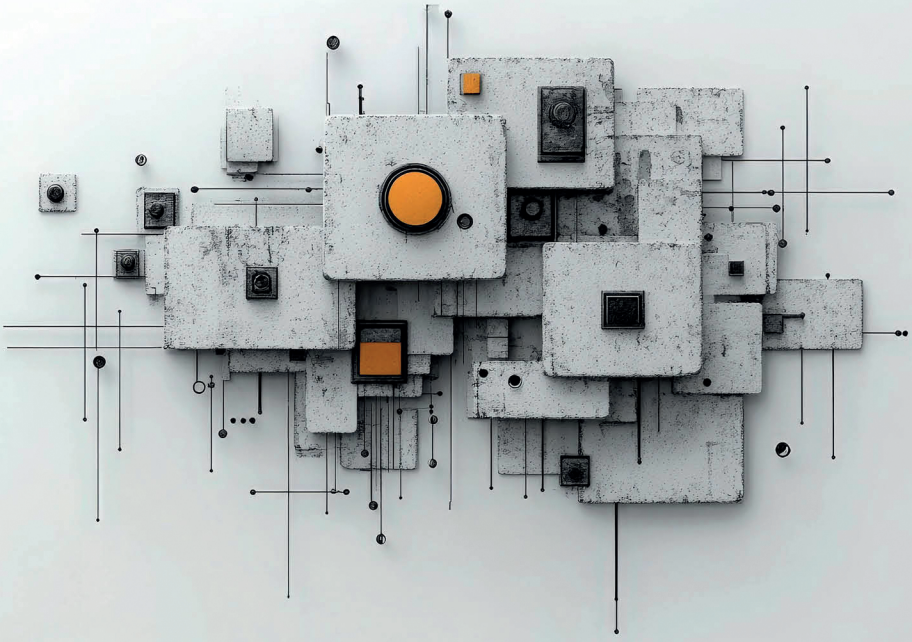
Governare gli ecosistemi di dati

Dinamiche, complessità e pratiche

a cura di

Niloofar Kazemargi e Simona Leonelli



Giappichelli

Governare gli ecosistemi dei dati

Dinamiche, complessità e pratiche


IUSTITIAM COLIMUS

Governare gli ecosistemi dei dati

Dinamiche, complessità e pratiche

a cura di

Niloofar Kazemargi e Simona Leonelli

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1780-6
ISBN/EAN 979-12-211-6545-6 (ebook-pdf)
ISBN/EAN 979-12-211-6714-6 (ebook-epub)

Questo lavoro è stato finanziato dal MUR (Ministero dell'Università e della Ricerca) attraverso il Progetto PRIN 2022 PNRR "Data4Innovation- Data ecosystem governance toward enhancing data sharing for innovation: implications for organizations" (P2022HXLBF), finanziato dal Piano Nazionale di Ripresa e Resilienza (PNRR), Italia, Missione 04 Componente 2 Investimento 1.1 – NextGenerationEU CUP Master D53D23017780001.
Il lavoro è stato rendicontato sui fondi dell'unità operativa LUISS – CUP I53D23006250001.

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: Stampatre s.r.l. - Torino

Indice

pag.

Ausili alla digitalizzazione delle PMI: cosa favorisce l'ottenimento di finanziamenti pubblici?

Filippo Ferrarini, Cosimo Checcucci, Bernardo Balboni e Simona Leonelli

Le PMI negli ecosistemi di dati: barriere, tensioni e ruoli nella governance dei dati

Simona Leonelli, Filippo Ferrarini e Tommaso Fabbri

pag.

Parte 2

La gestione dei dati per favorirne il riuso

pag.

pag.

pag.

Nota biografica sui curatori e autori

I curatori

Niloofar Kazemargi è ricercatrice presso l'Università G. d'Annunzio di Chieti-Pescara e professoressa a contratto presso l'Università Luiss di Roma. Ha conseguito il dottorato di ricerca in Economia Aziendale presso l'Università di Roma "Tor Vergata". È stata visiting researcher presso l'Università di Paderborn in Germania e, durante gli studi di dottorato, è stata visiting scholar presso la Cranfield University nel Regno Unito. Dal 2018 è membro del Centro di Ricerca su Leadership, Innovazione e Organizzazione dell'Università Luiss. I suoi interessi di ricerca includono ecosistemi di dati, agilità organizzativa e modelli organizzativi emergenti all'interno di ecosistemi digitali. Su questi argomenti ha pubblicato su varie riviste internazionali, tra cui Journal of the Association for Information Systems e IEEE Technology Engineering Management e ha contribuito scrivendo capitoli su libri curati da Springer ed Edward Elgar. Ha partecipato a varie conferenze internazionali e nazionali tra cui AoM, R&D, Euram, ItAIS. È PI di un progetto di ricerca intitolato "Data ecosystem governance toward enhancing data sharing for innovation: implications for organizations" e finanziato dal Ministero dell'Istruzione, dell'Università e della Ricerca (PRIN PNRR 2022), che esplora la governance dei dati in ambienti digitali complessi.

Simona Leonelli è professoressa associata di Organizzazione Aziendale e Gestione delle Risorse Umane presso l'Università di Modena e Reggio Emilia e professoressa a contratto presso l'Università di Padova. In precedenza, è stata ricercatrice presso l'Università di Padova e post-doc presso l'Università G. d'Annunzio di Chieti-Pescara dove ha conseguito il dottorato di ricerca in Accounting, Management and Finance. È stata visiting researcher presso la Skema Business School di Sophia Antipolis in Francia e visiting professor presso l'Università di Paderborn in Germania. Dal 2024 è membro del Centro Artificial Intelligence Research and Innovation (AIRI) dell'Università di Modena e Reggio Emilia. I suoi principali interessi di ricerca riguardano l'ambito dell'imprenditorialità (in particolare tratti di personalità, resilienza individuale, innovazione nelle start-up e orientamento imprenditoriale) e dell'organizzazione aziendale (resilienza organizzativa e ambidestrismo). Ha pubblicato in numerose riviste internazionali, tra cui Entrepreneurship Research Journal e Journal of Business Research ed è autrice di due monografie: Entrepreneurial Personality and Small Business Management (Edward Elgar Publishing) e Sustainable

Entrepreneurship (Emerald Publishing). Ha partecipato a varie conferenze internazionali e nazionali tra cui AoM, Euram, EGOS e WOA. È vice-PI di un progetto di ricerca intitolato "Data ecosystem governance toward enhancing data sharing for innovation: implications for organizations" e finanziato dal Ministero dell'Istruzione, dell'Università e della Ricerca (PRIN PNRR 2022) che esplora la governance dei dati in ambienti digitali complessi.

Gli autori

Bernardo Balboni è professore associato di Economia e Gestione delle Imprese presso il Dipartimento di Economia dell'Università di Modena e Reggio Emilia. I suoi interessi di ricerca riguardano l'academic engagement, l'imprenditorialità internazionale, i fattori interni e relazionali della crescita delle PMI e il marketing business-to-business. Su questi temi ha pubblicato numerosi articoli su riviste scientifiche internazionali, tra cui Journal of International Management, Industrial Marketing Management, Journal of Business Research e Technological Forecasting and Social Change.

Federica Ceci è professoressa ordinaria di Organizzazione e Innovazione presso l'Università "G. d'Annunzio" di Chieti-Pescara, dove coordina il corso di dottorato in Accounting, Management and Business Economics. Ha conseguito il titolo di dottore di ricerca in Ingegneria gestionale. Ha trascorso periodi di studio e lavoro all'estero presso il centro di ricerca Spru (UK) e la London Business School (UK). Insegna Digital innovation e organizzazione aziendale in master e corsi di perfezionamento presso diverse università e Business School italiane. Ha pubblicato su prestigiose riviste scientifiche italiane ed internazionali ed è autrice di tre libri pubblicati con case editrici internazionali.

Cosimo Checcucci ha conseguito una laurea magistrale presso il dipartimento di Economia Marco Biagi dell'Università di Modena e Reggio Emilia. Durante il percorso di studi si è specializzato in Analisi dei Dati per l'economia e il management. Dopo un'esperienza iniziale come Functional Analyst attualmente lavora come Junior SAP Specialist presso l'azienda SAPI S.p.A. a Modena. Tra le sue attività, si occupa di efficientamento dei processi aziendali tramite moduli SAP.

Alessandra Di Giacomo è dottoranda in Diritto e Impresa presso l'Università Luiss Guido Carli, dove conduce attività di ricerca nell'ambito di una borsa finanziata dall'Agenzia per la Cybersicurezza Nazionale (ACN). È componente dei centri di ricerca AI4Society e XAI Lab, istituiti presso Luiss, con cui collabora a progetti volti a supportare le PMI, grandi imprese e pubbliche amministrazioni nell'ideazione di soluzioni di intelligenza artificiale affidabili, sicure e integrate nei processi organizzativi in modo responsabile. Svolge attività accademica come cultrice della materia in Organizzazione Aziendale presso la Luiss Guido Carli e in Diritto Costituzionale presso l'Università degli Studi di Salerno. È, inoltre, membro del Comitato Scientifico

dell'Istituto per il Governo Societario (IGS) e abilitata all'esercizio della professione forense. I suoi interessi di ricerca si focalizzano sull'intersezione tra compliance regolatoria e trasformazione digitale, investigando come le tecnologie emergenti ridefiniscano i processi di verifica della conformità normativa e le dinamiche di governance.

Tommaso Fabbri è professore ordinario di Organizzazione e Gestione delle Risorse Umane, membro del Collegio del Dottorato in Lavoro, Sviluppo e Innovazione e Direttore del Dipartimento di Economia dell'Università di Modena e Reggio Emilia. È Coordinatore Scientifico e membro del Consiglio di Amministrazione della Fondazione Marco Biagi, nonché docente alla Bologna Business School. È membro dell'Associazione Italiana di Organizzazione Aziendale (ASSIOA) ed è stato Visiting Professor presso la Pennsylvania State University, Smeal College of Business Administration. La sua ricerca, di natura interdisciplinare e radicata in una prospettiva processuale dell'organizzazione, si concentra principalmente sui temi del cambiamento organizzativo, dell'apprendimento e del benessere. Svolge attività di consulenza per imprese private e istituzioni pubbliche in materia di progettazione organizzativa, gestione delle risorse umane e trasformazione digitale.

Filippo Ferrarini è assegnista di Ricerca in Organizzazione Aziendale presso il Dipartimento di Economia Marco Biagi dell'Università di Modena e Reggio Emilia. Ha conseguito il dottorato in lavoro, sviluppo ed innovazione presso la stessa università. I suoi interessi di ricerca includono l'organizzazione del lavoro e il benessere organizzativo, le pratiche di gestione delle risorse umane, l'innovazione, il comportamento innovativo e gli ecosistemi di dati.

Filippo Marchesani è ricercatore scientifico presso il dipartimento di Economia aziendale dell'Università "G. d'Annunzio" di Chieti-Pescara. È docente dei corsi magistrali di *Management of Innovation* e *Digital Consumer Behaviour* presso lo stesso ateneo e professore aggiunto presso la South Champagne Business School di Troyes (FR), dove insegna *International Business Management*. I suoi interessi di ricerca includono le *smart cities*, lo *smart tourism*, l'innovazione e l'imprenditorialità. Ha pubblicato i propri studi su prestigiose riviste nazionali e internazionali, oltre a contributi in diversi volumi, e un libro intitolato *The Global Smart City: Challenges and Opportunities in the Digital Age*, edito da Emerald.

Maria Notaristefano è avvocato del Foro di Perugia esercita presso lo Studio Duranti & Associati dal 2002. Svolge attività professionale in diritto delle nuove tecnologie, diritto d'autore e diritti su beni immateriali e svolge attività di formazione per imprese ed enti pubblici in materia di protezione dei dati personali e cybersecurity. Svolge attività di Responsabile per la Protezione dei Dati Personali (RPD o DPO) presso società private ed enti pubblici. Nel 1997, consegue la laurea presso la Facoltà di Giurisprudenza dell'Università degli Studi di Perugia. Nell'anno 2018 consegue il Master Universitario in Responsabile della Protezione dei Dati Personali Data Protection Officer e Privacy Expert presso l'Università degli Studi Roma Tre e nel 2021 il Master Universitario presso Università Luiss Guido Carli in Cybersecurity,

Politiche pubbliche, normative e gestione. Dall'anno accademico 2022-2023 è ammessa al corso di dottorato di ricerca in Cybersecurity, presso Sapienza Università di Roma e Università Luiss Guido Carli.

Loris Santarelli è dottorando in Accounting, Management and Business Economics (AMBE) presso l'Università G. d'Annunzio Chieti-Pescara, con background in Management e Marketing. La sua ricerca si concentra sul ruolo delle reti inter-organizzative nell'affrontare le "grand challenges", problemi sociali urgenti le cui soluzioni sono complesse e richiedono collaborazioni di molteplici attori. Attraverso i suoi studi, esplora come avviene l'orchestrazione dei network, la condivisione della conoscenza e la governance dei dati in contesti inter-organizzativi, con particolare attenzione a come questi processi possano generare impatti positivi sulla società. Attraverso il suo lavoro intende contribuire a teoria e pratica negli studi di management, offrendo spunti sul ruolo dei network collaborativi nel rafforzare la capacità organizzativa di affrontare problemi concreti, promuovendo al contempo pratiche sostenibili e socialmente responsabili.

Paolo Spagnoletti è professore ordinario di Organizzazione Aziendale presso il Dipartimento di Business e Management della Luiss e titolare della Fastweb+Vodafone Chair in Cybersecurity and Digital Transformation. È direttore del corso di laurea in Economia e Management della Luiss e di master e corsi executive nell'area dell'innovazione e governance del digitale. È Presidente del Competence Center Cyber 4.0 e visiting professor presso il Dipartimento di Information Systems dell'Università di Agder dove collabora con il Center for Integrated Emergency Management (CIEM). Nel 2023 è stato nominato Distinguished Member dell'AIS. Ha conseguito il dottorato di ricerca in Sistemi Informativi Aziendali presso la Luiss e ha ricoperto incarichi didattici e di ricerca presso le Università di Agder, Warwick, Georgia State, St. Gallen, Paris Dauphine, Lausanne, SKEMA e London School of Economics and Political Science. I suoi interessi di ricerca riguardano le piattaforme digitali e la cybersecurity. È autore di numerosi articoli pubblicati in riviste internazionali di rilievo quali JAIS, JIT e JSIS. È stato Associate Editor della rivista Information and Management ed Executive Editor della Serie Springer LNISO.

Elena Tomasella è una dottoranda in Management presso l'Università Luiss Guido Carli, impegnata in una ricerca finanziata dall'Agenzia Nazionale per la Cybersicurezza (ACN). È membro dello XAI Lab del centro di ricerca AI4Society presso Luiss, con il quale collabora a progetti a supporto di PMI, grandi imprese e pubbliche amministrazioni, nella definizione di soluzioni basate su intelligenza artificiale che siano affidabili, sicure e integrate in modo responsabile nei processi organizzativi. È Teaching Assistant in Organizzazione Aziendale presso la Luiss Guido Carli. I suoi interessi di ricerca si concentrano sulla gestione del rischio informatico e sulla valutazione strategica dei rischi.

Prefazione

Nelle Lezioni Americane, Italo Calvino descriveva l'opera letteraria come una '… rete di connessione tra i fatti, tra le persone, tra le cose del mondo'. Questa immagine è una potente chiave di lettura per comprendere le sfide della trasformazione digitale. Oggi, il valore non risiede nel singolo dato, ma nella rete di connessioni che siamo in grado di costruire e interpretare. I dati sono la materia prima di questa rete: la loro abbondanza, tuttavia, non genera automaticamente valore; è la governance a disegnarne l'architettura, a stabilirne regole e ruoli. Il governo di regole e ruoli trascende il dominio puramente tecnologico: abilitano l'innovazione, la competitività e la sostenibilità delle imprese. In questo scenario, dove le tecnologie riconfigurano i processi intra e inter-organizzativi, diviene pertanto cruciale spostare lo sguardo dal singolo attore alla nozione di ecosistema.

Il volume 'Governare gli ecosistemi dei dati: dinamiche, complessità e pratiche' indaga le modalità attraverso le quali le organizzazioni collaborano per generare valore dai dati, imparando a governare le tensioni e le sfide che emergono da queste complesse dinamiche. Il libro offre un'analisi approfondita e rigorosa della governance degli ecosistemi di dati, un tema attuale e sfidante.

Kazemargi e Leonelli offrono un contributo originale: scompongono la nozione di governance degli ecosistemi di dati nelle sue componenti fondamentali – attori, regole, incentivi, meccanismi di coordinamento. Questa scomposizione mette in luce la dinamica temporale delle relazioni inter-organizzative, la fluidità dei confini degli ecosistemi e le pratiche emergenti di coordinamento e regolazione. Le quattro sezioni del volume costruiscono un percorso coerente da un solido inquadramento teorico fino all'analisi empirica di casi concreti, nei quali il ruolo delle pubbliche amministrazioni e delle piccole e medie imprese risulta determinante per comprendere la natura distribuita e collaborativa degli ecosistemi.

Un elemento di particolare pregio di questo lavoro risiede nella sua capacità di integrare approcci teorici e metodologici differenti, coniugando contributi provenienti dagli studi organizzativi e dai sistemi informativi. Questo sforzo di sintesi permette di cogliere la complessità del fenomeno e di restituirne una visione sfaccettata, in cui i dati non sono solo un asset, ma un elemento che struttura interazioni e poteri, favorendo nuove forme di cooperazione tra attori.

Il libro offre così una lettura profonda delle dinamiche dei dati e delle pratiche di governo applicate su scala sistemica. La sfida consisterà nel saper costruire ecosistemi di dati che siano sostenibili, capaci cioè di bilanciare la spinta all'innovazione

DOI: 10.82018/9791221165456-1

con la tutela dei diritti fondamentali. Solo così potremo sfruttare appieno il potenziale trasformativo dei dati. Il volume fornisce inoltre strumenti di grande utilità per policy maker, manager e professionisti impegnati nella progettazione e nella gestione di infrastrutture di dati, evidenziando la necessità di modelli di governance inclusivi, trasparenti e adattivi.

In un'epoca in cui la trasformazione digitale ridisegna costantemente le relazioni tra istituzioni, imprese e cittadini, questo volume offre una interessante chiave di lettura per comprendere come i dati possano diventare il fulcro di nuovi processi di creazione di valore condiviso.

Andrea Prencipe – Luiss Guido Carli

Governare gli ecosistemi di dati: una introduzione

Niloofar Kazemargi [*] e Simona Leonelli [**]

1. Finalità e ambito del volume

Negli ultimi anni, i dati sono diventati una delle risorse strategiche fondamentali per le organizzazioni per ottenere un vantaggio competitivo. Infatti, le organizzazioni integrano, sempre di più, fonti e tecnologie differenti per creare ed acquisire conoscenza e, quindi, prendere decisioni in modo efficiente (Davenport, 2006). Questa crescente integrazione ha dato origine ai cosiddetti ecosistemi di dati ossia reti di attori che interagiscono e collaborano per creare, archiviare e condividere dati al fine di innovare, generare valore o nuovi modelli di business (Oliveira et al., 2019). Nonostante tali benefici, molti ecosistemi di dati non riescono a crescere o a sopravvivere nel tempo (Jacobides et al., 2024; Nikiforova et al., 2024). Tale fragilità deriva da una combinazione di fattori strutturali, organizzativi e istituzionali (Degen & Teubner, 2024). In primo luogo, la mancanza di modelli di governance chiari e condivisi rappresenta una criticità centrale: spesso i diritti di accesso, le responsabilità decisionali e i meccanismi di distribuzione del valore non sono definiti in modo trasparente, generando asimmetrie di potere e una conseguente perdita di fiducia tra gli attori coinvolti (Nikiforova et al., 2024; Ramalli & Pernici, 2023). Inoltre, quando la governance non è percepita come equa, gli attori tendono a ridurre la loro partecipazione o a non condividere pienamente i dati. In secondo luogo, molti ecosistemi di dati soffrono per la mancanza di sostenibilità economica. Numerose iniziative si fondano su finanziamenti pubblici o progetti pilota che, in assenza di modelli di business autosufficienti, non riescono a sopravvivere nel lungo periodo (Nikiforova et al., 2024). Ciò è aggravato dalla difficoltà di definire incentivi economici chiari e di misurare il ritorno sugli investimenti generato dallo scambio e dall'utilizzo dei dati (Azkan et al., 2022). A questi limiti si aggiungono ostacoli tecnici e infrastrutturali, come la scarsa interoperabilità dei sistemi, la mancanza di standard condivisi e le

[*] Niloofar Kazemargi (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" di Chieti-Pescara, Italia.
E-mail: niloofar.kazemargi@unich.it

[**] Simona Leonelli (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: simona.leonelli@unimore.it

DOI: 10.82018/9791221165456-2

difficoltà di integrazione tecnologica tra partner eterogenei (Ali et al., 2024). Infine, le barriere istituzionali e culturali, come la frammentazione normativa, la mancanza di coordinamento tra politiche pubbliche e private e una persistente resistenza al cambiamento organizzativo, riducono ulteriormente la capacità degli ecosistemi di evolversi e consolidarsi nel tempo (Nikiforova et al., 2024).

Di conseguenza, l'analisi della governance dei dati diventa cruciale per comprendere come favorire il coordinamento inter-organizzativo e massimizzare la creazione di valore, mitigando al contempo tutti questi rischi. In dettaglio, la governance dei dati si riferisce all'insieme di decisioni, meccanismi e pratiche che regolano la gestione, la qualità, la sicurezza e l'uso dei dati nei contesti inter-organizzativi (Spagnoletti et al., 2025). Quindi, la sfida principale è coordinare efficacemente attori eterogenei per massimizzare la creazione di valore, mitigando al contempo i rischi.

2. Linee tematiche

Come suggerito da un nostro precedente lavoro (Kazemargi et al., 2025), questo può avvenire solo risolvendo tre questioni principali: gestire le dinamiche temporali che favoriscono o influiscono sul coordinamento inter-organizzativo, gestire la fluidità dei dati per favorirne il riuso in diverse forme e creare nuove pratiche di governance dei dati. L'obiettivo di questo libro è, appunto, analizzare le questioni sopramenzionate e fornire delle proposte per mitigare e gestire al meglio ognuna di esse.

2.1. Le dinamiche temporali del coordinamento inter-organizzativo

Considerando le dinamiche temporali del coordinamento inter-organizzativo intendiamo analizzare come gli attori di un ecosistema di dati, che spesso sono eterogenei per natura, obiettivi e potere contrattuale, riescono ad allineare nel tempo ruoli, interessi e responsabilità in un contesto caratterizzato da continua evoluzione tecnologica e da obiettivi strategici mutevoli. Di conseguenza, la gestione delle tensioni e l'adattamento reciproco dei vari meccanismi di governance diventano elementi chiave per assicurare coerenza e sostenibilità dell'ecosistema di dati. La prima sezione di questo libro contiene tre capitoli che si occuperanno proprio di questo. In dettaglio, il Capitolo 2, scritto da Notaristefano e Spagnoletti, approfondisce le sfide legate al mantenimento della partecipazione delle imprese negli ecosistemi di dati urbani, concentrandosi sulla necessità di continui cambiamenti e adeguamenti delle strategie di governo del dato. Attraverso un'analisi longitudinale dell'evoluzione della piattaforma di dati certificati del Comune di Roma, Roma Data Platform, nell'assistente virtuale Julia, destinato a turisti e cittadini e lanciato in vista del Giubileo, si illustrano le modalità con cui le PMI contribuiscono alla governance dei dati nelle Smart City.

Il Capitolo 3, a cura di Ferrarini e colleghi, evidenzia il ruolo cruciale delle PMI nella crescita degli ecosistemi di dati, evidenziando tuttavia le difficoltà che molte di esse incontrano a causa degli elevati costi della digitalizzazione. Il capitolo analizza come dimensione, settore di appartenenza e area geografica influenzino l'accesso ai finanziamenti pubblici, prendendo come caso di studio il voucher per la digitalizzazione delle PMI del 2019. I risultati mostrano che tali variabili incidono significativamente sulla capacità delle imprese di innovare e partecipare attivamente agli ecosistemi di dati.

Il Capitolo 4, scritto da Leonelli e colleghi, analizza il ruolo delle PMI negli ecosistemi di dati, evidenziando le principali barriere e tensioni che possono riscontrare negli ecosistemi di dati e ruoli che esse possono ricoprire negli ecosistemi e nella governance dei dati. Il contributo mostra come fattori economici, tecnologici e culturali influenzino la partecipazione delle PMI e come, attraverso processi di apprendimento e collaborazione, possano evolvere da semplici utilizzatrici a co-creatrici di valore. Il capitolo propone infine un modello concettuale integrato che collega barriere, tensioni e ruoli, offrendo spunti utili per una governance più inclusiva e sostenibile degli ecosistemi di dati.

2.2. La gestione dei dati per favorirne il riuso

La seconda sezione del libro si focalizza, invece, sulla questione inerente alla gestione dei dati, in quanto fluidi, per favorirne il riuso in diverse forme. In particolare, il riuso dei dati per scopi differenti, anche completamente diversi da quelli previsti originariamente, amplia le opportunità di innovazione ma, al contempo, genera rischi legati alla privacy, alla sicurezza e all'uso improprio delle informazioni. L'obiettivo dei tre capitoli inseriti in questa seconda sezione del libro è individuare delle modalità di governance che consentano di gestire al meglio il problema della "riusabilità dei dati", promuovendo principi di trasparenza e responsabilità. In dettaglio, il Capitolo 5, a cura di Tomasella e Spagnoletti, affronta il tema della cybersecurity come leva strategica nella governance dei dati. La crescente digitalizzazione, pur favorendo innovazione e valore, espone le organizzazioni pubbliche e privare a nuove vulnerabilità. Per questo motivo la governance dei dati diventa essenziale per garantire la sicurezza, qualità e tracciabilità dei dati. Il capitolo propone un framework di valutazione ex-ante degli investimenti in sicurezza, sviluppato tramite "*l'action design research*" (ADR), per calcolo del *Return on Security Investment* (ROSI). Il modello supporta le decisioni informate in materia di cybersecurity e offre implicazioni per la governance dei dati in sistemi inter-organizzativi.

Il Capitolo 6, scritto da Marchesani e Ceci, si concentra sul fenomeno del lock-in dei dati nelle smart city, dove la dipendenza da piattaforme proprietarie, standard chiusi e contratti rigidi limita la capacità di innovazione e collaborazione della Pubblica Amministrazione. Attraverso un'analisi qualitativa condotta su 22 interviste a dirigenti pubblici del Comune di Pescara, il contributo mette in luce le cause

istituzionali e organizzative del lock-in e propone linee guida per promuovere modelli di governance aperta, flessibile e interoperabile.

Il Capitolo 7, redatto da Santarelli e Ceci, affronta il tema delle sfide nella gestione e valorizzazione dei dati in contesti complessi. A partire dal caso del Parco Nazionale d'Abruzzo, Lazio e Molise (PNALM), gli autori analizzano come diversi attori configurano la Data Value Chain in situazioni caratterizzate da elevata dispersione e varietà di fonti informative. Lo studio contribuisce alla comprensione delle modalità con cui la governance dei dati può supportare la sostenibilità e la cooperazione in ecosistemi territoriali eterogenei.

2.3. La creazione di nuove pratiche di governance dei dati

Infine, la terza sezione del libro analizza la necessità di ripensare alle pratiche di governance dei dati all'interno degli ecosistemi di dati, non solo per favorire la massimizzazione del profitto o l'efficienza organizzativa, ma principalmente per garantire una creazione di valore, tutelare gli attori più deboli e promuovere modelli collaborativi di gestione del dato. In dettaglio, i tre capitoli inseriti in questa sezione del libro si occuperanno di fornire consigli utili per migliorare e innovare la governance dei dati all'interno degli ecosistemi dei dati.

Il Capitolo 8, di Di Giacomo e Spagnoletti, analizza l'impatto dell'intelligenza artificiale agentica nei processi di revisione e della conformità. L'aumento della pressione normativa, con regolamenti come il GDPR e la Direttiva NIS2, richiede un monitoraggio continuo della conformità lungo l'intera catena del valore. Il capitolo esplora come i sistemi multi-agente possono trasformare la revisione tradizionale, automatizzando il rilevamento delle vulnerabilità e la gestione dei rischi. Gli autori evidenziano, infine, le sfide di governance dei dati necessarie per favorire l'adozione di questi strumenti predittivi e adattivi.

Il Capitolo 9, scritto da Kazemargi e Ceci, esplora la coordinazione delle pratiche di data governance lungo la catena del valore dei dati, mostrando come la governance può essere il *core* di negoziazioni inter-organizzative. Attraverso l'analisi di un caso studio qualitativo, le autrici dimostrano che la governance dei dati si costruisce dinamicamente attorno a tre dimensioni interconnesse che sono la *data practice*, cioè la definizione, creazione e accesso ai dati, la *data insight*, cioè la configurazione dei dati al fine di prendere decisioni in modo efficace e la *data value*, che riguarda il valore ottenuto e crescente nel tempo dei dati. Il capitolo sottolinea che queste dimensioni sono costruite attraverso accordi, adattamenti di processi e co-progettazione di interfacce.

Infine, il Capitolo 10, sempre a cura di Kazemargi e Ceci, affronta il tema dell'interoperabilità dei dati come leva fondamentale per la generazione di valore nelle organizzazioni pubbliche e private. Attraverso l'analisi di un caso studio qualitativo, le autrici analizzano come una pubblica amministrazione possa garantire l'integrazione dei dati tra sistemi eterogenei. Emergono due tensioni principali: i vincoli

dell'approvvigionamento di dati in mercati frammentati e il bilanciamento tra infrastrutture obsolete con nuove tecnologie interoperabili e scalabili. I risultati mostrano che l'efficacia dell'ecosistema di dati dipende dal coordinamento tra i diversi attori che ricoprono diversi ruoli. In particolare, la pubblica amministrazione come coordinatrice, gli enti regolatori come facilitatori e i fornitori come contributori all'ecosistema.

3. Conclusioni

Nel complesso, il volume mostra che la governance dei dati non è un insieme statico di regole, ma un processo dinamico di apprendimento e adattamento collettivo. Capirne le dimensioni temporali, relazionali e pratiche è essenziale per progettare ecosistemi di dati sostenibili, equi e innovativi.

Il libro contribuisce in modo significativo al dibattito teorico sugli ecosistemi di dati, esplorando le interazioni e le tensioni che si sviluppano tra gli attori pubblici e privati impegnati nella produzione, condivisione e valorizzazione dei dati. In particolare, approfondisce le dinamiche di competizione e cooperazione che emergono nei processi di governance, mostrando come tali tensioni possano limitare o stimolare la creazione di valore collettivo. Inoltre, il libro propone un approccio multidimensionale e multilivello alla governance dei dati, poiché integra aspetti strutturali, istituzionali e tecnologici con quelli culturali e organizzativi, superando le tradizionali prospettive che si focalizzano sulla singola impresa.

Dal punto di vista di contributi pratici, il libro fornisce linee guida e strumenti applicativi utili ai manager e alle imprese e ai policy maker. In primo luogo, il libro propone alcune raccomandazioni operative su come condividere, accedere e gestire i dati oltre i confini organizzativi, bilanciando diritti, responsabilità e opportunità d'innovazione. Particolare attenzione è rivolta alle PMI, per le quali la partecipazione agli ecosistemi di dati può rappresentare una leva strategica competitiva, ma anche una sfida in termini di risorse, competenze e fiducia. In secondo luogo, i risultati offrono elementi utili ai policy maker per la definizione di politiche pubbliche orientate alla condivisione responsabile dei dati, capaci di incentivare la collaborazione, prevenire comportamenti opportunistici e promuovere un uso etico e sostenibile delle informazioni.

Bibliografia

Ali, M., Papageorgiou, G., Aziz, A., Loukis, E., Charalabidis, Y., Alexopoulos, C. & Pellicer, F.J.L. (2024). A Framework for the Multi-Dimensional Assessment of Interoperability for Open Data Ecosystems Development. *Information Polity*, *29*(4), 439-466.

Azkan C. et al. (2022) Incentive schemes and economics of data sharing. Fraunhofer Institut für Software und Systemtechnik. https://ieds-projekt.de/wp-content/uploads/2022/08/IEDS-Whitepaper_Englisch.pdf.

Davenport, T.H. (2006). Competing on analytics. *Harvard Business Review*, *84*(1), 98.

Degen, K. & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, *34*(1), 50.

Jacobides, M.G., Cennamo, C. & Gawer, A. (2024). Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures. *Research Policy*, *53*(1), 104906.

Kazemargi, N., Leonelli, S., Spagnoletti, P., Ceci, F., Sinaimeri, B. & Marchesani, F. (2025). Data Governance in Data Ecosystems: A Research Note. *Prospettive in organizzazione*, *29*, 29-35.

Nikiforova, A., Simonofski, A., Zuiderwijk, A. & Rodriguez Bolivar, M.P. (2024). Towards sustainable public and open data ecosystems: An introduction to a special section. *Information Polity*. https://doi.org/10.1177/15701255241300620.

