INFORMATION-WAR vs OPEN-DATA: DALLA MENZOGNA ALLA VERITÀ PER LA RESILIENZA EUROPEA

DOMENICO CALIGIURI

SOCINT Società Italiana di Intelligence

SOCINT Press

© 2026 Domenico Caligiuri
Società Italiana di Intelligence
c/o Università della Calabria,
Cubo 18-b, 7° piano,
via Pietro Bucci – 87036
Arcavacata di Rende (CS) – Italia
https://www.socint.org
ISBN: 979-12-80111-76-0

Tutti i contenuti (testi, immagini, grafica, layout ecc.) presenti in questo elaborato appartengono esclusivamente ai rispettivi proprietari.

Indice dei Contenuti

Abstract 3

Introduzione 6

Capitolo I. Dalla radio ai satelliti low-orbit: viaggio nell'evoluzione Dell'OSINT 10

Capitolo II. L'officina dell'inganno: anatomia della guerra dell'informazione 15

Capitolo III. Infrastrutture aperte: l'impalcatura digitale degli Open-Data . 20

Capitolo IV. Tracce di realtà: dossier e casi studio 25

- *Ucraina* 25
- *Gaza: La saturazione informativa e il rumore emotivo* 27
- *Cyber-Operazioni transnazionali: Ghostwriter Domain Seizure e il campo infinito* 28
- *Conclusioni intermedie* 30

Capitolo V. Verso il 2030: strategie etiche per il governo dei dati e dell'infosfera 31

Conclusioni 39

Fonti 43

- *Bibliografia* 43
- *Sitografia* 44

INFORMATION-WAR vs OPEN-DATA: DALLA MENZOGNA ALLA VERITÀ PER LA RESILIENZA EUROPEA

a cura di Domenico Caligiuri

Abstract

L'erosione della fiducia pubblica è diventata l'arma più potente dei conflitti contemporanei. Nel momento in cui un'immagine manipolata raggiunge milioni di schermi prima che i reporter possano verificarla, la difesa di una società non si misura più soltanto in carri armati o firewall, ma nella capacità di accedere, interpretare e condividere rapidamente informazioni affidabili. Questo testo esplora proprio questo bivio: da un lato l'enorme potenziale dei dati aperti (cartografici, statistici, meteorologici, economici) e dell'Open-Source Intelligence che li trasforma in conoscenza; dall'altro la manipolazione sistematica che governi autoritari, reti criminali e lobby mercenarie scatenano per minare la coesione interna delle democrazie.

Il lavoro nasce dall'osservazione che l'Unione europea, con la Direttiva 2019/1024, il Data Governance Act e il Data Act, sta creando il più grande ecosistema di dati pubblici e di condivisione fiduciaria mai tentato, fondato su standard come DCAT-AP e sulle architetture federate dei *Common European Data Spaces*. I modelli generativi di ultima generazione, in grado di produrre testi, immagini e voci indistinguibili dal reale, riducono a pochi minuti il costo di una campagna di disinformazione, rendendo obsoleti gli schemi di verifica ex post. Le indagini open-source sull'invasione russa dell'Ucraina e sul conflitto israelo-palestinese hanno dimostrato che un fotogramma satellitare o un metadato *C2PA* possono ribaltare la narrativa ufficiale, ma solo se esistono infrastrutture, metodi e competenze capaci di convalidarne l'autenticità.

A partire da queste premesse, l'analisi procede sul piano tecnico e ricostruisce la catena di valore che parte dalla pubblicazione dei dataset

«ad alto valore», passa attraverso *pipeline ETL automatizzate* in formati *Parquet* o *RDF* e giunge a dashboard analitiche alimentate da modelli di machine-learning. Viene mostrato come la medesima catena, se privata di controlli di qualità, sia vulnerabile al *data poisoning*: un singolo file CSV manipolato può indurre un algoritmo decisionale della pubblica amministrazione a errori di allocazione di risorse o, peggio, a valutazioni operative sbagliate in tempo di crisi. Sul piano normativo il testo mette a fuoco la convergenza tra regolazioni europee Digital Services Act, AI Act, Cyber Resilience Act e dottrine NATO sulla *cognitive security*, sottolineando la necessità di far dialogare standard di provenienza dei contenuti con obblighi di due-diligence algoritmica. L'ambizione è superare lo stadio difensivo del *fact-checking* postumo e instaurare un modello di *verifica by design*, in cui firma crittografica, metadati e identità digitale accompagnino i dati lungo l'intero ciclo di vita.

La parte empirica ripercorre la documentazione degli *eccidi di Bucha*, mostrando come la combinazione di immagini *Planet open access*, mappe *OpenStreetMap* e *licenze CC-BY* abbia prodotto prove incontrovertibili in sede giudiziaria internazionale, riducendo drasticamente i *"costi di verità"* evocati da *Robert David Steele*. La saturazione informativa di *Gaza*, dove la riforma della piattaforma X/Twitter e la monetizzazione dei badge di verifica hanno amplificato video decontestualizzati, costringendo le ONG a sviluppare flussi di autenticazione basati su radar *Sentinel-1* e modelli di *change detection* addestrati su *dataset FAIR*. Il caso entra nel dominio cyber-informativo, con l'operazione *Ghostwriter* e la successiva operazione FBI di sequestro di trentadue domini: si dimostra come la combinazione di *log Cloudflare* aperti ai ricercatori e archivi *WHOIS* in trasparenza abbia consentito di smontare una campagna di propaganda prima che diventasse senso comune.

Dall'incrocio fra teoria e pratica emergono cinque linee d'azione per una governance etica orientata al 2030. L'adozione obbligatoria di metadati di provenienza *machine-readable* per tutti i contenuti visivi generati in territorio

UE, integrando *C2PA* nei dispositivi di registrazione; un sistema di rating pubblico della qualità dei dataset, legato a incentivi di bilancio e a un marchio di affidabilità riconoscibile dal grande pubblico; Le piattaforme *cloud* e richiede *SBOM pubblici* per i software che gestiscono i data-space, in coerenza con il Cyber-Resilience Act; Si passa al disegno di un percorso educativo permanente che dall'istruzione secondaria arrivi alla formazione continua per giornalisti e funzionari, colmando il divario tra alfabetizzazione digitale di base e competenze OSINT avanzate; Infine si suggerisce un indice di impatto rischio-beneficio per decidere quali dati rendere aperti, integrando variabili di sicurezza nazionale, valore economico e rischio di manipolazione.

In controluce a tutte le proposte aleggia la massima di *Steele* secondo cui *"la verità, a qualunque costo, riduce tutti gli altri costi".* Se l'Europa riuscirà a concretizzare una filiera in cui dati certificati, infrastrutture sicure e cittadini formati circolano più velocemente delle menzogne, allora l'open data diventerà non soltanto un bene comune ma uno scudo cognitivo. Diversamente, l'apertura priva di presidî si trasformerà in un'arma nelle mani di chi sfrutta la velocità del rumoroso per mettere a rischio la tenuta stessa delle istituzioni. Questo abstract, infine, costituisce un invito: a legislatori, ingegneri, giornalisti, educatori, perché facciano propria la regola aurea dell'intelligence aperta e colmino, insieme, la distanza che separa la menzogna dalla verità, rafforzando la resilienza democratica contro le sfide visibili e invisibili del prossimo decennio.

INTRODUZIONE

Questo white paper nasce dall'intreccio fra due traiettorie che, fino a pochi anni fa, viaggiavano su binari distinti: da un lato l'Open Source Intelligence (OSINT), ovvero la capacità di trasformare enormi volumi di informazioni liberamente accessibili in analisi strategica; dall'altro la guerra dell'informazione o war-information, un assemblaggio di disinformazione, attacchi cibernetici e manipolazione narrativa che accompagna ormai ogni crisi geopolitica. La progressiva adozione del principio *Open by Default* nelle pubbliche amministrazioni europee ha moltiplicato i dati pubblici disponibili: geografici, statistici, meteorologici, societari; rendendo più trasparente l'azione governativa ma, insieme, offrendo materia prima sia agli analisti sia nostro malgrado agli attori ostili.

L'ampiezza dei dataset *"ad alto valore*" previsti dal Regolamento 2023/138 (geospaziali, osservazione della Terra, mobilità, statistiche, registri d'impresa) e la loro erogazione gratuita via API accelerano il ciclo di produzione dell'intelligence: scoperta, estrazione, arricchimento, analisi e diffusione. Allo stesso tempo, la stessa ricchezza informativa facilita operazioni di propaganda, falsificazione di contesti e profilazione di bersagli. Le indagini collaborative sulla guerra russo-ucraina hanno mostrato come video, immagini satellitari e tracciati di volo possano smontare in poche ore la narrazione di Mosca; l'analisi open-source condotta da *Bellingcat* sull'attacco all'ospedale pediatrico *Okhmatdyt* dell'8 luglio 2024 ha attribuito senza ambiguità la responsabilità a un missile russo *Kh-101*, smentendo le affermazioni di *"false flag"* amplificate da reti di *bot.* Nello stesso lasso di tempo, piattaforme social come X/Twitter hanno dimostrato quanto velocemente un algoritmo di *"amplificazione a pagamento"* possa innalzare al rango di *"fatto"* contenuti manipolati, alimentando confusione nei media tradizionali e ritardando la risposta diplomatica.

Le pagine che seguono adottano una prospettiva olistica: collocano l'OSINT dentro le cornici normative dell'Unione europea, ne tracciano le evoluzioni

tecnologiche più recenti e, soprattutto, illustrano come questi strumenti vengano piegati, in positivo e in negativo, nei teatri contemporanei di conflitto ibrido. Ne emerge un messaggio netto: "*l'apertura dei dati non è soltanto una politica di trasparenza, ma un nuovo terreno di competizione strategica"*. Gli attori statali e non statali che sapranno integrare rapidamente fonti aperte verificate con intelligence classificate conserveranno un vantaggio decisionale; chi trascurerà la resilienza del proprio ecosistema informativo diventerà un bersaglio privilegiato di operazioni di *denial-of-truth*.

Il panorama geopolitico è in continua evoluzione, così come avviene dal 2020 ad oggi il concetto di *"multi-dominio esteso"* ha ridefinito la pianificazione militare: dimensioni cinetiche, cyber e cognitive non sono più compartimenti stagni, ma vasi comunicanti in cui la superiorità narrativa può risultare decisiva quanto quella missilistica. Il Comando Alleato per le Trasformazioni della NATO descrive le minacce informative come *"qualsiasi attività ostile che neghi, corrompa o distorca l'informazione avversaria al fine di comprometterne la volontà o la capacità di agire"*. In questo contesto, la democratizzazione degli strumenti di analisi open source ha abbassato la soglia di ingresso: potenze regionali, gruppi paramilitari digitali e perfino singoli cittadini dotati di buone competenze OSINT possono oggi competere o interferire con apparati statali tradizionali.

