

Luciano Colombo

# Custodire la conoscenza: la sicurezza della ricerca come sfida al paradigma della scienza aperta

(doi: 10.1430/118816)

L'industria (ISSN 0019-7416)

Fascicolo 3, luglio-settembre 2025

**Ente di afferenza:**

()

Copyright © by Società editrice il Mulino, Bologna. Tutti i diritti sono riservati.  
Per altre informazioni si veda <https://www.rivisteweb.it>

## **Licenza d'uso**

Questo articolo è reso disponibile con licenza CC BY NC ND. Per altre informazioni si veda <https://www.rivisteweb.it/>

# Custodire la conoscenza: la sicurezza della ricerca come sfida al paradigma della scienza aperta

Luciano Colombo

## Safeguarding Knowledge: Research Security as a Challenge to the Open Science Paradigm

In the current landscape of scientific knowledge, Open Science emerges not merely as a technical reform, but as a far-reaching epistemological and cultural shift. It redefines the relationship between science and society by treating knowledge as a common good, meant to be shared, critically engaged with, and harnessed for inclusive social progress. However, this transformative openness faces increasing tensions due to evolving geopolitical and technological threats. The proliferation of digital vulnerabilities, dual-use research, and foreign interference, to name just a few critical issues, calls for a new awareness about research security. This introduces a systemic tension between openness and protection, transparency and confidentiality, collaboration and control. In this essay, I advocate for a recalibration of Open Science towards a model that is both *conscious and resilient*. Rather than opposing security to openness, I propose a synthetic paradigm reconciling both through critical responsibility, multi-level risk governance, and robust public legitimacy.

**Keywords:** Open Science, Research Security, Dual-use, Knowledge Governance, Ethical Risk Management, Technological Threats.

**JEL Classification:** O38; D83; L86; H56; K24; Z18; I28

## 1. INTRODUZIONE

Nel contesto delle trasformazioni che, in misura diversa, investono il sistema contemporaneo della ricerca accademica, si riconosce nella Scienza Aperta un paradigma emergente e, al contempo, un terreno di forte tensione.

La Scienza Aperta<sup>1</sup> non si configura come un mero strumento tecnico finalizzato all'ottimale diffusione dei risultati scientifici, bensì come una radica-

<sup>1</sup> Sul punto si vedano i contributi offerti da molteplici iniziative internazionali ed europee come UNESCO Recommendation on Open Science (<https://www.unesco.org/en/open-science>), l'infrastruttura OpenAIRE (<https://www.openaire.eu/>), EOSC Association (<https://eosc.eu/>) e il portale italiano open-science.it (<https://open-science.it/>).

Luciano Colombo, Università di Cagliari, Dipartimento di Fisica, Cittadella Universitaria, SP Monserrato-Sestu km 0.700, I-09042 Monserrato, Cagliari, Italia; [luciano.colombo@unica.it](mailto:luciano.colombo@unica.it), <https://orcid.org/0000-0001-5335-4652>

Received: June 15, 2025 | Revised: August 25, 2025 | Accepted: September 5, 2025

le riformulazione di carattere epistemologico e culturale delle modalità attraverso cui la produzione di conoscenza e i nuovi saperi che ne derivano vengono generati, validati, valutati, condivisi e, per ultimo, resi disponibili alla collettività. Lungi dal potersi ridurre a un insieme di semplici (per quanto innovative) procedure, la Scienza Aperta riformula in profondità il rapporto tra la scienza e la società, tra i ricercatori e i cittadini, tra le istituzioni accademiche e le autorità pubbliche, fondandosi sul principio che la conoscenza debba essere trattata come un bene comune, destinato a circolare liberamente e a contribuire, in modo equo e inclusivo, al progresso sociale e civile.

Tale trasformazione, tuttavia, si confronta oggi con sfide e ambiguità significative, prodotte da un contesto globale profondamente mutato sotto il profilo geopolitico e tecnologico. In un'epoca caratterizzata dalla centralità dei dati, dalla crescente vulnerabilità delle infrastrutture digitali, dalla competizione strategica per la supremazia tecnologica e dalla proliferazione di minacce ibride, la questione della sicurezza della ricerca assume un rilievo che non può essere eluso (Commissione europea 2025; Consiglio dell'Unione europea 2024). L'accessibilità, che costituisce il cuore del paradigma aperto (*openness*), si trova a fare i conti con l'esigenza di protezione; la trasparenza metodologica entra in tensione con la necessità di riservatezza; la cooperazione scientifica internazionale si misura con i vincoli derivanti da logiche securitarie e da strategie di difesa nazionale. In tale quadro, si può facilmente individuare una tensione sistemica tra apertura e sicurezza che, attraversando trasversalmente l'intera *governance* della ricerca, interpella direttamente le responsabilità delle istituzioni e dei soggetti che ne fanno parte.

Questo breve saggio esplora alcune implicazioni teoriche e operative di tale tensione, richiamando l'attenzione tanto sui rischi di un irrigidimento difensivo (suscettibile di condurre alla iper-burocratizzazione dell'attività scientifica, all'autolimitazione tematica e alla rarefazione delle collaborazioni internazionali), quanto sui limiti insiti in una concezione dell'apertura come valore assoluto, privo di dispositivi di responsabilità e di governo del rischio. Da questa analisi di contesto, verrà sviluppata una riformulazione evolutiva del paradigma di *openness* in direzione di una «Scienza Aperta consapevole e resiliente»: un modello che, lungi dal rinunciare ai propri principi fondativi, sappia riaffermarli con maturità, dotandosi degli strumenti analitici, regolativi e organizzativi necessari per distinguere le esigenze legittime di protezione da quelle che rischiano di degenerare in restrizioni indebite.

Le argomentazioni si svilupperanno lungo alcune direttrici fondamentali. Verrà in primo luogo proposta una breve riflessione sulla necessità di una trasformazione istituzionale capace di integrare in modo coerente le dimensioni dell'apertura e della sicurezza, attraverso percorsi di formazione mirati, la valorizzazione di nuove figure professionali e la ristrutturazione delle architetture organizzative. Seguirà poi la messa in evidenza delle possibili critici-

tà derivanti dalla frammentazione normativa a livello europeo e dalle rigidità procedurali che caratterizzano il contesto italiano, le quali rischiano di svuotare di efficacia le misure di tutela, trasformandole in oneri amministrativi privi di reale capacità preventiva. Infine, verrà dedicata particolare attenzione alla dimensione etica della sicurezza della ricerca, sostenendo l'esigenza di istituire presidi di vigilanza indipendenti, dotati di legittimazione scientifica e di autonomia funzionale, in grado di garantire la trasparenza, la proporzionalità e la legittimità delle scelte restrittive.

Nella parte conclusiva, sarà presentata una proposta di carattere sistemico: promuovere una Scienza Aperta che sia al tempo stesso lucida nella consapevolezza dei rischi e salda nella fedeltà ai valori che ne costituiscono l'ossatura. Una Scienza che adotti pratiche multilivello per la diffusione dei risultati, che integri in modo consapevole diversi principi di gestione dei dati, che includa sistematicamente la valutazione del rischio etico-strategico nei processi decisionali, e che investa nella costruzione di infrastrutture digitali sicure e federate, fondate sul principio del «security and openness by design». Risulterà inoltre imprescindibile rafforzare il dialogo transdisciplinare tra i diversi ambiti del sapere e tra i soggetti coinvolti nella produzione e nella regolazione della conoscenza, quale condizione necessaria per la definizione di politiche efficaci, sostenibili e democraticamente legittimate.

Sotto il profilo metodologico, questo contributo adotta la forma del saggio argomentativo, fondato su un approccio qualitativo e concettuale. L'analisi è costruita principalmente attraverso la disamina critica di documenti di *policy* europei (Commissione europea, Consiglio UE, ERA, ecc.), integrata con riflessioni teoriche e comparazioni con la letteratura esistente su Scienza Aperta e Sicurezza della Ricerca. Pur non basandosi su dati quantitativi o su analisi econometriche, la metodologia scelta nondimeno risulta adeguata a cogliere le tensioni di *policy* e gli snodi concettuali che caratterizzano il tema, offrendo un contributo di carattere critico e strategico al dibattito accademico e istituzionale.