Oliveira, M.I., Barros Lima, G.D.F. & Farias Lóscio, B. (2019). Investigations into data ecosystems: a systematic mapping study. *Knowledge and Information Systems*, *61*, 589-630.

Spagnoletti, P., Kazemargi, N., Constantinides, P. & Prencipe, A. (2025). Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors. *Journal of the Association for Information Systems*, *26*, 1-33.

Parte 1
Le dinamiche temporali del coordinamento inter-organizzativo

Il governo partecipato del dato nelle smart city: dalla Roma Data Platform all'agente virtuale Julia

Maria Notaristefano [*] e Paolo Spagnoletti [**]

Abstract: Questo capitolo approfondisce le sfide legate al mantenimento della partecipazione delle imprese negli ecosistemi di dati urbani, concentrandosi sulla necessità di continui cambiamenti e adeguamenti delle strategie di governo del dato. Attraverso un'analisi longitudinale dell'evoluzione della piattaforma di dati certificati del Comune di Roma, Roma Data Platform, nell'assistente virtuale Julia, destinato a turisti e cittadini e lanciato in vista del Giubileo, si illustrano le modalità con cui le PMI contribuiscono alla governance dei dati nelle Smart City.

Parole chiave: Smart City, Roma Data Platform, Ecosistema di dati, Governance, Condivisione dei dati.

1. Introduzione

La rapida urbanizzazione delle società contemporanee e i progressi tecnologici hanno inaugurato l'era delle smart city. Nei centri urbani, in cui si sviluppano queste progettualità, si utilizzano diverse tecnologie tra cui sensori, Internet of Things (IoT), sistemi di intelligenza artificiale (AI) e assistenti virtuali, per migliorare la gestione urbana e la qualità della vita dei cittadini. Silva et al. (2018) e Bibri (2018) sottolineano che le smart city rappresentano un nuovo paradigma nella gestione e nell'utilizzo dei dati, con l'obiettivo di ottimizzare le operazioni e migliorare i servizi attraverso una loro integrazione completa.

In questo scenario, imprese e pubbliche amministrazioni giocano un ruolo attivo nelle smart city, che possono essere inquadrate come ecosistemi di servizi abilitati da architetture informatiche per la gestione collaborativa del dato (Abella et al., 2017). Per ecosistema si intende una forma interorganizzativa nella quale attori interdipendenti

[*] Maria Notaristefano (✉)
Università di Roma Sapienza & Università Luiss, Italia.
E-mail: mnotaristefano@luiss.it

[**] Paolo Spagnoletti (✉)
Dipartimento di Business and Management, Università Luiss, Italia.
E-mail: pspagnoletti@luiss.it

DOI: 10.82018/9791221165456-3

stabiliscono rapporti multilaterali per creare insieme valore (Spagnoletti et al., 2025). Nel presente lavoro si farà riferimento agli ecosistemi di dati, definiti come "*reti socio-tecnicnologiche complesse in cui gli attori interagiscono e collaborano tra loro per trovare, archiviare, pubblicare, consumare o riutilizzare dati, nonché per promuovere l'innovazione, creare valore e sostenere nuove imprese*" (Oliveira et al. 2019). Gli ecosistemi di dati producono valore facendo leva su un gruppo di attori che genera o comunque fornisce i dati, mentre altri li consumano (Janssen et al. 2012). La governance delle smart city presuppone l'esistenza di specifici meccanismi per coordinare attori eterogenei che utilizzano e condividono dati (Kazemargi & Ceci, 2025). Tali meccanismi devono incidere anche sulla motivazione e sul coinvolgimento dei fornitori e degli utenti dei dati (Janssen et al., 2012), che vanno incentivati a participare attivamente.

Per raggiungere risultati ottimali, si può intervenire su amministrazioni, grandi imprese, PMI e cittadini per incentivare e migliorare lo scambio di dati secondo le formule "Business to Government data sharing" (B2G), "Government to Business data sharing" (G2B), nonché incoraggiando la condivisione dei dati direttamente da parte dei cittadini (cosiddetta "Civic data sharing"). Per favorire questi scambi, le piattaforme digitali forniscono l'infrastruttura per l'erogazione di servizi ad alto contenuto informativo e per generare valore superando i limiti di una gestione centralizzata dei dati in silos (Spagnoletti et Al., 2015).

La crescente dipendenza dai dati, anche nelle smart city, porta in primo piano la questione critica della loro governance, ossia come i dati sono resi accessibili, elaborati e archiviati in modo sicuro in una complessa rete di attori pubblici e privati (Spagnoletti & Baskerville, 2025). Anche la creazione di valore dai dati non è un processo automatico ma dipendende dall'implementazione di una governance efficace che assicuri una gestione responsabile del dato, una definizione chiara dei diritti d'accesso e che generi fiducia negli attori coinvolti e negli utilizzatori. La governance o governo del dato, poi, è un processo che richiede continue modifiche e adattamenti per incentivare la partecipazione e la condivisione dei dati da parte dei vari stakeholder. Essendo un fenomeno emergente, politiche, strategie e pratiche relative agli ecosistemi di dati nelle smart city sono ancora in fase di sviluppo e consolidamento (Oldenburg et al., 2024; Rzevski et al., 2020).

Il governo del dato nel contesto delle smart city risulta strategico anche in relazione ai recenti sviluppi dei servizi urbani basati sull'intelligenza artificiale (Di Gregorio, 2025). Del resto, l'intelligenza artificiale, con le sue capacità di previsione e automazione, è destinata a svolgere un ruolo fondamentale nel rimodellare l'erogazione dei servizi nelle smart city (Wolniak et al., 2024) e offre nuove opportunità di coinvolgimento delle PMI locali (Marchesani & Ceci, 2024). Arkaraprasertkul (2024) afferma che nelle smart city anche gli agenti AI basati su Large Language Models (LLM) [1], sono strumenti innovativi in grado di processare dati provenienti

[1] Kalyuzhnaya, A. et al. (2025). LLM Agents for Smart City Management: Enhancing Decision Support Through Multi-Agent, AI Systems. *Smart Cities*, *8*(1), 19, defines LLM agent as "*An LLM*

dalle fonti più varie, ivi incluse le piattaforme di social media e i dispositivi IoT, e di analizzare in tempo reale i bisogni dei cittadini, fornendo loro risposte immediate e personalizzate. In questo modo, i cittadini ottengono risposte in tempi più rapidi, minori inconvenienti e in generale una migliore qualità della vita. L'interdipendenza dell'AI con i dati generati e raccolti dalla smart city offre dunque grandi opportunità per migliorare l'efficienza amministrativa e promuovere un'interazione più stretta con i cittadini e il tessuto imprenditoriale locale fatto anche, e soprattutto, di PMI. Gli studi sugli ecosistemi di dati nelle smart city indicano, in effetti, che una governance collaborativa tra pubblico e privato faciliti la condivisione di dati e il superamento delle barriere regolamentari, permettendo alle città di fare un uso efficace anche delle soluzioni di AI (Marchesani & Ceci, 2024; Ducuing, 2024).

2. La condivisione del dato nelle *smart city*

Affinché questi sviluppi si realizzino, la governance cittadina deve nutrirsi di dati e garantirne la circolazione, la condivisione, la portabilità e l'interoperabilità (Paolucci & Pollicino, 2023; Spagnoletti et al., 2025). In effetti, il presente ci consegna smart city che hanno continuo bisogno di grandi moli di dati (big data) per fornire ai cittadini servizi personalizzati e sempre più evoluti (Guggenberger et al., 2025; Colapietro, 2023; Vigorito, 2023; Tripodi, 2024). La governance di una smart city si basa, pertanto, principalmente sulla tecnologia, la gestione dei dati e l'automazione. In questo modo risultano più efficienti la gestione delle informazioni, la garanzia dei servizi, il controllo delle risorse e la produzione di valore (Pereira et al., 2018).

Recentemente, il termine smart urban governance è stato associato a piattaforme digitali appositamente progettate per gestire i servizi pubblici attraverso un'alta personalizzazione, nel tentativo di fornire servizi o vantaggi ottimizzati per tutti gli stakeholder coinvolti, inclusi cittadini, enti pubblici e privati. In tale contesto, la governance delle smart city ha come obiettivo quello di stabilire una compatibilità semantica tra diverse tecnologie e silos di dati, favorendo allo stesso tempo la connettività, l'interoperabilità e la collaborazione tra diversi stakeholder (Azzari et al., 2018).

È stato osservato che la collaborazione, la condivisione e il coordinamento avente ad oggetto dati tra gli stakeholder rappresentano il "motore principale" di una smart city e delle applicazioni che la supportano (Voorwinden 2021). Collaborazione e partnership tra diversi stakeholder sono necessarie per affrontare la crescente complessità della condivisione dei dati e raggiungere gli obiettivi di una smart city. Diversi stakeholder sono infatti coinvolti nel definire la governance del dato all'interno dell'intero sistema, ovvero nel definire, assegnare e ripartire le responsabilità in base alle norme, ai valori e agli obiettivi delle smart city (Choenni et al., 2022; Dameri & Bruzzone, 2023).

---

agent is an AI system that uses an LLM to reason through a problem, create a plan to solve the problem, and execute the plan with the help of a set of tools".

Tra le altre cose, le collaborazioni sui dati consentono di indirizzare i dati, che sono nel dominio di soggetti privati (imprese, in particolare), verso istanze di interesse collettivo. Ma si tratta ancora di pratiche non sufficientemente sperimentate, atteso che – soprattutto nel settore privato – i dati sono prevalentemente utilizzati all'interno delle organizzazioni. Si osserva che tradizionalmente lo scambio di dati nel settore privato è ostacolato da due cause principali [2]. Le aziende e, quindi, anche le PMI tendono a trattare i dati per il loro uso esclusivo e per mantenere un vantaggio competitivo rispetto ai loro concorrenti. Dopo di che, i privati mantengono i dati di cui sono titolari all'interno della loro organizzazione e non sono disposti a condividerli quando i benefici che ne trae il pubblico sono poco chiari o quando il loro utilizzo non è sufficientemente remunerativo rispetto alle loro missioni imprenditoriali (Grimaldi & Fernandez, 2019; Mossberger et al., 2023).

Liva (2023) afferma che l'accesso da parte della smart city ai dati del settore privato è particolarmente problematico e la condivisione dei dati nella forma business-to-government (B2G) è considerata un ostacolo da superare per lo sviluppo degli ecosistemi di dati nelle smart city. La mancanza di partenariati pubblico-privati suggerisce che debba essere ricercato un altro quadro integrato di incentivi per attrarre le imprese private. Osserva sempre l'autore che le soluzioni contrattuali degli accordi pubblico-privati non sono sempre ottimali, poiché creano costi di transazione e non portano con sé la fiducia di forme di collaborazione meno formali, ma più solide. Per questo motivo, nelle smart city egli osserva che raramente vengono istituiti modelli di governance dei dati che includano attori diversi dagli enti pubblici. Quindi, sono necessarie nuove forme di governance interorganizzative e di interazione che attirino e mantengano nel tempo la partecipazione nelle smart city delle imprese private in generale e delle PMI, in particolare, mediante la condivisione dei loro dati (Kazemargi & Ceci, 2025).

Per quanto riguarda lo specifico delle PMI, si osserva che – sebbene esse costituiscano la spina dorsale dell'economia del nostro paese e la loro partecipazione ai progetti di smart city sia fondamentale – il loro coinvolgimento attivo è ancora estremamente marginale.

Il miglioramento degli accordi di governance del dato potrebbe aiutare le PMI a crescere e prendere parte più attivamente allo sviluppo delle smart city. Accordi di governance che forniscano alle PMI l'accesso e facilitino l'uso dei dati e delle tecnologie e competenze correlate ai dati potrebbero aumentare la loro capacità di innovare e le loro possibilità di crescere, ottenendo una maggiore efficienza in termini di costi. In ogni caso, per raggiungere risultati soddisfacenti, si osserva che è necessario includere nelle iniziative di smart city misure per consentire alle PMI di accedere ai dati e migliorare la loro capacità di gestione (OECD, 2023).

Considerando questo scenario, risulta utile domandarsi e approfondire con quali modalità le PMI possano contribuire al governo del dato nelle smart city.

---

[2] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

3. Metodologia

Per rispondere a questa domanda di ricerca è stato condotto uno studio qualitativo longitudinale sugli sviluppi dell'infrastruttura digitale nella città di Roma. Basandoci su tre componenti chiave dell'ecosistema di servizi della città – la Roma Data Platform (RDP), la RomApp e l'agente virtuale Julia – lo studio illustra come le PMI locali hanno preso parte al governo del dato. Per lo studio empirico, sono stati raccolti dati primari e secondari. Attraverso interviste e interazioni informali con le figure chiave coinvolte nelle tre iniziative è stato possibile ricostruire il processo graduale di sviluppo e le funzionalità abilitate dalle scelte di progettazione dei sistemi e di governo del dato. La raccolta di dati primari si è rivelata particolarmente preziosa anche per comprendere le sfide e gli attuali limiti del sistema, nonché per individuare le aree da affrontare e gli ostacoli che hanno impedito a RDP e ad altre applicazioni di funzionare a pieno regime. In aggiunta, sono stati raccolti dati secondari attraverso fonti pubbliche che hanno fatto riferimento alle iniziative del Comune di Roma e mediante una rassegna della letteratura sulla condivisione e la governance distibuita dei dati nel contesto delle smart city.

4. Dalla Roma Data Platform all'agente virtuale Julia

In questo capitolo esaminiamo, il caso di studio della smart city di Roma per comprendere in che modo le PMI hanno preso parte alla gestione urbana del Comune, basandoci su tre componenti chiave dell'ecosistema dati della città, descrivendo il progetto RDP, presentando poi l'iniziativa della RomAPP, e soffermandoci infine sul nuovo assistente virtuale del Comune, lanciato per l'occasione del Giubileo 2025, che prende il nome di Julia.

Roma Data Platform. RDP è una piattaforma digitale della smart city del Comune di Roma ideata con una valenza sia strategica che operativa. È dotata di una propria infrastruttura, di propri dataset certificati, di logiche evolute di trattamento dei dati e anche di sensori distribuiti sul territorio. Essa è in grado di raccogliere ed elaborare dati eterogenei e costituisce uno strumento di governance utile per l'amministrazione comunale di Roma, interconnettendo i vari ed eterogenei silos di dati e facendoli comunicare tra loro. Questo consente all'amministrazione di fare inferenze che generano ulteriori informazioni utili a identificare anomalie, criticità e fenomeni emergenti. RDP consente anche di monitorare il territorio comunale da un punto di vista produttivo grazie alla grande massa di dati generati da un agglomerato urbano molto popoloso.

Dal punto di vista tecnologico e infrastrutturale, la RDP prevede una sofisticata integrazione di varie componenti FIWARE, un framework applicato da numerose città intelligenti nel mondo, che utilizza standard aperti e componenti open-source,

fondamentali per il suo funzionamento e la sua scalabilità (Notaristefano et al., 2024). L'architettura attuale della RDP è un sistema robusto e flessibile, ben attrezzato per gestire le complessità della gestione dei dati urbani e delle applicazioni per smart cities, gettando una solida base per miglioramenti futuri e l'allineamento con iniziative come Gaia-X (Kazemargi et al., 2023).

La RDP si compone di un "cruscotto" centralizzato per l'osservazione e la gestione delle informazioni relative agli aspetti essenziali della quotidiana vita urbana nella città di Roma (Ariano, 2021). La RDP è stata lanciata nel 2020 proprio con l'ambizioso scopo di valorizzare le enormi quantità di dati prodotte dalla Città di Roma, dai suoi partner e dai cittadini, tramite l'utilizzo di dispositivi connessi. Scopo di RDP era evidentemente quello di migliorare la governance della città basata sui dati (data-driven), facendola evolvere a grande velocità. Progettata per attività di pianificazione strategica e per supportare molteplici forme di condivisione dei dati, non solo tra soggetti pubblici ma anche tra i predetti e grandi imprese e PMI, la RDP è dotata di una architettura informatica in grado di raccogliere, registrare ed integrare più flussi di informazioni provenienti da fonti diverse, riuscendo ad incorporarle in un unico sistema. Tutte queste informazioni vengono elaborate dalla RDP che restituisce dei "data insights" utili per la governance cittadina, per le imprese e per gli stessi cittadini. In effetti, l'ulteriore obiettivo della RDP era proprio quello di promuovere la partecipazione di vari stakeholder, in modo tale che questa partecipazione potesse aggiungere valore per l'intero ecosistema, supportando ulteriormente una governance intelligente della città e dei suoi servizi.

Tuttavia, nel corso degli anni, il suo utilizzo è stato rivolto solo alla governance interna della città, mancando l'interoperabilità diretta e le connessioni e condivisioni dei dati con attori esterni. La configurazione attuale, gli archivi di dati e l'interoperabilità tra sistemi IoT sono efficaci solo per uso interno e non comunicano adeguatamente tra di loro. Tuttavia, nel corso del 2024, in collaborazione con le figure chiave coinvolte nella creazione e nell'amministrazione della piattaforma, è stato possibile condurre una valutazione strategica delle sue capacità e della possibilità di aprirsi allo scambio di dati con entità esterne come organizzazioni private e PMI, nonché definire idonee misure utili ad incentivarlo. In definitiva, RDP intende estendere il suo campo di applicazione a un sistema interconnesso di condivisione dei dati tra varie entità, nel tentativo di migliorare i propri servizi ai cittadini, mettendo a frutto il patrimonio informativo pubblico (conservato ora in un grande "data lake distribuito"), ma anche attirando il conferimento di dati da parte delle imprese, delle PMI e dei cittadini. Sarà, allora, interessante vedere se il nuovo progetto "Evoluzione Roma Data Platform" (rilanciato dal Comune di Roma a dicembre 2024) terrà conto di queste valutazioni e in che modo vorrà e/o riuscirà a favorire nuove forme di governance per spingere l'innovazione e lo sviluppo della smart city. Per ora, si legge nelle pagine del sito internet del Comune in cui è presentato il progetto che l'obiettivo è di "*creare uno strumento abilitante per la Smart City, operando come Decision Support System (DSS) a supporto delle attività amministrative e degli stakeholder. La piattaforma agisce come 'deposito virtuale' centralizzato dei dati generati da*

Roma Capitale, consentendo la loro aggregazione e scambio con altri sistemi in modo organizzato. La RDP rende disponibili ai cittadini servizi digitali, come app, cruscotti di data visualization, API e servizi web. Il progetto RDP avrà un impatto esteso anche ai comuni interessati, fornendo una solida base per il miglioramento della gestione amministrativa ed economica. L'interoperabilità dei dati creerà un ecosistema di cooperazione tra i comuni, permettendo lo sviluppo di strategie data-driven. I city user beneficeranno di servizi digitali aggiornati e basati su dati previsionali e consuntivi, arricchendo l'esperienza di residenti, turisti e pellegrini, soprattutto in vista del Giubileo del 2025" [3].

RomApp. Sempre sviluppata all'interno del progetto "Smart City – Roma Data Platform", l'applicazione software RomApp è stata concepita, invece, come una soluzione verticale, con due obiettivi principali: consentire ai cittadini di partecipare attivamente al governo della città, segnalando problemi e bisogni urbani vari (es.: necessità di rimuovere rifiuti ingombranti; esistenza di buche e altre problematiche legate a strade, trasporti, ecc.); acquisire informazioni sullo stato della città e dei servizi, utili per interpretare i dati forniti dai sensori IoT e dai sistemi informativi in uso nei diversi settori (economia, trasporti, cultura, turismo, welfare, etc.). Questo secondo sviluppo dell'App, originariamente previsto è stato, invece accantonato, funzionando semplicemente l'applicazione per segnalare inefficienze e/o situazioni di degrado che necessitassero l'intervento dell'amministrazione. Dopo il lancio di Julia, si può affermare senz'altro che quelle operatività sono, almeno in parte, integrate nelle funzioni dell'assistente virtuale.

RomApp era completamente collocata all'interno del progetto complessivo e negli standard di RDP ed era dotata di moduli funzionali che supportavano l'intero processo, dalla raccolta dei report all'elaborazione e analisi dei dati e ai feedback agli utenti. Disponibile per utenti Apple e Android, era caratterizzata da un design semplice e da una forte call to action per l'invio di report e proposte. La sua unicità risiedeva nel fatto che non era necessario registrarsi ed era assente qualsiasi forma di tracciamento, che incoraggiava un'adesione massiccia da parte dei cittadini e la raccolta di dati anonimi, ma sufficientemente numerosi per costruire dei modelli sulla base dei quali definire i bisogni e i sentimenti di apprezzamento o meno dei cittadini. RomApp, è stata chiusa il 20 settembre 2024, a causa dei costi di gestione e solo di recente riattivata. Nelle pagine web dell'App nel periodo di chiusura, si dichiarava che nonostante il supporto dei cittadini che hanno contribuito a risolvere molteplici problemi e i successi nel miglioramento dei servizi, la chiusura è stata inevitabile. Il gruppo che ha gestito la RomApp ha espresso profonda gratitudine per la numerosa partecipazione attiva e l'auspicio che altre iniziative simili proseguano questo percorso di collaborazione civica per il miglioramento della città.

Nel momento in cui si scrive questo capitolo, una PMI sembrerebbe essersi adoperata per riattivare e gestire RomApp, dandogli nuova vita auspicata dai suoi

[3] https://www.comune.roma.it/web/it/attivita-progetto.page?contentId=PRG1163717 (consultato il 23 marzo, 2025).

fondatori e presentandosi al pubblico con il seguente messaggio "*L'unica App a Roma attraverso la quale i cittadini possono far sentire la propria voce. L'App permette di partecipare attivamente alla vita del territorio condividendo ogni tipo di segnalazione in tempo reale. Una volta raggiunto il numero necessario di conferme, la domanda verrà esposta agli uffici competenti. Perché iscriversi a RomApp? Perché abbiamo tutti a cuore la Città Eterna e vogliamo che rimanga tale. Condividi la tua voce e noi ci impegneremo ad amplificarla!*". Le informazioni e le segnalazioni raccolte sono poi condivise con le amministrazioni comunali di riferimento per gli interventi necessari alla risoluzione delle problematiche individuate dai cittadini.

Julia. Julia, invece, è il nuovo assistente virtuale del Comune di Roma, che utilizza gli LLM per aiutare i visitatori della città a esplorarla e viverla in modo facile e piacevole. Anche Julia costituisce una interessante applicazione nella quale si intende valorizzare la condivisione e scambio di dati tra vari stakeholder, salvaguardando la correttezza dei dati e la tutela dei dati personali [4] per mettere al riparo cittadini e utenti da bias e allucinazioni prodotti del sistema di intelligenza artificiale utilizzato (Spagnoletti & Baskerville, 2025). La soluzione è stata pensata nel 2022 quando non era ancora uscita la versione più popolare di OpenAI/ChatGPT ed è stata orientata programmandola per rispondere prevalentemente alle domande dei visitatori della Capitale nel corso del Giubileo. Julia è, quindi, basata sull'integrazione del chatbot di OpenAI/ChatGPT, mediante un accordo con Microsoft, ed è stata sviluppata dal Comune di Roma, coadiuvato dalla Fondazione per l'Attrazione e da partner industriali quali NTT Data e Intellera. Nonostante ciò, Julia è diversa da ChatGPT "*Non prende le informazioni da internet. Le fonti sono tutte ufficiali e verificate: Atac per i bus, Aeroporti di Roma per i voli, Trenitalia e Italo per i treni, il Comune per hotel e strutture*" (Tommasi, 2025). Julia è raggiungibile mediante numero telefonico, attraverso i canali di messaggistica istantanea come Telegram e WhatsApp. Julia consente l'inserimento diretto delle informazioni da parte delle PMI (albergatori, ristoratori, uffici comunali, ecc.) ed è interrogata dagli utenti mediante domande poste attraverso i suddetti canali. Julia rappresenta un'opportunità unica per gli esercenti e le PMI della città e del territorio circostante che possono inserirsi in apposito database e partecipare attivamente alla sua piattaforma progettata per ottimizzare la gestione dei flussi turistici, migliorare la soddisfazione dei visitatori e rafforzare l'immagine di Roma come destinazione d'eccellenza e sostenibile. L'App consente agli utenti di interrogare database di diversi attori, come quelli relativi alla mobilità, al turismo, alla assistenza sanitaria, alle attrazioni culturali, al commercio e ad altri servizi urbani del Comune di Roma, utilizzando il linguaggio naturale in tutte le lingue gestite da ChatGPT. Grazie a Julia, Roma può offrire ai turisti un'accoglienza personalizzata e innovativa, e gli operatori locali possono promuovere i propri servizi in modo più efficace e immediato. Julia parla ottanta lingue e le informazioni e le risposte che fornisce sono generate attraverso un controllo diretto e garantito delle fonti dei dati, che dovrebbe assicurare pertinenza, aggiornamento, completezza e

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

accuratezza. Le attività ricettive che stanno dentro Julia devono essere "legali" e sono validate dall'ufficio attività produttive del Comune. Inoltre, Julia attinge all'importante patrimonio informativo della RDP (segnatamente, dal suo grande "data lake"), che per l'occasione è stata fatta oggetto anche di importanti interventi di reingegnerizzazione e riorganizzazione. Per creare la giusta fiducia, l'amministrazione comunale ha cura di precisare anche che Julia non ha scopi commerciali, non utilizza pubblicità e non utilizza le conversazioni private per l'addestramento dei propri modelli di AI. Julia si basa, allora, sulla condivisione di dati da parte dei vari stakeholder e afferma di operare nel rispetto della normativa in materia di protezione dei dati personali (Palmieri, 2025). Julia non registra i dati personali degli utenti e non fornisce loro informazioni personali.

Al momento della stesura di questo capitolo, l'App Julia (rilasciata in una nuova versione 2.0) rappresenta un promettente esempio di innovazione abilitata dalla governance collaborativa dei dati (Spagnoletti & Volpentesta, 2024; Manzocchi & Spagnoletti, 2024). Tuttavia, data la sua recente implementazione, non è ancora possibile valutare i limiti di questa soluzione. Saranno necessarie ricerche future per valutarne criticamente le implicazioni e l'efficacia a lungo termine [5].

5. Le PMI e la governance dei dati nell'agente virtuale Julia

Il lancio di Julia segna una nuova fase dell'ecosistema di dati della smart city di Roma. Il rapporto tra Julia e RDP non è di sostituzione o di esclusione reciproca, ma di evoluzione ed integrazione. RDP resta la fonte principale di approvvigionamento dei dati di Julia, la quale – come detto – attinge al suo enorme patrimonio informativo certificato.

Nella RDP, il Comune di Roma ha tentato di realizzare una perfetta integrazione dello sviluppo della smart city con lo sviluppo economico del territorio, raccogliendo e analizzando i dati delle attività produttive (e, quindi, anche della presenza e delle attività intraprese dalle PMI) e rendendoli fruibili e utilizzabili in tempo reale, attraverso la propria dashboard. Questo ha consentito di apportare molti benefici alle imprese, poiché la disponibilità di dati permette anche di supportare processi di

[5] Nel sito del Comune di Roma, al link https://www.comune.roma.it/web/it/notizia/julia-presentata-seconda-release-assistente-virtuale-roma.page, si legge "*Dopo quattro mesi dalla sua nascita Julia si evolve. Come sempre, non prende informazioni sulla rete, ma solo nozioni certificate. Fornisce informazioni in tempo reale, esegue funzionalità di calcolo e percorso come quella delle file al pronto soccorso, non ha scopi commerciali, non alcuna pubblicità, né occulta né esplicita, ma è un servizio pubblico. Julia 2.0 ora ha una maggiore capacità di comprensione e interazione, sa tutto sul Giubileo dei Giovani, sarà una guida interattiva utilissima per i pellegrini ed è maggiormente pronta per le richieste di turisti e romani. Nei prossimi mesi l'evoluzione sarà anche orientata alla creazione di una App, per avere una maggiore utilità per i cittadini, introducendo informazioni per il disbrigo delle pratiche amministrative*".

cocreazione di innovazione, in una logica di open innovation, che contribuisce alla evoluzione di tutto il tessuto produttivo sottostante.

Per un ecosistema di dati urbano di questo tipo, anche la partecipazione delle PMI è di vitale importanza. Le PMI costituiscono la spina dosale del sistema produttivo del nostro paese ma, nella maggior parte delle ipotesi, non hanno risorse economiche o ne hanno limitate per creare innovazione e prendere parte attivamente a questo inarrestabile veloce processo di trasformazione, basato sui dati (TIM Group, 2020).

Julia è stata, allora, concepita anche per affrontare le sfide di partecipazione delle PMI in questo processo di trasformazione, attraverso un modello di ingaggio diretto e senza barriere all'ingresso. Gli esercenti commerciali, come ristoranti e hotel, possono registrare la propria attività utilizzando la loro identità digitale su un portale a loro dedicato. Le informazioni che vengono fornite sono opportunamente verificate dall'amministrazione comunale e sono poi rese fruibili attraverso l'interfaccia dell'assistente virtuale. Questo processo di censimento degli esercenti garantisce dati aggiornati e di alta qualità, oltre a protocolli standardizzati per la loro gestione e interoperabilità.

In questo modello, il contributo delle PMI non si limita a fornire l'anagrafica della propria attività ma riguarda anche dati di dettaglio relativi alla descrizione dei propri servizi, agli orari, alla accessibilità dei locali, ecc. Sotto questo profilo, le imprese diventano parti attive nelle attività governance, influendo anche sulla qualità dei dati elaborati dal sistema. Fornire informazioni precise e aggiornate non è solo una richiesta dell'amministrazione e degli utenti, ma un incentivo, poiché l'accuratezza dei dati (es. orari di apertura, offerte speciali) influisce direttamente sulla visibilità delle PMI che prendono parte all'ecosistema e sul loro successo commerciale. La App Julia ha, quindi, esternalizzato una parte cruciale della funzione di data governance delle informazioni alle PMI, promuovendo una responsabilità a più livelli (Choenni, 2022). Julia non impone solo delle regole, ma ha creato un'architettura che motiva e abilita la partecipazione attiva delle imprese nel garantire la qualità e aggiornamento dei dati (Spagnoletti et al., 2015). Così facendo, la smart city di Roma ha, in definitiva, aperto il proprio ecosistema di dati ad una partecipazione attiva delle PMI. Le quali – pur non disponendo delle necessarie risorse tecnologiche ed informative – sono incentivate a partecipare e a conferire i propri dati, a condizione che il processo di ingaggio sia semplice e che i benefici siano chiari. In cambio, si adoperano per garantire, nel tempo, la qualità, la pertinenza e l'aggiornamento dei loro dati.

6. Conclusioni

Questo capitolo ha analizzato l'evoluzione dell'ecosistema di dati di Roma, seguendo lo sviluppo della smart city dalla RDP all'agente virtuale Julia. L'analisi ha evidenziato che – mentre RDP è uno strumento che serve prevalentemente alla smart

city per orientare e supportare le scelte di governance dell'amministrazione, la pianificazione urbana e l'ottimizzazione dello sviluppo del territorio e delle attività produttive (ivi comprese le PMI) – l'innesto di Julia nella RDP ha introdotto un nuovo modello di governance partecipato in modo attivo anche da parte delle PMI.

Le PMI assumono, infatti, un ruolo fondamentale nella governance dei dati urbani, attraverso un meccanismo di partecipazione che contribuisce attivamente a condividere dati e a controllarne la qualità, la rilevanza e l'aggiornamento. Con una governance robusta e partecipata – a sua volta – Julia garantisce agli utenti (cittadini, turisti e fruitori dei suoi servizi) che i dati delle PMI sono affidabili, verificati, aggiornati e conformi alla legge. Per uno sviluppo ulteriore e per il successo dell'ecosistema di dati urbano sarebbe importante che, nel futuro della RDP, le PMI non si limitassero solo a caricare la propria anagrafica ma svolgessero – a loro volta – attività di comunicazione all'esterno attraverso agenti virtuali che senz'altro contribuirebbero a rendere ancora più ricche e rilevanti le informazioni raccolte e presentate da Julia.

Il caso della smart city di Roma dimostra in modo tangibile come la governance dei dati si presti ad assumere forme variabili e dinamiche, il cui successo dipende non solo da una adeguata infrastruttura tecnologica, ma anche dalla capacità di incentivare la collaborazione, costruire la fiducia e definire ruoli chiari per tutti gli stakeholder dell'ecosistema. In definitiva, il successo di un'iniziativa di smart city non è garantito da una singola implementazione, ma dipende dalla sua continua capacità di evolvere e cambiare, adattando le proprie strategie di governance alle mutevoli esigenze tecnologiche ed economico-sociali locali.

Essendo quello della smart city di Roma uno dei primi casi di studio di creazione di agenti virtuali collegati alle basi di dati dell'ecosistema cittadino, il modello di governance partecipata di Julia potrebbe diventare un esempio da imitare anche per altre smart city che vogliano coinvolgere in modo attivo le attività produttive del territorio e il proprio tessuto imprenditoriale cittadino.