L'Evoluzione dell'OSINT da arte di nicchia a infrastruttura globale è stato un lento processo evolutivo, partito sin dagli anni Novanta dove l'intelligence in chiaro era perlopiù raccolta da enti governativi attraverso la stampa estera, le frequenze radio e i primi forum online. Nel 2025 la superficie informativa include: database open data governativi, flussi social in tempo reale, costellazioni satellitari commerciali con risoluzione inferiore ai 30 cm, reti di sensori *IoT*, nonché geodati *"bene comune"* prodotti da comunità volontarie come *OpenStreetMap*, il cui valore è riconosciuto persino dall'ONU e integrato nei progetti di mappatura umanitaria e di monitoraggio delle infrastrutture critiche. Tre forze convergono in questo salto di scala, la

velocità (*API* che aggiornano i dataset alla cadenza dell'orario di un autobus), la granularità (immagini sub-metriche che un tempo erano appannaggio dei satelliti-spia) e la collaborazione civica (laboratori di *citizen-forensics* in grado di validare o smentire un comunicato ministeriale nel giro di mezz'ora).

La war-information oggigiorno è come una vera e propria arte combinatoria col fine di *"Colpire la mente prima ancora di colpire il bersaglio"*. Questa massima, coniata negli anni Sessanta dagli strateghi sovietici delle *aktivnye meroprijatija*, trova oggi una declinazione digitale nella cosiddetta war-information: una miscela di disinformazione, operazioni psicologiche *(PSYOPS),* sabotaggio cibernetico e campagne di influenza che permea ogni fase di un conflitto. Le sequenze operative si ripetono con impressionante regolarità, raccolta massiva di dati social, segmentazione degli utenti più influenzabili, semina di narrazioni d'esca, amplificazione tramite reti di *bot* e, infine, travestimento dell'origine attraverso contenuti apparentemente neutrali o pseudo-giornalistici. L'attacco dello scorso luglio 2024 contro *Kyiv* lo conferma, venti minuti dopo l'impatto sul complesso pediatrico, account automatici fornivano già *"prove"* di un inesistente missile *AIM-120* ucraino, approfittando del vuoto informativo che precede le verifiche ufficiali.

L' Open Data Directive poi sono un principio *Open by Default* che rappresentano una rivoluzione ambivalente. Con la Direttiva 2019/1024/UE, l'Unione europea ha sancito che i dati prodotti con denaro pubblico devono essere riutilizzabili a costo marginale nullo, in formati leggibili da macchina e corredati di licenze standard. Il successivo Regolamento di esecuzione 2023/138 ha dettagliato l'elenco dei sei dataset ad alto valore, imponendo la fornitura via *API* e *bulk download*. Parallelamente, le Linee guida italiane *"Open by Default"* ribadiscono l'obbligo di pubblicazione dei dati dinamici della PA, l'impiego di vocabolari controllati DCAT-AP e l'adozione di licenze Creative Commons BY o analoghe.

Il risultato è un ecosistema in cui i portali *CKAN* di livello locale, il Catalogo Nazionale Dati (dati.gov.it) e il portale europeo data.europa.eu si intrecciano in una filiera che va dalla produzione di dati grezzi al loro arricchimento semantico con ontologie condivise. Questa infrastruttura, se da un lato potenzia la ricerca, l'innovazione e la trasparenza amministrativa, dall'altro apre spazi inediti a operazioni di *targeting* basti pensare ai dataset immobiliari demaniali o alle mappe di rete elettrica pubblicate a fini di accountability.

Infine le lezioni che abbiamo appreso dai conflitti contemporanei, come il caso ucraino ci dimostrano il potere dell'OSINT come strumento di accountability: la mappatura di fosse comuni a *Bucha*, le triangolazioni video-satellite sugli attacchi a *Mariupol* e, più di recente, l'analisi del raid su *Okhmatdyt* hanno alimentato dossier giudiziari internazionali e accelerato sanzioni mirate. Tuttavia la stessa campagna ha messo in luce il problema dell'*information overload*: l'enorme flusso di contenuti grezzi richiede filtri metodologici rigorosi, competenze interdisciplinari e strumenti automatici di *source-reliability scoring*.

Nel conflitto israelo-palestinese del 2023-24, i contenuti manipolati hanno registrato un'impennata nei primi tre giorni di escalation, complice la policy "*blue-check* a pagamento" di X che ha amplificato voci non verificate. Anche qui, la risposta di laboratori OSINT indipendenti che hanno geolocalizzato immagini contraffatte o ricontestualizzate è stata essenziale per ristabilire un minimo di verità fattuale, ma spesso è arrivata dopo che la notizia falsa aveva già raggiunto milioni di utenti.

Questo lavoro vuole essere un'introduzione alle complessità dell'Open-data nell'open-source intelligence, con il duplice obiettivo ossia mapparne le opportunità (innovazione, trasparenza, responsabilità democratica) e identificare i punti di vulnerabilità (*data poisoning,* privacy collettiva*,* sovraccarico cognitivo) lungo la catena che unisce la produzione pubblica di dati alla loro utilizzazione in scenari di conflitto ibrido.

CAPITOLO I. DALLA RADIO AI SATELLITI LOW-ORBIT: VIAGGIO NELL'EVOLUZIONE DELL'OSINT

La storia dell'Open Source Intelligence si apre ben prima che il termine entrasse nel lessico comune nel febbraio 1941, a pochi mesi dall'ingresso degli Stati Uniti nella Seconda guerra mondiale, la *Casa Bianca* costituì il Foreign Broadcast Monitoring Service poi divenuto Foreign Broadcast Information Service (FBIS) con l'obiettivo di trascrivere e tradurre le trasmissioni radio straniere e i dispacci della stampa internazionale. L'idea che le informazioni disponibili in chiaro potessero offrire un *"sismografo"* in tempo reale degli umori globali si dimostrò talmente valida che l'agenzia fu assorbita dalla CIA e operò fino al 2005, quando le sue funzioni confluirono nell'Open Source Center. In quella lunga fase analogica l'OSINT rimase un affare di specialisti, grandi antenne, abbonamenti ai giornali, bibliotecari esperti di microfilm.

La rivoluzione digitale degli anni Novanta e l'affermarsi dei motori di ricerca, dei forum tematici e delle prime banche dati commerciali abbassò drasticamente la soglia di accesso. Nacquero i primi software di *web-crawling* e i portali che aggregavano notiziari internazionali, ma fu l'invenzione dei *blog* a rompere il monopolio delle fonti istituzionali. A cavallo del 2003 gli analisti che seguivano la guerra in Iraq cominciarono a integrare nei propri report i diari online dei *reporter embedded*, fonte narrativamente più ricca e geograficamente distribuita rispetto ai lanci di agenzia. Il salto definitivo avvenne con la diffusione degli smartphone e delle piattaforme social. Da allora ogni testimone oculare, armato di connessione mobile, può trasformarsi in sensore in tempo reale. L'OSINT smette di essere soltanto un metodo di raccolta e diventa un ecosistema informativo planetario in cui testo, immagini, coordinate GPS e metadati scorrono alla velocità dell'algoritmo.

A cementare questo cambio di paradigma contribuisce la graduale apertura dei dati pubblici. L'Unione europea, con la Direttiva 2003/98/CE, pose le

basi per il riuso delle informazioni del settore pubblico, ma è la Direttiva 2019/1024/UE a sancire il principio *"Open by Default"*, poi recepito dalle linee guida italiane, secondo cui i dataset finanziati con denaro pubblico devono essere rilasciati in formati leggibili da macchina e con licenze standard. Il Regolamento 2023/138 ha poi individuato sei famiglie di *High Value Datasets,* dai geo-dati alle statistiche la cui messa a disposizione gratuita via *API* alimenta sia la ricerca accademica sia le indagini in chiaro. In pochi anni i portali *CKAN* comunali e il catalogo nazionale dati.gov.it si sono saldati alla piattaforma europea data.europa.eu, generando l'ossatura di una *"infrastruttura conoscitiva"* su scala continentale.

Nel 2011 il concetto di *"investigazione architettonica"* elaborato dal laboratorio londinese Forensic Architecture spinge oltre i confini disciplinari con planimetrie *3D*, fotografie georeferenziate e tracce audio vengono intrecciati per ricostruire violazioni dei diritti umani da *Gaza* al Messico. L'approccio, formalmente accademico, dimostra che l'open source può competere nei tribunali internazionali con la prova classificata, purché la catena di custodia digitale sia impeccabile. Tre anni dopo, nell'estate 2014, il blogger inglese *Eliot Higgins* fonda *Bellingcat* e applica la stessa logica di evidenza pubblica alla guerra civile siriana, identificando la provenienza delle bombole di cloro e successivamente il missile *Buk* che abbatté il volo *MH17*. *Bellingcat* diventa un caso-scuola divenendo da collettivo di volontari a redazione diffusa che collabora con tribunali internazionali, giornali d'inchiesta e perfino con la Corte Penale Internazionale.

Parallelamente l'OSINT si avvicina alla contabilità bellica. Nei primi giorni dell'invasione russa dell'Ucraina, il blog olandese *Oryx* inaugura una metodologia rigorosa, catalogare solo mezzi militari di cui esista prova fotografica o video. Quel censimento visuale consultato da ministeri della Difesa, media e *think-tank* dimostra a colpo d'occhio l'entità delle perdite russe e apre la strada a progetti di machine-learning destinati a contare i relitti da immagini satellitari. La stessa invasione segna l'ascesa dell'osservazione orbitale commerciale aziende come *Planet Labs*

pubblicano *timelapse* quasi quotidiani di ponti distrutti, convogli logistici e crateri d'artiglieria, innescando un rovesciamento di prospettiva. Per la prima volta, la vista dallo spazio non è più dominio esclusivo dei governi.
Al livello tattico si forma una nuova generazione di comunità. Il collettivo *Geo-Confirmed* raccoglie geolocalizzatori volontari che confermano in poche ore la posizione di video provenienti dal fronte, filtrando migliaia di clip virali e riducendo la finestra di fumo narrativo che Stato aggressore e Stato difensore cercano di creare. Sul versante cartografico, la comunità di *OpenStreetMap* continua a mappare aree di crisi, fornendo base dati ad agenzie ONU e ONG per pianificare corridoi umanitari o valutare i danni alle infrastrutture.

La traiettoria tecnologica dell'OSINT, dalla carta stampata al *cloud*, si intreccia con tre dinamiche complementari. La miniaturizzazione del sensore ad esempio la stessa camera che un escursionista porta sul casco diventa uno strumento di verifica geospaziale quando incrociata ai *layer open-source*; L'automazione algoritmica, dai modelli di *machine-vision* che riconoscono il tipo di carro armato a sistemi di *Natural Language Processing* capaci di setacciare *telegrammi-bot* alla ricerca di pattern di reclutamento; La più dirompente, è l'intelligenza artificiale generativa i *Large Language Models* sono ora in grado di riassumere dossier di migliaia di pagine, ma possono anche fabbricare testi e immagini realistiche, alimentando un ciclo di *synthetic disinformation* che complica la vita agli analisti, minaccia di cui la comunità OSINT è già consapevole, come dimostrano i primi progetti di *watermarking invisibile* e di *"firme di provenienza"* proposti dalla Coalition for Content Provenance and Authenticity.

