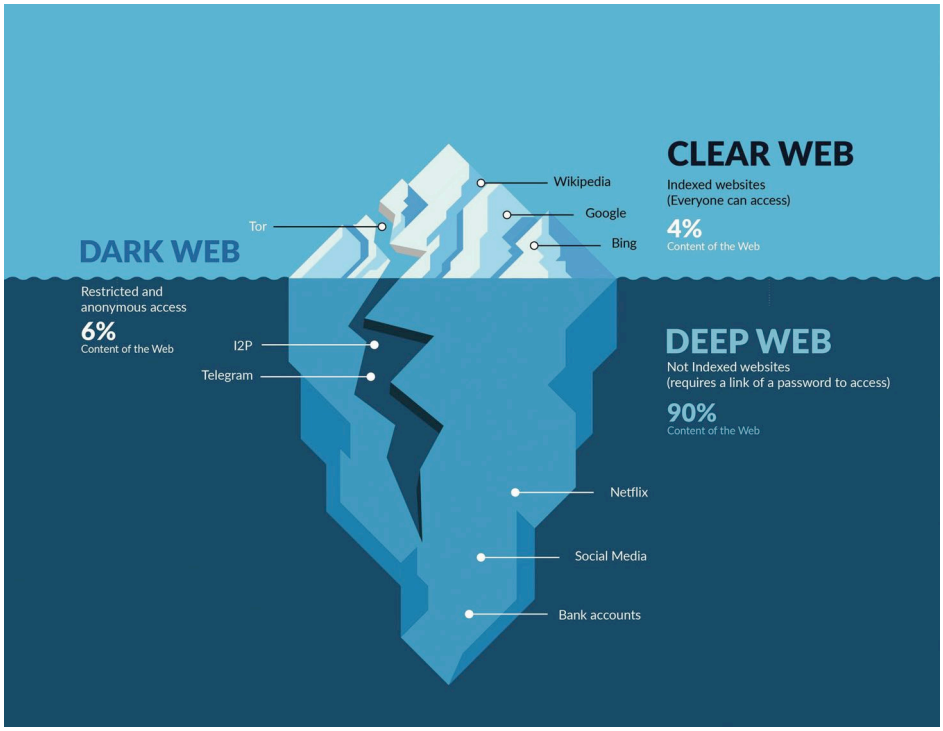
I proclami di *free speech* di gente come Musk non corrispondono a libertà costituzionali come previste originariamente dai padri fondatori delle democrazie: sono "libertà" così incontrollate da diventare minacce. Si combattono delle guerre con i social e sui social. L'uso spregiudicato di questi strumenti non ammette superficialità. Il tema oltre a presentare risvolti delicati che attengono alla cybersecurity, presenta impatti importanti di intelligence. Risulterà decisivo fare una mappatura dei soggetti che gestiscono in modo criminale le tecnologie della comunicazione se vogliamo venirne a capo.

Il dark web, una sfida per la cyber security

Veniamo al dark web, la faccia oscura di Internet. Le difficoltà normative di cui abbiamo parlato si presentano amplificate in questo ambito, con la conseguenza che il nostro senso di impotenza assume forme parossistiche. Come uscirne?

Nel dark web si dà per scontata non solo la libertà di parola, ma anche l'esercizio totalmente sregolato dei crimini più efferati dalla pedofilia al traffico di armi. Sembra di trovarsi come in certi quartieri periferici delle città: le forze dell'ordine sanno che vengono svolte molte attività illecite, ma si astengono in generale dall'intervenire perché preferiscono (la mia è un'ipotesi un po' azzardata ma forse non del tutto campata in aria) che la delinquenza rimanga "confinata" in un certo ambito.

Una zona volutamente franca, eslege come dicevano i giusnaturalisti, da tenere sotto controllo da lontano. L'aspetto più controverso riguarda i contenuti pedopornografici. Nel mondo occidentale la pornografia è stata come è noto liberalizzata con due uniche eccezioni: il sadomasochismo estremo che porta a lesioni gravi o persino alla morte e la pedofilia. La pedopornografia è il limite estremo al quale non si dovrebbe mai arrivare. Oggi sta accadendo, è questo il nodo cruciale, che non siamo in grado



di individuare chi detiene questi contenuti sul proprio computer. Il controllo delle forze dell'ordine scatta nel momento in cui un soggetto viene incriminato per comportamenti criminali, veri o presunti, solo a quel punto si va a setacciare il PC. Il tema su cui riflettere non riguarda il caso degli individui indagati che spesso presentano gravi patologie, riguarda la presunta normalità e quotidianità del dark web che consente il recupero di contenuti e immagini raccapriccianti senza che ci sia alcun responsabile. È evidente che ci sono dei vuoti normativi e gravi difformità che vanno sanate.

Molti dei problemi che Lei ha sollevato derivano da una visione della tecnologia che tende ad assolutizzarla, sganciandola dall'evoluzione della società. Come si fa a correggere il tiro?

Quello che solleva è un fattore cruciale che va chiarito. La tecnologia è un fatto culturale legato al linguaggio, alla comunicazione in tutte le sue forme e molto spesso anche alla capacità di chi la produce di elaborare contenuti originali. La cultura nel suo complesso è un fatto tecnologico, si serve di tecniche per svilupparsi e diffondersi. Il "tam tam" era ai primordi della civiltà una raffinata tecnologia, anche la musica lo è, come gli strumenti musicali che sono parte della storia della tecnologia, sono utensili con caratteristiche tecniche precise. Elenco ed esempi potrebbero continuare a dimostrazione che la separazione tra tecnologia e cultura è artificiosa, ed è stata interiorizzata dalle professioni. Pensiamo agli ingegneri che si presentano come conoscitori solo della tecnologia e ai letterati, storici e filosofi che fanno esattamente l'opposto, vantandosene.