Messaggi chiave:

- La governance dei dati urbani richiede il coinvolgimento attivo delle PMI, che contribuiscono alla condivisione e al controllo della qualità dei dati nelle smart city.
- L'evoluzione tecnologica favorisce nuovi modelli di governance partecipata tra amministrazione, PMI e cittadini, come dimostra l'evoluzione di Roma Data Platform (RDP) nell'agente virtuale Julia.
- L'approccio longitudinale adottato per lo studio dell'ecosistema di dati della smart city di Roma consente di cogliere la continuità evolutiva tra iniziative apparentemente distinte (RDP, Julia, RomApp), rivelando un percorso progressivo di costruzione di una governance collaborativa dei dati urbani.

Bibliografia

Abella, A., Ortiz-de-Urbina-Criado, M. & De-Pablos-Heredero, C. (2017). A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems. *Cities 64*, 47-53.

Aguilera, U., Peña, O., Belmonte, O. & López-de-Ipiña, D. (2017). Citizen-centric data services for smarter cities. *Future Generation Computer Systems*, *76*, 234-247.

Ariano, A. (2021). Il caso della Roma Data Platform. *Una geografia delle politiche urbane tra possesso e governo. Sfide e opportunità nella transizione*, 177-183.

Arkaraprasertkul, N. (2024). *AI-Powered Smart Cities: Transforming Urban Living with LLM*.

Azzari, M., Garau, C., Nesi, P., Paolucci, M. & Zamperlin, P. (2018). Smart City Governance Strategies to better move towards a Smart Urbanism. *International Conference on Computational Science and Its Applications*, 639-653. Doi:10.1007/978-3-319-95168-3_43.

Bibri, S.E. (2018). A foundational framework for smart sustainable city development: Theoretical, disciplinary, and discursive dimensions and their synergies. *Sustainable Cities and Society*, *38*, 758-794.

Choenni, S., Bargh, M.S., Busker, T. & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, *1*(1), 31-51.

Colapietro, C. (2022) Intelligenza artificiale e smart cities a mo' di introduzione. In Cremona, E., Laviola, F. & Pagnanelli, V. *Smart cities, Diritti, libertà e governance*, XVIII-XXXIV. Giappichelli.

Comune di Roma [Online] https://https://www.comune.roma.it/web/it/attivita-progetto.page?contentId=PRG1163717, consultato 30/5/2025.

Dameri, P.R. & Bruzzone, M. (2023). Le Dashboard urbane per la Smart governance. Il caso Controllo Dynamico. In Dameri, R.P. & Bruzzone, M. *Smart City, Prospettive di ricerca, Atti del Convegno "Smart city. Stato dell'arte e prospettive di ricerca"*, Università di Genova, 26/06/2023, 129-142. Genova University Press.

Di Gregorio, V. (2025). Circolazione dei dati e innovazione tecnologica. In *Accademia, Rivista dei civilisti italiani*, *7*, Pacini Giuridica.

Ducuing, C. (2024). The Regulation of Data in the European Union: the Data Governance Act and the Data Act. In Ziccardi G. *Smart City, Artificial Intelligence and Digital Tansformation Law*, 63-87. Milano University Press.

European Commission (2020). Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. [Online] https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1, consultato 20/08/2025.

Grimaldi, D. & Fernandez, V. (2019). Performance of an internet of things project in the public sector: The case of Nice smart city. *The Journal of High Technology Management Research*, *30*(1), 27-39.

Guggenberger, T.M. et al. (2025). Data spaces as meta-organisations. *European Journal of Information System*, 1-21.

Jansen, R.L. & Cusumano, M. (2012). Defining Software Ecosystems: A Survey of Software Platforms and Business Network Governance. In *Proceedings of the international Workshop on Software Ecosystems.*

Kalyuzhnaya A. et al. (2025). LLM Agents for Smart City Management: Enhancing Decision Support Through Multi-Agent, AI Systems. *Smart Cities*, *8*(1), 19.

Kazemargi, N. & Ceci, F. (2025). Data Governance for Creating Value in Data Ecosystems. In Heritier, P., Rossa, S. *Cibersecurity e Istituzioni democratiche*, fasc. II, 59-71. Mimesis Edizioni.

Kazemagi, N., Ceci, F., Leonelli, S., Spagnoletti, P., Sinaimeri, B. & Marchesani, F. (2025). Data Governance in Data Ecosistem. *Rivista Trimestrale di Organizzazione Aziendale.*

Kazemagi, N., Ceci, Spagnoletti, P. & Prencipe, A. (2023). Data control coordination in cloud-based ecosystems: the GAIA-X ecosystem. In Cennamo, C.; Dagnino, G. & Zhu F., *Handbook of Research on Digital Strategy*, 289-307. Edward Elgar Publishing.

Liva, G., Micheli, M., Schade, S., Kotsev, A., Gori M. & Codagnone, C. (2023). City data ecosystems between theory and practice: A qualitative exploratory study in seven European cities. *Data & Policy*, 5: e17. doi:10.1017/dap.2023.13.

Manzocchi, S. & Spagnoletti, P. (2024). Vettore IA. Algoritmi, impresa, società. Introduzione. *Rivista di Politica Economica*, *2*, 5-9.

Marchesani, F. & Ceci, F. (2024). Vettore IA. Algoritmi, impresa, società. Il ruolo dell'intelligenza artificiale come strumento organizzativo e strategico nelle smart city. *Rivista di Politica Economica, 2*, 131-148.

Mossberger, K., Cho, S., Cheong, P.H. & Kuznetsova, D. (2023). The public good and public attitudes toward data sharing through IoT. *Policy & Internet*, *15*(3), 370-396.

Notaristefano, M., Angeletti, F. & Spahiu, E. (2024). Privacy e cybersecurity nelle smart city: un caso di studio. In Bombelli, G. & Rossa, S. *Cybersecurity e Istituzioni Democratiche*, Fasc. I, 138-155. Mimesis Edizioni.

OECD (2023). *Smart City Data Governance: Challenges and the Way Forward*, OECD Urban Studies, OECD Publishing, Paris, https://doi.org/10.1787/e57ce301-en.

Oldenburg, J. & Pussinen, P. (2024). Exploring data ecosystem in smart city. *International Journal of Innovation Management*, vol. 28, Nov.-Dec., 1-18, doi: 10.1142/S13639 1962440005.

Oliveira, M.I., Barros Lima, G.D.F. & Farias Lóscio, B. (2019). Investigations into data ecosystems: a systematic mapping study. *Knowledge and information systems*, *61*, 589-630.

Palmieri, A.: *Julia, l'intelligenza artificiale che cambia il turismo e la vita a Roma* [Online] https://www.economyup.it/blog/julia-lintelligenza-artificiale-che-cambia-il-turismo-e-la-vita-a-roma/, consultato 25/3/2025.

Paolucci, F. & Pollicino, O. (2023). Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica? In Giannelli, M., Pagnanelli V., *Smart cities, Diritti, libertà e governance*, 17-43. Giappichelli.

Pereira, G., Parycek, P., Farco, E. & Kleinhansc, R. (2018). Smart governance in the context of smart cities: A literature review. *Information Polity 23*, 143-162. Doi 10.3233/IP-170067.

Rzevski, G., Kozhevnikov, S., Svitek, M. (2020). Smart City as an Urban Ecosystem. *Smart Cities Symposium*, Prague.

Silva, B.N. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable City*, *38*. Doi: 10.1016/j.scs.2018.01.053.

Spagnoletti, P. & Baskerville, R. (2025). Safe and Unsafe Information: Managing Risks in the Era of Generative Artificial Intelligence. In Abrahamsen, E.B., Aven, T., Bouder, F., Flage, R. & Ylönen, M. (Eds.), *Proceedings of the 35th European Safety and Reliability and the 33th Society for Risk Analysis Europe Conference*. https://doi.org/10.3850/981-973-0000-00-0.

Spagnoletti, P. & Volpentesta, T. (2024). Intelligenza artificiale generativa nelle piccole e medie imprese: evidenze empiriche nel contesto italiano. *Rivista di Politica Economica*, *2*. https://www.confindustria.it/home/centro-studi/rivista-di-politica-economica/dettaglio?doc=RPE_vettore_ia_algoritmi_impresa_societa_2024_2.

Spagnoletti, P., Resca, A., Lee, G. (2015). A Design Theory for Digital Platforms Supporting Online Communities: A Multiple Case Study. *Journal of Information Technology*, 1-17. Doi: 10.1057/jit.2014.37.

Spagnoletti, P., Kazemargi, N., Constantinides, P. & Prencipe, A. (2025). Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors. *Journal of the Association for Information Systems*, 977-1008, 26:4.

TIM Group, (2020). *Rome, an increasingly Smart city* – Gruppo Tim [Online] https://www.gruppotim.it/en/innovation/innovation-news/Rome-data-platform.html, consultato 22/09/2025.

Tommasi, G. (2025). *Julia, la nuova voce virtuale di Roma creata con l'IA* [Online] https://zetaluiss.it/2025/04/16/julia-la-nuova-voce-virtuale-di-roma-creata-con-lia/, consultato 20/9/2025.

Tripodi, E. (2024). Le prospettive potenziali della smart city "evoluta": la digital twin city. *Diritto di Internet*, (*1*)2024, 23-36.

Vigorito, A. (2023) Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo. *Media Laws*, *1*, 104-127.

Voorwinden, A. (2021). The privatised city: Technology and public-private partnerships in the smart city. *Law, Innovation and technology*, *13*(2), 439-463.

Wolniak, R. & Stecula, K. (2024). Artificial Intelligence in Smart Cities – Applications, Barriers, and Future Directions: A Review. *Smart Cities*, *7*, 1346-1389. https://doi.org/10.3390/.

Ausili alla digitalizzazione delle PMI: cosa favorisce l'ottenimento di finanziamenti pubblici?

Filippo Ferrarini [*], Cosimo Checcucci [**], Bernardo Balboni [***] e Simona Leonelli [****]

Abstract: La sostenibilità e la crescita degli ecosistemi di dati dipendono anche dal coinvolgimento e dalla partecipazione attiva delle piccole e medie imprese (PMI). Alcune di esse, però, non sono pronte a entrare a far parte di tali ecosistemi poiché necessitano di prepararsi adeguatamente adottando e integrando processi di digitalizzazione che a volte sono molto costosi. La pubblica amministrazione fornendo sussidi, incentivi e agevolazioni fiscali potrebbe aiutarle in questa trasformazione digitale. Questo capitolo vuole analizzare come alcune caratteristiche delle PMI, tra cui la dimensione, il settore di appartenenza e la posizione geografica, possano favorire l'ottenimento di un finanziamento pubblico. Lo studio prende in esame il voucher per la digitalizzazione delle PMI erogato nel 2019 dal Ministero delle Imprese e del Made in Italy, utilizzando un database di oltre 16.000 PMI dislocate sul territorio italiano. Attraverso una analisi descrittiva, i risultati mostrano che le caratteristiche delle PMI possono influenzare l'ottenimento di finanziamenti relativi alla digitalizzazione.

Parole chiave: Digitalizzazione, PMI, Finanziamenti pubblici, Competitività.

1. Introduzione

Negli ultimi anni si è assistito a un massiccio avvento della digitalizzazione. Essa ha determinato una trasformazione radicale per le organizzazioni (Curzi & Ferrarini,

[*] Filippo Ferrarini (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: filippo.ferrarini@unimore.it

[**] Cosimo Checcucci (✉)
SAPI spa, Modena, Italia.
E-mail: cosimocheccucci@gmail.com

[***] Bernardo Balboni (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: bernardo.balboni@unimore.it

[****] Simona Leonelli (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: simona.leonelli@unimore.it

DOI: 10.82018/9791221165456-4

2024; Rubino et al., 2019). Infatti, l'industria 4.0, e più recentemente le nuove tecnologie digitali come l'intelligenza artificiale, i *big data*, il *cloud computing* e *l'internet of things*, stanno ridefinendo i modelli di business tradizionali, i processi aziendali e le strategie competitive (Zott & Amit, 2017), comportando un aumento della produttività e dell'innovazione, una riduzione di costi di produzione e un aumento di competitività in generale (Freund & Weinhold, 2004; Hagsten & Kotnik, 2016; Marullo et al., 2024). Tuttavia, se è vero che le trasformazioni digitali sono spesso trainate da aziende di grandi dimensioni (European Commission, 2022), è altrettanto vero che le piccole e medie imprese (PMI), giocano un ruolo fondamentale in questa partita (Pfister & Lehmann, 2024). Infatti, da una parte le PMI rappresentano la stragrande maggioranza del settore produttivo e dei servizi a livello italiano ed Europeo, sia in termini di occupazione che in termini di produttività (Satı, 2024). Dall'altra parte, esse possono favorire la transizione digitale dei rispettivi settori produttivi, in quanto dispongono di competenze, flessibilità e capacità innovativa (Kitsios and Kamariotou, 2017; Oliveira et al., 2019).

Tuttavia, spesso le PMI non dispongono di quelle risorse finanziarie, strutturali o culturali per abbracciare a pieno questa trasformazione digitale (Bouncken & Barwinski, 2020; Gierlich et al., 2019). Pertanto, il ruolo degli enti pubblici e, in particolare, delle loro forme di finanziamento pubblico, diventa fondamentale. Finanziamenti specifici come *voucher* per l'innovazione o sussidi a fondo perduto consentono alle PMI, non solo di reperire importanti risorse finanziarie per supportare la transizione e l'ammodernamento tecnologico e digitale, ma anche di migliorare il loro assetto organizzativo e le loro performance (Chung & Kim, 2023; Kleine et al., 2022). Questo è ampiamente evidenziato dalla letteratura che sottolinea i benefici che le forme di supporto pubblico apportano alle organizzazioni (Hwang, 2023; Kahle et al., 2020; Khin & Hung Kee, 2022; Kolade et al., 2019; Ietto et al., 2022; Mahdiraji et al., 2023; Park et al., 2022; Prodi et al., 2022). Ad esempio, alcuni studi mostrano che forme di finanziamento e sussidio pubblico hanno un impatto diretto sulla produttività, sull'incremento delle spese di ricerca e sviluppo e sull'assunzione di nuovo personale, favorendo la creazione di valore (Dvouletý et al., 2021; Huynh et al., 2025; Li et al., 2023). Ciò nonostante, permangono alcune lacune in letteratura; infatti, la maggior parte degli studi ha analizzato l'impatto che i sussidi possono avere sulle performance aziendali (Kleine et al., 2022; Marullo et al., 2024; Mina et al., 2021), tuttavia, solo pochi hanno indagato gli antecedenti all'ottenimento degli stessi.

Pertanto, seguendo la letteratura recente (Børing et al., 2020; Marullo et al., 2024; Mulier & Samarin, 2021), il presente studio ha come obiettivo quello di capire se alcuni antecedenti come dimensione di impresa, dimensione aziendale e settore di appartenenza, possano favorire l'ottenimento di finanziamenti pubblici per la digitalizzazione. In particolare, verrà analizzato il *voucher* per la digitalizzazione erogato dal *Ministero del Made in Italy n*el 2019, e verranno prese in esame 16.000 PMI dislocate nel territorio nazionale.

Il capitolo offre un contributo originale alla letteratura esistente in merito alle sovvenzioni pubbliche per le PMI. In particolare, affrontando il tema dei

finanziamenti alla digitalizzazione, il capitolo contribuirà ad accrescere l'attuale conoscenza rispetto agli antecedenti di queste forme di finanziamento, un ambito ancora poco esplorato dai ricercatori. I risultati possono fornire indicazioni utili anche ai manager e ai proprietari delle imprese.

2. La digitalizzazione delle PMI e le varie forme di finanziamenti

Negli ultimi anni, la digitalizzazione ha portato ad una trasformazione radicale delle imprese in ogni settore e dimensione (Curzi & Ferrarini, 2024; Psister & Lehmann, 2024; Rubino et al., 2019). La digitalizzazione favorisce una maggiore interconnessione delle tecnologie dell'informazione (ICT) con le strutture di produzione più tradizionali, portando numerosi vantaggi tra cui l'aumento della produttività e della qualità dei prodotti, la riduzione dei costi e degli sprechi e l'innovazione dei servizi/prodotti e dei processi aziendali (Ardito et al., 2021; Brougham & Haar, 2018; Estensoro et al., 2022; Freund & Weinhold, 2004; Radicic & Petkovic´, 2023). La digitalizzazione massiva sta incentivando inoltre la produzione, la raccolta e l'utilizzo dei dati (Del Giudice, 2016; Di Vaio & Varriale, 2020; Hagsten & Kotnik, 2016; Wedel & Kannan, 2016). Infatti, essi sono diventati una risorsa strategica per le organizzazioni, ed in particolare per le piccole e medie imprese. Con l'aumento della disponibilità di dati relativi a consumatori, fornitori, concorrenti, partner e processi aziendali, le organizzazioni possono usare gli stessi per creare e aumentare valore (Ramalli & Pernici, 2023). Ad esempio, integrando l'analisi di grandi quantità di dati, come big data, con capacità analitiche e competenze del personale, le organizzazioni riescono ad ottimizzare i propri processi decisionali (Lavalle et al., 2011; Lee et al., 2013; Miles et al., 2014; Popovič et al., 2018). Allo stesso tempo, l'*internet of things* sta trasformando radicalmente le modalità operative delle aziende, contribuendo alla digitalizzazione della catena del valore, sia nei settori manifatturieri che nei servizi. Questo porta con sé vantaggi in termini di ottimizzazione dei processi aziendali, aumento della flessibilità e migliore adattabilità ai cambiamenti del mercato (Queiroz et al., 2020). Infine, l'adozione dell'intelligenza artificiale all'interno delle organizzazioni può portare a miglioramenti significativi nelle performance individuali ed organizzative, aumentando ricavi e quote di mercato e riducendo allo stesso tempo i costi (Joshi et al., 2010; Pfister & Lehmann, 2024; Wu et al., 2020).

Perciò, gli enti pubblici possono ricoprire un ruolo fondamentale al fine di supportare le strategie di digitalizzazione. Ad esempio, In Italia, negli ultimi anni, sono stati introdotti diversi incentivi per supportare le PMI, tra cui il *voucher* per la digitalizzazione, che finanzia le spese per l'introduzione di tecnologie innovative di digitalizzazione e analisi dati (MIMIT, 2025a). Un altro incentivo è quello del Capitale di rischio per lo sviluppo delle PMI, un fondo d'investimento volto a sostenere la crescita delle stesse (MIMIT, 2025b). La Nuova Sabatini, invece, è un'iniziativa progettata specificamente per le PMI che desiderano modernizzare il loro parco

macchine ed offre l'accesso a finanziamenti agevolati per l'acquisto o il leasing di macchinari, impianti, beni strumentali d'impresa e nuove attrezzature, compresi hardware e software. Un'altra forma di finanziamento è il piano dedicato alle startup e alle PMI innovative, che offre misure specifiche per accelerare la loro crescita e rafforzare l'ecosistema imprenditoriale. Le agevolazioni comprendono la costituzione digitale gratuita, l'esonero dalla disciplina sulle società di comodo, incentivi fiscali per gli investimenti in capitale di rischio, l'accesso facilitato al Fondo di Garanzia per le PMI, equity crowdfunding e Italia Startup Visa per attrarre investitori e imprenditori internazionali. Inoltre, le startup possono cedere le proprie perdite a società quotate sponsor migliorando così la loro sostenibilità finanziaria (MIMIT, 2025c).

Se da una parte la letteratura recente ha ampiamente indagato l'impatto delle forme di finanziamento pubblico sulle performance aziendali (Hwang, 2023; Kahle et al., 2020; Khin & Hung Kee, 2022; Kolade et al., 2019), ancora poco è stato esplorato su quali siano quegli antecedenti che possano favorire il successo dell'ottenimento di un finanziamento pubblico per una organizzazione. Ad esempio, Mulier & Samarin (2021) evidenziano come il settore di appartenenza possa essere una determinante importante per favorire l'accesso a finanziamenti pubblici, specie quelli altamente tecnologici e ad alti investimenti in ricerca e sviluppo. Similmente, Marullo et al. (2024) mostrano come il successo delle PMI nell'assicurarsi fondi nazionali dipenda dalla regione di appartenenza, ma anche dalla distanza tecnologica tra la PMI e il bando a cui fanno domanda. Un contributo molto interessante e simile all'obiettivo di questo studio è quello di Børing et al. (2020); gli autori analizzano la relazione tra dimensione dell'impresa, settore di appartenenza e paese di origine e l'ottenimento di un sostegno pubblico a livello Europeo. Attraverso l'analisi di 800.000 mila imprese negli anni tra il 2015 e il 2017, gli autori mostrano che la dimensione dell'impresa è una caratteristica importante per ottenere l'accesso ai fondi Europei, in quanto le imprese più strutturate hanno una maggiore probabilità di accedere a risorse pubbliche. Allo stesso tempo, il settore manifatturiero è quello che tra gli altri ha un maggior tasso di successo per l'ottenimento dei finanziamenti da parte delle imprese. I loro risultati sono simili a quelli di Galope (2014) che mostra come le PMI appartenenti ai settori più tecnologici, come quelli dell'ICT o dei servizi alle imprese, hanno una maggiore probabilità di ottenere sussidi pubblici.

3. Dati e metodi

Il dataset è stato composto selezionando tutte le PMI che hanno fatto domanda al *Voucher* per la digitalizzazione nel 2019. Il *voucher* è stato promosso dal Ministero delle Imprese e del *Made in Italy* per sostenere le PMI italiane nei processi di digitalizzazione. In particolare, l'obiettivo era quello di incentivare le PMI a: i) migliorare l'efficienza aziendale; ii) modernizzare l'organizzazione del lavoro tramite strumenti tecnologici e forme di flessibilità lavorativa; iii) sviluppare soluzioni di *e-*

commerce; iv) implementare la connettività a banda larga o tramite tecnologia satellitare; v) realizzare interventi di formazione qualificata del personale nel campo ICT. Il valore complessivo del *voucher* per singolo soggetto richiedente era di 10.000 euro, pari al 50% delle spese ammissibili. Il numero complessivo delle domande è stato di circa 24.000.

A questo dataset iniziale sono state aggiunte tutte le informazioni economico-finanziarie reperite tramite il database Analisi Informatizzata delle Aziende Italiane (AIDA), una banca dati realizzata e distribuita da Bureau van Dijk S.p.A., contenente i bilanci, dati anagrafici e merceologici di tutte le società di capitale italiane attive e fallite. Essendo che, molte PMI avevano tuttavia dei dati mancanti, il processo di pulizia del dataset ha dovuto eliminare alcune migliaia di osservazioni, ottenendo una base di dati finale di circa 16.800 PMI idonee.

La variabile dipendente principale è stata chiamata "Esito", essa assume il valore 1 se la PMI ha ottenuto il finanziamento, mentre il valore 0 se non l'ha ottenuto. Questo dato proviene dalle graduatorie approvate dal Ministero delle Imprese e del *Made in Italy* pubblicate a seguito della valutazione delle domande ricevute.

Le variabili indipendenti selezionate sono state 1) dimensione dell'impresa, 2) settore di appartenenza, 3) regione in cui si trova la sede dell'organizzazione. La dimensione dell'impresa è una variabile categorica creata per classificare meglio il campione in base al numero dei dipendenti: le microimprese hanno il valore 1 e sono quelle con massimo 10 dipendenti; le piccole imprese hanno il valore 2 e sono quelle con 11-50 dipendenti, le medie imprese hanno valore 3 e sono quelle con 51-250 dipendenti. Questo dato è stato reperito dal database AIDA. I settori di appartenenza sono stati invece classificati in quattro macro-categorie, prendendo come riferimento la classificazione ATECO 2007 [1]. In particolare una prima macro-categoria è stata quella relativa alla industria e manifattura, comprendente i codici B,C, D, E, ed F; una seconda macro-categoria è stata quella relativa ai servizi alle imprese, nella quale sono confluiti i codici J, L, M, N ed H; una terza macro-categoria è stata quella del turismo e commercio, comprendenti i codici G ed I; mentre la quarta categoria è stata definita come "Altro", dove sono confluiti i codici A, K, P, Q, R, S, T. Tale suddivisione ha aiutato a creare gruppi più omogenei in quanto alla numerosità. Anche questo dato è stato reperito dal database AIDA. Infine, per ciò che concerne le regioni di localizzazione dell'impresa, sono state considerate tutte e 20 le regioni italiane, poi riclassificate secondo le indicazioni ISTAT (ISTAT, 2020). In dettaglio, sono state create quattro macro-categorie regionali: Nord est, Nord ovest, Centro, Sud e isole. Questo dato era presente nelle domande iniziali per l'accesso al finanziamento.

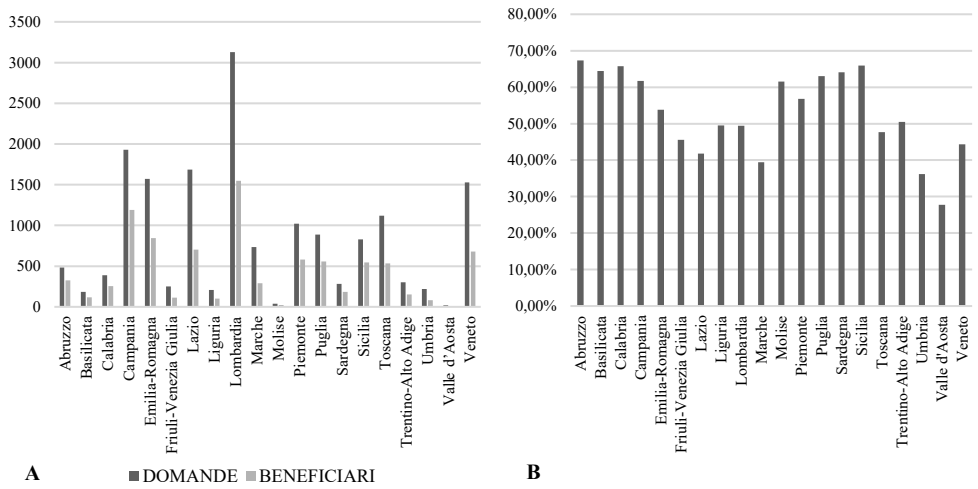
Per analizzare i dati sono stati utilizzati il programma Excel ed il programma SPSS. Il programma Excel ha permesso di creare i grafici e gli istogrammi, mentre il programma SPSS ha permesso di effettuare l'analisi della varianza a due vie per poter capire quali dimensioni avessero un maggiore impatto sulla probabilità di ottenere il finanziamento.

[1] www.rm.camcom.it.

4. Risultati

La Figura 1 mostra i dati relativi alle domande richieste ed ai finanziamenti ottenuti, sia valore assoluto (parte A), sia in percentuale (parte B) rispetto alle regioni di appartenenza. In dettaglio, nella parte A è stato riportato il valore assoluto delle domande presentate in ogni regione e delle relative PMI che hanno ottenuto il finanziamento. Si può notare che le regioni che hanno presentato il maggior numero di domande sono la Lombardia, la Campania e il Lazio. La Lombardia e la Campania sono anche quelle che hanno ottenuto, in valore assoluto, il maggior numero di finanziamenti, mentre l'Emilia-Romagna risulta essere al terzo posto, scavalcando il Lazio. Se, invece, osserviamo la percentuale di PMI finanziate rispetto al totale delle domande presentate in ogni regione (parte B), notiamo che le regioni del sud Italia e delle isole, in particolare Abruzzo, Sicilia, Calabria e Sardegna hanno ottenuto, in proporzione, un maggior numero di finanziamenti. Questo risultato denota una certa dinamicità territoriale delle PMI del sud Italia e delle isole rispetto alla capacità di ottenere dei finanziamenti pubblici. Allo stesso tempo, il dato fa notare che c'è una buona propensione ed attenzione degli imprenditori ad avviare processi e politiche di digitalizzazione ed ammodernamento tecnologico.

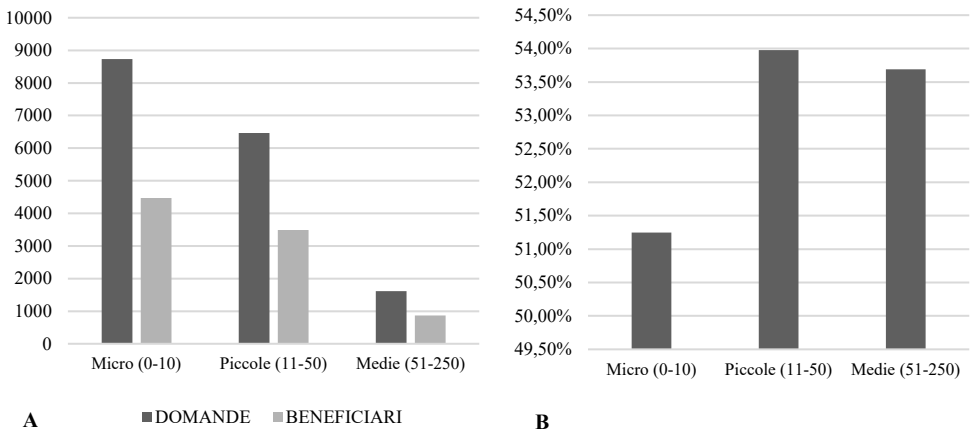
Figura 1. – Beneficiari per regione



La Figura 2 mostra i beneficiari suddivisi per dimensione di impresa. La parte A illustra il valore assoluto delle domande presentate suddivise per dimensione d'impresa e delle relative PMI che hanno ottenuto il finanziamento. Si può notare che la maggior parte delle domande proviene da PMI di micro-dimensioni, cioè imprese

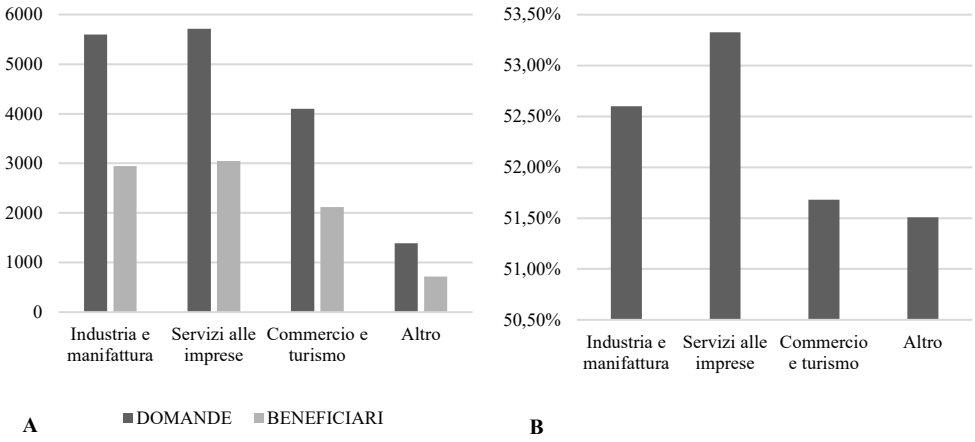
entro i 10 dipendenti. Tuttavia, se si osserva la parte B della figura, il tasso di successo nell'ottenimento del finanziamento è maggiore nelle PMI di piccole e medie dimensioni (con più di 10 dipendenti). Considerando che, l'importo del finanziamento era di massimo 10.000€, esso poteva essere di grande ausilio per le microimprese. Tuttavia, i risultati evidenziano una tendenza inversa, in quanto le componenti di struttura e di dimensione organizzativa sono diventate un elemento discriminante. Infatti, la struttura, le risorse e le competenze interne sono state ritenute importanti per elaborare proposte di successo. È quindi probabile che quelle realtà che mostravano una capacità e solidità finanziaria marcata, o coloro che avessero già dei progetti di digitalizzazione avviati o strutturati siano state preferite.

Figura 2. – Beneficiari per dimensione di impresa



La Figura 3 mostra, invece, le domande ed i beneficiari suddivisi per macro-settori. Quello che si può notare nella parte A è che i settori da dove provengono la maggior parte di domande sono quello dei servizi alle imprese e quelle dell'industria e manifattura. Questi stessi settori sono quelli che presentano un più alto livello di accettazione delle domande, rispetto al totale presentato (parte B). Questo risultato può essere dovuto dal fatto che sia il settore manifatturiero che il settore dei servizi alle imprese hanno una maggiore propensione alla digitalizzazione dei processi, anche attraverso l'acquisto di macchinari o all'acquisizione di nuove licenze software. Pensiamo, ad esempio, a tutto il tema dell'industria 4.0 e dei servizi digitali alle imprese come il *digital marketing* o i servizi di *cybersecurity*. Molto probabilmente questi fattori hanno contribuito in modo significativo ad allineare la proposta di domanda, rispetto alle tematiche del bando.