In conclusione, è opportuno riaffermare un concetto che orienta l'intero impianto della presente riflessione: la posta in gioco non riguarda esclusivamente la protezione della conoscenza, ma niente di meno che la sua stessa legittimità. In un'epoca in cui la fiducia nella scienza si rivela al tempo stesso più fragile e più indispensabile, costruire una Scienza Aperta consapevole e resiliente significa affermarne il valore pubblico, garantirne l'autonomia e custodirne la funzione critica, a beneficio di una società libera, equa e informata.

## 2. ANALISI DI CONTESTO PER LA SCIENZA APERTA

Un approfondimento definitorio appare necessario, in apertura, al fine di rafforzare la comprensione del paradigma della Scienza Aperta. Essa, infatti, non è riducibile a un singolo insieme di pratiche, bensì a un ecosistema di principi, strumenti e valori che si intrecciano in modo complesso. La Commissione europea (2015) ha definito la Scienza Aperta (*Open Science*) come un nuovo modo di fare ricerca, che si fonda sulla condivisione sistematica di conoscenza, dati, strumenti e infrastrutture lungo l'intero ciclo della produzione scientifica. A tale definizione si affianca quella proposta dall'UNESCO (2021) che individua la Scienza Aperta come un bene pubblico globale, chiamato a promuovere inclusività, equità e sostenibilità. Questa cornice istituzionale è stata ulteriormente estesa al punto che la Scienza Aperta non risulta essere soltanto una questione di accessibilità tecnica, ma implica la rinegoziazione del contratto sociale della scienza, ridefinendo i rapporti tra ricercatori, cittadini e istituzioni. In questo senso, parlare di Scienza Aperta significa parlare di una trasformazione culturale che riconosce la conoscenza come bene comune, superando la logica proprietaria e promuovendo modelli collaborativi di ricerca. Particolare rilievo assumono, in questa prospettiva, le dimensioni educative e formative: la Scienza Aperta non riguarda soltanto la diffusione dei risultati, ma anche la costruzione di competenze condivise e di pratiche di lavoro aperte, volte a garantire trasparenza, riproducibilità e responsabilità.

Il paradigma della Scienza Aperta si configura, quindi, come una delle più profonde e pervasive trasformazioni culturali che abbiano investito il sistema contemporaneo della ricerca. Non si tratta di una semplice evoluzione tecnica, né di un aggiornamento procedurale volto a rendere più efficiente la circolazione dei risultati scientifici. Si tratta, piuttosto, di un mutamento paradigmatico che riformula in profondità le modalità con cui il sapere scientifico viene generato e condiviso. In tal senso, la Scienza Aperta si fonda su un complesso coerente di principi epistemici e norme operative che mirano a rendere l'attività scientifica radicalmente più trasparente, accessibile, inclusiva e orientata alla responsabilità sociale.

Al cuore di questa visione sta una concezione della conoscenza come bene comune, un patrimonio collettivo che non può né essere reso esclusivo, né venire confinato entro i recinti dell'accademia o delle logiche proprietarie di mercato. La conoscenza, per essere tale, deve poter essere condivisa, discussa criticamente, riutilizzata e fatta circolare in modo aperto e non discriminatorio, non solo all'interno delle comunità scientifiche specialistiche, ma anche (anzi: soprattutto) al servizio della società nel suo insieme. L'idea di fondo è che una scienza più aperta è anche una scienza più equa, più efficace, più capace di affrontare le sfide complesse del nostro tempo, in una logica collaborativa e intersettoriale. Su questi concetti la letteratura accademica è ampia e consolidata. Tra i

contributi più influenti si possono citare le analisi di Fecher e Friesike (2014), che distinguono tra diverse anime della Scienza Aperta (efficienza, trasparenza, democratizzazione e partecipazione), o le riflessioni di Vicente-Saez e Martinez-Fuentes (2018), che la definiscono come un paradigma culturale prima ancora che tecnico. Questa pluralità di interpretazioni contribuisce a chiarire come la Scienza Aperta non si riduca a un insieme di pratiche amministrative, ma costituisca una vera e propria riformulazione del contratto sociale della scienza.

I pilastri che strutturano il paradigma della Scienza Aperta sono molteplici e tra loro fortemente interconnessi. L'accesso libero e gratuito alle pubblicazioni scientifiche (*Open Access*) consente di superare le barriere editoriali che limitano la fruizione dei risultati della ricerca, restituendo alla comunità globale ciò che spesso è stato prodotto con risorse pubbliche (European Commission 2025)<sup>2</sup>. La condivisione e la riutilizzabilità dei dati della ricerca secondo i principi FAIR (*Findable, Accessible, Interoperable, Reusable*) (Wilkinson *et al.* 2016)<sup>3</sup> si propone di garantire la tracciabilità e la replicabilità degli esperimenti, favorendo la possibilità di accumulo del sapere. La trasparenza metodologica (che comprende la registrazione aperta dei protocolli di ricerca, la pubblicazione dei dati negativi, la rendicontazione dei processi di *peer review*) rafforza l'integrità scientifica. L'inclusione dei cittadini nei processi di generazione del sapere (*Citizen Science*)<sup>4</sup> amplia le frontiere della partecipazione democratica alla scienza e rafforza il legame fiduciario tra istituzioni scientifiche e società civile. L'apertura dei codici, dei dati, degli algoritmi e degli strumenti digitali (*Open Source*) disinnesci le opacità tecnocratiche, favorendo l'innovazione collaborativa e la condivisione (European Commission 2020). Infine, la riforma dei sistemi di valutazione della ricerca (*Reforming Research Assessment*) mira a superare indicatori quantitativi eccessivamente semplificatori, promuovendo approcci qualitativi e responsabili che valorizzino la qualità, la diversità e l'impatto sociale della ricerca. Infine, le infrastrutture aperte<sup>5</sup> (*Open Infrastructures*), intese non solo come ambienti digitali condivisi, interoperabili e sostenibili, ma anche come spazi fisici e laboratori aperti accessibili alla comunità scientifica, rappresentano il fondamento tecnico-organizzativo su cui si reggono le pratiche della Scienza

<sup>2</sup> Sul punto si vedano anche <https://open-research-europe.ec.europa.eu/> e <https://science-europe.org/our-priorities/open-science/open-access/>.

<sup>3</sup> Sul punto si vedano anche <https://www.openaire.eu/how-to-make-your-data-fair> e <https://open-science.it/en/article?rpk=160581>.

<sup>4</sup> Al riguardo si vedano <https://www.ecsa.ngo/>, <https://eu-citizen.science/> e <https://www.citizenscience.it/>.

<sup>5</sup> Sul punto si vedano <https://sfidora.org/>, [https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/reforming-research-assessment-agreement-now-final-2022-07-20\\_en](https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/reforming-research-assessment-agreement-now-final-2022-07-20_en), <https://coara.eu/> e [https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science/european-open-science-cloud-eosc\\_en](https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science/european-open-science-cloud-eosc_en).

Aperta. *Repository* istituzionali, archivi federati, piattaforme per la gestione trasparente dei dati, insieme a laboratori attrezzati che promuovono la condivisione di risorse, saperi e tecnologie, sono tutti egualmente elementi cruciali per garantire un ecosistema di *openness*.

È importante sottolineare che questa trasformazione non è soltanto organizzativa, né si esaurisce in un aggiornamento delle pratiche gestionali della ricerca. Si tratta, in effetti, di un processo che investe simultaneamente le dimensioni epistemologica ed etica del fare scienza. La Scienza Aperta implica una ridefinizione profonda del rapporto tra la comunità scientifica e i suoi interlocutori (siano essi istituzionali, economici o della società civile) ponendo la ricerca come leva strategica di innovazione, non solo tecnologica ma anche sociale e culturale. In questo nuovo scenario, l'ampliamento del perimetro della partecipazione e la valorizzazione della trasversalità dei saperi divengono strumenti fondamentali per accelerare i processi innovativi e ricostruire, su basi più solide, il rapporto di fiducia tra scienza e società.