Perché nasce un simile equivoco?

Questa opposizione nasce da un errore antichissimo della cultura occidentale che da sempre tende ad opporre materia e spirito. La cultura avrebbe a che fare solo con lo spirito, la tecnologia con la materia: questa in soldoni la tesi di fondo. Tendiamo dunque a separarli arrivando a errori molto gravi. Uno dei motivi per cui lo sviluppo del web ha travalicato qualsiasi tentativo di governance risiede nel fatto che per troppo tempo è stato visto come un fatto puramene tecnico, i cui contenuti poco contavano. Da questa miopia ha tratto origine la mitizzazione del web come progresso puro in una prima fase, in seguito l'attenzione si è spostata sui contenuti, e si è così passati alla posizione contraria: il web ci sta portando al disastro, perché sta cambiando la nostra civiltà. È evidente che bisogna ritrovare un equilibrio nel modo di vedere questi fenomeni. Dobbiamo, detto in sintesi, sforzarci di guardare socialmente e culturalmente la tecnologia e di osservare tecnologicamente la cultura. Mi rivolgo in particolare a chi opera nel campo della cyber security: se volete migliorare la protezione degli asset a qualsiasi livello non dovete commettere il medesimo errore, separando le due sfere della tecnica e della cultura.

Oggi tendiamo a enfatizzare la dimensione della responsabilità sociale e civile dell'impresa in tutte le sue molteplici sfaccettature. Le chiedo in conclusione: siamo maturi per attuare questi principi o rimaniamo al di sotto di una certa soglia di valori, come spiega molto bene nel suo saggio "Sulla viltà"?

Il concetto di responsabilità può certo essere letto in chiave giuridica, ma per me è profondamento radicato nella dimensione etica. Le scelte dipendono da noi. Spesso si tende a trovare alibi, si ritiene perciò che le persone non siano responsabili per i loro atti. Prevalgono

logiche che attribuiscono la responsabilità delle scelte alla tecnologia troppo potente o a fattori esterni o, in molti casi, a componenti psicologiche che dettato i nostri comportamenti. Pascal diceva che bisogna scommettere su Dio. Anche se sono ateo, nutro la stessa convinzione del pensatore francese. Credo sia l'ora di scommettere sulla responsabilità delle persone. Bisogna partire dall'idea che le persone vanno rispettate nella capacità di controllare i propri atti. Lo vediamo nella concretezza del vivere: dobbiamo sempre rendere conto di ogni passo che compiamo. Si chiama, per citare Weber: *etica della responsabilità,* ogni ragionamento parte da lì. Non vado oltre perché non abbiamo il tempo, né lo spazio per aprire un capitolo troppo impegnativo, ma di importanza capitale per il futuro dell'umanità. ■

La rivoluzione digitale? Va vissuta con spirito critico se non vogliamo cadere nelle false promesse.

Intervista VIP a Vanni Codeluppi.

Autore: Massimiliano Cannata

Sono 5 miliardi i "cybernavigatori" che vivono "nella rete". Un mondo parallelo che si interseca con la vita reale, in un gioco di rimandi e di specchi di difficile interpretazione. Vanni Codeluppi, Professore ordinario di Sociologia dei consumi dell'Università degli Studi di Modena e Reggio Emilia, analizza in un agile e brillante saggio: *"I 7 tradimenti del digitale, ed. Laterza"*, le false promesse di una rivoluzione digitale che ha cambiato la nostra esistenza in maniera radicale, modificando il profilo delle relazioni, ma anche i modelli economici di riferimento.

BIO

Vanni Codeluppi è Professore ordinario di Sociologia dei consumi presso il Dipartimento di Comunicazione ed Economia dell'Università degli Studi di Modena e Reggio Emilia.

Professore, viviamo "nella rete in una dimensione omeopatica", per usare una celebre definizione di De Kerckhove. È per questa ragione che sta venendo meno quel distacco tra "soggetto" e "oggetto" che permette di sviluppare una critica ragionata della "ragione informatica"?

L'importante mediologo canadese Marshall McLuhan raccontava spesso una storiella che parlava di due giovani pesci, i quali incontravano un pesce più anziano. Questi li salutava e poi diceva: «Salve ragazzi! Com'è l'acqua oggi?». I due giovani pesci proseguivano per un po' e poi uno guardava l'altro e si domandava stupito: «Acqua? Che cos'è l'acqua?». Per McLuhan questa storiella esprimeva l'idea che un pesce non sa cos'è l'acqua finché non scopre l'esistenza dell'aria. Secondo lo studioso noi siamo un po' come questi pesci: siamo totalmente immersi nell'ambiente mediatico digitale e

proprio per questo facciamo un'enorme fatica a osservare e comprendere tale ambiente. Eppure, dobbiamo sforzarci di vederlo dall'esterno, per ristabilire quella giusta distanza che possa consentirci di sviluppare un'adeguata riflessione critica.

