IL SOLE 24 ORE – 16 LUGLIO 2025

La sicurezza digitale è una infrastruttura economica

di Pierluigi Iezzi

Da “corona” a “cornua”: il semplice errore di un copista medievale nella trascrizione della Vulgata di San Girolamo, traduzione latina dal greco della Bibbia dei Settanta, è bastato per gettare in confusione l’iconografia di uno dei massimi patriarchi dell’Antico Testamento e far spuntare sulla testa di Mosè, anche nelle rappresentazioni più celebri come quella di Michelangelo, un paio di corna. Quando invece il testo ebraico originale riportava che egli era disceso dal Sinai con la testa coronata di raggi dopo aver ricevuto un secondo paio di tavole della legge e aver visto il volto del Signore.

Se la trascrizione inesatta di una lettera in uno dei testi più controllati dell’umanità han potuto ingenerare per secoli un simile equivoco, nel mondo contemporaneo in cui l’integrità del dato è costantemente minacciata da errori – accidentali e no – il rischio di una rappresentazione erronea della realtà è alta. Soprattutto se essa, come ormai è comune, passa attraverso il mondo digitale.

La cybersicurezza da disciplina tecnica diviene quindi presidio della fiducia, un garante di senso, un custode del verbo. Proteggendo il dato, tutela soprattutto ciò che esso diviene.

Ogni singolo bit attraversa un intero ciclo di vita: viene raccolto, trasferito, conservato, analizzato. Lungo il percorso, esso acquisisce un determinato valore capace di farne la codificazione di un elemento di realtà, integrato in sistemi capaci di costruire mappe cognitive che orientano scelte e giudizi.

Una vulnerabilità nel tragitto altera il modo in cui la realtà viene rappresentata, compresa e agita. Le conseguenze non si fermano al malfunzionamento di un servizio: esattamente come le corna di Mosè,

possono riverberarsi in un ampio spettro di contesti, andando a riflettersi sulle relazioni internazionali, sulle opinioni pubbliche e sulla tenuta dei sistemi sociali.

La cybersecurity è quindi una infrastruttura epistemica. Assicurando che i dati non vengano rubati o alterati, preserva il processo attraverso cui il mondo viene appreso e narrato. È quindi una infrastruttura economica, perché protegge continuità operativa, catene di fornitura, proprietà intellettuale; politica, perché garantisce la coerenza del dibattito pubblico e la resilienza democratica; militare, perché rappresenta la prima linea di deterrenza e preparazione nei nuovi conflitti ibridi. È infine strumento di pace, perché prepara lo spazio digitale alla resistenza, alla vigilanza, al confronto strutturato.

La cybersicurezza, dunque, non si limita a difendere i sistemi: diventa un linguaggio condiviso, una grammatica operativa che consente il dialogo.

Dove mancano ponti politici, costruisce connessioni tecniche. Dove la fiducia vacilla, permette la verificabilità. Dove esistono asimmetrie militari, diventa strumento di deterrenza.

È questa la nuova lingua franca dell'ordine digitale. Esattamente così come il latino era la lingua franca del cristianesimo. Ma entrambi, come abbiamo visto, corruttibili. E pertanto, così come i filologi nel comparare le tradizioni manoscritte arrivano a un testo il più fedele possibile all'originale, allo stesso modo gli operatori della cybersicurezza, pubblici e privati, si adoperano per preservare o, se corrotto, ripristinare il dato.

Anche la normativa evolve in questa direzione, con obblighi e dettami precisi nella direttiva nel Regolamento dell'AI Act.

Ma la minaccia non è solo la manipolazione. È anche la non disponibilità del dato, dovuta a attacchi cyber. Un blackout informativo può interrompere servizi sanitari, bloccare catene produttive,

corrompere informazioni, mettere sotto scacco per giorni intere città. Anche qui, il rischio non è tecnico, ma cognitivo: si perde la continuità del sapere.

La cybersicurezza oggi è questo: l'infrastruttura del significato e la grammatica del potere. Agire in questo spazio non significa più semplicemente "proteggere reti": significa progettare fiducia, integrare tecnologie complesse, abilitare ecosistemi resilienti.

Fare cybersecurity, oggi, è ingegneria di senso, sovranità e coesione. È il lavoro di chi rende possibile un mondo digitale interoperabile, affidabile, stabile. In cui ognuno possa pensare, agire e comunicare con la certezza di non venire distorto. E di poter attingere a informazioni sicure. Chi opera in questo campo, pertanto, non costruisce muri, ma ponti. Non isola, ma connette. E decide, nel silenzio del codice, quali visioni del futuro siano possibili – e quali no.