La letteratura ha più volte sottolineato come tali rischi possano manifestarsi su diversi livelli. Willinsky (2006) mette in guardia dal confondere accessibilità con qualità della conoscenza; Bezuidenhout *et al.* (2017) analizzano invece i rischi geopolitici e tecnologici, distinguendo tra quelli legati ai dati, ai processi e agli stessi oggetti della ricerca. Si tratta dunque non solo del pericolo di un uso improprio dei risultati già pubblicati, ma anche della possibilità che i *dataset* sottostanti vengano sfruttati in modo malevolo o che l'intero oggetto di studio (ad esempio in ambito biotecnologico) generi rischi intrinseci.

Questa articolazione è fondamentale per comprendere la complessità della tensione apertura-sicurezza. Va certamente citato in primo luogo il rischio *dual use* dei prodotti della ricerca, ovvero la possibilità che conoscenze scientifiche, strumenti, prodotti o *software* progettati per fini pacifici vengano utilizzati in modi inaspettati o problematici (European Parliament 2021). La vigilanza su questi aspetti è intesa a prevenire che materiali e tecnologie potenzialmente sensibili possano essere usati per violare diritti umani, alimentare conflitti, contribuire alla proliferazione di armi di distruzione di massa o, nel caso europeo, favorire prassi contrarie ai principi e valori ispiratori dell'Unione europea. Sotto questo profilo va notato che l'apertura e la rapidità nella diffusione dei risultati scientifici possono facilitare un impiego malevolo, soprattutto in settori sensibili come biotecnologie, telecomunicazioni e cyber-sicurezza, tecnologie nucleari, elettronica avanzata, calcolo ad alte prestazioni, materiali speciali. L'accesso aperto può, di fatto, aumentare la probabilità di sviluppare strumenti utilizzabili a fini di disinformazione, bioterrorismo o produzione di armi di distruzione di massa. In secondo luogo, bisogna riconoscere una criticità nella questione della replicabilità: l'adozione di pratiche aperte non elimina la crisi della riproducibilità, anzi può talvolta amplificarla. La pressione a pubblicare rapidamente, tipica di alcuni modelli di diffusio-



ne «open», rischia di favorire pratiche scorrette come il *p-hacking* (insieme di pratiche che consistono nel manipolare i dati o i metodi statistici fino a ottenere risultati con apparente significatività statistica) o la pubblicazione selettiva. Un terzo rischio riguarda l'esclusione: la Scienza Aperta di per sé non garantisce automaticamente inclusività, poiché la carenza di risorse e competenze può amplificare le disuguaglianze tra comunità scientifiche e tra Paesi. Altri rischi attengono alla *privacy* e alla riservatezza dei dati: la condivisione estrema può compromettere la tutela dei soggetti coinvolti nella ricerca, sollevando delicati interrogativi etici e legali. Infine, va anche ricordato che la diffusione indiscriminata ha favorito l'espansione di pratiche editoriali predatorie, che minano la qualità e la credibilità della letteratura scientifica.

Proprio l'ambizione trasformativa e radicale della Scienza Aperta apre, dunque, inevitabilmente a criticità e vulnerabilità. L'accessibilità immediata della conoscenza, se non adeguatamente governata, può comportare rischi significativi. In altri termini, l'apertura non equivale automaticamente a trasparenza, né garantisce da sola l'integrità o la sicurezza dei processi conoscitivi. È pertanto essenziale che l'intero sistema (dalle università agli istituti di ricerca, dalle agenzie finanziatrici ai decisori politici) si faccia carico di una responsabilità collettiva nella costruzione di un quadro normativo e operativo, capace di garantire che l'apertura non si traduca in esposizione incontrollata o in vulnerabilità sistemica.

Queste preoccupazioni non sono astratte, ma rispecchiano trasformazioni molto concrete del contesto tecnologico e geopolitico in cui la ricerca oggi si colloca. Le infrastrutture digitali che supportano la produzione, conservazione e diffusione del sapere scientifico sono sempre più complesse e interconnesse e, dunque, crescentemente esposte a vulnerabilità in termini di sicurezza informatica. I settori tecnologici emergenti (quali l'intelligenza artificiale, le biotecnologie, le neuroscienze computazionali e le tecnologie quantistiche) presentano un potenziale intrinsecamente duale: le medesime conoscenze che possono generare benefici sociali straordinari possono, in determinati contesti, essere impiegate a fini di controllo, repressione o conflitto. Il fenomeno di *dual use* solleva dunque interrogativi etici e politici di primo piano. A ciò si aggiunga il fatto che attori statuali non appartenenti all'Unione europea, talvolta operando attraverso *partnership* apparentemente neutrali, cercano di accedere (in modo opaco e non sempre tracciabile) a conoscenze strategiche sviluppate all'interno delle università e dei centri di ricerca europei.

Di fronte a questi rischi crescenti, l'Unione europea ha intrapreso un'azione sistematica volta a promuovere una cultura diffusa della sicurezza all'interno del sistema della ricerca. Si tratta di un'azione che non è intesa a limitare l'apertura, bensì mira, almeno in linea di principio, a governarla responsabilmente, affiancando al principio della libertà scientifica quello della tutela del bene pubblico. Tra gli strumenti adottati vale la pena ricordare la



Comunicazione della Commissione europea sul *Global Approach to Research and Innovation*<sup>6</sup>, che delinea una strategia multilaterale per l'internazionalizzazione responsabile della ricerca; le Conclusioni del Consiglio UE sulla sicurezza della ricerca per il triennio 2022-2024<sup>7</sup>, che pongono l'accento sulla necessità di integrare le considerazioni di rischio nei processi di *governance* della ricerca; le *Guidelines on Foreign Interference*<sup>8</sup> del 2022, che forniscono raccomandazioni operative per prevenire forme di ingerenza indebita; e, infine, l'Agenda politica dell'*European Research Area*<sup>9</sup> che sollecita esplicitamente gli Stati membri e le istituzioni scientifiche a sviluppare approcci integrati tra apertura e sicurezza.

Tali documenti, pur riconoscendo l'indispensabile valore della Scienza Aperta, assegnano alle istituzioni scientifiche nuove e complesse responsabilità: dalla valutazione sistematica dei rischi connessi alla diffusione delle conoscenze sensibili, all'adozione di protocolli di *due diligence* per la selezione dei partner internazionali; dalla classificazione dei dati ad alto impatto strategico alla costruzione di competenze avanzate in ambito di cybersicurezza, fino all'introduzione di sistemi di controllo e monitoraggio delle collaborazioni scientifiche transnazionali.

### 3. APERTURA VS. PROTEZIONE: UNA TENSIONE SISTEMICA

La ricerca di un equilibrio tra apertura e protezione è certo legittima, anzi necessaria; ma il pericolo concreto è che, in nome della salvaguardia della conoscenza e della prevenzione di minacce esterne, si avvii un processo involutivo che finisca col comprimere progressivamente la libertà della ricerca scientifica. È una tensione sottile ma profonda, che non si risolve con il semplice richiamo al «giusto mezzo», bensì richiede un'elaborazione politica, culturale e giuridica molto più attenta e articolata. Il punto critico (qui si colloca il centro della presente riflessione) è rappresentato da un fatto molto concreto, fonte di non poca preoccupazione: la crescente enfasi sulla sicurezza della ricerca rischia di innescare una tensione sistemica, e forse strutturale, con i principi fondativi della Scienza Aperta. La crescente tensione tra apertura e protezione è già oggetto di indagine. David (2008) ha mostrato come l'aper-

<sup>6</sup> [https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/global-approach-research-and-innovation\\_en](https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/global-approach-research-and-innovation_en).

<sup>7</sup> <https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf>.