Figura 3. – Beneficiari per settore

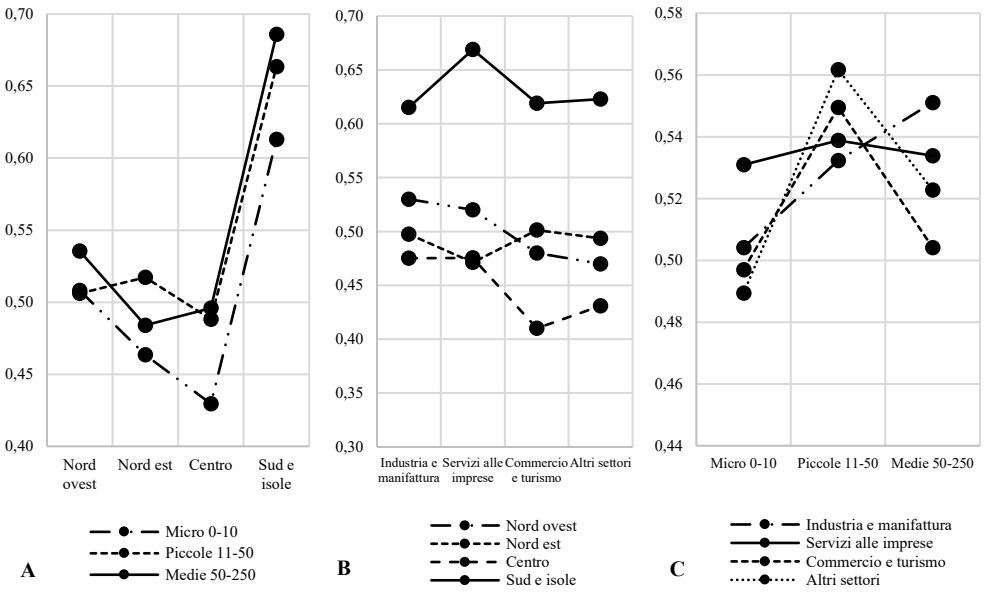


Abbiamo, inoltre, triangolato i risultati rispetto alle variabili d'interesse. La Figura 4 riporta la divisione per area geografica e dimensione d'impresa sulla probabilità di ottenere un finanziamento (parte A); la parte B invece riporta la divisione per settore di appartenenza e area geografica sulla probabilità di ottenere un finanziamento; infine, la parte C riporta la divisione per dimensione d'impresa e settore di appartenenza sulla probabilità di ottenere un finanziamento. La parte A mostra che l'area geografica, e quindi la componente territoriale, è un fattore che impatta sulla probabilità di ottenere il finanziamento. Infatti, il grafico mostra che tutte le PMI del sud Italia hanno avuto un tasso di successo maggiore nell'ottenimento del finanziamento, rispetto alle altre aree geografiche. L'analisi della varianza mostra come questo dato sia statisticamente significativo. Allo stesso tempo, c'è una differenza significativa tra le dimensioni delle imprese per area geografica; le PMI di maggiori dimensioni sono quelle che hanno tendenzialmente avuto maggior successo per l'ottenimento del finanziamento rispetto a tutte le macro-aree territoriali. Questo risultato è in linea con la letteratura recente (Børing et al., 2020). Tuttavia, osservando l'ammontare complessivo del finanziamento suddiviso per regioni, possiamo notare che le PMI del sud Italia hanno ottenuto un maggior numero di finanziamenti complessivi, rispetto alle regioni delle altre aree territoriali, spiegando il perché di questo effetto. Il risultato può anche significare una certa dinamicità territoriale del sud Italia ad avviare politiche di digitalizzazione per le PMI e ad una sensibilità imprenditoriale rispetto all'avvio di processi di digitalizzazione ed ammodernamento tecnologico.

La parte B conferma quanto riportato precedentemente, cioè le PMI situate nell'area sud e isole sono quelle che hanno una maggiore probabilità di ottenere il finanziamento anche rispetto ai settori di appartenenza. Allo stesso tempo, si può osservare come le PMI appartenenti al settore dell'industria e della manifattura nel centro Italia sono quelle che hanno ottenuto maggiori finanziamenti rispetto alle altre

aree territoriali. Mentre le PMI appartenenti al settore dei servizi alle imprese del sud Italia sono quelle che hanno ottenuto maggiori finanziamenti rispetto alle altre aree territoriali e agli altri settori. Infine, la parte C evidenzia come le piccole e medie imprese sono quelle che dimostrano una maggiore dinamicità per quanto riguarda gli investimenti in digitalizzazione. In particolare, le piccole imprese dei settori definiti come "Altro", ossia i settori A, K, P, Q, R, S, T, sono quelle che hanno una maggiore probabilità di ottenere i finanziamenti. Allo stesso tempo, le imprese di medie dimensioni appartenenti al settore dell'industria sono quelle che hanno una maggiore propensione ad ottenere il finanziamento rispetto alle micro e piccole imprese. Infine, le piccole imprese del settore dei servizi alle imprese e del commercio sono quelle che mostrano una maggiore dinamicità nell'ottenimento di finanziamenti pubblici. Nel complesso, le microimprese sono quelle che, rispetto a tutti i settori e rispetto a tutte le dimensioni, hanno maggiori difficoltà nell'ottenimento di fondi pubblici, sintomo di come le dimensioni aziendali siano una determinante importante.

Figura 4. – Probabilità di ottenere finanziamenti pubblici: effetti di area geografica, dimensione d'impresa e settore



5. Discussioni e conclusioni

La letteratura mostra come la digitalizzazione può avere ricadute positive in termini di produttività e competitività delle PMI (Di Vaio and Varriale, 2020; Queiroz

et al., 2020). Studi precedenti dimostrano che il sostegno pubblico può fornire uno dei principali incentivi per favorire l'ammodernamento tecnologico e digitale (Hwang, 2023; Kahle et al., 2020; Khin & Hung Kee, 2022; Ietto et al., 2022; Mahdiraji et al., 2023; Park et al., 2022). Tuttavia, la letteratura ha ancora poco indagato quali siano gli antecedenti che possano favorire l'accesso a finanziamenti pubblici da parte delle PMI. Attraverso l'analisi di un database di oltre 16.000 PMI sul territorio italiano, questo studio ha esplorato come la dimensione aziendale, la regione ed il settore di appartenenza della PMI possano essere considerate delle variabili significative per l'ottenimento di un finanziamento per la digitalizzazione, in particolare *voucher* per la digitalizzazione, erogato dal Ministero delle Imprese e del *Made in Italy* nel 2019.

I risultati mostrano che la localizzazione territoriale, la dimensione dell'impresa e il settore di appartenenza, sono variabili importanti che impattano sulla probabilità di ottenere finanziamenti pubblici. In particolare, è emerso che l'effetto della componente territoriale è abbastanza marcata, in quanto le PMI del sud Italia e delle isole sono quelle che hanno ottenuto maggiori finanziamenti in proporzione. Questo risultato si allinea con la letteratura recente, la quale mostra come la componente territoriale possa essere una dimensione importante per facilitare l'ottenimento di un finanziamento pubblico (Marullo et al., 2024). Ad esempio Piro et al. (2024), evidenziano come le regioni del sud Europa siano quelle che hanno una forte capacità di attrarre finanziamenti pubblici, anche in linea con la politica di coesione Europea. Un altro risultato che si allinea alla letteratura recente è come la dimensione dell'impresa sia una determinante importante nel favorire l'accesso a finanziamenti pubblici. Infatti, i nostri risultati sono molto in linea con quelli di Børing et al. (2020), i quali mostrano come le PMI di piccole dimensioni (11-50 dipendenti) e quelle di medie dimensioni (51-250 dipendenti) abbiano una maggiore probabilità di ottenere finanziamenti Europei, rispetto alle microimprese. Infatti, le realtà di più grandi dimensioni sono anche quelle che hanno maggiori risorse finanziarie, capacità, competenze e struttura, che possono essere delle determinanti per avviare e promuovere significativi progetti di digitalizzazione ed ammodernamento tecnologico ed attrarre capitali pubblici (Pfister & Lehmann, 2024).

In aggiunta, i settori che sembrano essere più sensibili ad avviare processi di digitalizzazione risultano essere quello manifatturiero e dei servizi alle imprese. Anche questo risultato è in linea con la letteratura precedente che mostra come i settori altamente tecnologici, ad esempio quello dei servizi alle imprese e quello manifatturiero, hanno una maggiore propensione ad attrarre risorse pubbliche (Kahle et al., 2020; Marullo et al., 2024; Mulier & Samarin, 2021). I risultati si allineano e rafforzano la letteratura esistente rispetto ai finanziamenti relativi alla digitalizzazione (Marullo et al., 2024), in quanto essi confermano e rafforzano evidenze recenti su come la dimensione di impresa, settore di appartenenza e regione territoriale sono delle determinanti importanti nel favorire l'accesso ai finanziamenti pubblici (Børing et al., 2020; Marullo et al., 2024; Mulier & Samarin, 2021).

I risultati sono particolarmente significativi dal punto di vista delle policy in quanto evidenziano come le determinanti territoriali, di settore e di dimensione

possono avere un'influenza sulla probabilità delle PMI di ottenere dei finanziamenti pubblici. Pertanto, il suggerimento che ne deriva, è quello che da un lato, l'attore pubblico dovrebbe continuare a sostenere le attività di digitalizzazione delle PMI in quanto hanno delle ricadute dirette e positive (Kleine et al., 2022; Mina et al., 2021). Dall'alto nell'elaborazione dei bandi si dovrebbero tenere conto anche degli aspetti organizzativi, territoriali e di settore. I nostri risultati suggeriscono inoltre di aumentare l'efficacia dei programmi di *voucher* per la digitalizzazione, ad esempio, concentrandosi sulle piccole imprese e dando delle linee guida più precise per quanto riguarda poi gli investimenti diretti, ad esempio stabilendo criteri più specifici per quanto riguarda l'utilizzo di tale finanziamento.

Per concludere, il presente studio presenta alcuni limiti. Il primo fra tutti è rappresentato dalla descrizione molto generica del bando del *Voucher* per la digitalizzazione, il quale non specifica criteri e modalità utilizzate per determinare l'esito positivo alla richiesta di finanziamento effettuata da parte delle imprese. Inoltre, la raccolta di dati basata su AIDA presenta dati molto aggregati e, di conseguenza, possono mancare di specificità quando si tratta di trarre conclusioni più dettagliate su aspetti particolari dell'attività aziendale.

Messaggi chiave:

- I finanziamenti pubblici sono chiave per sostenere la digitalizzazione delle piccole e medie imprese.
- Dimensione, settore e regione di appartenenza sono delle variabili che influenzano la probabilità di ottenere finanziamenti pubblici da parte delle PMI.
- Nel territorio italiano sono presenti delle differenze nelle capacità di accesso a finanziamenti pubblici da parte delle PMI.

Bibliografia

Ardito, L., Raby, S., Albino, V. & Bertoldi, B. (2021). The duality of digital and environmental orientations in the context of SMEs: Implications for innovation performance. *Journal of Business Research, 123*, 44-56.

Børing, P., Fevolden, A.M., Mark, M.S. & Piro, F.N. (2020). Bringing home the bacon: The relationship between firm characteristics and participation in EU Horizon 2020 projects. *Applied Economics Letters, 27*(19), 1556-1561.

Bouncken, R. & Barwinski, R. (2021). Shared digital identity and rich knowledge ties in global 3D printing – A drizzle in the clouds? *Global Strategy Journal*, *11*(1), 81-108.

Brougham, D. & Haar, J. (2018). Smart technology, artificial intelligence, robotics, and algorithms (STARA): Employees' perceptions of our future workplace. *Journal of Management & Organization*, *24*(2), 239-257.

Chung, H. & Kim, K. (2023). Can open innovation improve technological outcomes for digital transformation? Structural approach to strategic decisions of Korean ICT SMEs. *Managerial and Decision Economics*, *44*(8), 4404-4421.

Curzi, Y. & Ferrarini, F. (2024). High-performance work systems and firm innovation: The moderating role of digital technology and employee participation. Evidence from Europe. *Management Research Review*, *47*(13), 51-68.

Del Giudice, M. (2016). Discovering the Internet of Things (IoT) within business process management: A literature review on technological revitalization. *Business Process Management Journal, 22*(2), 263-270.

Di Vaio, A. & Varriale, L. (2020). Digitalization in the sea–land supply chain: Experiences from Italy in rethinking port operations within inter-organizational relationships. *Production Planning & Control*, *31*(2-3), 220-232.

Dvouletý, O., Srhoj, S. & Pantea, S. (2021). Public SME grants and firm performance in the European Union: A systematic review of empirical evidence. *Small Business Economics*, *57*(1), 243-263.

Estensoro, M., Larrea, M., Müller, J.M. & Sisti, E. (2022). A resource-based view on SMEs regarding the transition to more sophisticated stages of Industry 4.0. *European Management Journal, 40*(5), 778-792.

European Commission (2022). *Digital economy and society index (DESI)*. https://digital-strategy.ec.europa.eu/en/policies/desi.

Freund, C.L. & Weinhold, D. (2004). The effect of the internet on international trade. *Journal of International Economics, 62*(1), 171-189.

Galope, R.V. (2014). What types of start-ups receive funding from the Small Business Innovation Research (SBIR) program? Evidence from the Kauffman Firm Survey. *Journal of Technology Management & Innovation*, *9*(2), 17-28.

Gierlich, M., Schüritz, R., Volkwein, M. & Hess, T. (2019). SMEs' approaches for digitalization in platform ecosystems. In *Proceedings of the Twenty-Third Pacific Asia Conference on Information Systems (PACIS 2019)* (Paper 190).

Hagsten, E. & Kotnik, P. (2017). ICT as facilitator of internationalisation in small- and medium-sized firms. *Small Business Economics*, *48*, 431-446. https://doi.org/10.1007/s11187-016-9781-2.

Huynh, D.C., Van Nguyen, P., Quynh Truong, G. & Quang Bui, T. (2025). The interplay of government support, open innovation, and dynamic capabilities: Driving ambidexterity and performance in Vietnam. *Journal of Open Innovation: Technology, Market, and Complexity*, 100621.

Hwang, I. (2023). Evolution of the collaborative innovation network in the Korean ICT industry: A patent-based analysis. *Technology Analysis & Strategic Management*, *35*(2), 221-236.

Ietto, B., Ancillai, C., Sabatini, A., Carayannis, E.G. & Gregori, G.L. (2022). The role of external actors in SMEs'human-centered Industry 4.0 adoption: An empirical perspective on Italian competence centers. *IEEE Transactions on Engineering Management*, *71*, 1057-1072.

ISTAT (2020). *Descrizione dei dati geografici dei confini delle unità amministrative a fini statistici*.

Joshi, K., Chi, L., Datta, A. & Han, S. (2010). Changing the competitive landscape: Continuous innovation through IT-enabled knowledge capabilities. *Information Systems Research*, *21*(3), 472-495.

Kahle, J.H., Marcon, É., Ghezzi, A. & Frank, A.G. (2020). Smart products value creation in SMEs innovation ecosystems. *Technological Forecasting and Social Change*, *156*, 120024.

Khin, S. & Hung Kee, D.M. (2022). Identifying the driving and moderating factors of Malaysian SMEs'readiness for Industry 4.0. *International Journal of Computer Integrated Manufacturing*, *35*(7), 761-779.

Kitsios, F. & Kamariotou, M. (2017). Decision support systems and strategic information systems planning for strategy implementation. In A. Kavoura, D. Sakas & P. Tomaras (Eds.), *Strategic innovative marketing* (pp. 327-332). Springer. https://doi.org/10.1007/978-3-319-56288-9_43.

Kleine, M., Heite, J. & Rosendahl Huber, L. (2022). Subsidized R&D collaboration: The causal effect of innovation vouchers on innovation outcomes. *Research Policy*, 104515.

Kolade, O., Obembe, D. & Salia, S. (2019). Technological constraints to firm performance: The moderating effects of firm linkages and cooperation. *Journal of Small Business and Enterprise Development*, *26*(1), 85-104.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M.S. & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value. *MIT Sloan Management Review*, *52*, 21-32.

Lee, J., Lapira, E., Bagheri, B. & Kao, H.A. (2013). Recent advances and trends in predictive manufacturing systems in big data environment. *Manufacturing Letters*, *1*(1), 38-41.

Li, S., Yang, Z. & Tian, Y. (2023). Digital transformation and corporate performance: Evidence from China. *China Economic Journal*, *16*(3), 312-334.

Mahdiraji, H.A., Yaftiyan, F., Abbasi-Kamardi, A., Jafari-Sadeghi, V., Sahut, J.M. & Dana, L.P. (2023). A synthesis of boundary conditions with adopting digital platforms in SMEs: An intuitionistic multi-layer decision-making framework. *The Journal of Technology Transfer, 48*(5), 1723-1751.

Marullo, C., Shapira, P. & Di Minin, A. (2024). Enhancing SME innovation across European regions: Success factors in. *Technological Forecasting and Social Change*, 123207.

Miles, M.B., Huberman, A.M. & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE.

MIMIT (2025, settembre 15). *Capitale di rischio per lo sviluppo di PMI*. https://www.mimit.gov.it/it/incentivi/fondo-di-investimento-nel-capitale-di-rischio-per-lo-sviluppo-di-piccole-e-medie-imprese.

MIMIT (2025, settembre 15). *Fondo di garanzia per le PMI*. https://www.mimit.gov.it/it/incentivi/fondo-di-garanzia-per-le-pmi.

MIMIT (2025, settembre 11). *Voucher digitalizzazione*. Ministero delle Imprese e del Made in Italy. https://www.mimit.gov.it/it/assistenza/domande-frequenti.

Mina, A., Di Minin, A., Martelli, I., Testa, G. & Santoleri, P. (2021). Public funding of innovation: Exploring applications and allocations of the European SME Instrument. *Research Policy*, *50*(1), 104131.

Mulier, K. & Samarin, I. (2021). Sector heterogeneity and dynamic effects of innovation subsidies: Evidence from Horizon 2020. *Research Policy*, *50*(10), 104346.

Oliveira, M.I.S., Barros Lima, G.D.F. & Farias Lóscio, B. (2019). Investigations into data ecosystems: A systematic mapping study. *Knowledge and Information Systems*, *61*(2), 589–630. https://doi.org/10.1007/s10115-018-1323-6.

Park, J., Kim, J., Woo, H. & Yang, J.S. (2022). Opposite effects of R&D cooperation on financial and technological performance in SMEs. *Journal of Small Business Management*, *60*(4), 892-925.

Pfister, P. & Lehmann, C. (2024). Digital value creation in German SMEs: A return-on-investment analysis. *Journal of Small Business & Entrepreneurship*, *36*(4), 548-573.

Piro, F.N., Seeber, M. & Wang, L. (2024). Regional and sectoral variations in the ability to attract funding from the European Union's Seventh Framework Programme and Horizon 2020. *Scientometrics, 129*(3), 1493–1521.

Popovič, A., Hackney, R., Tassabehji, R. & Castelli, M. (2018). The impact of big data analytics on firms' high-value business performance. *Information Systems Frontiers*, 209-222.

Prodi, E., Tassinari, M., Ferrannini, A. & Rubini, L. (2022). Industry 4.0 policy from a sociotechnical perspective: The case of German competence centers. *Technological Forecasting and Social Change*, *175*, 121341.

Queiroz, M.M., Wamba, S.F., Machado, M.C. & Telles, R. (2020). Smart production systems drivers for business process management improvement. *Business Process Management Journal*, 26(5), 1075-1092.

Radicic, D. & Petkovic, S. (2023). Impact of digitalization on technological innovations in small and medium-sized enterprises (SMEs). *Technological Forecasting and Social Change*, 191, 122474.

Ramalli, E. & Pernici, B. (2023). Challenges of a data ecosystem for scientific data. *Data & Knowledge Engineering*, *148*, 102236. https://doi.org/10.1016/j.datak.2023.102236.

Rubino, M., Vitolla, F., Raimo, N. & Garzoni, A. (2019). Cultura nazionale e livello di digitalizzazione delle imprese europee: Evidenze empiriche. In F. Culasso & M. Pizzo (Eds.), *Identità, innovazione e impatto dell'aziendalismo italiano*. Università di Torino.

Satı, Z.E. (2024). Comparison of the criteria affecting the digital innovation performance of the European Union (EU) member and candidate countries with the entropy weight–TOPSIS method and investigation of its importance for SMEs. *Technological Forecasting and Social Change*, *200*, 123094. https://doi.org/10.1016/j.techfore.2023.123094.

Wedel, M. & Kannan, P.K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing, 80*(6), 97-121.

Wu, L., Hitt, L. & Lou, B. (2020). Data analytics, innovation, and firm productivity. *Management Science*, *66*(5), 2017-2039.

Zott, C. & Amit, R. (2017). Business model innovation: How to create value in a digital world. *NIM Marketing Intelligence Review*, *9*(1), 18.

Le PMI negli ecosistemi di dati: barriere, tensioni e ruoli nella governance dei dati

Simona Leonelli [*], Filippo Ferrarini [**] e Tommaso Fabbri [***]

Abstract: La crescente importanza dei dati come risorsa strategica sta favorendo la nascita degli ecosistemi di dati, ambienti collaborativi in cui diversi attori condividono e utilizzano informazioni per generare valore. Le piccole e medie imprese (PMI) possono essere attori chiave in questi ecosistemi, tuttavia la loro partecipazione è spesso ostacolata da barriere economiche, tecnologiche ed organizzative, nonché da tensioni legate alla governance e alla distribuzione del valore. Il presente capitolo analizza tali criticità e indaga i ruoli che le PMI possono assumere all'interno degli ecosistemi di dati, evidenziando come il superamento delle barriere e la gestione delle tensioni possano trasformarle da utenti periferici a co-creatrici e co-governatrici del valore. Viene proposto un modello concettuale integrato che collega barriere, tensioni e ruoli, offrendo riflessioni teoriche e implicazioni pratiche per favorire modelli di governance inclusiva e sostenibile, basati su fiducia, interoperabilità e partecipazione attiva.

Parole chiave: PMI, ecosistemi di dati, barriere, governance, tensioni.

1. Introduzione

Nell'attuale scenario economico e tecnologico, i dati sono diventati una delle risorse più strategiche per la creazione di valore, rappresentando il fulcro di trasformazioni economiche, sociali e organizzative di vasta portata (Zeng & Glaister, 2018). La progressiva *datafication* dei processi produttivi e decisionali ha reso i dati non solo un input per l'innovazione, ma anche un asset competitivo capace di ridefinire le logiche di mercato, la struttura delle relazioni tra organizzazioni e il funzionamento dei sistemi

[*] Simona Leonelli (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: simona.leonelli@unimore.it

[**] Filippo Ferrarini (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: filippo.ferrarini@unimore.it

[***] Tommaso Fabbri (✉)
Dipartimento di Economia Marco Biagi, Università di Modena e Reggio Emilia, Italia.
E-mail: tommaso.fabbri@unimore.it

DOI: 10.82018/9791221165456-5

economici nel loro complesso (Micheli et al., 2020). Di conseguenza, la gestione e la condivisione dei dati non sono più attività isolate, bensì processi interconnessi e cooperativi che coinvolgono una pluralità di attori pubblici e privati.

Tale trasformazione ha portato all'emergere dei cosiddetti ecosistemi di dati, definiti come reti sociotecniche in cui attori eterogenei, tra cui imprese, istituzioni pubbliche, centri di ricerca e cittadini, collaborano per creare, condividere e utilizzare dati a fini di innovazione e sviluppo (Brechtel et al., 2023). Gli ecosistemi di dati si fondano sull'idea che il valore dei dati non risieda nella loro mera disponibilità, ma nella capacità di metterli in relazione, generando nuove conoscenze e opportunità di business attraverso processi di interscambio e co-creazione (Oliveira et al., 2019; Micheli et al., 2020).

L'interesse per questi ecosistemi è cresciuto parallelamente all'espansione dell'economia dei dati (*data economy*), sostenuta da iniziative istituzionali e politiche europee come la Strategia Europea per i Dati e la creazione dei Common European Data Spaces (European Commission, 2020a). Queste iniziative promuovono un modello di circolazione sicura, equa e trasparente dei dati, fondato su principi di interoperabilità, sovranità digitale e fiducia reciproca tra i partecipanti (Farrell et al., 2023). Tuttavia, la costruzione di tali ecosistemi pone sfide rilevanti in termini di governance, infrastruttura tecnica e partecipazione attiva dei diversi attori coinvolti.

In particolare, il coinvolgimento delle piccole e medie imprese (PMI) rappresenta una delle principali sfide e, al contempo, una delle maggiori opportunità per la sostenibilità e la crescita degli ecosistemi di dati. Le PMI costituiscono la spina dorsale del tessuto economico europeo, generando oltre due terzi dell'occupazione e della ricchezza prodotta nell'Unione (European Commission, 2020b). Esse dispongono di flessibilità organizzativa, capacità di innovazione incrementale e prossimità ai mercati locali, caratteristiche che le rendono attori ideali per contribuire alla generazione di valore all'interno degli ecosistemi di dati (Otto et al., 2022; Jiang et al., 2023).

Nonostante ciò, la letteratura mostra come molte PMI incontrino barriere strutturali, culturali e tecnologiche che ne ostacolano la partecipazione attiva e la capacità di trarre vantaggio dall'uso dei dati (Ajibade et al., 2019; Gierlich et al., 2019). Tali difficoltà derivano da limitate risorse economiche, infrastrutture IT obsolete, carenze di competenze digitali e incertezza normativa in materia di data governance. Inoltre, anche quando le PMI entrano negli ecosistemi di dati, devono affrontare tensioni legate alla distribuzione del potere, alla fiducia e alla gestione dei diritti di accesso e utilizzo dei dati (Heinz et al., 2022; Lnenicka et al., 2024).

Alla luce di queste considerazioni, il presente capitolo si propone di analizzare tre questioni fondamentali: (i) Quali sono le principali barriere che le PMI devono affrontare prima di entrare a far parte degli ecosistemi di dati? (ii) In che modo le tensioni che emergono negli ecosistemi di dati si manifestano e influenzano le PMI? (iii) Quali ruoli possono assumere le PMI nella governance e nella creazione di valore all'interno di tali ecosistemi?

Comprendere come e in che misura le PMI riescano a superare tali ostacoli, e quale contributo possano offrire alla governance e alla co-creazione di valore negli ecosistemi di dati, rappresenta dunque una questione cruciale sia dal punto di vista

teorico che pratico. Infatti, attraverso l'integrazione della letteratura teorica e l'analisi di evidenze empiriche recenti, il capitolo intende contribuire alla limitata letteratura sul tema, fornendo lo spunto per un dibattito sulla partecipazione delle PMI negli ecosistemi di dati, offrendo una prospettiva che unisce le dimensioni tecnologica, organizzativa e istituzionale della digitalizzazione con quelle sociali e collaborative che caratterizzano la nuova economia dei dati. Invece, dal punto di vista pratico, il contributo di questo capitolo è in particolare per gli imprenditori e i policy maker, sottolineando l'importanza dell'identificazione di leve, strumenti e modelli di governance inclusiva, fondamentali per garantire una partecipazione equa e sostenibile all'interno degli ecosistemi di dati.

2. Gli ecosistemi di dati: concetto, attori e logiche di governance

Il concetto di ecosistema di dati nasce dall'incontro tra le prospettive dell'ecosistema dell'innovazione e della gestione dei dati. Gli ecosistemi di dati possono essere definiti come reti inter-organizzative e sociotecniche in cui diversi attori collaborano per condividere, combinare e utilizzare dati con l'obiettivo di creare valore economico e sociale (Oliveira et al., 2019; Micheli et al., 2020). Essi non rappresentano semplici network di collaborazione, ma sistemi complessi basati su relazioni dinamiche e interdipendenze multiple, che coinvolgono dimensioni tecnologiche, organizzative e istituzionali (Heinz et al., 2022).

Di conseguenza, negli ecosistemi di dati, la governance svolge un ruolo cruciale. I meccanismi di governance definiscono le politiche, le pratiche e gli standard per assicurare qualità, sicurezza e conformità nell'uso e nella condivisione dei dati (Lis & Otto, 2020; Nikolakopoulos et al., 2023). La sua finalità è creare un ecosistema equilibrato, basato su regole trasparenti e condivise, che garantiscano fiducia e cooperazione tra gli attori.

In Europa, l'interesse verso tali dinamiche è testimoniato dalla creazione dei Common European Data Spaces, promossi dalla Strategia Europea per i Dati (European Commission, 2020a). Tali spazi collaborativi rappresentano infrastrutture decentralizzate progettate per favorire la condivisione, l'interoperabilità e il riutilizzo dei dati in modo sicuro e affidabile (Farrell et al., 2023; Schneider et al., 2024). Il modello tecnologico di riferimento è quello degli International Data Spaces (IDS), che si fondano su architetture federate e standard comuni per garantire interoperabilità e fiducia tra le organizzazioni (Duisberg, 2022; Pettenpohl et al., 2022).

All'interno di questi ecosistemi, le PMI potrebbero ottenere benefici tangibili, quindi ad esempio creare un ritorno economico maggiore, ma anche intangibili avendo, ad esempio, dei benefici dal punto di vista strategico (Pfister & Lehmann, 2024). Inoltre, all'interno degli ecosistemi di dati, le PMI potrebbero ricoprire dei ruoli differenti – come fornitrici di dati, utilizzatrici, o intermediarie tecnologiche – contribuendo a rendere il sistema più dinamico e resiliente (Jiang et al., 2023). Alla

luce di questo inquadramento, è utile analizzare come la letteratura recente abbia affrontato il tema del rapporto tra PMI ed ecosistemi di dati, evidenziando i principali filoni teorici e le direzioni di ricerca emergenti. Questa rassegna consente di delineare il quadro concettuale di riferimento per le sezioni successive, dedicate all'analisi delle barriere, delle tensioni e dei ruoli assunti dalle PMI negli ecosistemi di dati.

2.1. La letteratura sugli ecosistemi di dati e il ruolo delle PMI

Negli ultimi anni, la letteratura sugli ecosistemi di dati ha conosciuto un rapido sviluppo, alimentato dal crescente riconoscimento del valore strategico dei dati come risorsa economica e organizzativa. Tuttavia, pur essendo un campo in espansione, gli studi presentano ancora una certa frammentazione e un'attenzione limitata al ruolo delle PMI. A partire da un'analisi approfondita dei contributi più significativi, è possibile individuare quattro principali filoni di ricerca, che rappresentano altrettanti modi di interpretare la relazione tra PMI e gli ecosistemi di dati. In dettaglio, gli studi in letteratura si sono concentrati sulla governance dei dati e delle infrastrutture digitali, sull'innovazione e la supply chain, sulla proprietà intellettuale e la tutela del valore dei dati e sulla sostenibilità e le tecnologie emergenti.

Gli studi che si concentrano sui temi della data governance, dei data spaces e della gestione dei big data affermano che essi possono essere definiti i pilastri teorici e operativi della creazione di valore negli ecosistemi di dati (Micheli et al., 2020; Jordão & Novas, 2024). La gestione efficiente e sicura dei dati è considerata un fattore che favorisce la collaborazione tra attori eterogenei, tra cui le PMI (Rehm et al., 2017). La *data architecture* diventa un elemento chiave per garantire l'interoperabilità, la qualità e la sicurezza dei flussi informativi (Bode et al., 2024). Le PMI che dispongono di architetture deboli o frammentate incontrano difficoltà di integrazione e di *compliance* ai modelli di governance, con ricadute sulla loro capacità di sfruttare pienamente il potenziale dei dati (Nikolakopoulos et al., 2023). Quindi, una governance dei dati efficace consente di ridurre le asimmetrie informative e di potere, promuovendo ecosistemi più inclusivi e democratici, dove le PMI possono contribuire in modo attivo alla generazione di valore (Wulf & Butel, 2017).

Il secondo filone riguarda la relazione tra ecosistemi di dati, innovazione e supply chain management, con particolare riferimento al contesto dell'Industria 4.0. Le PMI sono viste come agenti chiave di innovazione lungo la catena di fornitura, in grado di introdurre flessibilità, creatività e velocità di risposta nei processi produttivi e logistici (Aghazadeh et al., 2024; Chen et al., 2024). L'integrazione dei dati tra i diversi attori della filiera consente non solo di migliorare la pianificazione e la tracciabilità, ma anche di supportare modelli di business digitali in settori tradizionali, come l'automotive, in cui i dati abilitano nuove forme di mobilità e servizi personalizzati (Pérez-Moure et al., 2024). Infine, la letteratura più recente sottolinea che le PMI che fanno un uso strategico dei big data riescono a rafforzare le proprie capacità di

innovazione grazie a processi di co-creazione multi-attore (Alzoubi & Yanamandra, 2024; Büyükselçuk, 2024).

Il terzo filone analizza il ruolo dei diritti di proprietà intellettuale come leva per la partecipazione e la collaborazione negli ecosistemi di dati. La presenza di adeguati meccanismi di tutela della proprietà industriale è considerata un incentivo cruciale per le PMI, che si sentono più protette da eventuali comportamenti opportunistici degli altri attori e, perciò, più inclini a condividere dati e conoscenze (Yuan & Li, 2024). Diversi studi dimostrano che la protezione della proprietà intellettuale amplifica gli effetti positivi della partecipazione agli ecosistemi di dati sulla performance aziendale, rafforzando al contempo il capitale intellettuale delle imprese e dell'intero ecosistema (Ceccagnoli et al., 2012; Cunningham & Link, 2014; Rosyadi et al., 2020). Questa prospettiva, sebbene meno diffusa, suggerisce l'importanza di sviluppare modelli di governance che integrino meccanismi di protezione e di equa distribuzione del valore.