Accanto ai progressi tecnici emergono questioni etiche e operative. L'abbondanza di dati aperti, specie quelli delineati dalla Direttiva 2019/1024, rende possibile una profilazione di massa che pochi anni fa sarebbe stata appannaggio esclusivo dei servizi di sicurezza. Alcuni dataset, si pensi agli inventari degli immobili demaniali pubblicati in chiaro o alla mappa interattiva delle cabine primarie dell'energia elettrica italiana hanno

sollevato interrogativi sul bisogno di equilibrio tra trasparenza e sicurezza nazionale. Allo stesso tempo, l'uso di contributi volontari in zone di guerra impone procedure di tutela dei testimoni e protocolli di minimizzazione dei dati personali, pena il rischio di re-identificazione da parte di attori ostili.
Sul piano dottrinale, gli Stati Uniti hanno riconosciuto ufficialmente l'importanza dell'OSINT pubblicando nel 2024 un primo documento strategico dedicato esclusivamente alle fonti aperte, integrato nel budget del *Military Intelligence Program*. Sebbene il testo non sia per intero di pubblico dominio, il comunicato del Pentagono esplicita l'intenzione di fondere intelligence in chiaro e classificata già nelle fasi di pianificazione operativa. Nell'Unione europea, invece, il dibattito è ancora frammentato fra istanze di protezione dei dati personali (GDPR), necessità di contrasto alla disinformazione e volontà di promuovere l'innovazione *data-driven* delineata nella Digital Decade 2025.

Il percorso che ha trasformato l'OSINT da hobby di radio-amatori a infrastruttura cognitiva mondiale può essere letto dunque come un continuum scandito da soglie tecnologiche e da mutamenti culturali. La soglia della digitalizzazione massiva delle fonti rompe il monopolio degli archivi fisici. L'emergere di comunità transnazionali che collaborano in tempo reale senza gerarchie tradizionali. L'osmosi con l'economia dei dati aperti, in cui la licenza *Creative Commons* di un set cartografico o il formato *RDF* di un catalogo statistico diventano fattori di accelerazione analitica. Infine l'irruzione dell'intelligenza artificiale in tutti gli anelli della catena, dalla raccolta al *debunking*.

Se la trasparenza delle fonti apre una finestra di responsabilità democratica la *"forensic accountability"* che permette di portare prove di crimini di guerra davanti alle corti, la stessa finestra può diventare una porta d'ingresso per campagne di manipolazione di vasta scala. La lezione che proviene dai conflitti in Ucraina e in Medio Oriente è lapidaria, l'OSINT non è più una disciplina ancillare dell'intelligence tradizionale, bensì un teatro di competizione in cui governi, aziende, giornalisti investigativi e comunità

civiche si contendono tempo di latenza, legittimità narrativa e qualità metodologica.

In questo scenario fluido la governance diventa decisiva. Standard semantici come DCAT-AP, regole *FAIR* per la ricerca, linee guida *"Open by Default"* e pratiche di attribuzione saranno il discrimine fra un ecosistema di dati che abilita decisioni giuste e uno che amplifica gli errori. Altrettanto centrale sarà l'educazione al metodo, senza un salto culturale la capacità di controllare coordinate *EXIF*, verificare ombre solari, isolare rumore di compressione, la quantità di informazioni rischia di seppellire la qualità.

Il viaggio della prossima decade passa allora da una fusione fra strumenti automatizzati e occhio umano allenato, fra principi etici condivisi e flessibilità investigativa. L'OSINT del 2030, verosimilmente, incorporerà realtà aumentata sul campo di battaglia, sensori *IoT* che emettono dati firmati crittograficamente e algoritmi in grado di distinguere deep fake da originali in millisecondi. Sarà però ancora la rete di ricercatori, attivisti e giornalisti a dare senso, contesto e finalità a quelle informazioni. La traiettoria qui ricostruita mostra che ogni ondata tecnologica, dal microfilm al machine learning, ha riproposto la stessa domanda: come trasformare la visibilità in conoscenza affidabile senza sacrificare i diritti e la sicurezza? La risposta rimane aperta, ma il percorso compiuto finora dimostra che la trasparenza, quando è sorretta da metodo, può diventare il più potente antidoto alla guerra dell'informazione.

CAPITOLO II. L'OFFICINA DELL'INGANNO: ANATOMIA DELLA GUERRA DELL'INFORMAZIONE

Lo spazio in cui oggi si combatte per la supremazia narrativa sfugge all'immaginario tradizionale del fronte, non ha trincee, ma flussi di dati, non innalza bandiere su colline, ma hashtag nei *trend topic*. Gli strateghi chiamano questo teatro *"information environment"* e vi collocano tutto ciò che plasma la percezione collettiva dalla titolazione di un post su X fino alle (false) mappe meteorologiche che annunciano un imminente attacco chimico. Da quando i ponti digitali hanno reso permeabili le barriere fra politica estera, sicurezza interna e consumo mediatico, la guerra dell'informazione è divenuta il collante di qualsiasi operazione *"ibrida".*

Nell'ultimo quinquennio l'elenco degli attori si è ampliato in modo quasi organico. Permangono gli Stati con capacità industriale la Russia dell'Internet Research Agency**,** accusata dal *Guardian* di sfruttare TikTok per diffondere dubbi sulla legittimità dell'Ucraina, ma accanto ad essi operano laboratori semi-ufficiali, società di public relations, gruppi paramilitari digitali e community di attivisti mercenari che affittano competenze di *micro-targeting* come si noleggia potenza di calcolo in cloud. L'Iran orchestra catene di account copia-incolla che rigenerano in poche ore l'assetto cancellato dalle piattaforme, la Cina preferisce campagne a bassa intensità, innestate su reti d'influenza economica e *United Front*, il cosiddetto *"terrorismo di marca"* dall'ISIS all'ultimo *spin-off* jihadista innova invece sulle tecniche di *crowdsourcing* iconografico, moltiplicando in numero e velocità i contenuti destinati a inondare canali Telegram.

La tecnologia procede in tandem. Le prime *"fabbriche di troll"* puntavano su volumi di testo a basso costo, oggi la stessa operazione può contare su reti neurali che generano identità plausibili complete di foto, curriculum *LinkedIn*, storie *Instagram* dai colori saturi. *Graphika*, in un report d'aprile 2025, ha descritto *#OperationFFS*, una rete di profili con volti sintetici che sostenevano la narrativa *"anti-vaccino = pro-pace"* e che Instagram ha

smantellato solo dopo oltre trenta milioni di visualizzazioni. Nel frattempo i deepfake vocali superano le prime linee di riconoscimento automatico e i modelli generativi di testo, addestrati su stilemi giornalistici, sfornano editoriali che ricalcano perfettamente cadenze e citazioni di quotidiani ben noti.

Alle spalle di questi artificieri dell'informazione si intravvede un'architettura operativa in cinque stadi che i ricercatori di *EUvsDisinfo* definiscono *"from seed to narrative weapon"*. Il punto di partenza è la raccolta di dati psico-grafici, playlist Spotify, pattern di acquisto online, cronologia di localizzazione estratta da app innocue. Segue la fase di modellazione, in cui algoritmi di *clustering* dividono il pubblico in tribù emotive. Poi il laboratorio narrativo vero e proprio, dove si confezionano contenuti calibrati sulla suscettibilità di ciascun segmento. Quindi subentra l'amplificazione, che un tempo si affidava a troll salariati e oggi sfrutta reti di *bot "usa e getta"* capaci di riprodursi con la stessa logica virale di un ransomware. Ultimo anello è la normalizzazione il messaggio, già diffuso su account pseudo-giornalistici, filtra nei media generalisti, viene citato da *opinion leader* e diventa sfondo cognitivo, pronto a essere riattivato alla prossima crisi.

La cronaca fornisce esempi concreti. *"Secondary Infektion"*, smascherata nel 2019 da *Atlantic Council* e ripresa in un white paper di *Graphika*, pubblicava documenti falsi in dozzine di lingue allo scopo di generare dissidi inter-alleati. Nel 2023 l'operazione è ricomparsa su forum marginali con messaggi fabbricati da *LLM* che imitavano stilemi religiosi locali, segno di una costante evoluzione dell'arsenale retorico. *"Ghostwriter"*, attribuita al *gruppo UNC1151*, ha combinato la violazione di caselle di posta di funzionari polacchi con la pubblicazione selettiva delle email manipolate, piegando in un solo gesto dimensione cyber e dimensione informativa. In entrambi i casi, l'intreccio con piattaforme social consente di imbastire una *hoax* in poche ore: la prima ondata di tweet diffonde lo *screencap* di un documento, una seconda ondata riporta lo scoop come dato acquisito, la

fase tre consiste in commenti *“di esperti”* reclutati su mercati neri di *like e reply.*

Di fronte a questa complessità la NATO ha affinato il proprio lessico. L’Alleanza già disponeva di dottrina per *l’Information Operations*, tuttavia dal 2021 il Comando Trasformazione di *Norfolk* ha introdotto il concetto di *“cognitive warfare”,* definito come *“l’arte di degradare la razionalità dell’avversario alterandone il processo decisionale”*. A latere, il *Centro di Eccellenza per la Comunicazione Strategica* di *Riga* diffonde analisi di scenario su interferenze russe nella regione baltica e produce manuali di risposta che le forze armate di vari Paesi integrano nei propri *wargame* comunicativi. La novità tattica introdotta dal concetto di *“cognitive warfare”* è la dissoluzione del confine tra militare e civile: se l’obiettivo è la mente collettiva, ogni cittadino con uno smartphone diventa sia possibile sensore sia potenziale bersaglio.

Sul versante Unione europea il paradigma si articola sui pilastri della: prevenzione, affidata alla *Task Force East StratCom* del *Servizio Europeo* di Azione Esterna, che ogni settimana cataloga e demistifica centinaia di narrazioni ostili, rendendo pubblico un database in ventisette lingue utilizzato da giornalisti, ONG e centri di ricerca; la regolazione, il Digital Services Act, entrato in piena applicazione nel febbraio 2024, impone ai grandi intermediari obblighi di due-diligence sugli algoritmi di raccomandazione e procedure di crisi per la disinformazione di guerra, il Codice di Buone Pratiche aggiornato nel 2025 traduce tali obblighi in impegni concreti come ad esempio la tracciabilità dei *bot*, etichettatura dei deepfake, archivi pubblici di inserzioni politiche; la resilienza, incarnata dal Centro europeo di eccellenza per il contrasto alle minacce ibride di *Helsinki*, che promuove corsi congiunti UE-NATO su come proteggere i processi elettorali, le infrastrutture critiche e l’opinione pubblica dalle manipolazioni cognitive.