"I 7 tradimenti del digitale". ***Il titolo, molto ad effetto, evoca i sette vizi capitali. È corretta l'analogia?***

Dando alle stampe questo lavoro, il mio obiettivo era di sviluppare un'analisi critica dell'ideologia che sostiene attualmente lo sviluppo di Internet dal punto di vista industriale e commerciale. Un'ideologia che evidentemente non ha portato i benefici promessi sia ai singoli individui sia alla società nel suo complesso. È indubbio che il mondo digitale abbia portato dei notevoli vantaggi agli utenti, in quanto consente di mettere a disposizione degli elevati livelli di facilità e comodità d'uso, ma negli ultimi decenni si sono progressivamente evidenziati anche i suoi limiti. L'ideologia del web basa il suo funzionamento su sette concetti chiave, a ciascuno dei quali è stato dedicato all'interno del libro uno specifico capitolo. Ogni capitolo affronta un concetto importante di tale ideologia cercando di analizzarlo e di smontarlo.

Le tappe evolutive del digitale

Nel volume vengono ripercorse le tappe evolutive del digitale. È possibile riassumere i tratti salienti di una trasformazione che, soprattutto nell'ultimo ventennio, ha investito l'uomo e la società con una capillarità che non si era mai verificata nella storia di altre pur decisive rivoluzioni scientifiche e tecnologiche?

Credo che sia importante riflettere su quel processo di trasformazione che il mondo digitale opera costantemente sulla nostra realtà sociale. Il mondo digitale, infatti, ha successo perché è un sistema estremamente efficace nel convertire qualsiasi cosa esista nell'universo, come ad esempio i suoni o i dipinti, in un dato numerico quantificabile e calcolabile e pertanto in qualcosa che può essere facilmente stoccato, modificato e diffuso. Ciò spiega perché tutto oggi tenda a essere progressivamente trasformato mediante un processo di digitalizzazione. Gli strumenti digitali però non sempre riescono a registrare tutte le infinite sfumature di ciò che esiste nel mondo fisico. Dunque, la traduzione digitale semplifica e fa sì che inevitabilmente tenda a perdersi una seppur limitata porzione del mondo.

"In un garage può nascere l'idea vincente". ***Cosa rimane dell'insegnamento e della lezione di Steve Jobs?***

L'invenzione di una tecnologia in un garage da parte di un gruppo di giovani "nerd" è una mitologia che numerosi autori hanno dimostrato essere palesemente falsa. Detto questo, è evidente che Steve Jobs, Steve Wozniak e tanti altri geniali giovani americani sono stati in grado di dare vita a un mondo tecnologico innovativo e originale. Ma bisogna soprattutto ricordare che tale mondo non esisterebbe se la ricerca scientifica delle aziende e delle università non fosse stata massicciamente sostenuta dall'esercito e dallo Stato americano attraverso importanti quantità di denaro. È grazie a tali investimenti che abbiamo avuto aziende come Apple, con i suoi prodotti di successo. Un'azienda naturalmente che, dopo la scomparsa di Jobs, non possiede più quella capacità d'innovare che esprimeva in precedenza, anche se rimane comunque una delle realtà tecnologiche più avanzate nel panorama internazionale.

L'illusione della gratuità

Se tutto è gratis, come le multinazionali che hanno in mano il web vogliono farci credere, il valore in rete dove va ricercato?

È noto come nel mondo digitale non ci sia nulla di gratuito. Se non c'è una tariffa da pagare, il valore economico viene prodotto dalle aziende sfruttando il tempo e le informazioni che riguardano la vita degli utenti. Nei primi anni, sembrava che Internet potesse dare vita a un mondo nuovo in grado di realizzare quello spirito di libertà che era stato rivendicato dai movimenti giovanili californiani negli anni Sessanta. Quest'idea ha comportato che ogni richiesta di pagamento dei servizi offerti dalle imprese venisse sistematicamente rifiutata da parte degli utenti, ma tale situazione non poteva essere sostenibile da un punto di vista economico e non a caso si è determinato il fallimento di tutti i servizi d'informazione a pagamento lanciati sul mercato all'epoca.

Questo fenomeno che cosa ha comportato?

Il fenomeno ha reso necessaria un'apertura a forme commerciali di scambio, le quali hanno rapidamente assunto però una forma di tipo capitalistico. Una forma

legittimata da un modello ideologico neoliberista che ha permesso una grande libertà d'azione alle aziende, alcune delle quali, proprio grazie a tale libertà, hanno assunto delle posizioni di tipo monopolistico. Ciò è stato reso possibile anche da quel processo di crescente "mediatizzazione" che caratterizza le società ipermoderne e, all'interno di tale processo, dal ruolo svolto dalle marche aziendali, che operano come veri e propri "ambienti" dove è possibile stabilire una connessione costante tra produttori e consumatori. E dove le marche accumulano pertanto valore sfruttando le conoscenze, i modelli culturali e le innovazioni che vengono prodotte dagli individui e dalla società. Ciò, in generale, tende a

produrre un processo di "fluidificazione" che annulla le differenze culturali e sociali. La società si fa liquida e apparentemente più omologata.

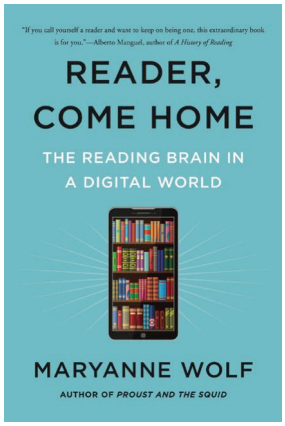
Difficile e impegnativa la* "tutela del corpo elettronico" *come ci aveva insegnato Stefano Rodotà, tanto più in una società in cui il dato è divenuto un* "asset sociale", *una merce preziosa che alimenta il business. Siamo alla società della sorveglianza? Come difenderci da questa deriva?