Infine, l'ultimo filone di studi, ancora in rapido sviluppo, esplora il legame tra ecosistemi di dati, sostenibilità e trasformazione digitale. Le PMI dotate di una maggiore sensibilità ambientale tendono a utilizzare i dati per promuovere innovazione verde, trasparenza e collaborazione con attori pubblici nell'ambito della transizione ecologica (Chen et al., 2024). Allo stesso tempo, stanno emergendo ricerche sull'uso dei social media e dei social network come strumenti per la costruzione di relazioni collaborative negli ecosistemi di dati (Gruner & Power, 2018; Scherer et al., 2015). Infine, l'adozione di tecnologie cloud rappresenta un ulteriore ambito di interesse, considerato essenziale per abilitare l'interoperabilità e la condivisione dei dati, ma ancora ostacolato da problemi di standardizzazione e integrazione tra piattaforme (Mujinga, 2020; Ghosh et al., 2011).

Le evidenze raccolte offrono una base teorica solida per le sezioni successive, che approfondiscono le barriere, le tensioni e i ruoli delle PMI negli ecosistemi di dati.

3. Barriere alla partecipazione delle PMI negli ecosistemi di dati

Nonostante il potenziale offerto dagli ecosistemi di dati, molte PMI non sono ancora in grado di parteciparvi attivamente o di trarre pieno vantaggio dall'uso dei dati (European Commission, 2020b; Otto et al., 2022). Le difficoltà principali si possono ricondurre a tre macrocategorie di barriere: (i) economiche e infrastrutturali, (ii) organizzative e culturali, e (iii) normative e relazionali.

La partecipazione agli ecosistemi di dati richiede investimenti significativi in infrastrutture tecnologiche, piattaforme digitali, sistemi di cybersecurity e strumenti di analisi (Kitsios et al., 2017; Oliveira et al., 2019). Tuttavia, molte PMI dispongono di risorse finanziarie limitate, che non consentono di sostenere pienamente i costi di digitalizzazione e aggiornamento tecnologico (Ajibade et al., 2019; Cenamor et al., 2019). Inoltre, le infrastrutture IT delle PMI risultano spesso obsolete o scarsamente

integrate, rendendo difficile l'adozione di standard interoperabili e la condivisione dei dati con altri attori (Gierlich et al., 2019). Questa situazione introduce le cosiddette barriere economiche e infrastrutturali (i), che producono una condizione di svantaggio strutturale, che può ampliare il divario digitale rispetto alle grandi imprese (Aldossari et al., 2023; Järvenpää et al., 2023).

Oltre agli ostacoli economici, le PMI si trovano ad affrontare significative barriere organizzative e culturali (ii). In molti casi, esse non hanno una cultura aziendale orientata ai dati (*data-driven culture*) e tendono a percepire la condivisione dei dati come un rischio piuttosto che come un'opportunità di crescita (Jiang et al., 2023). Inoltre, la mancanza di competenze digitali e analitiche, sia a livello tecnico sia manageriale, limita la capacità delle imprese di comprendere il potenziale strategico dei dati e, di conseguenza, la necessità di integrarli nei processi decisionali (Adhiatma et al., 2023). Inoltre, strutture organizzative rigide e processi decisionali accentrati possono ostacolare la diffusione di pratiche collaborative e di governance condivisa (Georgescu et al., 2022).

Infine, un ulteriore ostacolo alla partecipazione è rappresentato dalle incertezze normative e dalla mancanza di fiducia tra gli attori (iii). Le PMI, infatti, non dispongono sempre delle competenze legali necessarie per gestire questioni relative alla proprietà dei dati, alla privacy o alla conformità al GDPR (Li & Mei, 2024). Inoltre, la riluttanza a condividere dati con soggetti esterni deriva spesso dal timore di perdere il controllo sulle informazioni o di subire appropriazioni del valore creato (Bianchini & Michalkova, 2019). La costruzione di meccanismi di fiducia e di regole trasparenti di governance è dunque una condizione essenziale per favorire la collaborazione inter-organizzativa e la sostenibilità a lungo termine degli ecosistemi di dati (Lis & Otto, 2020; Micheli et al., 2020).

4. Le tensioni negli ecosistemi di dati dal punto di vista delle PMI

Gli ecosistemi di dati sono sistemi complessi e dinamici nei quali attori eterogenei interagiscono in modo interdipendente. Tale pluralità genera un ambiente fertile per l'innovazione e la creazione di valore condiviso, ma al tempo stesso produce tensioni strutturali che possono compromettere la stabilità e l'efficacia della collaborazione (Heinz et al., 2022; Lnenicka et al., 2024).

Nel caso delle PMI, queste tensioni risultano particolarmente evidenti, poiché esse operano in una posizione di relativa debolezza rispetto ad altri attori dotati di maggiori risorse economiche, tecniche e politiche (Otto et al., 2022). Le tensioni si manifestano su più dimensioni, tra cui asimmetrie di potere, contrasti tra apertura e protezione dei dati, differenze nei meccanismi di governance e divergenze temporali e strategiche.

Per quanto concerne le asimmetrie di potere, le PMI, pur essendo fonti rilevanti di dati e competenze, si trovano spesso in una posizione subordinata, con una

capacità limitata di influenzare le decisioni strategiche e i processi di governance (Li & Mei, 2024). Le grandi organizzazioni o le pubbliche amministrazioni, al contrario, tendono a detenere il controllo sulle infrastrutture tecnologiche, sugli standard di interoperabilità e sui modelli di business, determinando un disequilibrio strutturale all'interno dell'ecosistema (Heinz et al., 2022). Questa disparità può generare forme di dipendenza tecnologica e informativa, che riducono l'autonomia decisionale delle PMI e ne limitano la capacità di appropriazione del valore derivante dai dati condivisi. Secondo Micheli et al. (2020), tali tensioni si riflettono nella definizione delle regole di accesso e utilizzo dei dati, spesso orientate dagli interessi degli attori dominanti. Le PMI, in questo senso, rischiano di diventare *price-taker* all'interno del mercato dei dati, partecipando a logiche definite da altri piuttosto che contribuire attivamente alla loro costruzione.

Inoltre, per quanto riguarda il bilanciamento tra apertura e protezione, gli ecosistemi di dati si fondano sul principio della condivisione e del riutilizzo dei dati per generare valore collettivo; tuttavia, per le PMI, tale condivisione implica rischi di perdita di vantaggio competitivo e appropriazione indebita delle informazioni (Lis & Otto, 2020). La necessità di garantire trasparenza e interoperabilità si scontra con l'esigenza di proteggere dati sensibili o strategici. Ciò si traduce in dilemmi organizzativi che portano a dover scegliere fino a quanto dover aprirsi alla collaborazione senza compromettere la propria sicurezza o riservatezza. Inoltre, le PMI sono spesso penalizzate dalla complessità dei requisiti legali e tecnici relativi alla protezione dei dati, come le norme sul GDPR o i protocolli di cybersecurity, che richiedono risorse e competenze non sempre disponibili (Bianchini & Michalkova, 2019; Nikolakopoulos et al., 2023). Questa tensione tra apertura e protezione sottolinea la necessità di una governance adattiva e multilivello, capace di bilanciare incentivi alla condivisione e strumenti di tutela. In tale prospettiva, la fiducia emerge come condizione essenziale per la sostenibilità degli ecosistemi (Micheli et al., 2020; Jiang et al., 2023).

Un'ulteriore forma di tensione si manifesta nel rapporto tra governance centralizzata e autonomia degli attori locali. Negli ecosistemi di dati, la definizione delle regole di funzionamento può avvenire in modo top-down, soprattutto quando la leadership è esercitata da attori pubblici o da grandi imprese (Heinz et al., 2022). In questi casi, le PMI hanno spesso un ruolo marginale nei processi di decision-making, venendo coinvolte solo in fasi operative o di implementazione. Tuttavia, una governance eccessivamente centralizzata può compromettere la flessibilità e la capacità di adattamento del sistema. Le PMI, infatti, operano in contesti locali e settoriali differenti, dove l'eterogeneità delle competenze e dei bisogni richiede approcci personalizzati. Come sottolineano Oliveira et al. (2019), la sostenibilità di un ecosistema dipende dalla capacità di coniugare meccanismi di coordinamento centralizzati con forme di autonomia distribuita, che consentano agli attori minori di contribuire attivamente ai processi di innovazione e creazione di valore. Le PMI possono dunque diventare agenti di equilibrio tra standardizzazione e adattabilità, promuovendo pratiche di governance partecipativa e soluzioni contestuali, coerenti con le proprie capacità organizzative e territoriali.

Infine, un ultimo tipo di tensione riguarda la dimensione temporale. Le PMI operano con risorse limitate e orizzonti di investimento più brevi rispetto alle grandi imprese o agli enti pubblici. I benefici derivanti dalla partecipazione a un ecosistema di dati, tuttavia, tendono a manifestarsi nel lungo periodo, richiedendo un impegno costante in termini di risorse, adattamento tecnologico e coordinamento (Adhiatma et al., 2023). Questa asimmetria temporale può generare disallineamenti strategici: mentre gli attori più grandi possono permettersi di sostenere progetti di lungo respiro, le PMI necessitano di risultati tangibili in tempi più rapidi per giustificare gli investimenti (Costa-Climent et al., 2023). Inoltre, la rapida evoluzione delle tecnologie digitali comporta la necessità di aggiornare continuamente infrastrutture e competenze, aumentando la pressione sulle PMI.

La gestione di queste tensioni rappresenta, quindi, un aspetto cruciale per garantire la partecipazione equa delle PMI e la sostenibilità dell'ecosistema nel lungo periodo (Li & Mei, 2024).

5. I ruoli delle PMI nella governance degli ecosistemi di dati

Come già illustrato nel paragrafo precedente, la partecipazione delle PMI agli ecosistemi di dati non si limita a una funzione passiva o di semplice utilizzo delle risorse altrui. Al contrario, le PMI potrebbero assumere ruoli differenti e complementari che contribuiscono al funzionamento complessivo della governance dei dati, alla creazione di valore condiviso e alla sostenibilità dell'ecosistema nel tempo (Jiang et al., 2023; Otto et al., 2022).

Sebbene la letteratura accademica su questo tema sia ancora frammentata (Oliveira & Lóscio, 2018), è possibile individuare quattro ruoli che le PMI potrebbero ricoprire: (a) fornitore di dati (*data provider*), (b) utilizzatore dei dati (*data user*), (c) intermediario tecnologico (*data enabler*) e (d) co-governatore dell'ecosistema (*co-governor*). Questi ruoli non sono statici, ma evolvono nel tempo, riflettendo la natura dinamica e multilivello della governance negli ecosistemi di dati (Heinz et al., 2022).

Le PMI sono considerate fornitrici di dati (a) quando dopo aver raccolto le informazioni generate dai processi produttivi, dalle transazioni commerciali, dalle attività logistiche o dall'interazione con i clienti condividono i propri dati con l'intero ecosistema (Kitsios et al., 2017). Questi dati, anche se spesso sono granulari e settoriali, rappresentano un elemento di grande valore per l'intero ecosistema, poiché contribuiscono ad aumentare la varietà e la qualità dei dataset condivisi (Li & Mei, 2024). Tuttavia, per poter assumere questo ruolo, le PMI devono sviluppare capacità di gestione e standardizzazione dei dati, garantendo qualità, sicurezza e interoperabilità (Oliveira et al., 2019). Quindi, la loro partecipazione è strettamente legata alla capacità di adottare strumenti digitali adeguati e di instaurare relazioni di fiducia con gli altri attori dell'ecosistema (Micheli et al., 2020). Le PMI fornitrici di dati svolgono dunque una funzione fondamentale nella circolazione e arricchimento dei dati

all'interno dell'ecosistema, pur mantenendo un ruolo delicato nella tutela della proprietà e del valore informativo dei propri asset digitali (Lis & Otto, 2020).

Le PMI possono partecipare agli ecosistemi di dati come utilizzatrici e beneficiarie di dati (b), accedendo a dati condivisi, provenienti da enti pubblici, grandi imprese o altre PMI. L'integrazione dei dati provenienti dall'ecosistema nei processi aziendali porta ad un miglioramento dei processi decisionali, allo sviluppo di prodotti e servizi innovativi e ad un incremento della competitività (Jiang et al., 2023), consentendo alle PMI di ridurre inefficienze operative, ottimizzare la catena di fornitura e personalizzare l'offerta (Otto et al., 2022). In molti casi, la possibilità di accedere a dataset esterni riduce l'asimmetria informativa che tradizionalmente svantaggia le piccole imprese, promuovendo modelli di collaborazione e innovazione aperta (Oliveira et al., 2019). Tuttavia, la capacità delle PMI di trarre vantaggio dai dati dipende dalla loro maturità digitale e dalla disponibilità di competenze analitiche e manageriali per trasformare i dati in conoscenza utile (Adhiatma et al., 2023). La formazione di partnership strategiche e la partecipazione a programmi di data sharing promossi da enti pubblici o consorzi industriali possono rappresentare strumenti chiave per accrescere tale capacità.

Le PMI potrebbero ricoprire il ruolo d'intermediarie tecnologiche (*data enabler*) (c) negli ecosistemi di dati, ossia fungere da attrici che facilitano l'interoperabilità, la sicurezza e la valorizzazione dei dati tra diversi partecipanti (Schweihoff et al., 2024). Queste imprese, spesso appartenenti ai settori dell'ICT o della consulenza digitale, forniscono piattaforme, algoritmi, infrastrutture cloud e soluzioni di analisi che consentono lo scambio e l'elaborazione dei dati in modo sicuro e trasparente (Micheli et al., 2020). Le PMI in questa posizione fungono da ponte tra attori con differenti capacità tecniche e risorse, riducendo le asimmetrie informative e migliorando la qualità complessiva dei flussi di dati (Heinz et al., 2022). In alcuni casi, esse svolgono anche funzioni di *data stewardship*, cioè curano la gestione responsabile dei dati e assicurano la conformità a standard etici e normativi (Bernal, 2024). Inoltre, tali PMI possono contribuire alla resilienza infrastrutturale dell'ecosistema, promuovendo l'adozione di protocolli comuni e favorendo l'emergere di pratiche collaborative basate su trasparenza e fiducia reciproca (Lis & Otto, 2020; Pettenpohl et al., 2022).

Infine, le PMI potrebbero ricoprire il ruolo di co-governatrici (*co-governor*) (d) dell'ecosistema di dati. Le PMI, quindi, partecipano attivamente alla definizione delle regole, dei principi e delle pratiche di governance (Oliveira et al., 2019). Partecipando ai tavoli decisionali, nei consorzi o nei partenariati pubblico-privati, esse contribuiscono a delineare politiche di accesso, standard di interoperabilità e meccanismi di distribuzione del valore (Micheli et al., 2020; Lnenicka et al., 2024). Anche questo ruolo di co-governance si fonda su logiche di reciprocità e fiducia, dove le PMI vengono riconosciute come partner alla pari piuttosto che semplici utenti (Li & Mei, 2024). La partecipazione attiva rafforza la legittimità dei processi decisionali e favorisce la creazione di un ecosistema più inclusivo e bilanciato, capace di valorizzare le diversità di scala, settore e competenze. Inoltre, la co-governance rappresenta una leva per accrescere la capacità di apprendimento collettivo: la collaborazione tra

PMI, grandi imprese e attori pubblici consente lo sviluppo di nuove pratiche, modelli di business e strategie di gestione dei dati (Mbanefo & Grobbelaar, 2024). Quindi, le PMI diventano agenti di innovazione istituzionale, contribuendo a ridefinire i confini, le regole e le finalità degli ecosistemi di dati.

6. Discussione e conclusioni

L'analisi condotta mette in evidenza come la partecipazione delle piccole e medie imprese (PMI) agli ecosistemi di dati può essere un processo complesso, caratterizzato da interdipendenze multilivello tra fattori economici, tecnologici, organizzativi e istituzionali (Oliveira et al., 2019; Micheli et al., 2023). La capacità delle PMI di contribuire in modo significativo alla governance dei dati dipende dal superamento di barriere strutturali, dalla gestione delle tensioni inter-organizzative e dall'assunzione di ruoli dinamici coerenti con l'evoluzione dell'ecosistema.

Le barriere economiche, organizzative e normative individuate non costituiscono soltanto ostacoli alla partecipazione, ma rappresentano anche punti di apprendimento attraverso cui le PMI possono maturare competenze digitali e manageriali (Ajibade et al., 2019; Gierlich et al., 2019). Il superamento di tali barriere è un prerequisito per accedere alla fase successiva, in cui le imprese si confrontano con le tensioni tipiche degli ecosistemi di dati, come le asimmetrie di potere, i dilemmi tra apertura e protezione, e i conflitti tra governance centralizzata e autonomia locale (Heinz et al., 2022; Lnenicka et al., 2024). Queste tensioni, però, non devono essere viste con un'accezione negativa, ma, piuttosto, come spinte generative; esse, infatti, possono stimolare processi di adattamento, apprendimento e co-evoluzione tra gli attori (Micheli et al., 2020). In particolare, per le PMI, affrontare tali tensioni può diventare un'occasione per sviluppare capacità dinamiche (Adhiatma et al., 2023), ossia la capacità di integrare, riconfigurare e costruire risorse e competenze in risposta ai cambiamenti ambientali e tecnologici.

La letteratura suggerisce che gli ecosistemi di dati debbano implementare modelli di governance adattiva, in grado di bilanciare equità, apertura e protezione (Lis & Otto, 2020; Nikolakopoulos et al., 2023). Quindi, la governance assume una funzione regolativa, definendo regole e standard condivisi per la gestione dei dati e una funzione abilitante, creando le condizioni per la collaborazione e la fiducia reciproca tra gli attori.

Partecipazione ai processi di governance non è solo una questione di compliance per le PMI, ma anche un fattore strategico di empowerment. Attraverso la co-governance, le PMI possono contribuire alla definizione delle regole del gioco, negoziando forme più eque di distribuzione del valore e maggiore trasparenza nei processi decisionali (Lnenicka et al., 2024). Tuttavia, ciò richiede che la governance non sia solo formale, ma effettivamente inclusiva, ovvero capace di valorizzare la voce e le competenze anche degli attori di piccola scala. Come evidenziano Micheli et al. (2020),

solo una governance orientata alla fiducia e alla cooperazione può generare un ambiente favorevole all'innovazione e alla sostenibilità degli ecosistemi di dati.

Inoltre, la possibile assunzione di ruoli differenziati da parte delle PMI all'interno degli ecosistemi di dai suggerisce che la loro partecipazione non è lineare, ma adattiva e situata. In molti casi, la progressione delle PMI all'interno dell'ecosistema segue un processo evolutivo: inizialmente come beneficiarie dei dati, esse sviluppano progressivamente competenze e fiducia, fino a diventare co-creatrici e co-governatrici del valore (Otto et al., 2022; Jiang et al., 2023). Questa traiettoria evolutiva richiama i principi della co-evoluzione organizzativa (Jackson et al., 2024), secondo cui attori ed ecosistemi si influenzano reciprocamente. La partecipazione delle PMI contribuisce infatti a modificare la struttura dell'ecosistema stesso, spingendolo verso forme di governance più distribuite e inclusive (Heinz et al., 2022). Parallelamente, la loro interazione con altri attori favorisce processi di apprendimento interorganizzativo e di mutuo adattamento, in cui il valore dei dati è il risultato di una costruzione collettiva, più che di un possesso individuale (Lis & Otto, 2020).

In conclusione, sulla base delle evidenze emerse, in questo capitolo proponiamo un modello concettuale integrato che collega barriere, tensioni e ruoli delle PMI negli ecosistemi di dati. Le barriere di natura economica, organizzativa e normativa, costituiscono le condizioni di partenza che influenzano il livello di accesso e di maturità digitale delle PMI. Il loro superamento consente l'ingresso e la partecipazione attiva nell'ecosistema. Le tensioni emergono in questa fase come risultato dell'interazione tra attori eterogenei, generando conflitti di potere, fiducia o obiettivi. Tuttavia, tali tensioni non sono solo elementi disfunzionali; se gestite attraverso una governance inclusiva e multilivello, esse possono stimolare processi di apprendimento collettivo e innovazione organizzativa. Infine, i ruoli che le PMI assumono all'interno dell'ecosistema evolvono lungo un continuum, da utenti passivi dei dati a partner attivi e co-governatori del valore. Tale evoluzione è sostenuta dallo sviluppo di capacità dinamiche che permettono alle PMI di adattarsi, integrare competenze e contribuire alla sostenibilità dell'ecosistema. Il modello suggerisce dunque una relazione circolare e auto-rinforzante: la riduzione delle barriere abilita una partecipazione più consapevole, che facilita la gestione delle tensioni e promuove l'evoluzione dei ruoli. A loro volta, la partecipazione attiva e l'apprendimento organizzativo generano nuove competenze e risorse, contribuendo a ridurre ulteriormente le barriere iniziali e a rafforzare la resilienza complessiva dell'ecosistema.

6.1. Implicazioni teoriche e pratiche

Il presente capitolo fornisce un contributo alla letteratura sugli ecosistemi di dati, proponendo una visione integrata degli ecosistemi di dati come sistemi sociotecnici multilivello, nei quali le PMI non sono attori marginali, ma partecipano attivamente alla co-creazione di valore attraverso ruoli dinamici di fornitrici, utilizzatrici, intermediarie e co-governatrici dei dati. Inoltre, il capitolo colma una lacuna della letteratura che, come evidenziato dalle principali linee di ricerca, ha sinora concentrato

l'attenzione prevalentemente su aspetti tecnici della gestione del dato (data governance, data spaces, data architecture), trascurando le dimensioni organizzative, istituzionali e relazionali che condizionano la partecipazione delle PMI. Infine, l'analisi delle barriere e delle tensioni mostra come gli ecosistemi di dati non possano essere interpretati unicamente come infrastrutture tecnologiche, ma vadano letti come sistemi di governance adattiva, in cui l'equilibrio tra apertura, fiducia, protezione e condivisione è il risultato di negoziazioni continue tra attori di diversa scala e natura. Questo approccio consente di concettualizzare la partecipazione delle PMI come processo evolutivo di apprendimento e adattamento, in cui la gestione delle tensioni diventa una leva di sviluppo organizzativo e istituzionale, anziché una mera fonte di conflitto.

Inoltre, il capitolo fornisce anche interessanti implicazioni pratiche per le istituzioni pubbliche, per le PMI e per tutti gli altri attori appartenenti agli ecosistemi di dati. In dettaglio, una prima implicazione è diretta alle istituzioni pubbliche; emerge dalle analisi riportate nel capitolo la necessità di creare condizioni abilitanti per la partecipazione delle PMI agli ecosistemi di dati. Questo implica l'attivazione di incentivi economici, sgravi fiscali e programmi di formazione digitale (ad esempio sulla *data literacy*, sugli strumenti di governance partecipativa e sulle piattaforme digitali trasparenti e sicure), capaci di ridurre il divario infrastrutturale e culturale (Bianchini & Michalkova, 2019; European Union, 2022). Inoltre, le istituzioni pubbliche possono agire come facilitatori di fiducia, promuovendo piattaforme di condivisione sicure, trasparenti e conformi agli standard europei di interoperabilità (Farrell et al., 2023).

Un secondo contributo è per le PMI; la partecipazione a tali ecosistemi richiede una trasformazione non solo tecnologica ma anche organizzativa e culturale. È necessario sviluppare competenze digitali, capacità analitiche e una cultura orientata alla condivisione e alla collaborazione.

Infine, l'ultimo contributo per tutti gli altri attori coinvolti negli ecosistemi di dati; le tensioni strutturali che emergono negli ecosistemi devono essere affrontate come occasioni di apprendimento, promuovendo approcci flessibili e adattivi. In particolare le grandi imprese e le piattaforme digitali devono riconoscere che l'inclusione delle PMI costituisce una condizione di sostenibilità dell'ecosistema e questo richiede modelli di governance collaborativi e standard interoperabili.

6.2. Limiti e direzioni di ricerche future

Nonostante l'analisi teorica e concettuale condotta offra una prospettiva articolata sul ruolo delle PMI negli ecosistemi di dati, restano ancora diversi aspetti che richiedono approfondimento. Un primo limite riguarda la frammentazione della letteratura, che riflette approcci disciplinari differenti (gestione dei dati, imprenditorialità, supply chain, diritto industriale). Questa eterogeneità, se da un lato arricchisce la comprensione del fenomeno, dall'altro evidenzia la necessità di modelli teorici più

integrati e multidimensionali, capaci di coniugare le prospettive tecnologiche con quelle organizzative e istituzionali. In secondo luogo, le evidenze empiriche sul contributo delle PMI restano limitate e spesso concentrate su specifici contesti settoriali o geografici. Sono pertanto auspicabili studi comparativi in grado di valutare come la partecipazione delle PMI agli ecosistemi di dati vari in base alle politiche pubbliche, al livello di maturità digitale e ai modelli di governance adottati. Un ulteriore ambito di ricerca futura può riguardare il rapporto tra sostenibilità, digitalizzazione e data governance: i dati ambientali e sociali rappresentano oggi un nuovo terreno per l'innovazione guidata dalle PMI, ma servono analisi più approfondite sulle modalità con cui queste imprese sviluppano capacità *data-driven* a supporto della transizione ecologica. Inoltre, sarà importante indagare anche il ruolo delle nuove tecnologie abilitanti, come il cloud computing, l'intelligenza artificiale e i social network, nella costruzione di ecosistemi inclusivi e resilienti, in grado di bilanciare trasparenza, sicurezza e valore condiviso. Infine, studi futuri potrebbero esplorare i meccanismi di fiducia, le dinamiche di potere e i modelli di decision-making collaborativo che favoriscono la partecipazione equa delle PMI agli ecosistemi di dati andando a colmare il gap della letteratura che tratta i temi di governance inter-organizzativa.

Messaggi chiave:

- Le PMI sono attori fondamentali per promuovere lo sviluppo degli ecosistemi di dati.
- Le PMI presentano barriere che possono ostacolare la loro piena partecipazione agli ecosistemi di dati.
- All'interno degli ecosistemi di dati si generano delle tensioni tra gli attori coinvolti che devono essere risolte per ristabilire il clima ottimale.

Bibliografia

Adhiatma, A., Setiawan, A.B. & Hilmawan, D.R. (2023). Developing dynamic capabilities through digital transformation in SMEs. *Journal of Small Business Strategy*, *33*(2), 45-63.

Aghazadeh, H., Zandi, F., Amoozad Mahdiraji, H. & Sadraei, R. (2024). Digital transformation and SME internationalisation: Unravelling the moderated-mediation role of digital capabilities, digital resilience and digital maturity. *Journal of Enterprise Information Management*, *37*(5), 1499-1526. https://doi.org/10.1108/JEIM-02-2023-0092.

Ajibade, P., Mutula, S. & Grand, S. (2019). Barriers to digital transformation in small and medium enterprises: A systematic review. *Journal of Enterprise Information Management*, *32*(3), 450-474.

Aldossari, S., Mokhtar, U.A. & Abdul Ghani, A.T. (2023). Factor influencing the adoption of

big data analytics: A systematic literature and experts review. *Sage Open*, *13*(4), 21582440231217902. https://doi.org/10.1177/21582440231217902.

Alzoubi, H.M. & Yanamandra, R. (2024). Navigating the interplay between innovation orientation, dynamic capabilities, and digital supply chain optimization: Empirical insights from SMEs. *Uncertain Supply Chain Management*, *12*(2), 649-658.

Bernal, P. (2024). Trust and data stewardship in the digital economy. *Information Systems Journal*, *34*(1), 55-74.

Bianchini, S. & Michalkova, A. (2019). Digital innovation and SMEs: Managing cybersecurity and data governance. *Small Business Economics*, *52*(4), 921-940.

Bode, J., Kühl, N., Kreuzberger, D. & Holtmann, C. (2024). Toward avoiding the data mess: Industry insights from data mesh implementations. *IEEE Access*, *12*, 95402-95416.

Brechtel, M., Petrik, D. & Hölzle, K. (2023). From challenges to solution pathways for industrial data ecosystems – A socio-technical perspective. In *International Conference on Wirtschaftsinformatik* (pp. 113-129). Cham: Springer Nature Switzerland.

Büyükselçuk, E.Ç. (2024). Evaluation of industrial IoT service providers with TOPSIS based on circular intuitionistic fuzzy sets. *Computers, Materials & Continua*, *80*(1).

Ceccagnoli, M., Forman, C., Huang, P. & Wu, D.J. (2012). Cocreation of value in a platform ecosystem: The case of enterprise software. *MIS Quarterly*, 263-290.

Cenamor, J., Parida, V. & Wincent, J. (2019). How entrepreneurial SMEs compete through digital platforms: The roles of digital platform capability, network capability and ambidexterity. *Journal of Business Research*, *100*, 196-206.

Chen, Y., Li, J. & Zhang, J. (2024). Digitalisation, data-driven dynamic capabilities and responsible innovation: An empirical study of SMEs in China. *Asia Pacific Journal of Management*, *41*(3), 1211-1251. https://doi.org/10.1007/s10490-022-09845-6.

Costa-Climent, R., Segarra-Oña, M. & Martínez, A. (2023). Digital transformation and upskilling in SMEs: A European perspective. *Technovation*, *122*, 102764.

Cunningham, J.A. & Link, A.N. (2014). Fostering university-industry R&D collaborations in European Union countries. *International Entrepreneurship and Management Journal*, *11*, 849-860.

Duisberg, A. (2022). International Data Spaces (IDS): Legal and regulatory challenges in data sharing. *Computer Law Review International*, *23*(2), 47-58.

European Commission (2020a). *A European strategy for data*. Brussels: Publications Office of the European Union.

European Commission (2020b). *SMEs and data-driven innovation in Europe*. Brussels: Publications Office of the European Union.

European Union (2022). Data Governance Act and the development of data ecosystems in the EU. Official Journal of the European Union, L 152/1.

Farrell, T., Schüritz, R. & Thomas, O. (2023). Common European Data Spaces: Governance, interoperability, and value creation. *Government Information Quarterly*, *40*(2), 101767.

Georgescu, I., Crisan, E. & Marinescu, P. (2022). Organizational flexibility and innovation in SMEs: Evidence from digital ecosystems. *Management Decision*, *60*(6), 1487-1506.

Ghosh, S., Negahban, S., Kwak, Y.H. & Skibniewski, M.J. (2011, June). Impact of sustainability on integration and interoperability between BIM and ERP: A governance framework. In *First International Technology Management Conference* (pp. 187-193). IEEE.

Gierlich, M., Kühn, A. & Tschanz, T. (2019). SMEs and the digital transformation challenge: A capability perspective. *International Journal of Innovation Management*, *23*(8), 1950072.

Gruner, R.L. & Power, D. (2018). To integrate or not to integrate? Understanding B2B social media communications. *Online Information Review*, *42*(1), 73-92.

Heinz, M., Schönberger, M. & Otto, B. (2022). Governance mechanisms in data ecosystems: A multi-level perspective. *Information Systems and e-Business Management*, *20*(3), 693-718.

Jackson, P., Maier, F. & Stoughton, A. (2024). Co-evolutionary dynamics in digital ecosystems. *Research Policy*, *53*(1), 104687.

Järvenpää, A.M., Jussila, J. & Kunttu, I. (2023). Barriers and practical challenges for data-driven decision-making in circular economy SMEs. In *Big data and decision-making: Applications and uses in the public and private sector* (pp. 163-179). Emerald Publishing.

Jiang, F., Li, Y. & Zheng, S. (2023). SMEs in data ecosystems: Collaboration, learning, and innovation. *Information & Management*, *60*(3), 103717.

Jordão, R.V.D. & Novas, J.C. (2024). Information and knowledge management, intellectual capital, and sustainable growth in networked small and medium enterprises. *Journal of the Knowledge Economy*, *15*(1), 563-595.

Kitsios, F., Kamariotou, M. & Grigoroudis, E. (2017). Digital innovation and knowledge sharing in SMEs. *Journal of Knowledge Management*, *21*(6), 1367-1385.

Li, W. & Mei, X. (2024). Data ecosystems and firm performance: Balancing openness and protection. *Technological Forecasting and Social Change*, 197, 122493.

Lis, B. & Otto, B. (2020). Data governance in data ecosystems: Balancing control and value creation. *Information Systems Journal*, *30*(4), 912-939.

Lnenicka, M., Nikiforova, A. & Machova, R. (2024). Context-dependent governance in data ecosystems: A comparative study. *Government Information Quarterly*, *41*(1), 102001.

Mbanefo, U. & Grobbelaar, S. (2024). The influence of SMEs in digital ecosystems: A co-evolutionary approach. *Technovation*, *125*, 102874.

Micheli, M., Ponti, M., Craglia, M. & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 2053951720948087.

Mujinga, M. (2020, December). Cloud computing inhibitors among small and medium enterprises. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1385-1391). IEEE.

Nikolakopoulos, K., Milossis, D. & Rantos, K. (2023). Data governance and data sharing practices in the EU: Challenges and opportunities. *Information Systems Frontiers*, *25*(5), 2103-2120.

Oliveira, M.I.S. & Lóscio, B.F. (2018). What is a data ecosystem? In *Proceedings of the 19th Annual International Conference on Digital Government Research* (dg.o 2018) (pp. 1-9).

Oliveira, M., Lima, G. & Lóscio, B.F. (2019). Data ecosystems: Governance and architecture. In *Proceedings of the 21st International Conference on Enterprise Information Systems* (pp. 82-91).

Otto, B., Jarke, M. & Piatkowski, M. (2022). Designing data ecosystems: Roles, processes, and value co-creation. *Information Systems and e-Business Management*, *20*(4), 971-993.