L’architettura della war-information dimostra una caratteristica ricorrente: la *“frizione zero”* fra domini. Un attacco *DDoS* contro il sito di un ministero

genera, all'istante, un'ondata di meme che scherniscono l'inefficienza del governo, la voce di un ministro clonata con intelligenza artificiale annuncia una fittizia evacuazione mentre account *bot* traducono il messaggio in dieci lingue, pochi minuti dopo, un grafico meteorologico manipolato suggerisce l'imminenza di un rilascio chimico, inducendo la popolazione a riversarsi sulle strade e a intasare la rete cellulare, la sequenza si chiude con la comparsa di analisti-fantoccio che *"contestualizzano"* il panico, armando la narrativa che la democrazia non sa proteggere i propri cittadini. Gli studiosi del *Hybrid CoE* definiscono questo procedimento *"orchestrazione a scatole cinesi"* dove ogni azione, pur localizzata, è progettata per amplificare l'effetto delle precedenti e colonizzare il ciclo informativo di ventiquattr'ore.

Nel mezzo di questa tempesta informativa si muove anche il mondo dei dati aperti. Le mappe di flusso del traffico messe online da città intelligenti possono aiutare i soccorritori a pianificare corridoi umanitari, ma offrono al contempo indicazioni preziose a chi voglia dirigere missili o sfuggire ai droni. Le immagini *Sentinel-2*, rilasciate in *Copernicus* in open access, permettono di monitorare la deforestazione ma rendono visibile la logistica militare in ampie regioni. L'Unione europea, consapevole di questa ambivalenza, discute ora forme di *"privacy collettiva"* per i dataset spaziali, nonché *watermark crittografici* destinati a rivelare manipolazioni di contenuto.

La sfida principale per le democrazie resta la temporalità. Secondo il diario log delle piattaforme, nel caso dell'attacco all'ospedale pediatrico di *Kyiv* lanci di disinformazione organizzata hanno preceduto di trenta minuti il primo comunicato ufficiale ucraino. Una finestra temporale così ridotta rende evidente che la sola smentita ex post non basta. Occorre passare a modelli predittivi di *"early warning narrativo"*, analoghi agli allarmi meteo, che segnalino tempestivamente spike coordinati di attività anomala. Il Machine-learning addestrato su reti di bot può contribuire, ma la capacità di riconoscere la risonanza emotiva di uno slogan rimane prerogativa umana.

In conclusione, la war-information non vive in un unico hardware o dentro una specifica piattaforma ma è una costellazione di attori polimorfi, alimentata da tecnologie in rapida evoluzione e incastonata in un quadro normativo che tenta di correre in parallelo senza bloccare l'innovazione. La NATO proietta il concetto di *"cognitive superiority"* nella pianificazione militare. L'Unione europea sperimenta la regolazione delle piattaforme e i programmi di alfabetizzazione mediatica, i centri di eccellenza, da *Riga* a *Helsinki*, fungono da snodi di conoscenza fra università, forze armate e settore privato.

Tuttavia, guardando ai casi di *"Secondary Infektion"* o di *"Ghostwriter"*, è evidente che la pressione evolutiva favorisce l'adattamento continuo degli aggressori. Nei capitoli successivi vedremo come queste dinamiche si riflettano sulla filiera dell'Open Source Intelligence e quali protocolli tecnici, legali, etici possano rafforzare la capacità di filtrare il vero dal verosimile prima che la prossima onda mediatica travolga la ragione pubblica.

CAPITOLO III. INFRASTRUTTURE APERTE: L'IMPALCATURA DIGITALE DEGLI OPEN-DATA

Nel giro di poco più di un decennio l'apertura dei dati pubblici è passata dall'essere un esercizio di trasparenza amministrativa a diventare un'infrastruttura critica della sovranità digitale europea. Il percorso inizia con la Direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico, si consolida con la Direttiva 2019/1024/UE che introduce il principio *«Open by Default»* e raggiunge un nuovo stadio con il Regolamento 2023/138, il quale individua sei famiglie di *data-set* ad alto valore che devono essere resi disponibili gratuitamente e via *API*. Dai richiami alle licenze *Creative Commons* fino all'adozione obbligatoria di metadati DCAT-AP, condizione necessaria per assicurare l'interoperabilità semantica fra cataloghi locali, nazionali ed europei.

La catena del valore dell'open data può essere descritta come un flusso continuo che parte dal rilascio dei dati grezzi e giunge alla generazione di insight, passando per arricchimento, standardizzazione, federazione e, infine, consumo applicativo. Il momento della produzione non si limita più alla semplice esposizione di un file su un portale, la pubblica amministrazione è chiamata a produrre dati *«tre stelle»* in formato *CSV* quando le strutture sono semplici, *«quattro stelle» RDF* per le ontologie più ricche e perfino in formato Parquet quando la complessità e il volume suggeriscono architetture *colonne-oriented* per l'analisi *big-data*.
Questa granularità tecnica, apparentemente esoterica, influenza direttamente la velocità con cui i dati vengono caricati in pipeline di trasformazione, normalizzati con vocabolari controllati, collegati a identità giuridiche o coordinate geografiche e infine interrogati da algoritmi di machine-learning.

Sul versante della distribuzione il cuore dell'ecosistema europeo rimane la piattaforma data.europa.eu, che dal 2023 funge da nodo federatore tra i portali nazionali *CKAN* fra cui dati.gov.it e il crescente numero di cataloghi

settoriali. Il Rapporto di Maturità Open Data 2024 certifica i progressi nella copertura e nella qualità, con Francia, Polonia e Slovacchia ai vertici e l'Ucraina, nonostante la guerra, in grado di superare il 97 % di conformità. Questa infrastruttura non è soltanto una vetrina le *API* consentono di eseguire *query* semantiche, scaricare *bulk dump* periodici, ricevere *webhook* sugli aggiornamenti e, in prospettiva, abilitare flussi in tempo quasi reale per i cosiddetti dati dinamici.

La spinta verso l'interoperabilità si innesta sul paradigma dei Common European Data Spaces, un mosaico di ecosistemi settoriali (salute, mobilità, agrifood, energia, pubblica amministrazione, cultura, industria manifatturiera) la cui architettura di riferimento è al centro della strategia digitale dell'UE. Qui il concetto-chiave non è più la semplice apertura, bensì la condivisione fiduciarizzata: i dati possono rimanere presso i rispettivi titolari, ma devono essere accessibili tramite standard comuni di descrizione, protocolli di sicurezza omogenei e condizioni di licenza chiare. Per guidare questa trasformazione la Commissione ha finanziato il *Data Spaces Support Centre (DSSC)*, incaricato di produrre *blue-print* architetturali e linee guida operative destinate sia agli Stati membri, sia alle imprese che vorranno collegarsi ai nuovi spazi. Il *DSSC* collabora strettamente con l'International Data Spaces Association, che ha codificato nel Reference Architecture Model 4.0 i princìpi di scambio sicuro e sovrano dei dati, introducendo, tra l'altro, il concetto di *data contract machine-readable* e di *usage control* applicato a valle del download.

Parallelamente, il progetto *GAIA-X* tenta di offrire un livello infrastrutturale federato che consenta di distribuire servizi cloud e scambio dati evitando lock-in proprietari e assicurando la tracciabilità delle condizioni di utilizzo. Il Summit di *Helsinki* del novembre 2024 ha reso pubblico un primo set di specifiche tecniche armonizzate con i requisiti dei data-space europei e con lo schema di certificazione cloud di prossima emanazione, puntando a un ecosistema di nodi federati in cui identità digitale, localizzazione fisica e politica di *retention* dei dati siano verificabili a *runtime*.

Se la cornice tecnologica ruota su *reference model* e specifiche, la cornice giuridica si articola attorno a tre testi di legge che si intrecciano, la già citata Direttiva Open Data, il Data Governance Act con il suo impianto sugli intermediari di condivisione e sull'altruismo dei dati, e il Data Act che entrerà in piena applicazione nel 2025 e disciplinerà la portabilità e l'accesso ai dati generati dall'Internet delle Cose. Il Data Governance Act introduce un quadro di fiducia orizzontale, certifica i nuovi *data intermediaries*, vieta gli accordi di esclusiva fra operatori pubblici e privati e istituisce l'European Data Innovation Board come organo di coordinamento.

La concretizzazione di queste norme è resa possibile da standard semantici e tecnici. Il profilo DCAT-AP armonizza i metadati di catalogo, mentre le estensioni *sector-specific* permettono di descrivere dataset del turismo o del procurement con lo stesso vocabolario. La qualità dei metadati impatta direttamente sull'algoritmo di *discovery*: un dataset mal etichettato resta invisibile al motore semantico, frustrando il principio *«Findable»* dei *FAIR Data Principles*, su cui la Commissione insiste ormai come prerequisito anche nei bandi di ricerca europea. Sulla sponda opposta della filiera troviamo *l'Open Data Maturity Report* che, oltre a monitorare l'estensione dell'apertura, introduce indicatori sulla qualità intrinseca, sulla governance e sull'impatto economico, costruendo così una metrica unificata di ritorno sociale e industriale degli investimenti.

La catena di valore si completa con l'integrazione applicativa che avviene in tre domini. Il primo è quello della business intelligence, dove le piattaforme analytics consumano dataset aperti accanto a feed privati, incrociando registri d'impresa, flussi *AIS* e statistiche socioeconomiche per costruire indicatori di rischio. Il secondo è quello del giornalismo investigativo, dal 2019 *Bellingcat* integra API del *Land-Value Index* olandese e modelli di linguistica computazionale per tracciare la proprietà opaca di ville sulla Costa Azzurra, mostrando che un singolo outlier nel prezzo può rivelare la pista di un evasore sanzionato. Il terzo dominio è la pubblica utilità, la mappa dell'energia eolica dell'*Irish Marine Institute*,

realizzata su standard INSPIRE, alimenta un gemello digitale che aiuta i pescatori a pianificare rotte e lo Stato a valutare l'impatto cumulativo dei parchi offshore.

Il quadro italiano riflette e amplifica queste dinamiche. Le Linee guida "*Open by Default"* non si limitano a prescrivere formati; raccomandano la definizione di *pipeline ETL* automatizzate, l'adozione di *repository Git* per la storia delle trasformazioni e l'uso di test di qualità automatici che, in caso di regressione, bloccano la pubblicazione. Ad esempio: la Regione Puglia riorganizza i back-end dei propri sistemi verticali per esporre un'unica API geospaziale; l'*ISTAT* produce dataset turbolenti in formato Parquet per alimentare modelli predittivi; l'*Agenzia delle Entrate* sperimenta la combinazione di open data catastali con ontologie del patrimonio pubblico per individuare scostamenti e ottimizzare il canone di affitto.