È difficoltoso difendersi dal cosiddetto "capitalismo della sorveglianza". Abbiamo visto che la barriera della privacy, che proprio Rodotà ha cercato strenuamente di erigere in Italia, è una barriera piuttosto fragile. Assistiamo tutti i giorni a processi all'interno dei quali i nostri dati personali sono oggetto di strategie aziendali di appropriazione e trasformazione in valore economico. E nei prossimi anni il diffondersi dei nuovi programmi basati sull'intelligenza artificiale non potrà che peggiorare questa situazione, dato che tali programmi non possono fare a meno di nutrirsi di un'enorme quantità di dati.

La perdita del "logos" e la vetrina del metaverso

Il filosofo Paolo Ercolani affrontando le contraddizioni dell'IA nel saggio* "Nietzsche l'iperboreo", *ed.* Il Melangolo*) paventa il rischio di una perdita del "logos" già documentata nelle difficoltà cognitive registrate dalle nuove generazioni. Quanto è reale questo pericolo?

In effetti, questo rischio è piuttosto reale. È evidente che nel mondo digitale odierno si affermano dei nuovi "stili cognitivi" che sono principalmente fondati sul linguaggio visivo e sulla simultaneità. Degli stili nei quali la visione delle immagini opera come la fonte primaria per acquisire conoscenze. Le ricerche empiriche condotte negli Stati Uniti da Maryanne Wolf e altri studiosi mostrano che, in conseguenza di ciò, le persone stanno perdendo la capacità di effettuare quella che chiamano "lettura profonda". Ciò vale a maggior ragione per gli adolescenti, che sono maggiormente vulnerabili perché si trovano nella critica fase di costruzione dell'identità adulta. Essi, dunque, sembrano dipendere in una maniera quasi morbosa da quei linguaggi iconici che predominano all'interno dello smartphone e va considerato che questo strumento non è un concentrato solamente di funzioni, ma anche di promesse. Sono promesse di contatto con gli altri, di autorealizzazione, di comprensione della realtà. In una parola di felicità. Che purtroppo raramente si presenta, anzi gli studi più recenti ci dicono che proprio chi passa più tempo con questi strumenti possiede di solito un più elevato tasso d'insoddisfazione.



Lei dedica un capitolo alla realtà virtuale, che Pierre Levy in un celebre saggio considerava una categoria dell'essere che si aggiunge alle tradizionali categorie elencate da Aristotele e nella modernità da Kant. Sulla base di questa consapevolezza che dobbiamo dare per acquisita, quali prospettive si aprono per la riflessione teoretica e sociologica?

Credo che il concetto di realtà virtuale sia abbastanza sopravvalutato. Gli artisti hanno sempre cercato di costruire dei mondi di finzione alternativi rispetto a quelli quotidiani. Hanno utilizzato a tale scopo diversi strumenti espressivi, come il linguaggio orale, la parola scritta e la scrittura alfabetica. E a volte la funzione esercitata sul piano sociale dalle diverse forme di scrittura è stata affiancata dall'analogo ruolo svolto dalla rappresentazione teatrale. Quando è arrivata la stampa, tale invenzione ha spinto ulteriormente in avanti questo processo. E così è successo per i media successivi. Via via, dunque, le persone si sono abituate a una forma di conoscenza che è in grado di assumere un carattere autonomo rispetto al contesto sociale all'interno del quale agisce. La realtà virtuale è soltanto più potente, ma va considerato che la sua diffusione incontra ancora diversi ostacoli.

"La vetrinizzazione sociale" è il titolo di un suo scritto che ha riscosso molto interesse e successo. È il metaverso la nuova vetrina? Nel gioco degli specchi generato da una realtà che ancora non conosciamo stiamo aprendo* "il laboratorio dell'uomo immortale"*?

Credo si possa dire che anche il metaverso sarà uno spazio nel quale gli individui dovranno "vetrinizzarsi". Anche in questo caso ci sono ancora diversi ostacoli da superare sul piano tecnologico, se però entreremo nel "mondo del metaverso", questo non potrà che essere anch'esso "vetrinizzato". Già oggi il profilo personale che ciascun utente è in grado di costruirsi all'interno dei social media richiede agli individui di raccontarsi e presentarsi al meglio. Si dà così vita a una vera e propria vetrina virtuale personalizzata. E si riducono pertanto i contatti "faccia a faccia", nei quali ci si incontra fisicamente con gli altri, mentre aumentano le possibilità di manipolare la propria identità personale da "dietro le quinte" dello schermo di una qualche vetrina digitale. Grazie alle possibilità tecniche offerte dai social media, tutti sono dunque costantemente impegnati oggi nel definire l'immagine personale che desiderano e nel cercare di gestirla attivamente. E lo saranno probabilmente sempre più in futuro. ■

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Psicologia Comportamentale e Resilienza Operativa con il DORA

Nel campo della sicurezza informatica, il DORA rappresenta una normativa chiave per rafforzare la resilienza operativa digitale delle istituzioni finanziarie e delle infrastrutture critiche.

Per rispettare pienamente i requisiti del DORA, è importante considerare anche il comportamento umano a adottare una maggiore consapevolezza dei rischi comportamentali che possono compromettere la sicurezza.