Pérez-Moure, H., Lampón, J.F. & Cabanelas, P. (2024). Mobility business models toward a digital tomorrow: Challenges for automotive manufacturers. *Futures*, *156*, 103309. https://doi.org/10.1016/j.futures.2023.103309.

Pettenpohl, M., Heuer, H. & Otto, B. (2022). Federated architectures for data spaces: Lessons from IDS and Gaia-X. *Journal of Information Technology*, *37*(3), 234-248.

Pfister, P. & Lehmann, C. (2024). Digital value creation in German SMEs: A return-on-investment analysis. *Journal of Small Business & Entrepreneurship*, *36*(4), 548-573.

Rehm, G., He, J., Moreno-Schneider, J., Nehring, J. & Quantz, J. (2017, May). *Designing user interfaces for curation technologies. In International Conference on Human Interface and the Management of Information* (pp. 388-406). Cham: Springer International Publishing.

Rosyadi, S., Kusuma, A.S., Fitrah, E., Haryanto, A. & Adawiyah, W. (2020). The multi-stakeholders' role in an integrated mentoring model for SMEs in the creative economy sector. *SAGE Open*, *10*(4), 2158244020963604.

Scherer, S., Wimmer, M.A. & Strykowski, S. (2015). Social government: A concept supporting communities in co-creation and co-production of public services. In *Proceedings of the 16th Annual International Conference on Digital Government Research* (204-209). https://doi.org/10.1145/2757401.2757417.

Schneider, S., Zillner, S. & Riedl, C. (2024). Data spaces and the European data economy: Opportunities and challenges. *Journal of Strategic Information Systems*, *33*(1), 101746.

Schweihoff, J., Felden, C. & Otto, B. (2024). Data intermediaries and the orchestration of data ecosystems. *Information Systems Journal*, *34*(2), 367-392.

Wulf, A. & Butel, L. (2017). Knowledge sharing and collaborative relationships in business ecosystems and networks: A definition and a demarcation. *Industrial Management & Data Systems*, *117*(7), 1407-1425.

Yuan, N. & Li, M. (2024). Research on collaborative innovation behavior of enterprise innovation ecosystem under evolutionary game. *Technological Forecasting and Social Change*, *206*, 123508. https://doi.org/10.1016/j.techfore.2024.123508.

Zeng, J. & Glaister, K.W. (2018). Value creation from big data: Looking inside the black box. *Strategic Organization*, *16*(2), 105-140.

Parte 2
La gestione dei dati per favorirne il riuso

Le ramificazioni del ROSI per guidare gli investimenti in data governance e sicurezza cyber: spunti da un percorso di Action Design Research

Elena Tomasella [*] **e Paolo Spagnoletti** [**]

Abstract: La trasformazione digitale, ormai diffusa in tutti i settori, ha reso la cybersecurity una priorità strategica per le organizzazioni sia pubbliche che private. L'aumento della digitalizzazione, pur generando valore e innovazione, accresce anche le vulnerabilità dei sistemi informativi, come dimostrano i recenti dati europei e nazionali sugli attacchi informatici. In tale contesto, la data governance si configura come un ambito cruciale per garantire sicurezza, qualità e tracciabilità dei dati, favorendo al contempo la collaborazione inter-organizzativa. Tuttavia, le differenze in termini di risorse, competenze e infrastrutture rendono la sua adozione disomogenea, soprattutto nelle PMI e nelle pubbliche amministrazioni locali. Il presente lavoro affronta il problema della valutazione ex-ante degli investimenti in sicurezza, proponendo un framework, sviluppato attraverso un percorso di Action Design Research (ADR), per il calcolo del Return on Security Investment (ROSI). L'obiettivo è supportare decisioni informate in materia di cybersecurity e riflettere sulle implicazioni per la data governance in sistemi inter-organizzativi.

Parole chiave: Cybersecurity Investment, Return on Security Investment (ROSI), Action Design Research (ADR), Data Governance.

1. Introduzione

Con la trasformazione digitale ormai radicata sia nel settore pubblico sia in quello privato, la cybersecurity è emersa come priorità strategica per gli investimenti (Gordon & Loeb, 2002; Jonhson, Maurer, Torres, Guerra & Mohit, 2024). La digitalizzazione sta rimodellando i servizi sia in modo trasversale, influenzando tutti i

[*] Elena Tomasella (✉)
Dipartimento di Business and Management, Università Luiss, Italia.
E-mail: etomasella@luiss.it

[**] Paolo Spagnoletti (✉)
Dipartimento di Business and Management, Università Luiss, Italia.
E-mail: pspagnoletti@luiss.it

DOI: 10.82018/9791221165456-6

settori, sia in modo verticale, generando cambiamenti sistemici a diversi livelli. Sebbene la trasformazione digitale proceda a velocità differenti nei vari ambiti, il suo impatto rimane esteso e pervasivo. A tal proposito è opportuno precisare che, nonostante i parametri utilizzati per misurarla siano ancora in fase di definizione (Verhoef, et al., 2021), vi è un consenso generale riguardo questa accelerazione. D'altra parte, la crescente dipendenza delle organizzazioni dai sistemi digitali comporta un aumento delle vulnerabilità. A livello europeo, il settore pubblico è attualmente la principale vittima di attacchi informatici, con il 38,2% degli incidenti riportati rivolti alle pubbliche amministrazioni (ENISA, 2025). Dall'Operational Summary CSIRT del primo semestre 2025 emerge che, in Italia, nei primi quindici settori, che risultano le principali vittime di attacchi cyber, il numero di attacchi è in crescita rispetto al primo semestre 2024, anche se in diversa misura per ogni settore. In questo scenario, la data governance è un ambito di intervento che si posiziona trasversalmente a livello strategico, al fine di creare un ecosistema digitale sicuro. Favorisce infatti la creazione di valore inter-organizzativo del dato, garantendo però allo stesso tempo alti livelli di qualità, tracciabilità e affidabilità dei dati.

La digitalizzazione riguarda, a diversi livelli, tutti i settori e i tipi di organizzazione, ma la data governance non sempre risulta ugualmente accessibile come area di intervento. Le organizzazioni di piccole dimensioni, sia pubbliche che private, spesso non dispongono di strumenti, risorse e competenze adeguati a operare nell'ambito. Sono necessari, ad esempio, strumenti di monitoraggio, ruoli dedicati, una maggiore consapevolezza strategica sul valore dei dati e una gestione dell'informazione come asset. Le difficoltà non sono quindi limitate alla dimensione economica, ma si estendono a quello organizzativa e culturale. Nelle PMI, in particolare, la carenza di risorse dedicate e di competenze specialistiche comporta che i modelli di data governance siano percepiti come eccessivamente onerosi rispetto alla capacità operativa disponibile (Begg & Caira, 2011). Considerando il contesto degli ecosistemi, invece, gli attori devono accordarsi sui meccanismi di coordinamento di data control prima che di qualsiasi co-creazione di nuovo valore (Spagnoletti, Kazemargi, Constantinides & Prencipe, 2025). Spostando l'attenzione dal settore privato a quello pubblico, emergono ulteriori criticità, legate alla frammentazione delle infrastrutture e al limitato coordinamento interistituzionale a livello locale. In questo senso, lo sviluppo della data governance come area di intervento risulta fondamentale a sostegno della creazione di un ecosistema digitale, che sia capace di compensare tali difficoltà e favorire forme di collaborazione. Quest'ultimo aspetto non riguarda esclusivamente il settore pubblico, ma si estende anche a quello privato.

La sicurezza dei dati e dei sistemi di elaborazione rappresenta inoltre, da oltre un decennio, la principale preoccupazione dei responsabili delle funzioni IT (Jonhson, Maurer, Torres, Guerra & Mohit, 2024). Per le organizzazioni che operano in contesti ad alta interoperabilità, tale preoccupazione risulta ulteriormente accentuata considerate le interdipendenze che accrescono il rischio di incidenti ad alto impatto (Assenza, Ortalda & Setola, 2024). Ne risulta un importante bisogno di strumenti avanzati di supporto alle decisioni che siano in grado di fornire una stima degli investimenti necessari a mitigare il rischio rivedendo processi, strumenti e pratiche di

governo del dato. Tuttavia, valutare costi e benefici di questo tipo di investimenti risulta problematico per via della natura duale della sicurezza e del peso del contesto sulle conseguenze di un incidente. Il presente lavoro esamina il problema della valutazione ex-ante degli investimenti in sicurezza, illustrando i risultati di un percorso di Action Design Research (ADR) (Sein, Henfridsson, Purao, Rossi & Lindgren, 2011) finalizzato allo sviluppo di un framework per il calcolo del Return on Security Investment (ROSI – Ritorno sugli Investimenti in Sicurezza), e riflette criticamente sulle implicazioni per la data governance in ambito inter-organizzativo.

2. La misurazione del Ritorno sugli Investimenti in Sicurezza

Il ROSI è una metrica ampiamente riconosciuta, utilizzata per valutare i benefici finanziari derivanti dalle misure di sicurezza in rapporto ai loro costi. Originariamente sviluppato per il settore privato attraverso l'adattamento del concetto di Return on Investment (ROI) alle tematiche legate alla sicurezza, il ROSI fornisce un approccio strutturato per determinare se, e in quale misura, gli investimenti in sicurezza producono un ritorno positivo grazie alla prevenzione delle potenziali perdite causate da violazioni informatiche. Il modello tradizionale del ROSI considera la riduzione del rischio finanziario come principale indicatore dell'efficacia di un investimento. Questo approccio, però, risulta limitato in quanto trascura i benefici prodotti dagli investimenti in sicurezza al di là del risparmio economico. Oggi, infatti, un attacco informatico non comporta solo perdite finanziarie, ma incide anche sulla fornitura di servizi essenziali, la perdita di dati sensibili e informazioni proprietarie e causa danni reputazionali difficilmente calcolabili.

Per questo motivo, da un lato diventa urgente aggiornare gli strumenti manageriali in uso; dall'altro, al fine di ridurre l'impatto degli attacchi informatici e di implementare la loro resilienza, le organizzazioni necessitano di un'architettura di data governance che permetta di fornire una misurazione coerente e quanto più possibile completa dell'impatto trasversale delle potenziali minacce cyber. Per quanto riguarda l'aggiornamento degli strumenti manageriali, lo studio ADR propone un modello di ROSI che sarà illustrato in maggiore dettaglio nei prossimi paragrafi. In merito alla data governance invece, si evidenziano ora alcuni punti di convergenza emersi dalla letteratura in termini di importanza riconosciuta, in particolare con riferimento a contesti ad alta interoperatività e ad organizzazioni con risorse limitate.

Un importante lavoro di literature review strutturata (Abraham, Schneider & vom Brocke, 2019) ha identificato cinque macroaree di priorità per la ricerca futura in data governance, individuate a partire dai gap tra i framework concettuali e la loro effettiva applicazione. Una di queste aree riguarda in particolare il mantenimento del controllo e dell'interoperatività nei contesti inter-organizzativi. A partire dalla difficoltà riconosciuta nell'integrare i dati provenienti da diverse organizzazioni e dalle loro parti terze, e a fronte della consapevolezza del valore potenziale generato da tale integrazione, uno

studio ADR (Bodendorf & Bayr, 2025) ha contestualizzato lo sviluppo di artefatti IT volti a supportare la governance dello scambio di dati rispetto al livello inter-organizzativo. Tuttavia, la maggior parte dei framework di data governance disponibili risultano progettati per essere applicati all'interno di singole organizzazioni (Ribeiro, Barata & da Cunha, 2024) e in aggiunta, le PMI caratterizzate da un basso livello di computerizzazione investono generalmente meno risorse (da intendere sia a livello tecnico che di *expertise*) nella costruzione e nel mantenimento di policy e strategie di sicurezza informatica (Solek-Borowska & Wozniak, 2024; Rombaldo Junion & Johnson, 2023). Come anticipato, queste logiche di data governance verranno riprese a posteriori per discutere le implicazioni dello studio ADR in relazione a tale ambito.

Il Ritorno sull'Investimento in Sicurezza (ROSI) si basa su modelli formali per il calcolo di costi e benefici (Barik, Misra, Fernandez-Sanz & Koyuncu, 2023; Butler, 2002; Gheorghe, 2012; Liu, Zhang & Chen, 2014; Tsiakis & Stephanides, 2005; Arshad A., Abbas, Faisal Amjad, Shafqat & Yaqoob, 2019; Böhme & Moore, 2010; Collier, Briglia, Slutzky & Lambert, 2023; Marican, Othman, Selamat & Razak, 2024; Pontes, Guelfi, Silva & Kofuji, 2011). La varietà dei contesti organizzativi in cui il ROSI è adottato, ha comportato la nascita di diversi modelli (Arshad A., Abbas, Faisal Amjad, Shafqat & Yaqoob, 2019; Butler, 2002; Tsiakis & Stephanides, 2005; Gheorghe, 2012; Sonnenreich, Albanese & Stout, 2006). Ciononostante, diversi autori hanno evidenziato la necessità di identificare criteri standardizzati per l'inclusione delle componenti di costo, così come per la mappatura delle vulnerabilità e dei meccanismi di difesa per migliorare l'attendibilità delle stime (Arshad A., Abbas, Faisal Amjad, Shafqat & Yaqoob, 2019; Butler, 2002; Onwubiko & Onwubiko, 2019; Böhme & Moore, 2010; Liu, Zhang & Chen, 2014; Sonnenreich, Albanese & Stout, 2006). Di recente sono stati proposti anche approcci basati sul calcolo del valore a rischio: in particolare, uno studio sul Cyber Value at Risk (CVaR) ha presentato una metodologia per l'estrazione e il processo di informazioni da rapporti industriali relativi alla sicurezza cyber, un modello per stimare ex-ante il potenziale costo degli attacchi cyber sulla base di tali informazioni, e un applicativo web per l'analisi di costi e rischi fondato su questo modello (Franco, Künzler, Von der Assen, Feng & Stiller, 2024). L'approccio CVaR, seppur avanzato, presenta alcune limitazioni, tra cui il fatto che va calibrato opportunamente rispetto alle variabili di contesto dell'organizzazione di riferimento, e non è quindi uno strumento ancora generalizzato. Inoltre, si basa esclusivamente su report industriali e non su dati primari. Ciò evidenzia l'importanza di una collaborazione inter-organizzativa in cui, tramite un'appropriata data governance, non solo venga garantita la circolazione dei dati in modo sicuro, ma si assicuri anche una storicizzazione di eventuali eventi cyber, collezionando dati primari opportunamente anonimizzati che sono utili per modelli di questo tipo.

Sebbene alcune fonti facciano riferimento al ROSI con termini differenti (ad esempio cyber-ROI), vi è un consenso generale sulla sua definizione, che viene presentata come segue:

$$ROSI = \frac{Beneficio\ Economico - Costo\ dell'Investimento}{Costo\ dell'Investimento}$$

È importante sottolineare che una sfida cruciale riguarda la determinazione del Beneficio Economico, ossia il valore monetario delle perdite evitate grazie alle misure di sicurezza implementate. La sua stima risulta particolarmente complessa, sia perché richiede di attribuire un valore economico a eventi ipotetici, sia perché dipende da molteplici dimensioni, che spaziano dalla continuità operativa all'adozione di misure volte a prevenire sanzioni derivanti dalla non conformità normativa.

2.1. Radici ramificazioni del ROSI

Per il design del framework è stata inizialmente condotta un'analisi dei modelli esistenti, individuando gli assunti più problematici o restrittivi su cui si basano, e cercando soluzioni alternative. In particolare, l'attenzione del team di ricerca è stata rivolta alla costruzione di uno strumento personalizzabile per le singole organizzazioni, in grado di adattarsi a una serie di variabili di contesto che ne definiscono il profilo. Per dare al framework una veste modulare e adattiva, il team si è ispirato al lavoro di Bruno Munari (1978) intitolato "Disegnare un albero", che spiega come disegnare un albero partendo da una solida struttura di radici e sviluppando i rami in modo organico e progressivo. Ogni radice o ramo può essere approfondito o ampliato in modo indipendente, senza compromettere l'equilibrio e la coerenza complessiva del sistema. Sia le radici che la chioma sono modulari: possono crescere verticalmente, in una direzione alla volta, mantenendo la robustezza del modello. Le organizzazioni scelgono, in base al contesto, alle risorse disponibili e alle priorità strategiche, da quale dei due fattori del ROSI, il costo dell'investimento o il beneficio economico, iniziare lo sviluppo del modello. Infatti, proprio come un albero, il framework è radicato in questi due fattori e si sviluppa verso l'alto e verso l'esterno attraverso strategie mirate e asset dedicati, garantendo flessibilità, adattabilità e coerenza strutturale.

Da un punto di vista strutturale, l'approccio modulare è essenziale per garantire un modello scalabile e facilmente adattabile ad ogni livello, senza che vengano compromessi coerenza e significato. La metodologia è fortemente orientata a garantire la maggiore applicabilità e flessibilità dell'artefatto possibili. In pratica, l'approccio modulare comporta evitare assunzioni che non possano essere rifiutate in futuri adattamenti dello strumento. Due requisiti chiave per garantire la scalabilità sono la consapevolezza, da parte delle organizzazioni, che i dati costituiscono un asset strategico, e l'interesse ad adottare strumenti manageriali che facilitino il processo di crescita. In questo contesto, la data governance si conferma un'area di intervento prioritaria. I dati utilizzati per il prototipo dell'artefatto provengono quasi interamente da fonti secondarie per la maggior parte dei fattori. Ciò nonostante, sin dall'inizio è stata chiarita l'intenzione di integrare dati primari nei futuri aggiornamenti del modello. Un'opportuna architettura di data governance garantisce la qualità della collezione sistemica di dati primari. Non appena tali dati, utili per uno specifico modulo del modello ROSI, saranno disponibili, il modulo corrispondente potrà essere aggiornato con essi. Questo approccio permette un miglioramento progressivo del

modello, poiché i nuovi dati relativi ad un'area non influenzano negativamente le altre, ma aumentano l'appropriatezza complessiva del risultato.

Oltre a consentire aggiornamenti ed estensioni degli elementi fondamentali e delle applicazioni, la modularità permette all'artefatto di essere adattato efficacemente a contesti diversi senza comprometterne l'utilità. Ciò è reso possibile selezionando nell'applicativo le specifiche del contesto in esame – che fungono da appropriati strumenti per la creazione dei profili delle organizzazioni –, e progettando algoritmi in grado di calcolare i fattori del ROSI sulla base di tali moduli. Sotto questo punto di vista, un modello di data governance che sia applicato su larga scala nei contesti ad alta interoperatività semplificherebbe il processo di adattamento dello strumento ROSI. Infatti, il fatto di avere uno standard si traduce da un lato in una riduzione del tempo di analisi dell'organizzazione in considerazione, e dall'altro in una riduzione delle differenze per cui risulta necessario aggiornare le variabili ogni volta che si incontra un nuovo contesto.

2.2. Beneficio economico

La valutazione dei benefici economici riveste un ruolo di particolare rilevanza per due motivi: consente diverse applicazioni indipendentemente dalla successiva applicazione nel ROSI, e offre preziose indicazioni per la gestione strategica degli investimenti. Il fattore del beneficio economico si articola in tre componenti, esplicitate nella seguente formula: $EB = P_A * Eff * C_A$, dove P_A rappresenta la probabilità di un attacco, Eff l'efficacia associata alla postura di cybersecurity dell'organizzazione, C_A il costo dell'attacco. L'architettura di questo framework garantisce che le tre componenti siano contestualizzate e adattati al profilo specifico di ciascuna organizzazione, e che le variabili siano usate coerentemente nelle tre componenti.

La probabilità di un attacco (P_A) è intuitivamente influenzata da diversi fattori, tra cui la tipologia di attacco e il settore di appartenenza dell'organizzazione presa di mira. Tale probabilità può essere definita in modo empirico come:

$$P_A = \frac{\#attacchi\ avvenuti\ con\ successo}{\#attacchi}.$$

A lungo termine, il framework mira a raffinare questa definizione enunciata sopra, mantenendo una probabilità derivata empiricamente ma integrandola con approcci teorici, come le *threat probability functions* [1], in modo di non affidarsi esclusivamente a dati storici e di evitare assunzioni eccessivamente restrittive. L'obiettivo finale è quello di utilizzare un valore di probabilità di attacco che sia adattato alle caratteristiche specifiche dell'organizzazione in esame. Tuttavia, data la disponibilità di dati nazionali (ad esempio forniti dal CSIRT) sulla frequenza degli attacchi classificati per tipologia e altre caratteristiche rilevanti, si propone come primo passo un

[1] Funzioni di probabilità di attacco.

potenziamento della prima versione del framework con tali dati, senza introdurre in questa fase una pipeline analitica più complessa.

Per definizione, l'efficacia (Eff) rappresenta la probabilità che un'organizzazione sia completamente protetta da attacchi informatici. Tenendo presente questo aspetto, è importante chiarire che il valore dell'efficacia, nel contesto pratico di applicazione del ROSI, non viene calcolato attraverso formule probabilistiche, bensì è correlato alla postura cyber dell'organizzazione considerata. Serve introdurre quest'altra grandezza, per poi analizzare la relazione che intercorre tra i due. La postura cyber di un'organizzazione rappresenta lo stato di sicurezza complessivo delle sue informazioni, reti e sistemi, determinato dalle risorse di sicurezza informatica (ad esempio personale, hardware, software, politiche) e dalle capacità operative messe in atto per garantire la difesa dell'impresa e la sua capacità di risposta al mutare delle condizioni di rischio. In conformità alle linee guida nazionali per il framework di cybersecurity, il framework suggerisce di analizzare sei dimensioni, che sono *Governance e processi*, *Gestione del rischio informatico e continuità operativa*, *Gestione e risposta agli incidenti di sicurezza*, *Gestione degli accessi logici e delle identità digitali*, *Formazione e sensibilizzazione sulla cybersecurity*, *Sicurezza di applicazioni, dati e reti*. A ciascuna organizzazione si assegna un livello di maturità compreso tra 0 e 5 per ciascuna di queste dimensioni. Il modello adottato per questo fine è il Capability Maturity Model (CMM) preso come riferimento dal NIST. I livelli di maturità sono riportati di seguito.

- 0 – Non completato: Non esistono processi o capacità formalizzate in materia di cybersecurity.
- 1 – Iniziale / Ad hoc: Le misure di cybersecurity sono implementate in modo non strutturato e reattivo, senza politiche o procedure coerenti.
- 2 – Gestito: I processi di cybersecurity di base sono documentati e seguiti, ma restano prevalentemente reattivi e applicati in modo non uniforme.
- 3 – Definito: È stato istituito un framework di cybersecurity ben definito e standardizzato, con misure e politiche proattive in atto.
- 4 – Gestito quantitativamente: I processi di cybersecurity sono monitorati e misurati continuamente in termini di efficacia, con miglioramenti basati su dati.
- 5 – Ottimizzato: La cybersecurity è pienamente integrata nell'organizzazione, con miglioramento continuo, automazione e allineamento strategico agli obiettivi aziendali.

Lo studio ADR ha posto particolare attenzione al fatto che le diverse dimensioni della postura cyber non hanno la medesima rilevanza e che i livelli di postura cyber non sono, a priori, distribuiti secondo intervalli standardizzati. In termini realistici, ciascuna organizzazione può presentare una configurazione specifica sia per le dimensioni sia per la distribuzione dei livelli di postura cyber. La questione fondamentale emersa durante lo sviluppo dell'artefatto riguarda sostanzialmente come la postura cyber aumenti dal livello 0 al livello 5. Tale quesito dovrebbe essere posto per ciascuna dimensione su cui si misura la postura. Indagini successive potranno

approfondire ulteriormente tale relazione tra postura cyber ed efficacia del sistema analizzandola dimensione per dimensione, ma ciò non è previsto per il primo ciclo di implementazione dell'artefatto. Il problema è comunque duplice anche considerando i livelli di maturità in modo complessivo: da un lato la difficoltà intrinseca nella selezione della variabile più appropriata da cui far dipendente la dilatazione dei livelli, dall'altro la carenza di dati, qualunque sia la scelta effettuata. Un primo approccio risolutivo consiste nell'utilizzare direttamente l'efficacia, accettando la restrittività della scelta. Durante un workshop svoltasi nel mese di maggio 2025 che è stato fondamentale per la costruzione dell'artefatto, è stato chiesto a dodici esperti di rappresentare l'andamento dell'efficacia in relazione alla postura complessiva di cybersecurity per validare il modello. Il passo successivo consiste nel raffinare ulteriormente la relazione tra *Efficacia* e *Postura Cyber*, superando l'ipotesi di linearità. L'obiettivo ideale è quello di definire una funzione specifica per ciascuna dimensione. Nella seconda iterazione dell'ADR, è stato introdotto un grado di non linearità, applicato però solo alla postura cyber complessiva, e non alle singole dimensioni. Alcune dimensioni richiedono maggiore sforzo iniziale per migliorare la postura, ma mostrano rendimenti decrescenti man mano che si raggiungono livelli più elevati. A titolo esemplificativo, le curve concave possono rappresentare dimensioni più *labor-driven* (ad esempio, formazione del personale), dove piccoli investimenti iniziali generano benefici immediati, mentre le curve convesse risultano più adatte a contesti *capital-driven* (ad esempio, sicurezza di rete), in cui gli avanzamenti richiedono investimenti maggiori e più progressivi.

L'ultima componente del beneficio economico da discutere è il Costo di un Attacco (CA). La sua determinazione presenta diverse complessità, legate sia all'individuazione delle conseguenze da includere (dirette e indirette) sia alla durata del periodo di analisi dei danni conseguenti a un attacco. Per coerenza con le pratiche esistenti, il framework adotta un orizzonte temporale di un anno, con la possibilità di estenderlo a cinque anni per valutazioni a lungo termine, applicando un opportuno tasso di sconto se l'investimento è fissato al tempo zero. Nella prima implementazione del modello ROSI, si utilizza un costo medio standard tratto da fonti secondarie (IBM & Ponemon, 2024), ma in prospettiva si prevede di passare a valori più specifici e contestualizzati, basati su diverse tipologie di attacco e sulle caratteristiche dell'organizzazione. Il report IBM 2023 sul costo di un data breach rappresenta una base di riferimento utile e largamente utilizzata. Offre infatti stime differenziate per Paese, settore, dimensione aziendale e metodi di rilevazione, consentendo di allineare il costo stimato al profilo specifico dell'organizzazione. Ad esempio, una PA italiana del settore pubblico può avere un costo medio stimato inferiore rispetto a un'impresa privata. L'algoritmo proposto dal modello associa quindi a ciascun ente un valore personalizzato di costo, selezionando in modo conservativo il valore massimo tra quelli coerenti con i driver organizzativi (es. dimensione, settore, area geografica).

2.3. Costo dell'investimento

Il Costo dell'Investimento è il secondo fattore del ROSI e rappresenta il costo effettivo degli interventi. In base all'esperienza e alla letteratura, nella valutazione del ROSI la stima dell'investimento per gli interventi non costituisce una criticità primaria; tuttavia, l'assenza di un metodo standard per garantirne la confrontabilità rappresenta un ostacolo per l'uso dell'artefatto nelle valutazioni comparative, sia tra diversi insiemi di investimenti all'interno di una stessa organizzazione, sia tra interventi analoghi in organizzazioni differenti. Una volta calcolati i ROSI dei singoli investimenti, i risultati possono essere aggregati per determinare il ROSI complessivo per ciascuna organizzazione e si possono quindi confrontare i ROSI di diverse organizzazioni, identificando così dove le strategie di investimento risultano più efficaci, nonché attivando analisi di pattern tra le scelte adottate e le informazioni di contesto.

Un elemento critico riguarda la definizione delle voci di costo da includere nel calcolo dell'investimento associato a un singolo intervento, la cui coerenza è condizione necessaria per avere take-away dalle analisi comparative che non siano *misleading*. Possono emergere spese condivise tra più interventi, la cui attribuzione non è immediata; in tali casi, è necessario stabilire criteri di ripartizione appropriati, al fine di suddividere equamente e coerentemente i costi comuni. Senza un approccio rigoroso, due scenari di investimento potrebbero differire notevolmente nel ROSI semplicemente perché uno include una gamma più ampia di costi. Il framework sviluppato dallo studio contribuisce a mitigare tali disparità, garantendo una valutazione più oggettiva e coerente degli investimenti in sicurezza.

Specializzando il ROSI sia rispetto al settore dell'organizzazione considerata, sia rispetto alla tipologia di intervento, i risultati possono essere raggruppati secondo entrambe le dimensioni, facilitando l'identificazione di trend e supportando la prioritizzazione degli interventi. Gli interventi spesso richiedono aggiornamenti successivi che generano effetti a cascata, per cui è importante definire quali costi includere nella stima della spesa principale. Il framework proposto stabilisce delle soglie oltre le quali i costi aggiuntivi vengono limitati rispetto alla spesa principale. Si suddividono i costi in tre componenti: personale, software e hardware. La prima categoria include tutte le spese relative alla formazione del personale, mentre le altre due rappresentano i costi degli strumenti. Questa classificazione tripartita si applica sia all'intervento principale sia ai costi associati che lo abilitano o che ne derivano successivamente. Questo approccio, sebbene richieda uno sforzo maggiore iniziale, fornisce una base solida per impostare una determinazione standard dei budget e consente di raggruppare i costi secondo tipologia e scopo. Per future estensioni del framework, è importante ampliare la valutazione includendo sia le spese operative (OPEX) sia le spese in conto capitale (CAPEX). Una volta integrati questi elementi, sarà possibile approfondire ulteriormente la scelta dell'orizzonte temporale appropriato per l'analisi e determinare un tasso di sconto adeguato, rendendo il modello più completo e coerente con le pratiche di valutazione economica degli investimenti in sicurezza.

3. Discussione

Il framework ha due rami principali che corrispondono a due aree di applicazione del modello di ROSI. Il primo riguarda l'uso dello strumento manageriale ROSI per la valutazione degli investimenti passati, mentre il secondo consente applicazioni per la valutazione strategica degli investimenti a priori. Una valutazione disaggregata dell'impatto degli investimenti in cybersicurezza implementati consente una comprensione più granulare della loro efficacia nei diversi contesti organizzativi, e permette la creazione di una classificazione degli investimenti fatti. Sfruttando la modularità del modello ROSI proposto, questa valutazione può essere condotta lungo tre dimensioni principali.

– Per tipologia di PMI, al fine di individuare quale abbia ottenuto i risultati migliori rispetto all'investimento effettuato. Per operare un confronto tra diverse PMI, la partecipazione delle organizzazioni ad un ecosistema collaborativo diventa quindi un requisito essenziale. Nel lungo periodo, grazie a tale aggregazione, dovrebbero emergere informazioni sui fattori specifici di settore, sulla dimensione e sul livello di maturità che influenzano in modo significativo gli esiti degli investimenti in sicurezza.
– Per tipologia di intervento o anche di sotto-intervento, così da identificare quali categorie di misure di cybersicurezza, ad esempio aggiornamenti tecnologici piuttosto che programmi di formazione, abbiano prodotto i migliori ritorni.
– Per fasce di ROSI, in modo da distinguere i cluster di performance e agevolare il benchmarking.

Una raccolta sistematica di dati sul livello di postura cyber di un'organizzazione in diversi momenti temporali, nonché dei valori disaggregati di ROSI per tipo di investimento, categoria organizzativa o settore, permetterebbe non solo delle analisi ex post più approfondite, ma anche l'addestramento di modelli di machine learning. Questi dataset potrebbero costituire input utili a sistemi progettati per individuare pattern nelle caratteristiche organizzative che si correlano a ritorni elevati (o bassi) sugli investimenti in cybersicurezza, con lo scopo di sviluppare strumenti di supporto decisionale sempre più mirati. Analogamente ad altre metodologie data-driven, se progettati con cura e implementati correttamente, questi approcci consentono di acquisire una maggiore consapevolezza della natura complessa e multivariata delle sfide legate alla cybersecurity.

L'altro ramo applicativo del framework economico è costituito dalle valutazioni ex ante dei futuri fabbisogni di investimento delle organizzazioni, identificando le aree a cui dare priorità per gli investimenti in cybersicurezza. Questo approccio proattivo garantisce che le risorse vengano allocate in modo efficiente e in coerenza con gli obiettivi organizzativi e di sicurezza. Considerando l'utilità di questa ricerca e la possibilità, nel lungo periodo, di renderla orientata all'utente a livello manageriale, è possibile sviluppare in parallelo uno strumento operativo. Sfruttando i dati specifici dell'organizzazione, tale strumento potrebbe fornire valutazioni personalizzate del ROSI, migliorando il processo decisionale attraverso analisi contestualizzate e promuovendo la consapevolezza e l'informazione riguardo a strategie di investimento in cybersicurezza.