Tuttavia, densità di standard e maturità legale non bastano a evitare due crinali critici. Il primo canale critico riguarda la sicurezza i dataset cartografici troppo granulari, per esempio, le cabine primarie dell'alta tensione, possono agevolare pianificazioni ostili. Su questo terreno l'UE discute ora meccanismi di opacizzazione selettiva, *watermark* crittografici e modelli di licensing graduato che limitino l'uso in base allo scopo. Il secondo crinale critico riguarda l'equità economica, benché il Data Act miri a riequilibrare il potere contrattuale fra big-tech e PMI, la capacità di analisi avanzata rimane concentrata in poche mani. Il progetto European Data Market Study 2024-2026 mostra che i primi tre player cloud coprono da soli oltre il 62 % del valore aggregato del mercato dati UE, sollevando interrogativi sulla reale realizzazione della sovranità digitale.

All'orizzonte si profilano evoluzioni chiave come la convergenza fra data-space e identità digitale europea (EUDI Wallet): la possibilità di firmare e verificare *smart-contract* di condivisione direttamente da un *wallet* riconosciuto in tutti gli Stati membri aprirà scenari di micropagamento e di tracciabilità d'uso impossibili finora, e la normalizzazione dell'intelligenza

artificiale come *“utente*” dei data-space: il regolamento AI Act introduce obblighi di trasparenza sulle fonti di addestramento, che potrebbero incrociarsi con attributi di provenienza e licenza già presenti nei cataloghi open data, creando un ciclo virtuoso dove la qualità dei dataset alimenta la robustezza degli algoritmi e viceversa.

In definitiva, l’infrastruttura open data europea sta passando da un modello di deposito centralizzato a uno di federazione regolata, supportata da architetture di data-space***,*** standard semantici e quadri giuridici che puntano a bilanciare innovazione, sovranità e sicurezza. La sfida, come emerge dai casi nazionali e dai più recenti rapporti di maturità, non consiste più nel convincere gli enti a *«rilasciare»* i dati, bensì nel costruire catene di fiducia che garantiscano qualità, interoperabilità e controllo sull’uso. È proprio lungo queste catene che l’Open Source Intelligence troverà la materia prima per analisi sempre più sofisticate, ma anche i punti in cui una manipolazione intenzionale può distorcere la percezione del reale.

Nei capitoli che seguono esploreremo casi concreti di impiego dei data-space nel monitoraggio di conflitti e crisi globali, nonché gli strumenti di governance capaci di trasformare l’apertura in un vantaggio strategico senza trasformarla in vulnerabilità.

CAPITOLO IV. TRACCE DI REALTÀ: DOSSIER E CASI STUDIO

La convergenza fra dati aperti, indagine in chiaro e guerra dell'informazione trova il suo banco di prova in tre crisi che hanno contrassegnato il quadriennio 2022-2025. Analizzarle in profondità significa osservare come ogni maglia della filiera open-source dalla raccolta, alla verifica, e gli standard, e le infrastrutture siano state messe sotto sforzo e abbiano, talvolta, rivelato criticità inattese.

UCRAINA

Quando, alle prime luci del 24 febbraio 2022, i convogli russi varcarono il confine settentrionale, una rete diffusa di giornalisti civici, volontari di *OpenStreetMap*, analisti di *Bellingcat* e sviluppatori di *bot Telegram* era già all'opera. La prima sfida fu geolocalizzare il movimento dei mezzi, fotografie scattate da autisti sui corridoi di *Gomel* venivano incrociate con la base cartografica *OSM* aggiornata in nottata grazie all'ortofoto *Sentinel-2*. L'assenza di restrizioni di licenza permise al collettivo *GeoConfirmed* di integrare quel layer con dati di traffico rilasciati in open API dai portali Bielorussi prima del blackout, nel giro di poche ore la *"colonna di 60 km"* diretta verso *Kyiv* era visibile al pubblico in una mappa interattiva condivisa su *GitHub*.

La vera frattura epistemica emerse però a *Bucha*. Il 3 aprile, quando le prime immagini dei civili uccisi affiorarono sui social, l'ecosistema OSINT reagì con uno sforzo di verifica coordinato, coordinate delle vie, lunghezza delle ombre, metadati *EXIF* e cross-match con riprese satellitari *Planet* del 19 marzo. L'indagine, sintetizzata da *Bellingcat* nel dossier *"Notes from the Digital Field"*, isolò il posizionamento dei corpi in data precedente al ritiro russo, invalidando il tentativo di Mosca di ribaltare la responsabilità su *Kiev.* Lo stesso metodo fu replicato a *Mariupol*, lì l'*Associated Press* costruì un modello 3D del Teatro Drammatico, inserendo 41 video Telegram nei punti

corrispondenti alle finestre aperte il giorno prima del bombardamento; la stima indipendente di oltre seicento vittime civili costrinse le Nazioni Unite a classificare l'evento come *"attacco sproporzionato".*

La partita narrativa più serrata si giocò, poi nell'estate 2024. L'8 luglio un *Kh-101* russo colpì l'ospedale pediatrico *Okhmatdyt* di *Kyiv*: nel giro di venti minuti i primi post su X, firmati da account con spunta blu acquistata, diffusero la tesi di un missile ucraino fuori controllo. L'articolo di *Bellingcat* pubblicato il giorno stesso, corredato da fotogrammi estratti da telecamere di sorveglianza e confrontati con la sagoma del motore turbofan del *Kh-101* demolì la versione russa. L'episodio segnò una svolta: il governo di *Kyiv* istituì un centro di *"rapid debunk"* con accesso prioritario ai dataset satellitari commerciali e alle serie temporali *Copernicus* open access, integrandolo con un archivio DCAT-AP sul portale open data nazionale per garantire la riproducibilità delle prove.

Sul piano militare l'OSINT ha inciso persino sulla valutazione degli arsenali. Il blog olandese *Oryx*, ammettendo solo perdite documentate per immagine, ha compilato una contabilità visuale che i ministeri occidentali utilizzano per parametrare i flussi di aiuti, il metodo si fonda sull'identificabilità dei mezzi corazzati e sulla licenza permissiva delle fotografie caricate dagli stessi soldati su *VKontakte* e Telegram. L'incrocio con registri societari russi, esposti come open data dal 2019, ha aiutato investigatori come i russi *exiliati* di *iStories* a ricostruire la catena di subappalti e a proporre liste di sanzioni mirate.

La crisi ucraina dimostra dunque come l'apertura dei dati e l'accesso a immagini commerciali abbiano ridisegnato il ritmo della narrazione bellica, l'intervallo fra evento e verifica si è compresso da settimane a ore, ma, di riflesso, anche la contro-disinformazione si è fatta più rapida, sfruttando algoritmi di amplificazione proprietari per colonizzare la *"finestra d'incertezza"* che precede il fact-checking.

GAZA: LA SATURAZIONE INFORMATIVA E IL RUMORE EMOTIVO

Alle 6.30 del mattino del *7 ottobre 2023* la rottura del confine fra Gaza Strip e Israele spalancò il secondo grande campo sperimentale dell'OSINT contemporaneo. A differenza dell'Ucraina, il territorio densamente popolato e con banda mobile intermittente generò un paradosso, una marea di video TikTok in bassa definizione, punteggiata da silenzi di connettività. Lo squilibrio fra offerta di immagini e capacità di verifica produsse un ecosistema tossico. NewsGuard registra oltre duecento miti disinformativi diffusi nelle prime quarantotto ore e quasi quattrocento siti coinvolti, molti dei quali monetizzavano tramite pubblicità programmatica.

A innescare il caos contribuì la riforma di X/Twitter, dove la spunta blu a pagamento sostituiva la certificazione redazionale. Un'analisi *dell'Università di Stanford* dimostrò che i tweet con badge acquistato circolavano in media tre volte di più, anche se contenevano video riciclati da altre guerre, il tempo medio prima di una rettifica ufficiale superava le ventiquattro ore. In risposta, gruppi umanitari come *UN Mappers* e *HOT OSM* attivarono task-force per aggiornare la mappa di Gaza ogni notte, sfruttando fotografie satellitari *Planet* e big-tile *Sentinel-1* radar per individuare edifici crollati anche sotto la coltre di fumo. Quella base geospaziale divenne il fondamento *della Gaza Interim Damage Assessment* pubblicata congiuntamente da UE, Banca Mondiale e Nazioni Unite, che stimò in 18 miliardi di dollari le perdite infrastrutturali.

Il contesto urbano, privo di libertà di movimento per verificatori indipendenti, trasformò la collaborazione open-source in un esercizio di telerilevamento spinto, i volontari confrontavano l'effetto Doppler della colonna di fumo per calcolare il calibro dei proiettili. Algoritmi di *change detection*, addestrati su dataset di training aperti dal programma *ESA World Cover*, stimavano metri cubi di macerie, i feed AIS dei traghetti al largo di *Ashdod*, rilasciati in licenza CC BY, fornivano indizi sui corridoi umanitari. Eppure, la saturazione

emotiva rendeva più difficile l'ascolto della verità, ogni video di esplosione, decontestualizzato, poteva essere rilanciato come prova di crimini dell'una o dell'altra parte. Quando, il 17 ottobre, un razzo colpì il parcheggio dell'ospedale *Al-Ahli*, fu necessaria una triangolazione di boati registrati su telecamere domestiche a *Ramat Gan*, analisi del cratere e streaming *IR* delle batterie *Iron Dome* per dimostrare che l'ordigno era partito dalla Striscia. Nel frattempo, però la narrativa contraria aveva già raccolto milioni di visualizzazioni.

Il *caso Gaza* evidenzia una seconda faccia dell'open data ossia la moltiplicazione delle fonti aumenta la probabilità di rumore e la necessità di alfabetizzazione visuale. Gli stessi dataset che permettono di valutare danni strutturali, per esempio, le mappe *vector-tiling* open-source di *Mapbox* possono diventare terreno di manipolazione quando selezionati in modo strumentale. La lezione è che la qualità metodologica e la trasparenza delle catene di citazione diventano essenziali quasi quanto la rapidità di pubblicazione.

CYBER-OPERAZIONI TRANSNAZIONALI: GHOSTWRITER DOMAIN SEIZURE E IL CAMPO INFINITO

Se il terreno cinetico di Ucraina e Gaza rende tangibile la posta in gioco, il dominio cyber-informativo mostra la plasticità della guerra narrativa. L'operazione *Ghostwriter*, attribuita al gruppo *UNC1151* collegato ai servizi bielorussi e russi, incarna l'archetipo dell'attacco ibrido, violazione di caselle e-mail di parlamentari polacchi e lituani, estrazione di conversazioni riservate, pubblicazione parziale sui blog compromessi di media locali, amplificazione sui social con account generati da *GAN*, eco finale sulle piattaforme di disinformazione in lingua tedesca. Il rapporto *dell'Università di Cardiff* stima che, tra il 2020 e il 2023, la campagna abbia raggiunto oltre venti milioni di visualizzazioni in Europa occidentale prima di essere riconosciuta come minaccia avanzata.