DORA e Comportamento Umano: Costruire una Cultura di Resilienza

PROMOZIONE DI UNA CULTURA DELLA SICUREZZA
Il DORA richiede una cultura della sicurezza a tutti i livelli aziendali. Considerare fattori come il senso di urgenza, la paura, aiuta a costruire una cultura dove i dipendenti sono attivamente coinvolti e consapevoli del loro ruolo nella sicurezza, rispettando le direttive del DORA.

FORMAZIONE PSICOLOGICA PER LA SICUREZZA
Integrare la formazione psicologica è cruciale per aiutare i dipendenti a gestire pressioni come il sovraccarico informativo e i bias cognitivi. Questo tipo di formazione li prepara a riconoscere e contrastare comportamenti rischiosi, rendendo le difese aziendali più forti e resilienti.

RIDUZIONE DEGLI ERRORI UMANI
I fattori psicologici come l'eccesso di fiducia o la sottovalutazione delle conseguenze sono spesso alla base degli errori che compromettono la sicurezza. Lavorare su questi aspetti aiuta le aziende a rispettare gli standard di resilienza richiesti dal DORA.

In questo modo, l'azienda oltre a rispettare i requisiti di compliance, sviluppa anche una cultura resiliente, capace di adattarsi alle sfide digitali.

Un approccio integrato, che includa elementi psicologici, può aiutare i dipendenti a riconoscere e prevenire comportamenti rischiosi, proteggendo l'organizzazione da possibili minacce.

Attraverso una formazione mirata, i dipendenti imparano a gestire le pressioni quotidiane, acquisendo una maggiore consapevolezza dei rischi e delle proprie reazioni emotive, sviluppando così abitudini di sicurezza più solide.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Mario Caligiuri
MALEDUCATI
Luiss University Press

Autore: Massimiliano Cannata

Un nesso inscindibile deve legare qualità dell'istruzione, informazione e democrazia

Conoscere il mondo per leggere i fenomeni e anticipare i cambiamenti, abbiamo progressivamente smarrito questa fondamentale capacità interpretativa del tempo presente per una ragione tanto semplice quanto evidente: l'educazione ha perso la sua centralità. Da fattore di progresso civile e democratico è stata derubricata nelle agende dei governi, dimostrando la grave malattia di cui sono affette le *élite* che hanno in mano il futuro dell'umanità. Questa la tesi di fondo dell'interessante e intenso saggio di Mario Caligiuri ***(Maleducati, Luiss University Press)*** che sta suscitando un ampio dibattito. Quanto sia cruciale il tema appare persino superfluo sottolinearlo. In questo cambiamento epocale, bisognerebbe attrezzarsi di un corredo sempre più ampio e articolato di saperi, per sfidare i livelli di complessità crescente che segnano la contemporaneità. Invece, per un'incomprensibile inversione delle priorità, la politica sembra dimenticarsi della scuola e dell'Università, salvo richiamarla in causa in occasione di qualche comizio o programma preelettorale. Così mentre assistiamo a un eccezionale progresso della scienza e della tecnologia che stanno portando le macchine "intelligenti" a dialogare con l'individuo, mimandone anche le facoltà superiori, che credevamo fossero nostra esclusiva prerogativa di specie, si registra, non solo nelle nuove generazioni, un grave deficit cognitivo. "Servirebbero – scrive Caligiuri – risposte visionarie, mentre di fatto restiamo atrocemente fermi, prigionieri di metodi di trasmissione della conoscenza vetusti, costruiti su linguaggi superati, su pratiche obsolete".

Il sistema educativo deve fare un "passo oltre"

La denuncia suona come uno schiaffo nei confronti di tutto un sistema educativo chiamato a compiere un "passo oltre" per interpretare, per dirla con le parole di Emanuele Severino, "la tendenza fondamentale del tempo che viviamo". La riluttanza al cambiamento che si è intrecciata con una diffusa resistenza all'innovazione, ha permesso al potere di conservare le posizioni e di vivere di rendita. Siamo così precipitati in una "società fantasma", sono parole dell'autore, che senza remore da pedagogista intende scuotere i colleghi, auspicando un radicale ripensamento della disciplina. "Siamo tra i paesi occidentali in cui più drammatico si presenta lo scarto tra realtà e percezione della realtà. Nuotiamo come pesci dentro l'acqua di una disinformazione creata ad arte. Come sosteneva **Marshall McLuhan** proprio perché ci viviamo dentro, non sappiamo valutare le caratteristiche del liquido da cui traiamo il nutrimento". Un liquido va detto, sempre più tossico a giudicare dal crescente fenomeno delle fake news e dal costante e sistematico lavoro di disinformazione, che "avvelena i pozzi" disarmando il pensiero critico del corpo collettivo.

In questa drammatica "allegria dei naufragi" la verità è rimasta sommersa, entrata in crisi. La sua ricerca aveva orientato tutto il pensiero occidentale fin dalle origini, sembra ormai una pratica passata di moda. Nei regimi autoritari viene calpestata, nelle democrazie, invece di essere il fulcro del dibattito, viene artatamente soffocata da potentati economici transnazionali, che muovono la "macchina del fango" traendo profitti dalla falsificazione della realtà. Ed è così che è avvenuto nella "società liquida" di **Zygmunt Bauman**, si è imposta una sorta di "consenso solido" determinato dall'esclusione di una base sociale sempre più ampia, (più del 50% il dato italiano) che non prende parte al gioco democratico, il cui esito risulta scollato dalla volontà del paese reale. In questa dinamica prende corpo quella che molti studiosi definiscono autocrazia elettorale, che dà origine a una grave perdita di interesse per la "cosa pubblica". Il fenomeno, che purtroppo sta investendo numerosi Stati dell'Occidente, esprime e si sostanzia nel filo rosso su cui si regge la trattazione di Caligiuri: il delicato rapporto che dovrebbe legare educazione, disinformazione e democrazia.