Vi sono due elementi particolarmente versatili in questo senso, che sono rispettivamente la probabilità di attacco e la valutazione della postura cyber complessiva delle organizzazioni. Se derivata da una mappatura completa delle vulnerabilità, la stima della probabilità di attacco offre informazioni significative sul profilo di rischio dell'organizzazione. In merito invece alla postura cyber complessiva: consente di delineare una visione del potenziale ritorno sull'investimento basata sulla configurazione di sicurezza e sul livello di maturità presenti. Infine, riguardo le valutazioni economiche ex-ante, un altro filone applicativo è la switching point analysis, ovvero l'analisi del punto di pareggio temporale in cui i benefici cumulativi di un investimento eguagliano il suo costo iniziale. È particolarmente utile perché offre una stima immediata della durata media necessaria affinché una spesa per la sicurezza si trasformi in un investimento capace di generare ritorni. Tuttavia, è necessario stabilire alcune specifiche metodologiche anche in questo caso. Occorre definire un tasso di sconto, che dovrebbe basarsi su una revisione accurata della letteratura. Il team ha adottato un tasso di sconto annuale del 15% (Economics, Rate of Return to Investment in R&D, London; Economics, Rates of return to investment in science and innovation, July 2014). Un'ultima nota: qualora si considerino le spese indirette e operative (OPEX) nella componente di costo del ROSI, le quali richiedono un trattamento più dinamico dei costi di investimento nel tempo, il tema dei tassi di sconto diventa più articolato.

Avendo ora chiare sia la radici che i rami applicativi del modello ROSI, si può osservare con maggiore consapevolezza che le pratiche di data governance servono sia per abilitare una corretta misurazione del ROSI, sia per potenziare le applicazioni e gli sviluppi di un tale strumento nel contesto organizzativo. Si riprendono ora uno alla volta alcuni punti cardine dell'ambito precedentemente citati, per discutere le eventuali implicazioni di questo studio ADR su ciascuno di questi punti.

Il primo riguardava la complessità della data governance in organizzazioni ad alta interoperatività. I dati secondari provenienti da report, insieme ai take-away del workshop che ha caratterizzato una delle iterazioni dell'ADR, hanno confermato che il problema cyber è amplificato nei contesti organizzativi ad alta interoperatività. È dunque importante avere una metodologia di gestione dei dati per le aree non coperte dai framework delle singole organizzazioni, che operi con una visione ad un ampio spettro, considerando il sistema nella sua totalità. In un ecosistema, nessun elemento attore ha il controllo completo sui dati (Spagnoletti, Kazemargi, Constantinides & Prencipe, 2025). La standardizzazione delle pratiche di cyber risk management delle singole organizzazioni è una risorsa per semplificare l'integrazione dei dati, e per la valutazione del rischio associato. Inoltre, considerando un sistema di organizzazioni, la compatibilità delle loro pratiche di data governance individuali diventa un tema time-consuming di notevole complessità. Supponendo però che le singole organizzazioni abbiano un framework standard, modulare, predisposto all'interoperatività, il problema della compatibilità tende a ridursi. In aggiunta, nel momento di integrazione, il fatto che le organizzazioni siano standardizzate nei loro processi interni facilita l'individuazione delle differenze, sia di contesto che in termini di postura cyber. In tal senso, l'interoperatività si rivela come un'opportunità di compensazione reciproca delle rispettive carenze.

Il secondo punto tratta un aspetto più pratico della data governance, ovvero quello

della cooperazione facilitata da strumenti IT ad hoc. Il team ADR ha sviluppato un prototipo in Python per il calcolo di ROSI, perché lo studio è orientato ad essere utile a medio termine all'utente manageriale, tramite lo sviluppo parallelo di uno strumento con interfaccia operativa. Sfruttando i dati specifici dell'organizzazione, tale strumento potrebbe fornire valutazioni personalizzate del ROSI, migliorando il processo decisionale attraverso analisi contestualizzate e promuovendo strategie di investimento in cybersicurezza più consapevoli e informate. Similmente, un analogo progetto potrebbe essere portato avanti per la semplificazione delle pratiche di data governance. Anche in questo caso, avere un'interfaccia adeguato comporterebbe diversi vantaggi: renderebbe più fruibili le pratiche di data governance anche per organizzazioni medio-piccole o con carenza di expertise, semplificherebbe la gestione a medio e alto livello organizzativo, e faciliterebbe la comunicazione e la comprensione della rilevanza delle pratiche stesse.

Concludiamo considerando la data governance nei contesti organizzativi con risorse limitate, sia in termini economici sia di competenze. Lo studio ADR ha mostrato che un approccio incrementale al framework per gli investimenti in cybersicurezza è possibile. Dunque, si può pensare di estendere questa impostazione anche all'ambito della governance, così da consentire di compiere i primi passi soprattutto in contesti in cui manca consapevolezza della rilevanza del tema. A tal proposito, risulta appropriato riportare un altro risultato emerso dall'ADR, nello specifico uno dei take-away del workshop in cui hanno avuto voce esperti del settore. Per fare un passo avanti nella postura cyber, la dimensione su cui si interviene influenza l'impatto dell'intervento iniziale. Per le dimensioni labour-driven, che comprendono anche tutta la parte relativa alla formazione del personale sui temi cyber, un piccolo avanzamento nella postura cyber comporta un sostanziale miglioramento in termini di efficienza. Considerata la generalità di queste dimensioni, è lecito sospettare che quanto osservato valga analogamente per i temi di data governance, rendendo quindi conveniente includere nel primo raggio di intervento per le PMI la parte relativa alla formazione su questo campo.

4. Conclusioni

Negli ultimi anni il numero globale di attacchi è quasi raddoppiato – passando da una media mensile di 156 eventi nel 2020 a 295 nel 2024 – e l'Italia, pur rappresentando appena lo 0,7% della popolazione mondiale e l'1,8% del PIL globale, ha registrato nel territorio nazionale il 10% degli attacchi del 2024, a fronte del 4% della Francia e del 3% di Germania e Regno Unito (CLUSIT, 2025). Il rapporto ENISA Threat Landscape 2025 (ENISA, 2025) identifica i cinque settori maggiormente targetizzati in Europa, che rappresentano il 53,7% del numero totale di incidenti registrati: la pubblica amministrazione, i trasporti, le infrastrutture e i servizi digitali, il settore finanziario e quello manifatturiero. Tra questi, le PA emergono come il settore più preso di mira e contano il 38,5% degli attacchi in EU (principalmente DDoS a basso impatto); in particolare, in Italia gli attacchi alle PA sono passati da 560 nel 2023 a

1430 nel 2024. Allo stesso tempo, rimangono un target importante sia i trasporti che le infrastrutture e i servizi digitali, settori che richiamano particolarmente i temi di interoperatività precedentemente citati.

Questi dati non solo evidenziano la centralità delle PA nel panorama del rischio cyber, ma suggeriscono anche che future indagini empiriche finalizzate a migliorare il framework dell'ADR presentato potrebbero estendersi al design di una misura sistemica per ottimizzare gli investimenti in data governance, sia nel pubblico che nel privato. Considerando poi la crescente realtà dei contesti organizzativi ad alta interoperatività, la ricerca futura si dovrebbe anche spostare verso una prospettiva integrata. Le PMI ricoprono in questo scenario un ruolo di parte debole per la scarsità delle risorse, e proprio per questo risultano allora ambienti in cui analizzare costi marginali, elaborare le priorità di investimento e valutare le ricadute sulla continuità operativa. Un soggetto invece particolarmente sensibile agli attacchi sono le catene di fornitura, ma d'altra parte sono proprio quelle per cui la data governance è un fattore di coordinamento particolarmente strategico. Sarebbe dunque vantaggioso estendere la ricerca ADR svolta per gli investimenti in cybersicurezza a quelli in data governance, mantenendo invariati gli obiettivi di ottimizzazione e il principio di modularità con cui l'artefatto è progettato. In termini concettuali, si tratterebbe si applicare un approccio analogo a quello che, in machine learning, viene definito transfer learning. Un esempio è ben riportato dalla Tabella 1, in cui si mostra come alcuni risultati dell'ADR possano orientare le priorità e le modalità di ricerca nel dominio della data governance.

Tabella 1. Esempi di risultati dell'Action Design Research (ADR) applicati alla data governance

Tema di Data Governance	Risultati ADR	Implicazioni relative a future ricerche
Complessità della data governance in contesti ad alta interoperatività	Rischio cyber è amplificato nei contesti inter-organizzativi; la standardizzazione riduce l'incompatibilità.	Promuovere framework modulari e standard per facilitare l'integrazione dei dati e la valutazione dei rischi nel contesto ad alta interoperatività.
Tools facilitatori per la data governance	Strumenti operativi (es.: prototipo ROSI in Python) traducono il framework in supporto gestionale.	Sviluppare interfacce dedicate alla data governance per semplificare le pratiche, anche in organizzazioni medio-piccole o con scarsa expertise.
Data governance in contesti con risorse limitate (PMI)	L'approccio incrementale è sostenibile anche per realtà con risorse ridotte.	Adottare strategie graduali, partendo dalla formazione del personale, per rafforzare la maturità nella data governance.

Messaggi chiave:

- ROSI come strumento decisionale strategico modulare e adattabile.
- Standardizzazione graduale delle pratiche delle PMI, per facilitare il coordinamento in contesti organizzativi ad alta operatività.
- Trasferibilità del metodo di ricerca ADR dagli investimenti in cybersecurity a quelli in data governance.

Bibliografia

Abraham, R., Schneider, J. & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research T agenda. *International Journal of Information Management*, 424-438.

Arshad, A., Abbas, H., Faisal Amjad, M., Shafqat, N. & Yaqoob, T. (2019). Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations. *Future Generation Computer System*, 754-763.

Arshad, Abbas, Amjad, F., Shafqat & Yaqoob. (n.d.).

Assenza, G., Ortalda, A. & Setola, R. (2024). Redefining systemic cybersecurity risk in interconnected enviroments. *ACIG*, vol. 3, no. 2, 144-169.

Barik, K., Misra, S., Fernandez-Sanz, L. & Koyuncu, M. (2023, 10 14). RONSI: a framework for calculating return on network security investment. *Telecommunication System*, Vol. 84, 533-548.

Begg, C. & Caira, T. (2011). Data governance in practice: the SME quandary reflections on the reality of data governance in the small to medium enterprise (SME) sector. *Proceedings of the 5th European Conference on Information Management and Evaluation (ECIME)*, 75-83.

Bodendorf, F. & Bayr, C. (2025, March). Shaping Platform Governance Principles to Manage Interorganizational Data Exchange. *Information Systems Journal*, *35*(5), 1477-1496.

Böhme & Moore. (2010). The Iterated Weakest Link. *IEEE Security and Privacy Magazine*, 53-55.

Butler, S.A. (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach. *Proceedings of the 24th international conference on Software engineering*, *ACM*, 232-240.

CLUSIT (2025). *Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2025.* Security Summit.

Collier, Z., Briglia, B., Slutzky, D. & Lambert, J. (2023). On metrics and prioritization of investments in hardware security. *Systems Engineering*, 425-437.

Economics, F. (July 2014). *Rates of return to investment in science and innovation.* London: Frontiers Economics Ltd.

Economics, F. (2023). *Rate of Return to Investment in R&D.* March 2023: Frontier Economics Ltd.

ENISA (2025). *ENISA THREAT LANDSCAPE October 2025.*

Franco, M.F., Künzler, F., Von der Assen, J., Feng, C. & Stiller, B. (2024). RCVaR: An economic spproach to estimate cyberattacks costs using data from industry reports. *Computers & Security*.

Gheorghe, M. (2012). Investment Decision Analysis In Information Security. *Révista Economica – Information Security Management*, 85-93.

Gordon, L.A. & Loeb, M.P. (2002). The Economics of Information System Security. *ACM Transactions on Information and System Security*.

IBM, S. & Ponemon, I. (2024). *Cost of a Data Breach 2023 Report.* IBM Security.

Jonhson, V., Maurer, C., Torres, R., Guerra, K. & Mohit, H. (2024). The 2023 SIM IT Issues and Trends Study. *MIS Quaterly Executive*, Vol. 23, Iss. 1, Article 7.

Liu, G., Zhang, J. & Chen, G. (2014, 09 19). An approach to finding the cost-effective immunization targets for information assurance. *Decision Support Systems*, 40-52.

Marican, M.N., Othman, S.H., Selamat, A. & Razak, S.A. (2024). Quantifying the Return On Security Investments for Technology Startups. *Baghdad Science Journal*, 2449-2461.

Oliva, G., Faramondi, L., Setola, R., Tesei, M. & Zio, E. (2021). A multi-criteria model for the security assessment of large-infrastructure construction sites. *International Journal of Critical Infrastructure Protection*.

Onwubiko, C. & Onwubiko, A. (2019). Cyber KPI for Return on Security Investment. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA).*

Pontes, E., Guelfi, A.E., Silva, A.A. & Kofuji, S.T. (2011). A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI). *Risk Management in Environment Production and Economy*, p. Chapter 7.

Ribeiro, V., Barata, J. & da Cunha, P.R. (2024). Modeling inter-organizational business process governance in the age of collaborative networks. *Electronic Markets*, 34-51.

Rombaldo Junion, C.B. & Johnson, S. (2023). *A Systematic Review of SME Cybersecurity*, 1-32.

Sein, M.K., Henfridsson, O., Purao, S., Rossi, M. & Lindgren, R. (2011). Action Design Research. *MIS Quarterly*, Vol. 35 No. 1, 37-56.

Solek-Borowska, C. & Wozniak, J. (2024). Data and IT Systems Security in Contemporary Organizations. *Journal of Computer Information System*.

Sonnenreich, W., Albanese, J. & Stout, B. (2006). Return On Security Investment (ROSI) – A Practical Quantitative Model. *Journal of research and practice in information technology*, *38*(1), 45-56.

Spagnoletti, P., Kazemargi, N., Constantinides, P. & Prencipe, A. (2025). Data Control Coordination in the Formation of Ecosystems in Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors. *Journal of the Association for Information Systems*, *26*(4), 977-1008.

Tsiakis, T. & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, 105-108.

Verhoef, P.C., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N. & Haenlein, M. (2021). In *Digital transformation: A multidisciplinary reflection and research agenda* (pp. 233-341). *Journal of Business Research*, 122.

Lock-in dei dati nelle smart city: meccanismi, effetti e sfide nella governance urbana

Filippo Marchesani [*] e Federica Ceci [**]

Abstract: Nelle smart city, la disponibilità e l'uso dei dati sono considerati leva fondamentale per ottimizzare servizi, politiche e processi urbani. Tuttavia, le città rischiano di rimanere vincolate da dinamiche di lock-in dei dati, che limitano l'innovazione, l'interoperabilità e la capacità di adattarsi alle nuove tecnologie. Questo studio esplora i meccanismi istituzionali, contrattuali e organizzativi del lock-in dei dati in contesti urbani emergenti, con un'analisi qualitativa basata su 22 interviste a dirigenti pubblici coinvolti in progetti smart city nel comune di Pescara. I risultati identificano tre logiche principali: rigidità contrattuale nei processi di procurement, dipendenza da piattaforme proprietarie e standard chiusi, e monopolio sui diritti di accesso ai dati. Questi meccanismi operano in sinergia, generando costi di switching elevati per la Pubblica Amministrazione e riducendo la capacità di collaborazione, apertura dei dati e innovazione urbana. Il contributo mostra che il lock-in dei dati deriva da scelte di governance, assetti organizzativi e contrattuali, non solo da fattori tecnici. Evidenzia la necessità di strategie di acquisto flessibili, modelli di governance chiari e standard aperti e interoperabili per mitigare la dipendenza dai fornitori.

Parole chiave: Smart Cities, Data, Data Ecosystem, Lock-in, Trasformazione Digitale.

1. Introduzione

Negli ultimi anni il concetto di smart city ha assunto una centralità crescente nelle agende politiche, nelle pratiche amministrative e nella ricerca accademica (Caragliu & Del Bo, 2019). Con il termine smart city si fa riferimento a un modello urbano che utilizza tecnologie digitali, dati e connettività per migliorare l'efficienza dei servizi, favorire la sostenibilità ambientale ed economica, e accrescere la qualità della vita dei cittadini (Vanolo, 2014). Le smart cities non sono semplicemente città dotate di

[*] Filippo Marchesani (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: filippo.marchesani@unich.it

[**] Federica Ceci (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: federica.ceci@unich.it

DOI: 10.82018/9791221165456-7

tecnologie avanzate, ma veri e propri ecosistemi socio-tecnici in cui amministrazioni, imprese, fornitori di tecnologie e cittadini interagiscono attraverso piattaforme digitali, infrastrutture di dati e sistemi di governance complessi (Marchesani & Ceci, 2025).

Se da un lato le smart city incarnano la promessa di una gestione più efficiente, trasparente e inclusiva dei processi urbani, dall'altro emergono criticità legate alla dipendenza tecnologica, alla frammentazione delle competenze e ai vincoli contrattuali che limitano l'apertura e l'innovazione. In questo quadro, uno dei nodi più rilevanti è rappresentato dal lock-in dei dati, ovvero la tendenza delle città a rimanere vincolate a specifici fornitori, piattaforme o standard tecnologici che rendono difficile, costoso o addirittura impossibile il cambiamento, l'interoperabilità e la scalabilità delle soluzioni digitali adottate nelle dinamiche di governance urbana (Bibri & Krogstie, 2020; Marchesani et al., 2024; Marchesani & Ceci, 2024). In questo senso, il concetto di governance urbana assume un ruolo fondamentale nell'analizzare questi processi. Con governance, in accordo con Pittaway & Montazemi (2020), non si intende soltanto l'insieme delle regole formali e delle istituzioni, ma anche le pratiche, le responsabilità e le relazioni che determinano come le decisioni vengono prese, attuate e monitorate in un contesto urbano. Nelle smart city, la governance si configura come un processo multi-attore che coinvolge amministrazioni pubbliche, aziende tecnologiche, fornitori di servizi urbani, organizzazioni semi-pubbliche e comunità di cittadini.

Il passaggio a una governance basata sui dati comporta una profonda trasformazione organizzativa. I dati diventano non solo input informativi per le decisioni, ma asset strategici che definiscono poteri, ruoli e responsabilità (Mora, 2023). Chi controlla i dati detiene infatti un vantaggio competitivo e politico, poiché può indirizzare le politiche urbane, sviluppare nuovi servizi e definire le priorità di investimento (Schiavone et al., 2020). Per questo motivo la sovranità dei dati e la capacità delle amministrazioni di esercitare un controllo effettivo sulla loro raccolta, gestione e utilizzo sono diventate questioni cruciali per le città.

L'emergere delle smart city ha portato con sé la creazione di veri e propri ecosistemi di dati, considerati reti complesse in cui informazioni provenienti da sensori, piattaforme digitali, servizi pubblici e privati vengono raccolte, elaborate e integrate (Kazemargi et al., 2025; Oliveira et al., 2019). Questi ecosistemi sono caratterizzati da confini fluidi, poiché coinvolgono attori diversi con logiche e interessi eterogenei. Da un lato vi sono le amministrazioni locali, responsabili della gestione dei servizi e della tutela dell'interesse pubblico; dall'altro, le imprese tecnologiche e i fornitori di piattaforme, che offrono soluzioni digitali e infrastrutture di raccolta e analisi dei dati. Accanto a questi attori, un ruolo crescente è svolto dai cittadini, non solo come destinatari dei servizi ma anche come produttori attivi di dati attraverso l'uso quotidiano di applicazioni e dispositivi connessi. Questa molteplicità di attori rende gli ecosistemi di dati urbani al tempo stesso dinamici ma vulnerabili (Li & Liao, 2018). Da un lato, infatti, la collaborazione pubblico-privato consente di sviluppare soluzioni tecnologiche avanzate anche in contesti caratterizzati da risorse limitate, come le città di medie dimensioni (Gascó, 2017). Dall'altro, la dipendenza da fornitori

esterni e da standard proprietari genera rischi significativi di lock-in in quanto i dati prodotti e gestiti attraverso piattaforme chiuse possono risultare difficili da migrare verso altri sistemi, ostacolando l'interoperabilità e limitando la possibilità di sfruttare appieno il potenziale di innovazione (Kummitha, 2024).

La relazione tra città, fornitori tecnologici e cittadini si gioca in gran parte sul terreno dei dati. Le imprese tecnologiche forniscono piattaforme, software e infrastrutture digitali, spesso attraverso contratti di lungo periodo che vincolano i comuni a specifici standard. Le amministrazioni, pur mantenendo formalmente la titolarità dei dati, si trovano spesso in una posizione di debolezza nei confronti dei fornitori, a causa della scarsità di competenze interne e della complessità tecnica dei sistemi (Linde et al., 2021). I cittadini, a loro volta, contribuiscono costantemente alla generazione di dati attraverso le loro interazioni digitali, ma raramente hanno un reale controllo su come tali dati vengono utilizzati.

In questo scenario, il lock-in dei dati non riguarda soltanto la dimensione tecnologica, ma si manifesta come un fenomeno istituzionale e organizzativo. Le regole di procurement, le responsabilità frammentate e le procedure burocratiche contribuiscono a rafforzare la dipendenza dai fornitori e a ridurre la capacità della città di esercitare una governance autonoma e adattiva. Nonostante la crescente attenzione verso le smart city e l'importanza dei dati come infrastruttura abilitante, la letteratura ha finora trascurato di analizzare in profondità i meccanismi di lock-in dei dati e le loro implicazioni per la governance urbana. Restano dunque aperti interrogativi fondamentali su come le città possano bilanciare la necessità di collaborare con attori esterni e la salvaguardia della propria autonomia strategica. Alla luce di queste considerazioni, il presente studio si propone di rispondere alle seguenti domande di ricerca: "*Quali meccanismi di lock-in dei dati emergono nella gestione delle smart city e in che modo influenzano la capacità di innovazione e apertura delle amministrazioni urbane?*" e "*Come le città di medie dimensioni possono sviluppare strategie di governance dei dati in grado di ridurre la dipendenza dai fornitori esterni e salvaguardare la sovranità digitale e l'accountability pubblica*?" al fine di comprendere la gestione, dell'ecosistema dei dati all'interno dei progetti di smart city.

2. Analisi della letteratura e framework concettuale

La letteratura sulle smart city si è in gran parte concentrata sul potenziale delle tecnologie digitali per rendere le città più efficienti, sostenibili e inclusive (Caragliu & Del Bo, 2019; Linde et al., 2021; Marchesani & Ceci, 2025). Tuttavia, l'attenzione agli effetti vincolanti e ai rischi di lock-in dei dati è rimasta limitata, specialmente nel caso delle città di medie dimensioni, che dispongono di risorse e competenze ridotte rispetto ai grandi centri urbani. Il lock-in tecnologico, in accordo con la definizione proposta da Foxon (2007) può essere definito come un fenomeno di dipendenza da percorsi e scelte passate, che rende difficile abbandonare determinate

soluzioni tecnologiche, istituzionali o organizzative anche quando emergono alternative più efficienti o innovative. Nel contesto delle smart city, il lock-in si manifesta principalmente lungo tre dimensioni che riguardano (i) la rigidità contrattuale nei processi di procurement, (ii) la dipendenza da piattaforme proprietarie e standard chiusi, ed (iii) il monopolio sui diritti di accesso ai dati. Queste tre forme di vincolo interagiscono tra loro, rafforzandosi reciprocamente e generando un circolo vizioso che ostacola apertura, innovazione e scalabilità.

2.1. Rigidità contrattuale nei processi di procurement

Il procurement è uno dei principali strumenti attraverso cui le amministrazioni pubbliche adottano tecnologie digitali. La letteratura sottolinea come i contratti pubblici possano fungere sia da leva di innovazione (van Winden & Carvalho, 2019) sia da freno, qualora risultino troppo prescrittivi e rigidi (Eckersley et al., 2023). Nei contesti urbani, procedure di gara altamente dettagliate tendono a vincolare le città a specifiche soluzioni tecnologiche, definendo standard che non possono essere facilmente modificati nel tempo.

Questa rigidità genera lock-in contrattuale, poiché le città restano legate a fornitori e specifiche tecniche anche quando emergono soluzioni più avanzate. Una volta assegnata la gara, i costi di switching diventano elevati, sia in termini economici che di competenze necessarie a sostituire il sistema. Questo fenomeno è stato documentato in vari contesti europei, dove la burocrazia e la necessità di garantire trasparenza limitano la possibilità di adottare approcci più flessibili (Pereira et al., 2018).

Per le smart city, il procurement rigido può impedire la sperimentazione, l'adattamento rapido e la co-creazione con attori locali. In assenza di contratti adattivi o clausole di interoperabilità, le città rischiano di trasformare processi di innovazione in percorsi vincolati, riducendo la capacità di apprendere e adattarsi (Fu & Zhu, 2020). La mancanza di competenze interne nella stesura dei bandi accentua il problema, favorendo posizioni dominanti da parte dei grandi fornitori tecnologici.

2.2. Dipendenza da piattaforme proprietarie e standard chiusi

Le piattaforme digitali rappresentano il cuore degli ecosistemi di dati urbani, poiché consentono la raccolta, l'elaborazione e l'analisi delle informazioni provenienti da sensori, servizi digitali e interazioni dei cittadini (Curry, 2016). Esse assumono la forma di infrastrutture urbane digitali che, una volta implementate, definiscono l'architettura entro cui si svolge la governance dei dati. Quando le piattaforme sono proprietarie e basate su standard chiusi, le città entrano in una condizione di dipendenza tecnologica (Katz & Shapiro, 1985). Questo fenomeno genera barriere all'ingresso per nuovi attori, ostacola l'interoperabilità tra sistemi diversi e limita la possibilità di sviluppare soluzioni open-source. Inoltre, i dati raccolti e gestiti attraverso tali

piattaforme restano intrappolati in ambienti chiusi, riducendo la trasparenza e le opportunità di riuso.

La letteratura mostra come grandi multinazionali dell'ICT (es. IBM, Cisco, Microsoft) abbiano assunto un ruolo di primo piano nel definire gli standard tecnologici delle smart city (Kummitha, 2018; Marchesani & Ceci, 2025). Questi attori non solo forniscono infrastrutture e software, ma influenzano direttamente le scelte di governance, imponendo architetture proprietarie difficilmente sostituibili. In tal senso, la dipendenza da piattaforme proprietarie si configura come un meccanismo di lock-in che, una volta instaurato, è difficile da invertire senza ingenti costi di transizione.

Le città di medie dimensioni sono particolarmente vulnerabili a tali dinamiche, poiché mancano delle risorse per sviluppare piattaforme proprie o per negoziare condizioni più favorevoli con i fornitori (Barba-Sánchez et al., 2019). Il risultato è un ecosistema digitale in cui la flessibilità promessa dalle tecnologie smart si traduce in rigidità strutturale, con scarsa capacità di adattamento e innovazione locale.

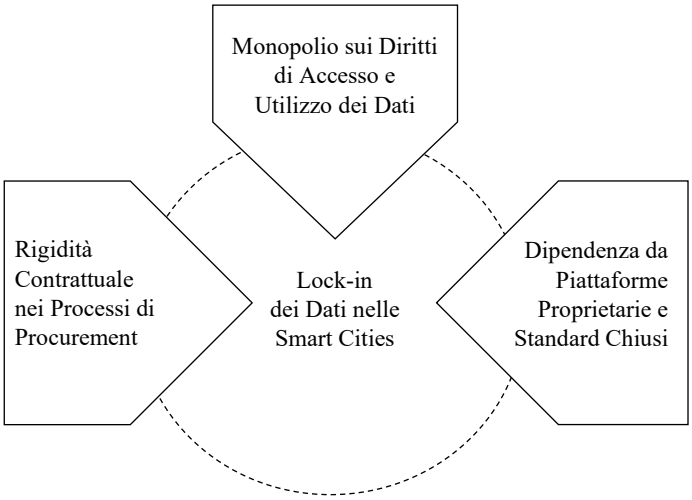
2.3. Monopolio sui diritti di accesso ai dati

I dati urbani costituiscono sempre più un bene comune (Bibri & Krogstie, 2020), cruciale per la pianificazione, il monitoraggio delle politiche e la creazione di nuovi servizi. Tuttavia, il controllo su chi può accedere ai dati e in che modo rappresenta un nodo cruciale della governance delle smart city. Spesso i diritti di accesso restano concentrati in mano a pochi attori come le amministrazioni comunali, che detengono la titolarità, o i fornitori tecnologici, che ne gestiscono la raccolta e lo stoccaggio (Lnenicka et al., 2022). Questo monopolio sui diritti di accesso produce un duplice effetto in quanto da un lato, rafforza la sovranità dei dati da parte dei comuni, garantendo protezione e sicurezza; dall'altro, limita la possibilità di sperimentazione, innovazione aperta e collaborazione con imprese locali o startup (Yun et al., 2015). Il lock-in si manifesta dunque non solo come dipendenza tecnologica, ma anche come vincolo istituzionale che riduce la circolazione dei dati.

La chiusura dei dati ostacola lo sviluppo di modelli di innovazione aperta, come living labs o hackathon, che si basano sulla disponibilità di dataset pubblici e interoperabili (Gascó, 2017). Inoltre, l'asimmetria di accesso tra grandi provider e piccoli attori locali rischia di rafforzare ulteriormente le disuguaglianze, consolidando posizioni dominanti e limitando la pluralità dell'ecosistema urbano (Cledou et al., 2018).

Sulla base della discussione precedente e del dibattito accademico in corso, emerge la configurazione presentata in Figura 1, che sintetizza la struttura concettuale del lock-in dei dati nella gestione delle smart city. Il framework integra le tre dimensioni individuate mostrando come esse si intreccino e si rafforzino reciprocamente, generando meccanismi di vincolo che ostacolano l'apertura, l'innovazione e la capacità di adattamento delle città.

Figure 1. – Framework Concettuale



3. Metodologia

Considerata la natura governativa e strategica del fenomeno analizzato e la necessità di esplorare in profondità i diversi ambiti organizzativi e istituzionali coinvolti, questo studio adotta un approccio qualitativo fondato su interviste semi-strutturate. Tale scelta metodologica consente di indagare in modo articolato le percezioni, le pratiche e le strategie attraverso cui le amministrazioni locali affrontano le dinamiche di lock-in dei dati nella gestione delle smart city (Mergel et al., 2019). L'obiettivo è comprendere come si configurano i meccanismi che limitano l'apertura e la flessibilità dei sistemi urbani digitali, nonché le modalità con cui i dirigenti pubblici cercano di mitigarne gli effetti.

L'analisi si inserisce nel contesto italiano, caratterizzato da una diffusa spinta alla digitalizzazione dei servizi pubblici e da un crescente interesse politico verso la trasformazione delle città in ecosistemi intelligenti (Caragliu et al., 2011; De Matteis et al., 2021; Marchesani et al., 2025; Marchesani & Ceci, 2025). In particolare, lo studio si concentra sul caso della città di Pescara, scelta come riferimento empirico per tre motivi principali. In primo luogo, Pescara rappresenta una delle realtà urbane di medie dimensioni più avanzate in Italia in termini di digitalizzazione e adozione di tecnologie smart, collocandosi tra le prime dieci città nella classifica nazionale delle smart city. In secondo luogo, la sua dimensione intermedia (circa 120.000 abitanti) offre un equilibrio interessante tra scala amministrativa e capacità innovativa, consentendo di analizzare in modo realistico le sfide di governance tipiche delle città non metropolitane. In terzo luogo, la città si trova in una fase di forte evoluzione istituzionale e territoriale: il processo di fusione con i comuni limitrofi di Montesilvano e

Spoltore, previsto entro il 2027, comporta una riorganizzazione profonda delle competenze, delle infrastrutture e delle relazioni interistituzionali, creando un contesto ideale per osservare come il lock-in dei dati si manifesta e si riproduce durante la transizione digitale.

La scelta di un caso singolo è coerente con l'obiettivo esplorativo dello studio, che mira a costruire un quadro interpretativo approfondito piuttosto che a generalizzare i risultati. Attraverso un'analisi qualitativa, è possibile cogliere la natura situata e contestuale dei meccanismi di lock-in, spesso invisibili in analisi di tipo quantitativo o comparato (Gioia et al., 2013). In questa prospettiva, il caso di Pescara offre spunti teorici e implicazioni pratiche per altre città di dimensioni simili impegnate nei processi di trasformazione digitale.

Lo studio si propone quindi di contribuire al dibattito accademico sulla governance dei dati urbani e di fornire indicazioni operative utili alle amministrazioni pubbliche che intendono rafforzare la propria autonomia digitale, prevenendo fenomeni di dipendenza tecnologica e istituzionale.

3.1. Protocollo interviste e raccolta dati

L'indagine si fonda su un approccio qualitativo basato su interviste semi-strutturate, condotte nell'arco di quindici mesi, tra gennaio 2023 e aprile 2024. Questo arco temporale ha consentito di osservare in modo continuativo l'evoluzione dei progetti di digitalizzazione e di cogliere le diverse modalità attraverso cui la municipalità ha affrontato le sfide legate alla gestione dei dati e ai meccanismi di lock-in che ne derivano. La struttura delle interviste è stata progettata per esplorare in profondità le dimensioni operative e strategiche della trasformazione digitale all'interno dell'amministrazione comunale, con particolare attenzione alla relazione tra governance, processi tecnologici e gestione dei dati.

Le interviste erano basate su un protocollo articolato in cinque sezioni, che spaziavano dalle informazioni preliminari sui ruoli, le responsabilità e le competenze degli intervistati, all'analisi dei principali progetti di digitalizzazione sviluppati all'interno dei diversi settori municipali. Le conversazioni hanno permesso di esaminare le tecnologie e le piattaforme digitali adottate, le competenze tecniche e relazionali richieste per la loro gestione, nonché la valutazione dei risultati ottenuti e degli ostacoli incontrati. Particolare attenzione è stata riservata alla comprensione dei vincoli generati da procedure di procurement rigide, dall'uso di piattaforme proprietarie e dai meccanismi di controllo sui diritti di accesso ai dati, poiché tali aspetti rappresentano le principali fonti di lock-in nel contesto delle smart city.