La filiera dati dell'operazione sfrutta l'apertura delle API dei motori di blog open-source e la disponibilità dei WHOIS in chiaro per mascherare la proprietà dei domini. Quando, nel novembre 2024, il Dipartimento di Giustizia USA ha sequestrato trentadue siti registrati da un intermediario dell'*FSB*, ha illustrato la dinamica, domini con nomi plausibili di testate locali reindirizzavano contenuti fabbricati da *LLM*, firmati da *"giornalisti"* generati da *Synthesia*. L'accusa federale si è basata su log di *Cloudflare*, integrati con la cronologia pubblica di Archive.org e con il dataset *Shodan* in licenza freemium, dimostrando ancora una volta come l'open-source si trovi simultaneamente su entrambi i lati del ring.

A livello europeo, *EUvsDisinfo* identifica pattern atomici ricorrenti: la disinformazione agricola secondo cui *"l'UE imporrà una dieta di insetti"*, la narrativa energetica sulla *"fine dei motori endotermici"*, i falsi scoop sanitari. Per ognuno di questi cluster, la task force del *SEAE* pubblica schede con URL originali, snapshot grafici e contesto. La metodologia, esplicitamente figlia dei principi FAIR, prevede la reperibilità (metadati DCAT-AP), l'accessibilità (licenza CC BY), l'interoperabilità (formato *JSON-LD)* e la riusabilità. Gli analisti OSINT inseriscono quelle schede in pipeline che, in base alle stringhe *SHA-256*, individuano la comparsa del meme su nuovi server e generano allerte.

La triangolazione fra disinformazione e vulnerabilità cyber si è mostrata nel 2023 durante la campagna anti-vaccini portata avanti dal collettivo *Doppelgänger* lo *spear-phishing* a medici romeni rubava credenziali di database sanitari open-source. I compromessi permettevano di clonare dati de-identificati e di costruire grafici falsificati che indicavano un aumento di mortalità post-vaccino. Il ciclo si chiudeva con la pubblicazione sui canali Telegram e la ripresa in testate complottiste francesi. L'efficacia della catena sfruttava non tanto la vulnerabilità tecnica, quanto la semantica, la credibilità dei dataset aperti legittimava la narrativa fabbricata.

La risposta occidentale ha cominciato a maturare. Il NATO Cyber Defence Centre, nella simulazione Locked Shields 2024, ha integrato il modulo *"Narrative Resilience"*: oltre a ripristinare i sistemi DDoS, i team dovevano analizzare feed open-source e produrre smentite entro un'ora dalla falsità. La Commissione europea, con il Regolamento DSA, ora impone alle very large online platforms di fornire accesso API ai ricercatori certificati, affinché possano monitorare in tempo quasi reale la mobilitazione narrativa.

Questi casi dimostrano che la dimensione cyber-informativa si alimenta di una materia prima infinita come domini a basso costo, dataset aperti, modelli generativi, marketplace di competenze. La difesa, di riflesso, deve unire controlli di provenienza, firma digitale dei contenuti, archiviazione distribuita, divulgazione rapida, alfabetizzazione di massa.

CONCLUSIONI INTERMEDIE

Ucraina, Gaza e l'ecosistema cyber dimostrano che l'OSINT, potenziato dall'open data, può essere strumento di trasparenza radicale tanto quanto vettore di manipolazione. Dove gli analisti dispongono di accesso a immagini satellitari, vocabolari interoperabili e repository pubblici, la verità fattuale può emergere in poche ore, sostenuta da prove riproducibili.

Ma la stessa infrastruttura facilita l'iniezione di falsi credibili e l'automazione della propaganda. La posta in gioco, allora, non è se aprire o chiudere i dati, bensì come governarli: standard forti, licenze chiare, catene di custodia e soprattutto formazione di comunità capaci di leggere e contestualizzare documenti complessi. Nei capitoli conclusivi verrà delineato un quadro di raccomandazioni affinché l'Europa trasformi l'asimmetria informativa in vantaggio democratico, anziché in tallone d'Achille cognitivo.

CAPITOLO V. VERSO IL 2030: STRATEGIE ETICHE PER IL GOVERNO DEI DATI E DELL'INFOSFERA

La storia degli ultimi conflitti insegna che la trasparenza dei dati pubblici e la potenza delle analisi open-source possono diventare una formidabile garanzia di responsabilità democratica, ma anche un catalizzatore di rischi se mancano regole, infrastrutture e competenze adeguate. Immaginare la governance del 2030 significa perciò intrecciare tre dimensioni solo in apparenza distinte: la prima è quella normativa, dove l'Unione europea ha ormai costruito un corpus di testi che va dalla Direttiva Open Data al Data Governance Act, dal Data Act al nuovissimo AI Act approvato a marzo 2024, con l'obiettivo esplicito di trasformare l'Europa nella *"casa dell'IA affidabile"*. La seconda dimensione è tecnologica, standard semantici come *DCAT-AP v3*, protocolli di tracciabilità dei contenuti come il *C2PA*, sostenuto da Adobe, Microsoft e Google, e architetture di data-space fondate sul *Reference Model* dell'*International Data Spaces Association* e sul Trust Framework di Gaia-X. La terza, infine, è culturale, senza alfabetizzazione di massa e professionalità intermedie capaci di saldare diritto, ingegneria dei dati e giornalismo investigativo, la migliore piattaforma resta lettera morta.

Una governance etica all'altezza dei prossimi cinque anni dovrà anzitutto interiorizzare il principio di *"responsabilità distribuita"*. Il legislatore europeo lo ha già statisticamente intuito quando, nel Data Governance Act, ha inventato la figura dell'intermediario affidabile che custodisce dati protetti da terzi e ne autorizza il riuso in base a licenze *machine-readable*.
Ma il meccanismo si rivelerà davvero efficace solo se i contratti d'uso diventeranno oggetti digitali incorporati nel flusso dell'informazione come i token semantici che viaggiano insieme ai file e che si aggiornano quando lo stesso file transita da un nodo all'altro. La bozza di Trust Framework Gaia-X in circolazione dal maggio 2024 fornisce esempi di ontologie e regole di ragionamento capaci di rendere operativa questa visione, traducendo valori come privacy, interoperabilità e autodeterminazione in metadati leggibili

dalle macchine. Se entro il 2030 tali token diventeranno default nei portali open data e nei data-space settoriali, la *“catena di custodia semantica”* potrà ridurre drasticamente il contenzioso e i rischi di abuso, perché ogni passaggio lascerà una firma crittografica non ripudiabile.

Il secondo asse della strategia riguarda la qualità intrinseca dei dataset, tema che si annida dietro la sigla FAIR ma che finora è rimasto spesso relegato a linee guida volontarie. L’ISO 31700-1, pubblicata nel 2023 e dedicata al *privacy-by-design*, stabilisce requisiti di alto livello per l’intero ciclo di vita di un prodotto o servizio basato sui dati. La sua adozione all’interno dei portali open-data, però, richiede incentivi chiari, fondi europei 2027-2033 potrebbero essere subordinati a audit di qualità indipendenti, sul modello di quanto accade già per le certificazioni energetiche. Negli stessi termini, il Rapporto di Maturità Open Data 2024 introduce indicatori che legano il rating di un Paese alla ricorsività dei test automatici sui dataset rilasciati. Se questi indicatori verranno legati alla ripartizione del fondo coesione post-2027, la pressione politica verso la qualità si tradurrà rapidamente in prassi operativa.

Un capitolo cruciale è la tracciabilità dell’autenticità dei contenuti multimediali. La diffusione di modelli generativi sempre più capaci di produrre immagini e video indistinguibili dal reale minaccia l’intero ecosistema dell’informazione. Il consorzio C2PA, citato da *The Verge* e *Axios* nel 2024, offre già un meccanismo di firma crittografica che incapsula metadati di provenienza e cronologia delle modifiche. Ma finché le grandi piattaforme non integreranno nativamente la lettura di questi *marker* e finché fotocamere e smartphone non li scriveranno di default la soluzione resterà elitaria. La governance etica per il 2030 dovrebbe dunque fissare un orizzonte vincolante, entro il 2027 tutti i dispositivi certificati nell’Unione dovranno emettere contenuti con firma C2PA o equivalente, mentre le *Very Large Online Platforms*, già soggette al Digital Services Act, saranno obbligate a visualizzare l’informazione di origine e ad avvisare l’utente se

essa è assente o manomessa. Solo in questo modo il contrasto alla disinformazione potrà spostarsi dal piano reattivo al piano preventivo.

La sicurezza informatica è l'altro pilastro indispensabile. Il Cyber Resilience Act, adottato nel 2024, impone requisiti di sicurezza lungo l'intero ciclo di vita dei prodotti digitali, dai router domestici ai *software embedded*. In vista del 2030, la sfida consisterà nell'estendere quei requisiti al software che governa i data-space; ciò comporta la creazione di *SBOM (Software Bill of Materials)* pubblici per tutte le piattaforme *CKAN* e per gli *API gateway* federati, inserendo clausole di disclosure responsabile delle vulnerabilità. Senza questa estensione, i dati aperti rischiano di diventare cavallo di troia per attacchi su larga scala.

Sul fronte intelligenza artificiale, il nuovo AI Act stabilisce un approccio *risk-based* che vieta i sistemi di manipolazione subliminale e impone audit ex ante sugli usi ad alto rischio. L'AI Office, con sede a Bruxelles e operativa dal 2025, dovrà però coordinare una rete di autorità nazionali e di centri di prova accreditati per evitare duplicazioni, la governance etica suggerisce di innestare questa rete nel sistema dei *"trusted flaggers"* del *DSA*, creando corsie veloci per la segnalazione di modelli generativi che violino il divieto di *deepfake* politico non dichiarato. Una tale integrazione ridurrebbe l'intervallo oggi troppo ampio fra la scoperta di un abuso e l'imposizione di misure correttive, che la cronaca dei conflitti mostra essere la finestra decisiva per il successo di una campagna di disinformazione.

Il compito di armonizzare standard, infrastrutture e regole ricadrà in gran parte sullo *European Data Innovation Board*, organismo previsto dal Data Governance Act che, nel 2024, ha pubblicato le prime *"guidelines for high-value dataset governance"*. Perché il Board non rimanga un tavolo consultivo, occorrerà dotarlo di un segretariato tecnico che possa emettere schemi di certificazione rapidi, analoghi agli *"Ecolabel"* ambientali, un dataset sanitario che rispetta ISO 31700, C2PA embedded e DCAT-AP v3 dovrebbe ottenere un marchio riconoscibile dagli utenti e un punteggio

preferenziale nei bandi Horizon Europe. Il collegamento fra rating etico e vantaggio competitivo è, in ultima analisi, il motore più efficace di adozione.