La democrazia non può ridursi a "procedura elettorale"

Solo l'educazione dei cittadini e delle *élite* può rendere effettiva la pratica democratica senza ridurla a semplice procedura elettorale, cosa che sta causando l'inefficienza degli esecutivi in molti paesi. Esiste una discrasia tra il tempo educativo e l'immediatezza dell'informazione. Abbiamo probabilmente dimenticato che la professionalità si costruisce in percorsi lunghi, faticosi, spesso accidentati, che non possono risolversi nel "singhiozzo" di un semplice tweet. La conseguenza di questa grave contraddizione la si può vedere nella progressiva perdita di competitività del nostro sistema-paese. Le multinazionali finanziarie e gli Stati autoritari si alimentano della straordinaria capacità di manipolazione delle informazioni, guadagnando, in una sorta di "guerra ibrida" non convenzionale che non ha bisogno apparentemente di nessuna "arma", terreno nello scacchiere geopolitico. Se per quanto detto appare incerta la comprensione, incerta la descrizione del contesto del cambiamento, instabile diventa l'organizzazione sociale che ne discende, che porta con sé un'inevitabile arretratezza dei sistemi legislativi. L'autore fa riferimento a **Hans Magnus Enzensberger** che ha denunciato in molti scritti l'inanità di una politica che

non decide più nulla del futuro. Entra in campo quando fatti e idee diventano un banale oggetto di nutrimento di quella che il grande pensatore tedesco **Martin Heidegger** chiamava "chiacchiera", e che oggi definiamo, in modo ancora più prosaico, gossip. Questa "pericolosa distrazione" delle classi dirigenti è forse l'alert più urgente che Caligiuri, (che ricordiamolo oltre ad essere uno stimato pedagogista è, non a caso, il fondatore e direttore del Master in intelligence dell'Università della Calabria, scuola superiore accreditata a livello internazionale) lancia all'opinione pubblica.

Una pedagogia per il XXI secolo

Nella fluidità dell'universo delle "non cose" per usare una brillante immagine del filosofo **Byung Chul Han**, che ci fa perdere l'abitudine di vivere il reale, bisogna rimettere in sintonia il tempo educativo, con il tempo dei diritti e del rispetto dei valori democratici, la cui conquista è costata il sacrificio di intere generazioni di donne e uomini.

Bisogna mettere in campo una pedagogia per il XXI secolo, da costruire pezzo per pezzo, per sanare un'*"inferma scienza"*, si potrebbe sintetizzare con queste parole il manifesto di impegno culturale che l'autore mette in campo, per sconfiggere la dittatura del "pensiero debole" che ha defocalizzato la mission strategica delle agenzie del sapere che dovrebbero amministrare, senza discriminazioni e con universale apertura, il prezioso giacimento delle conoscenze. Se questo non avverrà assumeremo le sembianze, come viene sottolineato nelle ultime pagine di "Maleducati", degli ***orologi di Dalì "molli che segnano ore diverse",*** senza forma scivolano su piani inclinati, che sembrano rappresentare il precipizio della nostra crescente ignoranza, rispetto al mondo e ai fenomeni antropologici, sociali ed economici che lo attraversano. ■

Paolo Benanti, Sebastiano Maffettone
Noi e la macchina
Luiss University Press

Autore: Massimiliano Cannata

Ipotesi di dialogo tra etica, scienza e tecnologia

"Umanizzare la tecnica, non macchinizzare l'uomo". Si potrebbe condensare in questa sintetica affermazione, contenuta nell'introduzione del saggio, la tesi di fondo attorno a cui ruota il fitto dialogo tra padre Paolo Benanti e Sebastiano Maffettone.

Teologo, specializzato in bioingegneria e neuroscienze, consigliere del Papa, il primo; filosofo della politica, direttore dell'Osservatorio Ethos della Luiss, grande conoscitore e divulgatore

del pensiero di John Rawls in Italia, il secondo. Due voci impegnate nel Pianeta e per il Pianeta. Siamo nel post-umano, dove macchine intelligenti parlano con noi e meglio di noi, dove il virtuale è una categoria dell'essere, dove viviamo la rete senza una distinzione tra dentro e fuori. Padre Benanti spiega: "Dobbiamo gestire un nuovo potere, il potere computazionale, in cui la realtà è definita dal software. L'auto è l'emblema di questa trasformazione. Non negoziamo più il suo acquisto, possediamo solo la licenza d'uso degli oggetti. Possiamo, una volta acquistato, usare a nostro piacimento lo smartphone, ma lo sfruttamento dei dati che convergono su quel bene, che sia un cellulare o un'auto è solo parzialmente e temporaneamente appannaggio nostro. Le stesse gerarchie di potere si stanno modificando, mentre le categorie del possesso e della sicurezza stanno mutando il loro profilo". Nella *software defined reality* si gioca la sfida delle etiche contemporanee, mentre i livelli di automazione sempre più spinti rendono sfumata la linea del percepibile. Fatti come quelli avvenuti in Libano con l'esplosione simultanea degli strumenti cerca persone, la guerra ibrida che non ha più un fronte individuabile, fanno riflettere sulle categorie della sicurezza e del possesso che hanno cambiato codice e che devono essere ancora metabolizzate culturalmente e socialmente nella nuova dimensione del digitale.