<sup>8</sup> [https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-publishes-toolkit-help-mitigate-foreign-interference-research-and-innovation-2022-01-18\\_en](https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-publishes-toolkit-help-mitigate-foreign-interference-research-and-innovation-2022-01-18_en).

<sup>9</sup> <https://european-research-area.ec.europa.eu/policy-agenda-2022-2024>.

tura sia condizione storica di sviluppo scientifico, ma al tempo stesso potenziale vulnerabilità. Più recentemente, in Bonn *et al.* (2023) è stato discusso il rapporto tra letteratura scientifica e l'approccio *openness*. Il dibattito rimane aperto e conferma la necessità di un approccio equilibrato, che eviti sia l'ingenuità regolativa sia le derive securitarie.

Il rischio, in questo senso, non è un'astrazione teorica: si delinea come possibilità concreta che potrebbe tradursi in molteplici dispositivi operativi i quali, se non progettati e governati con equilibrio, rischierebbero di trasformarsi in strumenti di dissuasione, controllo o restrizione. Si pensi, ad esempio, alla possibile introduzione di controlli preventivi e vincoli procedurali sulle collaborazioni con università e centri di ricerca di paesi terzi, talvolta ispirati da generiche preoccupazioni geopolitiche piuttosto che da criteri rigorosamente scientifici. Oppure alla classificazione crescente dei dati come «sensibili», «strategici» o «riservati», in assenza di criteri condivisi e trasparenti che aiutino a distinguere la protezione giustificata dalla mera opacità. Ancora, si consideri la proposta di valutare *ex ante* il rischio etico, strategico o duale connesso a ogni singolo progetto di ricerca o alla mobilità internazionale dei *visiting scholar*, secondo logiche che talvolta sfiorano il sospetto sistematico, anziché la fiducia.

Questi strumenti, pur giustificati dalle mutate condizioni del contesto globale, possono produrre effetti collaterali non trascurabili, soprattutto se applicati con rigidità o secondo logiche securitarie non sufficientemente ponderate. Essi rischiano infatti di rallentare sensibilmente l'avvio di progetti, scoraggiando la collaborazione internazionale; di introdurre dinamiche di autocensura tematica o metodologica, con la conseguenza che alcune linee di ricerca, considerate ad alto rischio o politicamente sensibili, vengano abbandonate o non finanziate; e di alimentare un clima generale di sospetto che mina il terreno stesso su cui la scienza si fonda: quello dello scambio libero e del confronto tra prospettive diverse.

Non si tratta evidentemente di negare l'esistenza di minacce reali o di sottovalutare le responsabilità delle istituzioni scientifiche nel tutelare l'integrità e la sicurezza dei propri ecosistemi conoscitivi. Si tratta piuttosto di evitare che il legittimo sforzo di protezione si trasformi in una (cattiva) «cultura della sorveglianza», in cui la libertà di ricerca venga subordinata a considerazioni esterne che, se non ben bilanciate, possono impoverire la ricerca stessa, privandola del suo respiro internazionale, del suo dinamismo creativo, della sua apertura metodologica.

La storia, del resto, ci ammonisce con chiarezza: la libertà della scienza è un bene intrinsecamente fragile. Non è mai garantita una volta per tutte, ma va custodita e continuamente riconquistata, proprio nei momenti in cui appare più minacciata. Difenderla significa vigilare affinché le misure di protezione non si trasformino in dispositivi di conformismo o in barriere amministra-

tive che soffocano la curiosità intellettuale. Significa ribadire che la ricerca si alimenta di scambi aperti, di mobilità intellettuale, di dialoghi interculturali: essa non prospera nell'isolamento, ma si nutre dell'alterità, della contaminazione, dell'incontro con il diverso. In tal senso, ogni tentativo di normare eccessivamente la conoscenza, di restringerne l'accessibilità o di ostacolarne la libera circolazione in nome della sicurezza, rischia di compromettere il senso stesso della ricerca come spazio critico, come esercizio di libertà e come ponte di fratellanza tra i saperi e tra i popoli. La sicurezza della conoscenza, dunque, non può diventare un pretesto per irrigidire le procedure, né per chiudere varchi nel nome di una protezione assoluta che, come spesso è accaduto, si rivela illusoria.

#### 4. UNA TRANSIZIONE IMPEGNATIVA: L'ONERE SULLE ISTITUZIONI

La tensione tra apertura e sicurezza non si esaurisce nel solo ambito dei conflitti di principio: essa si traduce in una sfida concreta e urgente per le università e per gli enti di ricerca, chiamati a ripensare in profondità le proprie strutture organizzative, le proprie prassi operative, e le competenze che mettono in campo. Se il paradigma della Scienza Aperta impone di riprogettare il ciclo della conoscenza in chiave di trasparenza, condivisione e accessibilità, le nuove istanze di sicurezza richiedono, per contro, un controllo più attento dei flussi informativi, una vigilanza costante sui rischi e un governo proattivo delle interazioni con l'esterno. In questa dialettica si gioca oggi una transizione impegnativa, che richiede un livello di consapevolezza e di preparazione che, ad oggi, a me appare ancora largamente sottovalutato.

Si tratta, a ben vedere, di un compito che per estensione, complessità e impatto può essere paragonato a una vera e propria trasformazione istituzionale. Non basta infatti introdurre qualche protocollo di sicurezza, né limitarsi a emettere circolari che raccomandino cautela: occorre una ristrutturazione complessiva, che coinvolga in modo trasversale tutti i livelli dell'organizzazione universitaria e che tenga insieme cultura, competenze, responsabilità e infrastrutture. In altre parole, per costruire un'autentica (buona) «cultura della sicurezza» all'interno delle istituzioni scientifiche, non è sufficiente implementare regole: è necessario innanzitutto promuovere una vasta azione formativa e culturale, capillare e inclusiva, che si rivolga all'intera comunità universitaria, dal personale docente e ricercatore a quello tecnico e amministrativo, fino ai vertici gestionali e agli organi di governo.

Tale formazione non può essere generica o meramente informativa. Essa deve puntare a costruire consapevolezza critica e competenze operative, declinate secondo le funzioni e le responsabilità di ciascuno. Ai ricercatori in particolare occorrerà offrire strumenti per comprendere le implicazioni eti-

che, giuridiche e geopolitiche delle proprie attività scientifiche, soprattutto in ambiti ad alto impatto strategico o tecnologico. Sarà necessario sviluppare capacità nella gestione responsabile dei dati, nel trattamento delle informazioni classificate o sensibili, e nell'uso accorto delle infrastrutture digitali. Il personale tecnico e amministrativo, da parte sua, dovrà essere formato all'analisi e alla valutazione dei rischi, alla redazione di documenti di conformità normativa, alla gestione delle collaborazioni con soggetti esterni in contesti ad alta vigilanza. Più in generale è facile immaginare che le università dovranno dotarsi di nuove figure professionali (quali, ad esempio, i responsabili della sicurezza della ricerca) in grado di operare all'intersezione tra ambiti disciplinari diversi: diritto internazionale, scienza e tecnologia, relazioni istituzionali, etica della ricerca, informatica e cybersicurezza.

Questa trasformazione, sebbene necessaria, si prospetta in un contesto italiano segnato da condizioni strutturalmente sfavorevoli. Le risorse disponibili sono spesso limitate, e l'equilibrio economico-finanziario delle istituzioni universitarie italiane rischia di diventare ancor più precario nella fase immediatamente successiva al ciclo straordinario di finanziamenti previsti dal Piano Nazionale di Ripresa e Resilienza<sup>10</sup>. I carichi burocratici sono già oggi eccessivi e la capacità amministrativa degli atenei è messa a dura prova da processi normativi sempre più complessi, da sistemi informativi frammentati, da una cronica lentezza nell'innovazione organizzativa. In questo scenario, l'introduzione di ulteriori obblighi, per quanto legittimi, rischia di tradursi in un aggravio insostenibile se non è accompagnata da un'adeguata infrastruttura di supporto.