Sul versante difesa e sicurezza, la NATO ha incluso la dimensione cognitiva nella riflessione *"NATO 2030"* pubblicata nel rapporto del gruppo di riflessione guidato da *Madeleine Albright*. L'Alleanza propone esercitazioni che integrino risposta cyber, operazioni informative e gestione dei dati aperti. È essenziale che gli Stati membri sviluppino catene di comando interministeriali dove il ministero della Difesa possa accedere in tempo reale a cataloghi open data certificati, così da produrre smentite supportate da evidenza entro l'ora critica. Perciò, entro il 2028, i data-space nazionali della pubblica amministrazione potrebbero essere obbligati ad attivare *"canali di priorità emergenziale"*, sul modello di quelli previsti dal Regolamento sulle reti transeuropee dell'energia, consentendo l'accesso rapido a dataset geospaziali di supporto alla protezione civile.

Dal punto di vista educativo la governance etica esige un salto di scala. I corsi OSINT dimostrano che è possibile formare funzionari esperti di licenze, API e verifica geospaziale. Ma entro il 2030 servirà una filiera scolastica continua, istituti tecnici superiori con moduli su *metadata engineering,* lauree magistrali che combinino giornalismo, crittografia ed etica, programmi di micro-certificazione aperti a cittadini *"digital volunteers"*. L'Unione europea potrebbe incanalare parte dei fondi Erasmus+ nel creare una *"OSINT Academy"* diffusa, riutilizzando la struttura del *Cybersecurity Skills Academy* lanciata nel 2023.

Lo strato economico non può essere trascurato. Il mercato europeo della condivisione dei dati valeva, secondo il *Data Market Study*, 58 miliardi di euro nel 2024 e mira a superare i 130 entro il 2030. Un sistema di crediti fiscali orientato alla pubblicazione di dataset *"cinque stelle"*, inclusi audit di qualità e licenze aperte, risponderebbe alla necessità di ampliare l'offerta, soprattutto da parte delle PMI. Sul fronte opposto, chi riutilizza i dati a scopo di lucro potrebbe aderire a un obbligo di *"revenue sharing"* dello 0,1 % a

beneficio di un fondo europeo per la manutenzione dei cataloghi. Questa logica di *data dividend* riequilibrerebbe il vantaggio competitivo di chi, come i colossi cloud, estrapola valore scalabile da dati finanziati dai contribuenti.

Un'ultima raccomandazione riguarda la valutazione di impatto: oggi i Documenti di Valutazione *Red Line* quelli che stabiliscono l'equilibrio fra sicurezza nazionale e trasparenza sono redatti caso per caso. Entro il 2030 occorrerà un quadro di valutazione quantitativa che metta in tensione rischi e benefici. L'indice proposto dal centro *Hybrid CoE* di *Helsinki* nel 2024 combina otto fattori: criticità dell'infrastruttura associata al dato, granularità, frequenza di aggiornamento, facilità di anonimizzazione, beneficio socioeconomico previsto, esposizione a minacce ibride, grado di disinformazione potenziale e disponibilità di misure tecnico-organizzative. Se questo indice diventasse obbligatorio per i dataset ad alto valore, l'Europa disporrebbe di uno strumento trasparente per decidere se e come aprire un'informazione sensibile.

In sintesi, la governance etica verso il 2030 deve fondarsi su un patto tripolare, una infrastruttura tecnica verificabile, quadro giuridico coerente e cultura diffusa della prova. L'esperienza dei conflitti di Ucraina e Gaza ha mostrato che l'opinione pubblica reagisce positivamente alle ricostruzioni documentate, ma solo se può seguirne la filiera di verifica. Chi elabora politiche dovrà quindi premiare la tracciabilità semantica, la qualità certificata e la trasparenza procedurale. Se questi tre pilastri saranno sorretti da incentivi economici e da un sistema educativo adeguato, il 2030 potrebbe vedere un'Unione europea in cui l'apertura dei dati non è soltanto un dovere amministrativo, ma un fattore di resilienza democratica e di vantaggio strategico in un mondo dove la verità si misura, sempre più, alla velocità del bit.

Concludere un lavoro dedicato all'Open Source Intelligence e alla guerra dell'informazione senza evocare *Robert David Steele* significherebbe ignorare una delle figure che, prima di molti altri, hanno intravisto il

potenziale della conoscenza aperta come volano di sicurezza, ma anche come argine all'opacità dei poteri. Ex ufficiale dei Marine e analista del Foreign Broadcast Information Service, *Steele* fu tra i primi a sostenere che le fonti in chiaro non rappresentavano un complemento dell'intelligence tradizionale ma bensì erano l'intelligence stessa, purché fossero coniugate con una ferrea etica della trasparenza.

Il suo motto, ripetuto in interviste, libri e nel blog *Public Intelligence* fino alla sua scomparsa nel 2021, riassume più di qualsiasi trattato la filosofia che ha ispirato questo white paper: *"The truth at any cost lowers all other costs".* Pronunciata all'inizio degli anni duemila, la frase suonava come un paradosso in un ambiente abituato a custodire il segreto per principio; oggi, alla luce delle evidenze presentate nei capitoli precedenti, rivela la propria forza di legge economica. Abbiamo visto come la mancanza di verità certificata a *Bucha*, a *Mariupol*, nel parcheggio dell'ospedale *Al-Ahli* o nei domini sequestrati dall'FBI abbia generato costi sociali, diplomatici e perfino militari incalcolabili. Al contrario, la mappa *OSM* che localizza un convoglio, il fotogramma satellitare che svela l'origine di un missile o il metadato C2PA che autentica un video riducono immediatamente la spesa cognitiva, giudiziaria e politica necessaria a discernere il reale dal fabbricato.

Steele parlava di Open-Source Everything: non soltanto software, ma anche dati governativi, processi decisionali, standard industriali, saperi accademici. La sua visione prefigurava l'attuale architettura dei *Common European Data Spaces*, il modello di fiducia di *Gaia-X* e perfino il Data Governance Act, che istituisce intermediari per custodire e condividere contenuti protetti. Tuttavia egli avvertiva che l'apertura senza integrità rischiava di produrre caos anziché liberazione. Era il senso della sua invocazione a un'*"intelligence with integrity"*, capace di coniugare rigore metodologico e accessibilità pubblica.

Il viaggio compiuto in queste pagine, dalle linee guida *Open by Default* alla resilienza narrativa NATO, dai data-space sanitari ai deepfake politici

dimostra quanto la realtà del 2025 si sia avvicinata al suo progetto. Ma ci ricorda anche il pericolo indicato dall'autore ossia la verità deve correre più in fretta della menzogna, altrimenti il costo sociale si gonfia fino a diventare insostenibile.
La mia proposta di governance etica per il 2030 punta precisamente a innescare il circolo virtuoso sognato da *Steele*: dati certificati, catene di custodia trasparenti, firme di provenienza, infrastrutture sicure, competenze diffuse. Se riusciremo a realizzarlo, ogni euro investito in apertura ridurrà di un multiplo i costi della manipolazione e dell'opacità.

A vent'anni dalla sua prima *Open Source Intelligence Handbook*, la comunità OSINT mondiale conta centinaia di migliaia di volontari, data-scientist e investigatori civici. Il loro lavoro quotidiano (geolocalizzare un video, verificare una tabella, tradurre un documento) è la prova concreta che l'idea di *"verità come bene comune"* non era un'utopia. Nelle stesse settimane in cui la Commissione europea perfeziona il regolamento sull'AI trasparente e l'UNESCO coordina l'attuazione della Raccomandazione per la Scienza Aperta, il monito di *Steele* suona più attuale che mai *"la trasparenza non è una concessione, ma la prima linea di difesa della democrazia".*

Chi legge questo white paper troverà nelle pagine precedenti strumenti pratici, standard tecnici e scenari di rischio. Vorrei chiudere, però, con una dimensione più personale, quasi deontologica. Ricorderemo *Bucha* non solo per i numeri, ma per i volti restituiti alla memoria grazie a una prova in chiaro, ricorderemo così Gaza per l'angoscia di immagini decontestualizzate e per la fatica degli analisti che hanno ricostruito l'attimo originario, ricorderemo poi le campagne cyber come *"Ghostwriter"* per l'abilità di insinuarsi nelle crepe narrative delle nostre istituzioni. In tutti questi casi, la differenza l'ha fatta un metodo fondato su apertura, dubbio, replicabilità. È il metodo che *Robert David Steele* sintetizzava in sette parole semplici.

Prenderle alla lettera significa scegliere di pagare il prezzo della verità, che è fatto di lavoro, fatica, esposizione pubblica, per evitare i costi esponenziali della disinformazione, dell'insicurezza e della sfiducia.

È un investimento che non figura nei bilanci contabili, ma definisce il capitale reputazionale di una democrazia. Se nel 2030 l'Europa avrà saputo intrecciare le proprie infrastrutture dati con una cultura della verifica aperta, allora potremo dire di aver onorato davvero l'eredità di *Steele* e di aver trasformato la trasparenza in scudo anziché in vulnerabilità.

Fino ad allora, il suo motto resta sia bussola sia promemoria del lavoro ancora da compiere.

CONCLUSIONI

La traiettoria descritta in queste pagine converge in un punto focale ossia la verità come bene pubblico. Nel corso del lavoro abbiamo osservato come l'apertura dei dati abbia affrancato l'intelligence in chiaro dai margini, trasformandola in un ecosistema globale di monitoraggio, prova e decisione. La stessa apertura, però, ha reso più fragile il tessuto informativo, perché l'enorme superficie di esposizione consente a operatori ostili di inserire menzogne granulari là dove prima esistevano costosi muri di accesso.

Per la pubblica amministrazione italiana ed europea, il primo dovere è riconoscere che i dataset aperti non sono più un adempimento meramente procedurale rivolto a un pubblico specialistico, ma un'infrastruttura strategica che condiziona la resilienza democratica. Le Linee guida ***"Open by Default"***, pubblicate da *AgID*, stabiliscono che la qualità dei dati, la leggibilità meccanica e la presenza di metadati non sono optional, bensì prerequisiti per il riuso legittimo e per la prevenzione di distorsioni interpretative. Questa prescrizione, spesso giudicata un aggravio burocratico, si rivela in realtà la prima linea di difesa contro la guerra dell'informazione, un dataset ben documentato è meno suscettibile di manipolazione, perché riduce il margine di ambiguità su cui prosperano la disinformazione e le teorie del complotto.

Accanto alla dimensione tecnica emerge la questione della velocità. I casi di *Bucha*, *Mariupol* e *Gaza* hanno dimostrato che la finestra decisionale si è compressa a poche ore. Una pubblica amministrazione che non sia in grado di rilasciare rapidamente i propri dati, corredati da licenza e metadati, perde la capacità di inserirsi nel ciclo mediatico con la propria evidenza fattuale, cedendo così terreno a narrazioni ostili. Il principio *"API first"* contenuto nella Direttiva 2019/1024 e ribadito dal Regolamento 2023/138 sui dataset ad alto valore viene quindi a coincidere con un imperativo di sicurezza nazionale. Solo portali capaci di offrire feed in tempo quasi reale

(mobilità, meteo, assetti infrastrutturali non riservati) mettono gli analisti OSINT, i giornalisti e gli stessi decisori istituzionali nelle condizioni di anticipare o confutare campagne di propaganda.