È evidente che ci sarà molto da lavorare non solo per gli scienziati, ma anche per giuristi, economisti e filosofi. Non bisogna avere paura di raffermare il "pregiudizio umanistico" scrivono gli autori, magari nella speranza di far rifiorire "l'umano nella stagione dominata dalla *machina sapiens* che vuole competere con la nostra specie. È urgente riportare al centro dei processi di *decision making* non solo le tecniche, ma anche tutta una serie di dimensioni antropologiche ed etiche. C'è bisogno di una nuova agorà dove tornare a rendere possibile la convivenza umana". Affermazione forte perché chiama in causa il luogo del confronto dove nasce la democrazia, che senza la partecipazione di cittadini che appaiono sempre più lontani dalla politica "ingoiati" dal virtuale, appare destinata a tramutarsi in una pericolosa "democratura", per usare un neologismo oggi in voga.

L'alba di un nuovo mondo

Siamo all'alba di un nuovo mondo? Difficile dirlo. Neanche Colombo all'alba del 3 agosto del 1492 dopo aver allestito le tre caravelle poteva immaginare la portata della rivoluzione che avrebbe innescato. Le sue mappe geografiche erano lacunose, anche le nostre mappe cognitive lo sono. Il grande navigatore agognava la meta, sicuro che durante il percorso

avrebbe aggiornato la cartografia senza farsi disorientare. La nostra condizione è la stessa, camminiamo verso l'ignoto, non sappiamo la catena di implicazioni che l'uso dei potenti strumenti del digitale comporterà, intanto andiamo avanti. Per governare la paura, istintiva e incomprimibile possiamo solo tentare di aumentare il grado di conoscenza di cui disponiamo. Se ormai l'"anima dell'universo è data dal software, come sostiene padre Benanti, il tesoro che muove economia e società è rappresentato dai dati e dalle informazioni. Quello che dobbiamo affrontare soprattutto in un'Europa sconvolta che ha sperimentato il disastro del totalitarismo, è un nuovo inizio, una nuova "età dei diritti", per usare la celebre definizione di Norberto Bobbio.

L'innovazione richiede competenza e consapevolezza

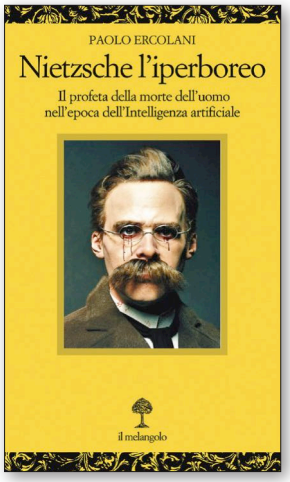
È venuto insomma il tempo di cominciare a maturare una coscienza giuridico – filosofica oltre che tecno-scientifica, che ci permetta di proteggere l'individuo nel divenire di un eco-sistema che sarà segnato dalla prepotente evoluzione del digitale. La riemersione dell'etica comincia proprio da qui, non vuole assumere (almeno nell'intento degli autori) le sembianze di uno strumento per eleganti disquisizioni accademiche, ma quale cemento fondante degli stili di comportamento di chi a un diverso livello opera nella sfera pubblica. Le stesse dinamiche evolutive del capitalismo potranno beneficiare dalla ricerca di un bilanciamento tra *psiche e techné*, le due sfere di quella polarità indagata a fondo in un celebre scritto di Umberto Galimberti. Dentro le due sfere è, infatti, possibile trovare la struttura profonda del "salto di paradigma" che ci ha trascinato dentro una rivoluzione epocale tutta ancora da indagare e conoscere. ■

Paolo Ercolani
Nietzsche l'iperboreo
Ed. Il Melangolo

Autore: Massimiliano Cannata

IA, transumanesimo e potere della tecno-scienza

Nel ponderoso e affascinante saggio *"Nietzsche l'iperboreo"* Paolo Ercolani - filosofo dell'Università "Carlo Bo" di Urbino, ricercatore presso il "Dipartimento di scienze dell'uomo" - traccia un percorso molto preciso mettendo in guardia il lettore dalla pericolosa prospettiva, alimentata da una significativa schiera di cantori acritici della potenza tecnologica, che vede come attuabile il sogno dell'uomo di ogni tempo: superare la morte. Sgombriamo subito il campo da un possibile equivoco: Ercolani non è un "apocalittico", conosce bene il digitale, lo adopera nelle sue lezioni quotidiane, se ne serve per rendere più capillare ed efficace il suo insegnamento, frequenta i social dove instaura un vivace dialogo