Per questo motivo è fondamentale che i decisori pubblici, a livello nazionale ed europeo, si facciano carico di accompagnare questa transizione con misure strutturali e coerenti. Servono finanziamenti dedicati, che consentano di coprire i costi della formazione, della creazione di nuove competenze e della riorganizzazione degli uffici. Servono linee guida armonizzate, che riducano l'incertezza interpretativa e favoriscano una gestione integrata delle diverse normative, evitando sovrapposizioni o contraddizioni. E servono strumenti di supporto concreti (modelli, *toolkit*, piattaforme collaborative) che permettano agli atenei di affrontare con efficacia le nuove sfide, senza dover reinventare ogni volta soluzioni *ad hoc*.

In assenza di questo accompagnamento istituzionale, il rischio è duplice: da un lato, che le università non riescano a rispondere alle nuove esigenze di sicurezza, esponendosi a criticità reputazionali e operative; dall'altro, che la paura di non essere conformi induca un irrigidimento difensivo, fatto di chiusure precauzionali e rinunce, che penalizzano l'ambizione trasformativa

<sup>10</sup> <https://www.italiadomani.gov.it/content/sogei-ng/it/it/home.html>.

della Scienza Aperta. Governare la transizione significa dunque riconoscerne la complessità, investire con decisione e dotare le istituzioni di ricerca degli strumenti necessari per affrontarla con lucidità, equilibrio e lungimiranza.

## 5. SFIDE DA VINCERE: FRAMMENTAZIONE LEGISLATIVA E IPER-BUROCRAZIA

Nonostante gli sforzi di armonizzazione portati avanti dalla Commissione europea attraverso documenti strategici, raccomandazioni e iniziative coordinate nell'ambito dello Spazio Europeo della Ricerca<sup>11</sup>, la sicurezza della ricerca resta, almeno allo stato attuale, una competenza fortemente ancorata alle prerogative nazionali. Ogni Stato membro è infatti libero di recepire e declinare a proprio modo i principi generali proposti dalle istituzioni europee, adattandoli alla propria cultura istituzionale, alle proprie priorità politiche e strategiche, nonché agli equilibri, spesso delicati, tra università, enti di ricerca, strutture di governo, agenzie di sicurezza e organismi di controllo.

Questa eterogeneità, se non affrontata con lungimiranza, rischia di produrre un mosaico normativo frammentato, con la possibile creazione di ventisette sistemi di sicurezza paralleli, potenzialmente non interoperabili, ciascuno con proprie logiche, tempi di attuazione e soglie di allerta. Si tratta di uno scenario che potrebbe compromettere gravemente la coerenza e l'efficacia della politica scientifica europea, rendendo sempre più difficile la gestione operativa dei grandi progetti di ricerca transnazionali, in particolare in quei settori (come l'intelligenza artificiale, le tecnologie quantistiche o le scienze dei dati) che richiedono un grado elevato di coordinamento, rapidità d'azione e condivisione continua di dati e risorse.

Le conseguenze pratiche di questa disomogeneità normativa sono già oggi intuibili. I gruppi di ricerca che lavorano in consorzi europei potrebbero trovarsi a dover rispettare regole divergenti su cosa debba essere considerato un «dato sensibile», su quali collaborazioni internazionali siano ritenute ammissibili, su quali protocolli di sicurezza e di *due diligence* siano imposti come obbligatori. Questa situazione introduce un grado di incertezza giuridica e operativa che rischia di rallentare l'attività scientifica e di scoraggiare le sinergie tra Paesi.

Inoltre, in un quadro così frammentato, è plausibile che si inneschi un fenomeno di *forum shopping* tra ricercatori e istituzioni: i gruppi di ricerca potrebbero essere spinti a orientarsi verso quei Paesi che offrono un quadro normativo più chiaro, meno oneroso o più favorevole alle proprie esigenze progettuali. Una simile dinamica, oltre a creare distorsioni nella competizione scientifica europea, compromette il principio di equità tra le istituzioni, pena-

<sup>11</sup> <https://european-research-area.ec.europa.eu/>.

lizzando in modo strutturale quei sistemi nazionali che, per eccesso di cautela o per rigidità normativa, impongano vincoli più gravosi o ambigui.

A questa già complessa cornice europea si aggiunge, nel caso italiano, un elemento ulteriore di criticità: il rischio che l'implementazione di un sistema di sicurezza della ricerca finisca per tradursi in un esercizio eccessivamente formalistico e burocratico, più attento alla produzione di adempimenti che all'effettiva costruzione di capacità di protezione. Questa eventualità, lungi dall'essere remota, si iscrive in una dinamica ben nota e ricorrente nel sistema pubblico italiano, in cui ogni nuova esigenza, anche quando legittima e condivisibile, viene frequentemente affrontata attraverso una stratificazione normativa fatta di circolari, linee guida, moduli obbligatori, richieste di autorizzazione multilivello, controlli incrociati e certificazioni reiterate. Questo tipo di risposta, che predilige la forma alla sostanza, rischia di compromettere la flessibilità operativa indispensabile alla ricerca, trasformando la gestione della sicurezza in un ulteriore carico procedurale, spesso poco incisivo. Sul piano accademico, il tema della burocratizzazione della ricerca è stato più volte segnalato: Geuna (2001) ha descritto i rischi di un eccesso di regolamentazione sui sistemi universitari europei, mentre più di recente Hicks e Wouters (2015) hanno mostrato come la pressione valutativa possa trasformarsi in iper-burocratizzazione, con effetti negativi sulla creatività e sull'efficienza della ricerca. Queste analisi consentono di collocare l'esperienza italiana in un contesto comparato più ampio, dimostrando che il problema non è solo nazionale, ma strutturale.

A rendere ancora più difficile questo scenario vi è il fatto che molte università ed enti di ricerca italiani già oggi operano in condizioni di forte pressione amministrativa. Il personale tecnico e amministrativo, spesso numericamente insufficiente e sovraccarico di compiti, fatica a trovare il tempo e le risorse per aggiornare le proprie competenze su temi nuovi e complessi, come la cybersicurezza, la *open source intelligence*<sup>12</sup>, l'audit legale o la gestione del rischio strategico. Senza un investimento serio e strutturale in formazione continua, il rischio è che l'apparato amministrativo non riesca a sostenere la transizione richiesta, lasciando i ricercatori privi del supporto necessario o, peggio, bloccando le attività per timore di non essere pienamente conformi.

A questo si aggiunge una questione di mentalità, che potremmo definire come la (cattiva) «cultura del sospetto». In mancanza di una visione sistemica e di una *governance* orientata alla responsabilizzazione, l'applicazione delle misure di sicurezza rischia di essere intesa non come gestione consapevole e integrata del rischio, ma come sorveglianza sistematica e controllo invasivo delle attività scientifiche. Questa possibile deriva è tanto più pericolosa quan-

<sup>12</sup> <https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence>.

to più essa si mimetizza sotto le apparenze della legittimità normativa, finendo per alimentare sfiducia interna, autocensura e conflittualità.

Il timore è che in un simile contesto, segnato dal binomio frammentazione europea e iper-burocrazia nazionale, il principio di sicurezza, anziché costituire un valore da integrare armonicamente nel sistema della ricerca, rischi di trasformarsi in un onere aggiuntivo. Più che uno strumento di tutela, esso potrebbe diventare allora una zavorra: un insieme di vincoli che ostacolano l'apertura, rallentano l'innovazione, comprimono la libertà scientifica e riducono la capacità delle istituzioni di rispondere con efficacia alle grandi sfide globali. Riconoscere questo rischio non significa negare l'importanza della sicurezza, ma richiede il coraggio di affrontarla con intelligenza e... buon senso, evitando che essa si traduca in nuovi steccati normativi o in meccanismi difensivi che paralizzano anziché proteggere.