La seconda sfida concerne la tracciabilità e l'integrità delle informazioni. L'evoluzione del deepfake, dei modelli generativi e delle reti neurali di sintesi vocale rende insufficiente la tradizionale delega alla reputazione di chi pubblica.
A livello internazionale il consorzio C2PA ha messo a punto specifiche per incorporare firme crittografiche e cronologia delle modifiche nei contenuti multimediali, integrarle nei *workflow* di produzione delle PA equivale a garantire che le immagini di una discarica abusiva, di un ponte danneggiato o di una manifestazione di protesta non possano essere alterate senza lasciare traccia. Questo requisito non è più confinato alla sfera volontaria, il Digital Services Act impone alle piattaforme di alto impatto di collaborare con le autorità fornendo strumenti di verifica trasparenti, mentre l'AI Act vieta l'uso di sistemi di manipolazione subliminale e fissa l'obbligo di segnalare i contenuti sintetici. Se le amministrazioni pubbliche incorporeranno sistematicamente la firma di provenienza nei propri dataset multimediali, disporranno di un marchio invisibile che permetterà ai cittadini, ai media e agli stessi algoritmi di riconoscere la fonte originale e di misurarne le eventuali alterazioni.

Sul piano organizzativo, la terza sfida riguarda la convergenza di competenze. Nella dimensione locale, spesso il patrimonio informativo è frammentato fra uffici con vocabolari e architetture eterogenee. Una governance etica richiede team interfunzionali che combinino *data engineering*, giurisprudenza digitale, comunicazione strategica e competenze OSINT. Non si tratta di aggiungere personale, ma di ripensare i processi, la pubblicazione di un dataset non termina con l'upload, bensì prosegue con la sorveglianza del suo riuso, con la risposta rapida alle richieste di correzione e con la comunicazione attiva dei limiti e delle incertezze che il dato porta con sé. In assenza di tale manutenzione, il

dataset rischia di diventare fossile, terreno fertile per interpretazioni arbitrarie o, peggio, per l'estrazione di porzioni strumentali che alterano il quadro complessivo.

La quarta sfida eredita il nodo politico della sovranità digitale. Il *Trust Framework Gaia-X* e il *Reference Architecture Model* dell'*International Data Spaces Association* insegnano che non esiste apertura senza sovranità sui metadati di policy. Chi detiene il dato deve specificare le finalità consentite, le condizioni di sicurezza, i limiti di ritenzione. Nel contesto delle PA, ciò significa che gli stessi portali dei comuni, delle regioni o dei ministeri dovranno integrare meccanismi di gestione dei contratti di uso che i sistemi terzi possano leggere e rispettare automaticamente. Senza questa automazione, la scala continentale dei data-space resterebbe teorica e l'asimmetria con le Big Tech continuerebbe a espandersi.

L' ultima sfida infine, riguarda il rapporto con i cittadini. L'esperienza di *Monithon*, *Openpolis*, *UN Mappers* e della miriade di progetti *civic tech* mostra che la società civile è in grado di trasformare i dataset pubblici in strumenti di controllo diffuso ma la stessa energia può essere dirottata da campagne emotive prive di fondamento. Per invertire il trend, la PA deve offrire strumenti di lettura *micro-dashboard*, glossari di qualità dei dati, link di contesto che accompagnino ogni download, sul modello delle *"schede EUvsDisinfo"*. L'alfabetizzazione dell'utente finale non va considerata un bonus, bensì l'ultima maglia della catena di sicurezza. Se l'utente non comprende la fonte o i limiti di un indicatore, sarà vulnerabile a chi propone interpretazioni estreme o allarmistiche. Una democrazia resiliente, dunque, non si limita a rilasciare il dataset, ma lo spiega, lo visualizza, lo aggiorna e rende trasparente la genealogia di ogni valore.

Guardando al 2030, queste cinque sfide si traducono in un'unica missione: le pubbliche amministrazioni debbono diventare orchestratori di fiducia. Ciò implica budget dedicati alla qualità dei dati, strumenti di firma automatica dei contenuti, integrazione delle API in tempo reale, formazione continua e

un dialogo strutturato con la comunità investigativa indipendente. Se realizzata, questa orchestrazione riduce i costi sociali della menzogna, costi che *Steele* invitava a considerare non meno reali di quelli economici, perché accelera la verifica e innalza la soglia tecnica della manipolazione. Viceversa, se le amministrazioni si limiteranno a pubblicare open data senza presidio, l'equilibrio si sposterà verso gli attori ostili, che nel vuoto di documentazione troveranno spazio per piegare l'informazione alla propria strategia.

L'intero percorso delineato in questo studio, dall'evoluzione dell'OSINT alla governance etica, converge nel punto che la resilienza democratica non è il risultato di una sola tecnologia o di una sola legge, ma l'esito di un ecosistema dove infrastruttura, regola e cultura si sostengono a vicenda. Le pubbliche amministrazioni ne sono il pilastro centrale, perché detengono la materia prima della verità fattuale, le statistiche, mappe, registri, immagini satellitari. Se sapranno custodirla con rigore, descriverla con chiarezza, distribuirla con tempestività e accompagnarla con formazione, il costo della menzogna si alzerà fino a rendere poco redditizia la guerra dell'informazione. Se invece lasceranno che l'apertura rimanga un'operazione di facciata, la verità continuerà a rincorrere la propaganda e la resilienza resterà un auspicio più che una condizione concreta.

Giunti al termine di questo viaggio, ci si impone una responsabilità collettiva trasformare i principi in prassi, i pilastri in procedure, la massima di *Steele* in budget, capitolati tecnici e programmi educativi. Solo allora, nel 2030, potremo dire che l'Europa, e con essa l'Italia, hanno fatto dell'open-data e dell'OSINT non soltanto un simbolo di modernità, ma un vero scudo cognitivo a difesa della libertà.

FONTI

BIBLIOGRAFIA

- Francesca De Chiara, Maurizio Napolitano. Il valore dei dati pubblici, 2021, FBK Press.
- Steele, R. D. The Open-Source Intelligence Handbook. Open Source Solutions Press, ed. riv. 2020.
- Intelligence. Spie e segreti in un mondo aperto, Robert D. Steele ,M. Caligiuri, Rubbettino, 2002.
- The Open-Source Everything Manifesto: Transparency, Truth, and Trust: 2. Robert David Steele , Howard Bloom. EVOLVER EDITIONS, 2012.
- NATO. NATO 2030: United for a New Era. Reporto del Gruppo di Riflessione, 2021.
- Open Data, ricerca scientifica e privatizzazione della conoscenza, Roberto Caso, 2022. Trento Law and Technology Research Group Research Paper n. 48
- Unione Europea. Regolamento (UE) 2022/868 – Data Governance Act.
- Unione Europea. Artificial Intelligence Act (testo concordato, marzo 2024).
- Unione Europea. Digital Services Act – Regolamento (UE) 2022/2065.
- Unione Europea. Proposta di Cyber Resilience Act, COM(2022) 454 final.
- Mario Caligiuri, Geopolitica della mente. L'intelligence nel campo di battaglia definitivo. 2023, Mazzaniti libri.
- GAIA-X AISBL. Trust Framework v2.0, Bruxelles, 2024.
- Consumer protection – Privacy by design for consumer goods and services. ISO/IEC 31700-1:2023,
- UNESCO. Recommendation on Open Science, Parigi, 2021.
- U.S. Department of Defense. Open-Source Intelligence Strategy 2024-2028. Washington D.C., 2024.
- Graphika. Secondary Infektion – Rolling Updates on a Persistent Disinformation Operation, 2019-2023.

- Mandiant. UNC1151 / Ghostwriter – Activity Update, rapporto tecnico, 2023.
- EUvsDisinfo. Disinformation Review – Annual Compendium 2024. Servizio Europeo per l'Azione Esterna.

SITOGRAFIA

- https://www.bellingcat.com/news/2024/07/09/russian-missile-identified-in-kyiv-childrens-hospital-attack/
- https://www.bellingcat.com/resources/2024/04/25/oshit-seven-deadly-sins-of-bad-open-source-research/
- https://apnews.com/article/russia-ukraine-war-mariupol-theater-c321a196fbd568899841b506afcac7a1
- https://www.agendadigitale.eu/cittadinanza-digitale/il-data-analytics-framework-daf-e-la-piattaforma-digitale-nazionale-dati-i-punti-chiave/
- https://www.ondata.it/dal-data-analytics-framework-daf-alla-piattaforma-digitale-nazionale-dati-pdnd/
- https://agenda.infn.it/event/32982/contributions/184081/attachments/100118/139238/PATRUNOpdnd.pdf
- https://www.medialaws.eu/wp-content/uploads/2020/07/RDM-2-2020.pdf
- https://www.act.nato.int/activities/cognitive-warfare/
- https://www.infodata.ilsole24ore.com/2021/02/02/think-tally-talk-perche-vogliamo-gli-open-data-giorgia-lodi/
- https://www.slideshare.net/slideshow/open-data-e-big-data-le-potenzialit-offerte-per-la-pa/197893998
- https://techeconomy2030.it/2022/04/20/open-data-per-lsdg-17-rafforzare-le-modalita-di-attuazione-e-rilanciare-il-partenariato-globale-per-lo-sviluppo-sostenibile/
- https://techeconomy2030.it/2022/03/18/open-data-per-gli-sdgs-1-e-2-sconfiggere-la-poverta-e-la-fame/
- https://techeconomy2030.it/2022/02/02/open-data-per-lsdg-16-pace-giustizia-e-istituzioni-forti/

- https://techeconomy2030.it/2021/12/23/obiettivo-9-costruire-uninfrastruttura-resiliente-e-promuovere-linnovazione-ed-una-industrializzazione-equa-responsabile-e-sostenibile/
- https://techeconomy2030.it/2021/03/06/opendataday-open-data-per-la-sostenibilita/
- https://cris.fbk.eu/retrieve/ddb241a5-491a-ba8a-e053-3a05fe0afd55/1359-5822-1-PB.pdf
- https://forges.forumpa.it/assets/Speeches/27549/napolitano_academy_opendata.pdf
- https://open.gov.it/notizie/sovranita-digitale-intelligenza-artificiale
- https://digital-strategy.ec.europa.eu/
- https://c2pa.org/
- https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html
- https://apnews.com/article/russia-ukraine-entertainment-europe-donetsk-59fbc059a9fe9b5825841ff25025b5cc
- https://www.open.online/2022/05/04/inchiesta-ap-raid-russo-teatro-mariupol-video/

Pubblicato nel gennaio 2026
Società Italiana di Intelligence
SOCINT Press
https://press.socint.org

979-12-80111-76-0

Direzione editoriale: Alice Felli