con colleghi, studenti, fruitori dei suoi scritti. Dove sta allora il problema verrebbe da dire? Il problema esiste perché viviamo in un tempo ricco di opportunità, come dimostrano le straordinarie applicazioni dell'IT e delle reti neurali che promettono un allungamento della vita, un potenziamento delle capacità diagnostiche, persino la possibilità di regolare il traffico liberandoci da questa "prigione" della modernità, ma non tutto converge verso un reale progresso della condizione umana. Qualcosa non funziona se si guarda all'innalzamento dei rischi fisici e informatici, al generale male di vivere che coglie le generazioni trasversalmente, al solipsismo tecnologico nuova malattia del nostro tempo, all'emersione *dell'homo stupidus stupidus*, al contraltare di quella specie *sapiens* che sembrava inattaccabile, come ben tratteggiato da un celebre saggio di Vittorino Andreoli (ed Rizzoli). Ed ecco che in questo orizzonte chiaroscurale apparire l'ombra di Nietzsche che si proietta sulla prospettiva del post umano, che il prepotente sviluppo dell'IA e dei più sofisticati strumenti della tecnica rendono di pressante attualità. Stiamo aprendo il laboratorio dell'uomo immortale. "Le conseguenze potrebbero essere molto gravi. I teorici del transumanesimo - la corrente filosofica che sta dietro all'Intelligenza artificiale spiega Ercolani - partono proprio da Nietzsche e dal suo proclamare la «morte» di Dio, sostanzialmente per dichiarare la fine di ogni riferimento che si sappia aggrappare ad appigli trascendenti. In sintesi, ogni ragionamento speculativo vuole convergere in una tesi di fondo: il «superuomo» va realizzato in questa vita, superando l'umanità come l'abbiamo conosciuta fino ad oggi, con tutti i suoi limiti e le sue miserie. Questo può avvenire a condizione che gli uomini siano disposti a fondersi con le macchine, a divenire cyborg, a trasferirsi nel Metaverso, dove tutto diviene lecito. Non c'è dubbio che ci troviamo di fronte a una nuova religione, che diffonde speranze anche approfittando della crisi del Cristianesimo. Se il cielo è vuoto, occorre restare «fedeli alla terra» e qui cercare il modo di costruire la superumanità. Evolversi o morire, questo il mantra dei transumanisti".

Scrivere col "sangue", ma la verità non muore

Il riferimento a uno dei pensatori più complessi della contemporaneità, che scriveva "col sangue" come si legge nel testo preda di una malattia creativa che lo manteneva sul difficile crinale della pazzia, corre lungo il filo argomentativo di una ricerca densa di riferimenti alla storia della filosofia. "Leggere Nietzsche – prosegue l'autore - è una boccata d'ossigeno puro per il cervello nonché un'iniezione di adrenalina per l'anima. Il suo pensiero è «dinamite», per usare le sue stesse parole, e questa può rivelarsi assai pericolosa, perciò dobbiamo riflettere, imparando ad

analizzare le cose. Così come nel Novecento furono i nazisti a trarre ispirazione dal suo pensiero, nel XXI secolo lo sono i transumanisti. Questo conferma la grandezza oltre che l'imperitura attualità di Nietzsche, ma deve anche mettere in guardia tutti coloro che a un'umanità di ariani o di cyborg ne preferisca un'altra composta da individui per quanto possibile liberi, uguali e fratelli nel senso della comunanza della condizione esistenziale".

La catena di implicazioni affrontata nel saggio è molto ampia, presentando delle ricadute, pratiche decisive anche per chi fa il difficile mestiere della cyber sicurezza. In ossequio all'insegnamento di Domenico Lo Surdo, maestro di Paolo Ercolani, bisogna ricordare la lezione che abbiamo appreso da Hegel, Marx e Gramsci: "la teoria è sterile senza prassi, ma la prassi è cieca senza teoria". Infatti, c'è bisogno di molta capacità speculativa oltre che di visione, merce rara nel mondo superficiale in cui ci muoviamo, se non si vuole cadere in un relativismo senza prospettiva che porta alla perdita di orientamento e alla mortificazione della verità, schiacciata dalla forza degli interessi di un mercato globale, che non va incontro ai reali bisogno dei cittadini, mortificando quel bene comune, che dovrebbe essere la "stella polare" cui orientare ogni sforzo.

Il filosofo tedesco ha tentato di squarciare *"l'aurora boreale delle illusioni"* (in questa chiave si spiega il titolo del saggio n.d.r.) ha guardato l'abisso restando prigioniero della cieca volontà di potenza, noi dobbiamo riaverci, uscire dalla gabbia delle falsificazioni per ritrovare la capacità di una lettura critica del presente.

"Filosofia è potere"

Altro aspetto inedito che la corrente del transumanesino sta mettendo in campo è quello di una filosofia che va a braccetto con il potere. "Non parlerei di alleanza – precisa lo studioso - il transumanesimo è il potere stesso. Musk, Zuckerberg, Page, solo per fare alcuni nomi, si definiscono tutti transumanisti e non credo vi siano dubbi sul fatto che queste figure detengono un'influenza enorme sull'opinione pubblica mondiale. Le prime sette società della Silicon Valley hanno dei ricavi che superano di gran lunga il PIL di molti Stati di dimensioni medio-grandi. Il potere odierno è quello tecno-finanziario, in grado di dettare l'agenda ai governi politici. Mi sembrano evidenti le implicazioni per le nostre democrazie: un sistema che riesce a impoverire le facoltà critiche del popolo e, allo stesso tempo, stabilire l'agenda politica ai governi eletti da quello stesso popolo, si rivela come un tipo di potere dalle facoltà inaudite". Quello denunciato da Ercolani è un totalitarismo che non ha neanche bisogno dell'uso della censura per imporsi. "Tutti noi, ormai ipnotizzati dagli schermi colorati, ci siamo consegnati mani e piedi a questi "poteri" con l'entusiasmo di tanti "novelli" Pinocchio".

Insomma, è ora di svegliarsi dal "sonno dogmatico", il messaggio che ne ricaviamo noi lettori. D'altra parte, i filosofi ci sono da sempre soprattutto per questo, altrimenti di che cosa stiamo parlando? ■

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

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

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