#### 6. ETICA, INTEGRITÀ E RESPONSABILITÀ NELLO SCENAZIO DELLA SICUREZZA

La questione della sicurezza della ricerca non può essere confinata nel solo ambito tecnico, giuridico o geopolitico. Al contrario, essa è forse prima di tutto una questione eminentemente etica. Ogni decisione relativa a cosa debba essere reso pubblico e cosa invece debba essere riservato, ogni valutazione su chi includere o escludere da una collaborazione internazionale, ogni giudizio sul livello di rischio associato a una determinata attività scientifica implica, inevitabilmente, una scelta valoriale. E, come ogni scelta valoriale, richiede di essere esplicitata, argomentata e sottoposta a un processo di deliberazione trasparente e partecipato.

In tale prospettiva, la protezione della ricerca non dovrebbe mai ridursi a un atto unilaterale di interdizione, né tantomeno trasformarsi in una manipolazione degli obiettivi scientifici subordinata a logiche esclusivamente securitarie. Difendere la sicurezza della ricerca non dovrebbe mai voler dire piegarne i contenuti agli interessi del momento o censurarne gli esiti scomodi. Al contrario, una corretta concezione della sicurezza deve porsi al servizio dell'integrità della ricerca, intesa come fedeltà ai principi di libertà intellettuale, rigore metodologico, trasparenza dei processi e orientamento al bene comune. È su questi principi, consacrati nei codici europei e internazionali di condotta scientifica, che deve fondarsi ogni misura volta alla tutela della conoscenza.

Da ciò discende l'esigenza di elaborare e promuovere una vera e propria etica della sicurezza della ricerca, che non sia semplicemente un'appendice alla normativa, ma ne rappresenti la premessa culturale e la cornice di legittimazione. Un'etica che assicuri, in primo luogo, il rispetto della dignità e dei diritti fondamentali di tutte le persone coinvolte nella produzione, nella diffusione e nell'utilizzo della conoscenza: dai ricercatori ai soggetti parteci-



panti, dalle comunità locali ai partner istituzionali. In secondo luogo, un'etica che preveda meccanismi decisionali fondati su criteri di trasparenza, verificabilità e proporzionalità, in grado di giustificare (e non semplicemente imporre) eventuali limitazioni alla diffusione di dati, risultati o collaborazioni. Tali limitazioni, ove necessarie, dovrebbero essere motivate pubblicamente, sottoposte a revisione periodica, e sempre bilanciate rispetto al principio generale della libera circolazione del sapere.

Ma, soprattutto, questa etica dovrebbe fondarsi su una concezione della responsabilità come bene condiviso. La sicurezza della ricerca non può essere affidata esclusivamente a organi di vigilanza o a strutture tecniche distanti dal tessuto scientifico: essa deve diventare parte integrante della cultura quotidiana di chi fa ricerca, amministra le istituzioni accademiche o definisce le politiche pubbliche. È necessario costruire un dialogo costante e consapevole tra scienziati, amministratori, giuristi, esperti di sicurezza e decisori politici, affinché le scelte siano frutto di una riflessione collettiva, e non di imposizioni verticali.

Perché ciò sia possibile, occorre che i dispositivi dedicati alla sicurezza siano affiancati da contropoteri deliberativi e consultivi in grado di garantirne il bilanciamento. È auspicabile, in tal senso, che le politiche di sicurezza della ricerca siano integrate da organi indipendenti di valutazione etica (li si chiami «comitati etici di ricerca», «presidi di integrità», o con qualunque altra denominazione) il cui ruolo non sia meramente formale, ma incisivo e sostanziale. Tali organismi dovrebbero essere dotati di autonomia funzionale e autorevolezza scientifica, ed essere coinvolti fin dalle prime fasi della definizione delle strategie di protezione, affinché possano esprimere pareri vincolanti o comunque influenti su situazioni complesse, ambigue o controverse.

Il loro compito non dovrebbe essere limitato a vigilare sull'eticità delle scelte scientifiche: essi dovrebbero, soprattutto, impedire che la categoria della «sicurezza» diventi un alibi per il controllo, una giustificazione pretestuosa per introdurre misure di sorveglianza, restrizione o censura incompatibili con la missione della scienza. La sicurezza della conoscenza non può essere scissa dalla sua integrità epistemica e dalla sua responsabilità sociale: ogni tentativo di proteggerla deve essere anche un impegno a renderla più giusta, più inclusiva e più libera.

## 7. PER UNA SCIENZA APERTA, CONSAPEVOLE E RESILIENTE

Quale possibile futuro è ipotizzabile per la ricerca scientifica europea e globale? Come evitare l'ingenuità di un'apertura incondizionata che, nel nome della trasparenza assoluta, ignora le asimmetrie di potere, le vulnerabilità tecnologiche, i rischi di appropriazione indebita senza, tuttavia, ricadere

nell'errore speculare, quello di una chiusura difensiva che sacrifica la libertà scientifica sull'altare della sicurezza?

Una possibile risposta fondata sull'osservazione critica della realtà è che la soluzione si trovi ancora all'interno del paradigma della Scienza Aperta. Ma di una Scienza Aperta che abbia saputo evolversi, maturare, apprendere dalle proprie tensioni interne e dalle sfide esterne, trasformandosi in una «Scienza Aperta consapevole e resiliente». Non si tratta di una retorica del compromesso, bensì della costruzione di una nuova sintesi, capace di preservare i valori fondanti dell'apertura e della cooperazione (*openness*), ma dotata degli strumenti culturali, normativi e infrastrutturali per governare il rischio, tutelare l'integrità del sapere e sostenere la propria sostenibilità nel tempo.

La crisi pandemica che ha colpito il mondo tra il 2020 e il 2022 costituisce un esempio emblematico e tragicamente didattico di ciò che può accadere quando la conoscenza scientifica viene chiusa, frammentata, gestita come un asset competitivo piuttosto che come un bene comune globale. Ritardi nella condivisione dei dati, opacità nelle metodologie, inaccessibilità dei protocolli clinici, disuguaglianze nell'accesso ai risultati: tutti elementi che hanno compromesso l'efficacia della risposta collettiva, amplificando la sofferenza umana e rallentando l'innovazione. Al tempo stesso, quella stessa crisi ha mostrato anche quanto potente possa essere una Scienza Aperta ben governata: i casi virtuosi di condivisione precoce delle sequenze genomiche, di collaborazione tra piattaforme pubbliche e private, di scambio aperto di dati clinici hanno contribuito in modo decisivo allo sviluppo tempestivo dei vaccini e alla comprensione evolutiva del virus. È su queste lezioni che occorre costruire il nuovo paradigma.

Dunque, in primo luogo una scienza consapevole, perché fondata su una piena coscienza dei rischi connessi alla condivisione del sapere in un mondo complesso. Rischi che non sono solo tecnologici, ma anche geopolitici, economici, bioetici. Una scienza consapevole è una scienza che non si nasconde dietro l'ingenuità della neutralità, ma che riconosce i propri limiti, affronta con rigore le proprie responsabilità e si dota di strumenti di autovalutazione, *accountability* e dialogo strutturato con la società. Questa consapevolezza deve tradursi in pratiche sistematiche di classificazione multilivello dei risultati della ricerca, distinguendo chiaramente ciò che può essere reso immediatamente pubblico, ciò che necessita di protezione temporanea, e ciò che in via eccezionale deve essere condiviso in modo selettivo o posticipato.

Al tempo stesso, si impone l'idea di una scienza resiliente, cioè capace di adattarsi a contesti instabili, a tensioni geopolitiche, a shock sistemici, senza per questo tradire i propri principi costitutivi. La resilienza, in ambito scientifico, non è la semplice capacità di resistere al cambiamento, ma la competenza ad affrontarlo in modo critico e, se del caso, trasformativo. Una scienza resiliente protegge sé stessa non chiudendosi, ma investendo nella qualità della propria *governance*, nella trasparenza dei suoi processi, nella costruzione

di alleanze strategiche fondate sulla fiducia reciproca. Questo implica, tra le altre cose, l'adozione simultanea e integrata dei principî FAIR (*Findable, Accessible, Interoperable, Reusable*) con quelli CARE<sup>13</sup> (*Collective Benefit, Authority to Control, Responsibility, Ethics*), riconoscendo che la gestione responsabile dei dati deve tener conto non solo della loro interoperabilità tecnica, ma anche dei contesti culturali, sociali e giuridici da cui quei dati provengono.

In questa visione, ogni fase del ciclo della ricerca deve essere ripensata alla luce di un doppio registro: apertura e protezione. La valutazione del rischio etico e strategico (oggi ancora marginale nei processi di finanziamento) dovrebbe essere inclusa in modo sistematico nelle fasi *ex ante*, come criterio di responsabilità progettuale e non come ostacolo burocratico. Le agenzie di finanziamento europee e nazionali potrebbero prevedere, in tal senso, meccanismi di autovalutazione etico-strategica, con *checklist* condivise, pareri di comitati etici multilivello e moduli di trasparenza da allegare alle proposte.

Parallelamente, si rende urgente la promozione di accordi internazionali su standard condivisi di «sicurezza aperta:» un'espressione solo apparentemente ossimorica, che invece racchiude la chiave per superare la frammentazione normativa. Solo attraverso regole comuni, compatibili e reciprocamente riconosciute, sarà possibile evitare che la sicurezza diventi una barriera alla collaborazione scientifica, o una scusa per rafforzare egemonie. Questi accordi dovranno essere accompagnati dalla costruzione di infrastrutture digitali federate e sicure, fondate su architetture aperte che incorporino, sin dalla fase di progettazione, i principî «security and openness by design». Infrastrutture che non siano solo tecnologiche, ma anche istituzionali, capaci di promuovere fiducia, interoperabilità e trasparenza.

Infine (ma, in realtà, forse prima di tutto) la realizzazione di una Scienza Aperta consapevole e resiliente richiede un rafforzamento sostanziale del dialogo tra i saperi. I confini disciplinari non bastano più a governare la complessità dei nuovi scenari. Occorre un confronto costante, strutturato e paritario tra scienziati, giuristi, filosofi della scienza, esperti di etica, professionisti della cybersicurezza, rappresentanti della società civile. Solo una comprensione realmente transdisciplinare della sicurezza potrà dar luogo a politiche efficaci, sostenibili e legittimate.

La posta in gioco è alta: si tratta di scegliere che tipo di scienza vogliamo promuovere nei prossimi decenni. Una scienza chiusa, opaca, difensiva, sospettosa del mondo? O una scienza aperta, ma capace di conoscere i propri rischi, di adattarsi senza arretrare, di proteggersi senza snaturarsi? La risposta non può che essere la seconda. E per costruirla abbiamo bisogno di coraggio istituzionale, visione politica, investimento culturale. La Scienza Aperta del

<sup>13</sup> <https://www.gida-global.org/care>.

futuro non sarà ingenua né fragile: sarà, se sapremo costruirla, una scienza forte proprio perché capace di interrogarsi, di ascoltare e di cambiare, senza mai smettere di essere fedele alla propria vocazione originaria: quella di conoscere per comprendere, e comprendere per servire la società.

## 8. CONCLUSIONI

In sintesi, il percorso di analisi sviluppato in questo contributo ha messo in luce come la Scienza Aperta rappresenti un paradigma trasformativo, capace di ridefinire le modalità con cui la ricerca viene prodotta, validata e condivisa. Tuttavia, essa non può essere interpretata come un processo avulso dal contesto geopolitico generale né, pertanto, privo di tensioni, soprattutto se espresso in termini di sicurezza: i rischi legati al *dual use*, alla sicurezza dei dati, alla proliferazione di pratiche predatorie e alle disuguaglianze di accesso richiedono un approccio di *policy* attento e bilanciato. Per questa ragione, emerge da questa riflessione una serie di proposte che, se pur qui formulate sul piano concettuale, posseggono caratteristiche di adesione a principi di realtà e concreta possibilità di implementazione.

Il paradigma della Scienza Aperta non deve essere abbandonato né ridotto, ma piuttosto rafforzato attraverso politiche intelligenti e lungimiranti, capaci di custodire la conoscenza come bene comune e al contempo difenderla da minacce interne ed esterne. La sfida per i prossimi anni consisterà proprio nel riuscire a coniugare apertura e sicurezza, trasformando una potenziale contraddizione in una nuova alleanza per il futuro della ricerca. L'analisi qui condotta ha evidenziato come la Scienza Aperta, lungi dall'essere una semplice tendenza amministrativa o un'opzione tra molte, rappresenti oggi una trasformazione strutturale e ineludibile dell'intero sistema della conoscenza. Essa interpella i fondamenti stessi del modo in cui intendiamo produrre, valutare e mettere a disposizione il sapere, reclamando una ridefinizione dei rapporti tra la ricerca e la società, tra l'autonomia scientifica e le esigenze di responsabilità pubblica.

A fronte di tale trasformazione pare tuttavia evidente che l'emergere della questione della sicurezza (nella sua dimensione tecnica, normativa, geopolitica ed etica) abbia introdotto un elemento di complessità ulteriore, che sollecita una rielaborazione del paradigma stesso dell'apertura. Lungi dal rappresentare un ostacolo in sé, la sicurezza va piuttosto intesa come uno dei contesti strutturali all'interno dei quali la Scienza Aperta deve oggi operare, senza rinunciare ai propri principi né ignorare le condizioni materiali e politiche della propria attuazione.

In questa direzione, emerge la necessità di un'evoluzione del modello verso una forma di apertura dotata di consapevolezza e di resilienza: una forma

che sappia affrontare con lucidità le vulnerabilità sistemiche, senza scivolare né in forme di ingenuità regolativa, né in derive difensive che compromettano la libertà intellettuale e la cooperazione internazionale. Una tale evoluzione esige un investimento profondo e coordinato su più fronti: la ristrutturazione delle competenze istituzionali, la semplificazione intelligente delle regole, la costruzione di presidi etici indipendenti, la progettazione di infrastrutture digitali capaci di coniugare apertura e protezione fin dalla loro architettura originaria.

Risulta anche imprescindibile l'adozione di una postura critica e riflessiva da parte dell'intera comunità scientifica. Occorre ripensare il ruolo della scienza nello spazio pubblico globale, assumendone la fragilità ma anche il potenziale trasformativo. Occorre promuovere un nuovo patto tra sapere e società, fondato su responsabilità condivise e su una capacità collettiva di distinguere, con rigore e giustizia, ciò che deve essere reso accessibile da ciò che esige una prudente riservatezza. Occorre, infine, che le scelte in materia di sicurezza non siano mai imposte in modo unilaterale, ma risultino sempre motivate, discusse, bilanciate e reversibili.

Alla luce di quanto argomentato, la nozione di «Scienza Aperta consapevole e resiliente» emerge quale possibile architrave per sostenere una nuova stagione della ricerca pubblica. Essa si configura, da un lato, come un paradigma dotato della maturità necessaria per riconoscere i rischi che attraversano l'ecosistema scientifico contemporaneo (siano essi di natura tecnologica, geopolitica o etico-sociale), dall'altro, come un modello capace di farvi fronte non mediante la chiusura difensiva, bensì attraverso il rafforzamento della trasparenza, della responsabilità e della qualità dei processi conoscitivi. In questa prospettiva, l'apertura non viene né sacrificata né mitizzata, ma governata con competenza, con strumenti adeguati e con una visione integrata che sappia tener conto dei diversi livelli di sensibilità e di rischio. Al contempo, la resilienza non si esprime nella semplice resistenza, ma nella capacità di adattamento creativo e di trasformazione intelligente, fondata su alleanze strategiche, dialogo transdisciplinare e investimento istituzionale. Una Scienza, dunque, che sappia restare fedele alla propria missione di servizio pubblico anche nelle condizioni più incerte, difendendo la propria autonomia non contro la società, ma per essa, e ponendosi come presidio culturale indispensabile in un tempo che reclama più che mai conoscenza affidabile, accessibile e giusta.

Detto altrimenti, si impone l'urgenza di passare da una reazione difensiva e frammentata a una strategia integrata, fondata su un equilibrio virtuoso tra protezione e condivisione, tra responsabilità e apertura.

In tale prospettiva, anzitutto, i decisori politici sono chiamati a promuovere un quadro normativo armonizzato a livello europeo, che sappia coniugare le esigenze della sicurezza della ricerca con i principî della Scienza Aperta, evitando il rischio di una deriva protezionistica o, al contrario, di una

liberalizzazione ingenua. Tale quadro dovrebbe muoversi nella direzione di un'«open strategic autonomy» della ricerca europea, capace di tutelare i valori democratici e gli interessi scientifici comuni senza ricadere in approcci difensivi e isolazionisti. È necessario, in questo senso, rafforzare il coordinamento inter-istituzionale tra gli Stati membri, garantendo coerenza tra le politiche di sicurezza, le strategie di innovazione e gli standard di apertura della conoscenza.

In parallelo, le agenzie di finanziamento (che svolgono un ruolo cruciale nel definire criteri di valutazione e i meccanismi di controllo) non dovrebbero soffocare la ricerca, ma piuttosto orientarne l'etica dell'impatto. Occorre, dunque, introdurre strumenti di *risk assessment* e *due diligence* che siano chiari, proporzionati, contestualizzati rispetto ai diversi domini scientifici e non eccessivamente onerosi sul piano burocratico. Tali strumenti dovrebbero includere indicatori per valutare i rischi *dual use*, gli impatti geopolitici, le implicazioni sulla cybersicurezza e la *governance* dei dati sensibili, nel rispetto del principio di proporzionalità e dell'autonomia della ricerca.

Le istituzioni di ricerca, dal canto loro, dovrebbero assumere un ruolo proattivo nell'integrare le dimensioni della sicurezza sin dalle fasi di progettazione delle attività scientifiche e delle infrastrutture di supporto. Ciò implica investimenti strategici in formazione trasversale su aspetti etici, legali e tecnologici della sicurezza; la creazione di nuove figure professionali ibride (ad esempio, esperti di sicurezza della ricerca, *data stewards*, *open science officers* con competenze in *risk management*); e lo sviluppo di infrastrutture digitali resilienti, capaci di supportare una ricerca collaborativa ma controllata. In quest'ottica si impone un approccio di *security and openness by design*, nel quale i principi di trasparenza e quelli di protezione non si escludano a vicenda, ma siano co-progettati come elementi complementari.

Infine, la comunità accademica nel suo complesso è chiamata a non subire passivamente l'evoluzione del contesto, ma a diventarne protagonista critica e consapevole. Ciò significa alimentare un dibattito pubblico informato sulle implicazioni della ricerca in relazione ai rischi globali (dalle tecnologie emergenti all'instabilità geopolitica), assumendo un ruolo attivo nella definizione delle *policy* e nel monitoraggio delle loro ricadute. È essenziale che il mondo della ricerca eserciti una funzione di vigilanza civica, affinché le necessarie misure di protezione non degenerino in restrizioni indebite, censure preventive o logiche di controllo incompatibili con la libertà accademica.

Solo attraverso queste azioni coordinate, che pongano al centro la co-evoluzione tra apertura e responsabilità, sarà possibile costruire una Scienza Aperta consapevole, resiliente e all'altezza delle sfide del presente. Una scienza che sappia affrontare la complessità e i rischi dell'epoca contemporanea non abdicando alla propria missione universale, ma rafforzandola attraverso una nuova alleanza tra conoscenza, etica e lungimiranza politica.



## Riferimenti bibliografici

- Bezuidenhout, L., S. Leonelli, A. Kelly e B. Rappert. 2017. «Beyond the Digital Divide: Towards a Situated Approach to Open Data». *Science and Public Policy* 44, n. 4: 464-75. <https://doi.org/10.1093/scipol/scw036>.
- Bonn, M., J. Bolick e W. Cross. 2023. *Scholarly Communications Librarianship and Open Knowledge*. Association of College and Research Libraries. [https://www.ala.org/sites/default/files/acrl/content/publications/booksanddigitalresources/digital/9780838936566\\_OA.pdf](https://www.ala.org/sites/default/files/acrl/content/publications/booksanddigitalresources/digital/9780838936566_OA.pdf).
- European Commission. 2015. *Open Innovation, Open Science, Open to the World – A Vision for Europe*. Publications Office. <https://data.europa.eu/doi/10.2777/061652>.
- European Commission. 2020. *Communication to the Commission. Open Source Software Strategy 2020-2023. Think Open*. [https://commission.europa.eu/document/download/97e59978-42c0-4b4a-9406-8f1a86837530\\_en?filename=en\\_ec\\_open\\_source\\_strategy\\_2020-2023.pdf](https://commission.europa.eu/document/download/97e59978-42c0-4b4a-9406-8f1a86837530_en?filename=en_ec_open_source_strategy_2020-2023.pdf).
- European Commission. 2025. *Strategic Autonomy and European Economic and Research Security*. [https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security\\_en](https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en).
- European Parliament. 2021. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast)*. <https://eur-lex.europa.eu/eli/reg/2021/821>.
- Council of the European Union. 2024. *Council Recommendation of 23 May 2024 on Enhancing Research Security*. <https://www.europeansources.info/record/council-recommendation-of-23-may-2024-on-enhancing-research-security/>.
- David, P.A. 2008. «The Historical Origins of “Open Science”: An Essay on Patronage, Reputation and Common Agency Contracting in the Scientific Revolution». *Capitalism and Society* 3, n. 2. <https://doi.org/10.2202/1932-0213.1040>.
- Fecher, B. e S. Friesike. 2014. «Open Science: One Term, Five Schools of Thought». In S. Bartling e S. Friesike (a cura di), *Opening Science*. Springer. [https://doi.org/10.1007/978-3-319-00026-8\\_2](https://doi.org/10.1007/978-3-319-00026-8_2).
- Geuna A. 2001. «The Changing Rationale for European University Research Funding: Are There Negative Unintended Consequences?». *Journal of Economic Issues* 35, n. 3: 607-32. <https://doi.org/10.1080/00213624.2001.11506393>.
- Hicks, D. e P. Wouters. 2015. «The Leiden Manifesto for Research Metrics». *Nature* 520: 429-31. <https://doi.org/10.1038/520429a>.
- UNESCO. 2021. *Recommendation on Open Science*. <https://www.unesco.it/wp-content/uploads/2023/11/RECOMMENDATION-ON-OPEN-SCIENCE-2021-Certified.pdf>.
- Vicente-Saez, R. e C. Martinez-Fuentes. 2018. «Open Science Now: A Systematic Literature Review for an Integrated Definition». *Journal of Business Research* 88: 428-36. <https://doi.org/10.1016/j.jbusres.2017.12.043>.
- Wilkinson, M.D., M. Dumontier, I.J. Aalbersberg, G. Appleton, M. Axton, A. Baak, N. Blomberg, J.-W. Boiten, L. Bonino da Silva Santos, P.E. Bourne, J. Bouwman, A.J. Brookes, T. Clark, M. Crosas, I. Dillo, O. Dumon, S. Edmunds, C.T. Evelo, R. Finkers, A. Gonzalez-Beltran, Alasdair J.G. Gray, P. Groth, C. Goble, J.S. Grethe, J. Heringa, P.A.C. t Hoen, R. Hooft, T. Kuhn, R. Kok, J. Kok, S.J. Lusher, M.E. Martone, A. Mons, A.L. Packer, B. Persson, P. Rocca-Serra, M. Roos, R. van Schaik, S.-A. Sansone, E. Schultes, T. Sengstag, T. Slater, G. Strawn, M.A. Swertz, M. Thompson, J. van der Lei, E. van Mulligen, J. Velterop, A. Waagmeester, P. Wittenburg, K. Wolstencroft, J. Zhao, B.



- Mons. 2016. «The FAIR Guiding Principles for Scientific Data Management and Stewardship». *Scientific Data* 3, 160018. <https://doi.org/10.1038/sdata.2016.18>.
- Willinsky, J. (2006). *The Access Principle: The Case for Open Access to Research and Scholarship*. MIT Press.