Le interviste hanno consentito di delineare un quadro chiaro dei ruoli e delle responsabilità dei dirigenti pubblici, di comprendere le logiche di funzionamento delle unità operative e di individuare le pratiche di collaborazione con fornitori tecnologici, imprese private e attori semi-pubblici. Il dialogo con i manager e i responsabili dei vari settori municipali (tra cui trasformazione digitale, servizi informativi,

mobilità, ambiente, infrastrutture e pianificazione urbana) ha permesso di osservare le differenze nelle strategie di gestione dei dati, nei livelli di autonomia tecnologica e nei gradi di dipendenza dai provider esterni. Parallelamente, l'analisi dei documenti amministrativi e dei contratti di fornitura digitale ha offerto un ulteriore livello di approfondimento, permettendo di comprendere in che modo le regole di procurement e le clausole contrattuali influenzino la possibilità della città di mantenere il controllo e la proprietà dei propri dati. Complessivamente, sono state realizzate 22 interviste, un numero in linea con gli standard qualitativi più consolidati negli studi sulle smart city, che di norma prevedono un campione di venti-trenta interlocutori chiave (Kummitha & Crutzen, 2019; Wiig, 2015). Gli intervistati comprendevano dirigenti, funzionari e responsabili di servizio appartenenti ai principali dipartimenti municipali, assicurando una copertura equilibrata delle aree di governance, economia, mobilità, qualità della vita e ambiente in linea con la definizione di smart cities proposta da Vanolo (2014). Le conversazioni, della durata compresa tra venti e sessantacinque minuti, sono state registrate, trascritte integralmente e successivamente analizzate per garantire la massima accuratezza interpretativa.

3.2. Analisi dei dati e procedura di codifica

Il materiale empirico raccolto ha generato un corpus di dati estremamente ricco, composto da circa 228 pagine di trascrizioni, escludendo le domande dell'intervistatore. L'analisi è stata condotta seguendo l'approccio delineato da Hannah e Robertson (2015), che consente di sintetizzare le informazioni emerse dalle interviste e di tradurle in categorie analitiche coerenti con l'obiettivo di ricerca. Il dataset è stato esaminato attraverso il software MAXQDA (versione 2024), che ha permesso di identificare pattern ricorrenti, connessioni e co-occorrenze tra concetti, restituendo un quadro sistematico delle pratiche e dei vincoli legati alla gestione dei dati urbani in linea con approcci simili utilizzati nel dominio della ricerca sulle smart cities (Linde et al., 2021; Neumann et al., 2019).

Questo processo ha reso possibile individuare e interpretare i tre meccanismi di lock-in più ricorrenti: la rigidità contrattuale nei processi di procurement, la dipendenza da piattaforme e standard proprietari, e il monopolio sui diritti di accesso e utilizzo dei dati. L'approccio metodologico adottato ha permesso di coniugare l'analisi empirica delle pratiche amministrative con una riflessione teorica più ampia sui modelli di governance dei dati urbani, offrendo così una prospettiva integrata su come le città di medie dimensioni, come Pescara, affrontano i vincoli imposti dalle infrastrutture digitali e dalle relazioni di dipendenza che ne derivano. In questo modo, il lavoro contribuisce a colmare il divario tra teoria e pratica, evidenziando come la gestione dei dati rappresenti non solo una sfida tecnologica, ma soprattutto un problema di governance, coordinamento e capacità istituzionale.

4. Risultati e contributi

L'analisi dei dati ha consentito di mettere in luce la natura e l'articolazione dei meccanismi di lock-in dei dati che si manifestano nella gestione delle smart city. Le evidenze empiriche raccolte mostrano come il blocco dei processi di innovazione non sia soltanto il risultato di vincoli tecnologici, ma derivi soprattutto da dinamiche istituzionali, organizzative e contrattuali che limitano la capacità delle amministrazioni locali di esercitare un controllo pieno e strategico sui propri dati.

In generale, emerge che le città di medie dimensioni, come Pescara, si trovano in una condizione di asimmetria informativa e di potere nei confronti dei fornitori tecnologici. In linea con la letteratura sulle smart cities (Linde et al., 2021; Linders, 2012; Mora, 2023; Pittaway & Montazemi, 2020), la scarsità di competenze interne, la complessità dei contratti pubblici e la frammentazione delle responsabilità determinano un sistema in cui i dati, pur formalmente appartenenti alla municipalità, sono spesso gestiti e resi operativi da soggetti esterni. Questo genera una tensione strutturale tra sovranità dei dati e dipendenza tecnologica, che si traduce in vincoli di lungo periodo e ostacola la scalabilità dei progetti digitali.

I risultati dell'analisi, emersi attraverso la codifica delle interviste e l'esame incrociato delle categorie tematiche, evidenziano tre forme principali di lock-in che definiscono la struttura e le dinamiche del sistema urbano dei dati: (i) la rigidità contrattuale nei processi di procurement, (ii) la dipendenza da piattaforme proprietarie e standard chiusi, e (iii) il monopolio sui diritti di accesso e utilizzo dei dati. Ciascuna di queste dimensioni rappresenta un ostacolo specifico alla costruzione di un ecosistema urbano aperto, interoperabile e realmente innovativo.

4.1. Rigidità contrattuale nei processi di procurement

Dalle interviste emerge che il primo e più pervasivo meccanismo di lock-in riguarda le modalità con cui i contratti pubblici definiscono l'acquisizione e la gestione delle tecnologie digitali. I dirigenti municipali intervistati hanno sottolineato come le gare d'appalto, spesso formulate in modo estremamente dettagliato, tendano a fissare specifiche tecniche rigide e durature, rendendo difficile modificare o aggiornare le soluzioni adottate. Questa rigidità contrattuale nasce dal tentativo di garantire trasparenza e tracciabilità, ma finisce per produrre l'effetto opposto. Infatti, questa rigidità blocca la capacità di adattamento dell'amministrazione e la vincola a soluzioni tecnologiche superate o non più efficienti. Queste evidenze estendono il discorso sulle dinamiche amministrative della pubblica amministrazione (Fu & Zhu, 2020; Pereira et al., 2018). Molti dei progetti digitali analizzati mostrano come le clausole contrattuali definiscano non solo i termini economici della fornitura, ma anche gli standard operativi e gli strumenti tecnologici da utilizzare, impedendo così l'introduzione di innovazioni successive. In diversi casi, la necessità di rinnovare le gare o ridefinire le specifiche comporta costi elevati e

ritardi significativi nei processi decisionali. I dirigenti riconoscono inoltre che la mancanza di competenze interne nella redazione dei bandi amplifica il rischio di lock-in, poiché le amministrazioni tendono ad accettare soluzioni preconfezionate proposte dai fornitori, con scarsa possibilità di personalizzazione o evoluzione (Thabit & Mora, 2023).

Questo tipo di vincolo istituzionale si traduce in una forma di dipendenza procedurale, in cui l'innovazione amministrativa viene subordinata alla logica contrattuale. In prospettiva, ciò limita la possibilità di adottare approcci sperimentali, di sviluppare partenariati flessibili e di implementare soluzioni basate su standard aperti. Il procurement, anziché costituire uno strumento di stimolo per l'innovazione, diventa così un meccanismo di cristallizzazione delle scelte passate.

4.2. Dipendenza da piattaforme proprietarie e standard chiusi

Il secondo meccanismo individuato riguarda la dipendenza da piattaforme tecnologiche proprietarie, che si traduce in una perdita di autonomia nella gestione dei dati e dei processi digitali. L'analisi delle interviste ha mostrato che la maggior parte delle soluzioni implementate dal Comune di Pescara è fornita da pochi grandi operatori tecnologici, in particolare da imprese che gestiscono infrastrutture digitali e servizi in cloud per numerose amministrazioni italiane.

Queste piattaforme, pur offrendo affidabilità e standardizzazione, generano vincoli strutturali poiché operano su protocolli chiusi e linguaggi spesso non interoperabili (Fu & Zhu, 2020; Scholl & Alawadhi, 2016). Una volta adottate, le amministrazioni faticano a migrare verso altri sistemi senza sostenere costi economici e organizzativi considerevoli. Le informazioni raccolte dai manager municipali indicano che la dipendenza non è soltanto tecnica, ma anche strategica: i fornitori controllano non solo gli strumenti, ma anche la conoscenza dei sistemi, le modalità di manutenzione e gli aggiornamenti futuri.

Questo crea un forte squilibrio di potere a favore dei provider, i quali diventano interlocutori privilegiati e, in molti casi, insostituibili (Wiig, 2015, 2016). Le amministrazioni si trovano così intrappolate in un circuito in cui la continuità operativa dei servizi digitali dipende dalla disponibilità e dalle condizioni imposte dai fornitori esterni. In diversi casi, la necessità di garantire la sicurezza dei dati o la continuità del servizio giustifica la scelta di mantenere l'intero sistema sotto il controllo del provider, rafforzando ulteriormente la dipendenza tecnologica e riducendo la capacità della pubblica amministrazione di sviluppare competenze interne autonome.

In questo scenario, il lock-in tecnologico si trasforma in un fenomeno sistemico che ostacola la creazione di un ecosistema urbano realmente aperto. Le piattaforme proprietarie, nate per semplificare la gestione dei dati, finiscono per limitare l'interoperabilità e ridurre la trasparenza, minando la sostenibilità a lungo termine delle strategie digitali urbane.

4.3. Monopolio sui diritti di accesso e utilizzo dei dati

Il terzo meccanismo di lock-in emerso riguarda il monopolio sui diritti di accesso e utilizzo dei dati urbani. Come evidenziato da Bibri & Krogste (2020) e da Lnenicka et al.,(2022), nella maggior parte dei casi, le informazioni prodotte dalle piattaforme digitali restano sotto il controllo di un numero ristretto di attori come le amministrazioni comunali, che ne detengono la titolarità formale, e i fornitori tecnologici, che ne gestiscono la raccolta, l'archiviazione e la protezione.

Questa struttura duale produce una tensione tra la necessità di garantire la sicurezza e la privacy dei dati e l'esigenza di favorire la condivisione e la collaborazione tra attori dell'ecosistema urbano (Gascó, 2017). I dirigenti comunali intervistati hanno sottolineato che la priorità assegnata alla protezione dei dati, sebbene legittima, finisce spesso per limitare l'accesso anche ad altri soggetti pubblici o privati che potrebbero contribuire allo sviluppo di servizi innovativi. Il risultato è un sistema chiuso, in cui i dati non circolano liberamente e non generano valore condiviso. Questo rappresenta un forte limite in quanto la letteratura evidenzia chiaramente il ruolo positivo dell'innovazione aperta all'interno dei progetti di smart cities (Marchesani & Ceci, 2025).

In molti casi, le imprese locali e le startup non riescono ad accedere ai dataset pubblici necessari per sviluppare applicazioni o soluzioni tecnologiche, poiché i contratti stipulati con i fornitori esterni stabiliscono restrizioni sull'uso secondario dei dati o richiedono autorizzazioni multiple. Questo tipo di configurazione rafforza la posizione dominante dei grandi operatori e riduce la possibilità di creare forme di innovazione aperta, come laboratori urbani, piattaforme di co-creazione o partenariati pubblico-privati più inclusivi.

Il monopolio sui diritti di accesso si traduce quindi in un blocco alla partecipazione e alla trasparenza, minando la possibilità di costruire una cultura dei dati condivisa e limitando la legittimazione delle politiche digitali urbane (Malecki, 2010). Di conseguenza, la governance dei dati si configura come un campo di tensione tra controllo e apertura, tra tutela della sovranità pubblica e promozione dell'innovazione collaborativa.

4.4. Contributi e implicazioni

Nel loro insieme, i risultati di questa ricerca contribuiscono ad ampliare la comprensione del lock-in dei dati come fenomeno multidimensionale che attraversa le sfere istituzionali, tecnologiche e organizzative delle smart city (Kummitha, 2018; Marchesani, 2023; Marchesani & Ceci, 2025; Mora, 2023; Thabit & Mora, 2023). I tre meccanismi individuati delineano un sistema in cui le scelte iniziali delle amministrazioni pubbliche condizionano profondamente la capacità di innovare nel lungo periodo. La rigidità dei processi di procurement definisce le condizioni di partenza della dipendenza, gli standard tecnologici chiusi ne consolidano la struttura

operativa, mentre il controllo esclusivo sui dati ne perpetua gli effetti, riducendo progressivamente l'autonomia decisionale delle città.

Da un punto di vista teorico, lo studio offre un contributo significativo alla letteratura sulla governance dei dati urbani, mostrando che il lock-in non deve essere interpretato come un semplice vincolo tecnico, ma come un problema di governance e di potere. Le dinamiche osservate evidenziano come la distribuzione del controllo sui dati definisca nuove forme di interdipendenza tra amministrazioni e fornitori, con implicazioni dirette sulla sovranità digitale, sulla capacità di coordinamento interno e sulla possibilità di generare innovazione pubblica. In tal senso, il lavoro propone di leggere il lock-in dei dati come una forma di path dependence istituzionale, che può essere mitigata solo attraverso processi di apprendimento organizzativo e modelli di governance adattiva capaci di ridefinire ruoli e regole di accesso.

Sul piano pratico, le implicazioni riguardano la necessità di trovare un equilibrio tra due obiettivi complementari: da un lato, preservare la sovranità e la sicurezza dei dati pubblici, garantendo che la loro gestione resti ancorata a principi di trasparenza e accountability; dall'altro, ridurre i meccanismi di lock-in che rallentano la diffusione dell'innovazione e impediscono la partecipazione di nuovi attori. Aprire l'ecosistema dei dati, favorendo interoperabilità e standard aperti, consentirebbe non solo di accelerare i processi di trasformazione digitale, ma anche di creare valore per le imprese locali, stimolando la nascita di nuovi servizi e soluzioni basate su un uso condiviso e responsabile delle informazioni urbane.

In questa prospettiva, il superamento dei lock-in non implica la perdita di controllo da parte delle amministrazioni, ma la costruzione di forme di governance collaborativa in cui il potere sui dati sia distribuito in modo equo tra pubblico e privato, e orientato alla creazione di valore collettivo. Ridurre la dipendenza dai fornitori tecnologici e rafforzare le competenze interne delle città rappresenta quindi un passaggio cruciale per trasformare la gestione dei dati da vincolo a risorsa, da strumento di controllo a leva di innovazione territoriale e sviluppo sostenibile.

Messaggi chiave:

- Il lock-in dei dati riflette un problema strutturale di governance urbana. Nelle smart city, la dipendenza tecnologica non deriva solo da vincoli tecnici, ma da regole, procedure e responsabilità frammentate che limitano la capacità decisionale e l'autonomia delle amministrazioni pubbliche.
- Superare i meccanismi di lock-in richiede un equilibrio tra sovranità e apertura dei dati. Le città devono preservare il controllo e la sicurezza delle informazioni pubbliche, ma al tempo stesso promuovere interoperabilità, standard aperti e competenze interne per ridurre la dipendenza dai fornitori esterni.
- Ridurre il lock-in accelera la trasformazione digitale e genera valore territoriale. Una governance dei dati più flessibile e collaborativa consente di ampliare la

partecipazione di imprese locali e attori pubblici, rafforzando innovazione, trasparenza e sviluppo sostenibile nelle smart city.

Bibliografia

Barba-Sánchez, V., Arias-Antúnez, E. & Orozco-Barbosa, L. (2019). Smart cities as a source for entrepreneurial opportunities: Evidence for Spain. *Technological Forecasting and Social Change*, *148*(March 2017), 119713. https://doi.org/10.1016/j.techfore.2019.119713.

Bibri, S.E. & Krogstie, J. (2020). The emerging data–driven Smart City and its innovative applied solutions for sustainability: the cases of London and Barcelona. *Energy Informatics*, *3*(1). https://doi.org/10.1186/s42162-020-00108-6.

Caragliu, A. & Del Bo, C.F. (2019). Smart innovative cities: The impact of Smart City policies on urban innovation. *Technological Forecasting and Social Change*, *142*(December 2017), 373-383. https://doi.org/10.1016/j.techfore.2018.07.022.

Caragliu, A., del Bo, C. & Nijkamp, P. (2011). Smart cities in Europe. *Journal of Urban Technology*, *18*(2), 65-82. https://doi.org/10.1080/10630732.2011.601117.

Cledou, G., Estevez, E. & Soares Barbosa, L. (2018). A taxonomy for planning and designing smart mobility services. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2017.11.008.

Curry, E. (2016). The big data value chain: Definitions, concepts, and theoretical approaches. In *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*. https://doi.org/10.1007/978-3-319-21569-3_3.

De Matteis, F., Preite, D., Striani, F. & Borgonovi, E. (2021). Cities'role in environmental sustainability policy: The Italian experience. *Cities*, *111*(November 2020), 102991. https://doi.org/10.1016/j.cities.2020.102991.

Eckersley, P., Flynn, A., Lakoma, K. & Ferry, L. (2023). Public procurement as a policy tool: the territorial dimension. *Regional Studies*, *57*(10), 2087–2101. https://doi.org/10.1080/00343404.2022.2134850.

Foxon, T.J. (2007). Technological lock-in and the role of innovation. In *Handbook of Sustainable Development*. https://doi.org/10.4337/9781847205223.00017.

Fu, Y. & Zhu, J. (2020). Trusted data infrastructure for smart cities: a blockchain perspective. *Building Research and Information*. https://doi.org/10.1080/09613218.2020.1784703.

Gascó, M. (2017a). Living labs: Implementing open innovation in the public sector. *Government Information Quarterly*, *34*(1), 90-98. https://doi.org/10.1016/j.giq.2016.09.003.

Gioia, D.A., Corley, K.G. & Hamilton, A.L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15-31. https://doi.org/10.1177/1094428112452151.

Hannah, D.R. & Robertson, K. (2015). Why and how do employees break and bend confidential information protection rules? *Journal of Management Studies*, *52*(3). https://doi.org/10.1111/joms.12120.

Katz, M.L. & Shapiro, C. (1985). Network externalities, competition, and compatibility. In *American Economic Review* (Vol. 75, Issue 3).

Kazemargi, N., Leonelli, S., Spagnoletti, P., Ceci, F., Sinaimeri, B. & Marchesani, F. (2025). Data Governance in Data Ecosystems: A Research Note. In *PROSPETTIVE IN ORGANIZZAZIONE* (Vol. 29).

Kummitha, R.K.R. (2018). Entrepreneurial urbanism and technological panacea: Why Smart City planning needs to go beyond corporate visioning? *Technological Forecasting and Social Change*, *137*(September 2017), 330-339. https://doi.org/10.1016/j.techfore.2018.07.010.

Kummitha, R.K.R. (2024). Smart city governance: assessing modes of active citizen engagement. *Regional Studies*, *0*(0), 1-15. https://doi.org/10.1080/00343404.2024.2399262.

Kummitha, R.K.R. & Crutzen, N. (2019). Smart cities and the citizen-driven internet of things: A qualitative inquiry into an emerging smart city. *Technological Forecasting and Social Change*, *140*(October 2018), 44-53. https://doi.org/10.1016/j.techfore.2018.12.001.

Li, Z. & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151-160. https://doi.org/10.1016/j.giq.2017.10.006.

Linde, L., Sjödin, D., Parida, V. & Wincent, J. (2021). Dynamic capabilities for ecosystem orchestration A capability-based framework for smart city innovation initiatives. *Technological Forecasting and Social Change*, *166*. https://doi.org/10.1016/j.techfore.2021.120614.

Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly*, *29*(4), 446-454. https://doi.org/10.1016/j.giq.2012.06.003.

Lnenicka, M., Nikiforova, A., Luterek, M., Azeroual, O., Ukpabi, D., Valtenbergs, V. & Machova, R. (2022). Transparency of open data ecosystems in smart cities: Definition and assessment of the maturity of transparency in 22 smart cities. *Sustainable Cities and Society*, *82*(July). https://doi.org/10.1016/j.scs.2022.103906.

Malecki, E.J. (2010). Global knowledge and creativity: New challenges for firms and regions. *Regional Studies*, *44*(8). https://doi.org/10.1080/00343400903108676.

Marchesani, F. (2023). *The Global Smart City: Challenges and Opportunities in the Digital Age*. Emerald Group Publishing Limited. http://www.nber.org/papers/w16019.

Marchesani, F. & Ceci, F. (2024). Il ruolo dell'intelligenza artificiale come strumento organizzativo e strategico nelle smart city. *Rivista di Politica Economica*, *2*, 131-148.

Marchesani, F. & Ceci, F. (2025). A quadruple helix view on smart city: Exploring the effect of internal and external open innovation on public services digitalization. *Technovation*, *139*(January 2024), 103141. https://doi.org/10.1016/j.technovation.2024.103141.

Marchesani, F., Masciarelli, F. & Bikfalvi, A. (2025). Exploring the (dis)advantages of smart cities'inclusive, integrative and social practices in new business creation: the effect of human capital inflow. *Entrepreneurship & Regional Development*, *37*(1-2), 157-187. https://doi.org/10.1080/08985626.2024.2358969.

Marchesani, F., Masciarelli, F. & Ceci, F. (2024). Digital trajectories in contemporary cities : Exploring the interplay between digital technology implementation, the amplitude of social media platforms, and tourists inflow in cities. *Cities*, *146*(July 2023), 104749. https://doi.org/10.1016/j.cities.2023.104749.

Mergel, I., Edelmann, N. & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4). https://doi.org/10.1016/j.giq.2019.06.002.

Mora, L. (2023). Organizing for Smart City Development: Research at the crossroads. Introduction to the Special Issue. *Organization Studies*, *44*(10), 1559-1575. https://doi.org/10.1177/01708406231197815.

Neumann, O., Matt, C., Hitz-Gamper, B. S., Schmidthuber, L. & Stürmer, M. (2019). Joining forces for public value creation? Exploring collaborative innovation in smart city

initiatives. *Government Information Quarterly*, *36*(4), 101411. https://doi.org/10.1016/j.giq.2019.101411.

Oliveira, M.I.S., Lóscio, B.F., Fátima, G. De & Lima, B. (2019). Investigations into Data Ecosystems : a systematic mapping study. In *Knowledge and Information Systems* (Vol. 61, Issue 2). Springer London. https://doi.org/10.1007/s10115-018-1323-6.

Pereira, G.V., Parycek, P., Falco, E. & Kleinhans, R. (2018). Smart governance in the context of smart cities: A literature review. *Information Polity*, *23*(2), 143-162. https://doi.org/10.3233/IP-170067.

Pittaway, J.J. & Montazemi, A.R. (2020). Know-how to lead digital transformation: The case of local governments. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2020.101474.

Schiavone, F., Appio, F.P., Mora, L. & Risitano, M. (2020). The strategic, organizational, and entrepreneurial evolution of smart cities. *International Entrepreneurship and Management Journal*, *16*(4), 1155-1165. https://doi.org/10.1007/s11365-020-00696-5.

Scholl, H.J. & Alawadhi, S. (2016). Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *Information Polity*, *21*(1). https://doi.org/10.3233/IP-150369.

Thabit, S. & Mora, L. (2023). The collaboration dilemma in smart city projects: Time to ask the right questions. *Organization*, 1-12. https://doi.org/10.1177/13505084231183949.

van Winden, W. & Carvalho, L. (2019). Intermediation in public procurement of innovation: How Amsterdam's startup-in-residence programme connects startups to urban challenges. *Research Policy*, *48*(9), 103789. https://doi.org/10.1016/j.respol.2019.04.013.

Vanolo, A. (2014). Smartmentality: The Smart City as Disciplinary Strategy. *Urban Studies*, *51*(5), 883-898. https://doi.org/10.1177/0042098013494427.

Wiig, A. (2015). IBM's smart city as techno-utopian policy mobility. *City*. https://doi.org/10.1080/13604813.2015.1016275.

Wiig, A. (2016). The empty rhetoric of the smart city: from digital inclusion to economic promotion in Philadelphia. *Urban Geography*, *37*(4), 535-553. https://doi.org/10.1080/02723638.2015.1065686.

Yun, J.H.J., Jeong, E.S. & Yang, J.H. (2015). Open innovation of knowledge cities. *Journal of Open Innovation: Technology, Market, and Complexity*, *1*(2), 1-20. https://doi.org/10.1186/s40852-015-0020-x.

Data governance per le *grand challenges*: configurazione di ruoli e dimensioni della catena del valore dei dati

Loris Santarelli [*] e Federica Ceci [**]

Abstract: Il rapido sviluppo delle tecnologie basate sui dati espone le organizzazioni a sfide significative nella loro raccolta, archiviazione e valorizzazione, amplificate dall'eterogeneità e dispersione crescenti dei dati tipici di contesti smart city, siti produttivi o iniziative di sostenibilità. Queste sfide sono particolarmente rilevanti nei contesti denominati "grand challenges", dove le organizzazioni affrontano problemi complessi con frequenti operazioni estese su ampi territori, collaborazioni con diversi attori, impiego di strumenti analogici e digitali e necessità di approcci innovativi. Questa complessità si traduce in difficoltà di coordinamento, gestione delle risorse e trattamento dei dati dispersi ed eterogenei che richiedono di essere integrati, conservati e condivisi. Questo studio esplora come diversi attori nel Parco Nazionale d'Abruzzo, Lazio e Molise (PNALM) configurano la Data Value Chain (DVC), caratterizzata da operazioni sul campo, fonti multiple e flussi combinati tra domini fisici e digitali, a supporto della conservazione ambientale e faunistica. Basandoci su osservazioni, interviste e documenti, identifichiamo sfide e risposte organizzative utili a valorizzare ecosistemi complessi di dati.

Parole chiave: Data value chain, Data governance, Grand challenges, Collaboration.

1. Introduzione

Il rapido aumento del volume e dell'eterogeneità dei dati rappresenta una sfida crescente per le organizzazioni, alimentata dai progressi nelle tecnologie *IoT*, nei sensori, nel cloud computing e nella connettività (Cohen et al., 2017; Dosi, 1982). Queste tecnologie generano nuove opportunità di collaborazione oltre i confini fisici,

[*] Loris Santarelli (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: loris.santarelli@unich.it

[**] Federica Ceci (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: federica.ceci@unich.it

DOI: 10.82018/9791221165456-8

creando interdipendenze tra attori diversi e facilitando forme di collaborazione prima difficilmente realizzabili (Kapoor & Teece, 2021). Tuttavia, la loro integrazione comporta cambiamenti rilevanti nelle logiche dei modelli di business, strategie e pratiche operative (Kraus et al., 2021). In questo scenario, i dati diventano una risorsa strategica in grado di guidare trasformazioni nelle strategie manageriali, nei processi decisionali e nelle opportunità di collaborazione (Adner & Levinthal, 2002; Brynjolfsson & McElheran, 2016; Curry, 2016; Watch, 2017).

Per capitalizzare sul valore dei dati, le organizzazioni devono configurare la Catena del Valore dei Dati (*Data Value Chain* – DVC), un *framework* che descrive le fasi fondamentali attraverso cui i essi vengono raccolti, elaborati, arricchiti e infine utilizzati per supportare processi decisionali e strategie organizzative (Curry, 2016; Orlandi et al., 2016). Sebbene le tecnologie digitali consentano progressi significativi nell'estrazione di valore dai dati, diverse sfide di varia natura persistono. Infatti, non tutte le attività della DVC si svolgono in ambienti virtuali come piattaforme online e software. Al contrario, esse si estendono spesso all'interno di ambienti fisici, quali siti di produzione (Åkerman et al., 2018; Schreiber & Metternich, 2022), punti vendita retail (Martijn et al., 2015), infrastrutture urbane e *smart city* (Marchesani, 2023; Wu et al., 2025; Zhang et al., 2013).

La gestione dei dati diventa particolarmente complessa in quei contesti denominati *grand challenges*, dove le organizzazioni sono impegnate nell'affrontare rilevanti problematiche sociali. Qui le organizzazioni sono spesso impegnate in attività complesse e distribuite su ampi territori, che richiedono collaborazioni tra più attori, strumenti eterogenei e approcci innovativi. Da iniziative per il contrasto alla povertà alla tutela dell'ambiente, le organizzazioni che operano in questi contesti complessi devono orchestrare input, operazioni e output lungo la DVC, integrando dati da fonti disperse, tecnologie digitali e analogiche, attori interni ed esterni e attività distribuite sul territorio (Akter et al., 2024a; Angeli et al., 2022; George et al., 2016). Di conseguenza, la configurazione della DVC richiede particolare attenzione in termini di coordinamento e gestione delle risorse (Curry, 2016).

Questo studio approfondisce le sfide emergenti in contesti *grand challenges*, dove le organizzazioni necessitano di orchestrare input, operazioni, strumenti, attori e output con il fine di estrarre valore attraverso la DVC. Pertanto, abbiamo condotto un caso studio che approfondisce un'iniziativa *grand challenge* di salvaguardia ambientale, analizzando come un'organizzazione affronta la gestione dei dati in un *network* di unità organizzative e partner esterni. Il nostro studio si concentra sul Parco Nazionale d'Abruzzo, Lazio e Molise (PNALM), dedicato alla conservazione della fauna e del paesaggio naturale. Il PNALM conduce attività legate ai dati, come il monitoraggio della fauna, censimenti e ricerca scientifica, supportate da strumenti analogici e digitali.

L'organizzazione opera in un ecosistema complesso di attori e affronta molteplici sfide nella gestione dei dati, rendendo la sua configurazione della DVC unica e adatta a contesti di *grand challenge* (Angeli et al., 2022; Davidson et al., 2023). L'integrazione di tecnologie come *cloud* e *IoT*, il coordinamento continuo tra attori e i molteplici processi di *data sharing* rendono questo contesto ideale per studiare il ruolo di

una tale configurazione nell'identificazione di *pattern*, nello sviluppo di soluzioni *real-time* e nel supporto di processi decisionali (Åkerman et al., 2018; Akter et al., 2024a). Pertanto, la domanda di ricerca che guida questo studio è: *In che modo le organizzazioni configurano ruoli, dimensioni e gestiscono dati eterogenei lungo la DVC in contesti grand challenges?*

Per rispondere a questa domanda, ci siamo basati sulla collezione di dati qualitativi, tra cui interviste, osservazioni partecipative e documenti d'archivio. La parte restante di questo lavoro è strutturata come segue: introduzione alla letteratura sulla DVC e gestione dei dati, descrizione della metodologia, includendo la descrizione del contesto, raccolta dei dati e analisi. Infine, riportiamo il contributo dello studio e individuiamo possibili direzioni per ricerche future.

2. Background Teorico

2.1. La Catena del Valore dei Dati

Le organizzazioni che adottano tecnologie basate sui dati e ne riconoscono il loro potenziale strategico sperimentano cambiamenti significativi nelle infrastrutture, nelle strategie e nei processi decisionali (Constantiou & Kallinikos, 2015; Curry, 2016; Porter & Heppelmann, 2015; Redman, 2008). Affinché queste trasformazioni producano un cambiamento sostanziale, i dati devono essere convertiti in risorse di valore attraverso diverse fasi che delineano un percorso che parte dalla loro acquisizione, fino all'utilizzo finale degli stessi (Curry, 2016; Rayport & Sviokla, 1995). Questo percorso è descritto nel modello della DVC sviluppato da Curry (2022) che illustra come il flusso di dati generi valore in cinque passaggi. Comprendere questi passaggi è cruciale per riconoscere il modo in cui il valore può essere estratto dai dati:

- **Acquisizione**: raccolta, verifica e organizzazione dei dati prima della loro memorizzazione.
- **Analisi**: processi di preparazione dei dati per la scoperta di informazioni significative o nascoste.
- **Cura**: gestione attiva volta a garantirne qualità e affidabilità.
- **Archiviazione**: conservazione per assicurare la loro disponibilità, accesso e riutilizzo.
- **Utilizzo:** l'effettivo impiego dei dati per ottenerne il valore.

Nonostante le opportunità, la gestione dei dati pone importanti sfide manageriali, soprattutto in contesti complessi che richiedono l'integrazione di strumenti digitali e analogici, il coordinamento di varie attività distribuite in ampi territori e la collaborazione di molteplici attori interni ed esterni all'organizzazione.

2.2. Sfide nella configurazione della catena del valore dei dati

2.2.1. Fronteggiare l'eterogeneità dei dati

Nonostante crescente diffusione di tecnologie basate sui dati stia trasformando diversi settori, persistono sfide tecniche e manageriali che incidono su attività, processi decisionali e cultura organizzativa persistono (Curry, 2016; McAfee & Brynjolfsson, 2012). I dati provenienti da fonti eterogenee, strutturate e non strutturate, devono essere acquisiti, standardizzati, archiviati e analizzati per generare valore (Cavanillas et al., 2016; Wirén et al., 2019). Queste operazioni, pur supportate da molteplici strumenti tecnologici, richiedono spesso ancora l'intervento umano, soprattutto in settori fortemente caratterizzati da attività sul campo, come siti produttivi e manifatturieri, retail, logistica e ricerca sul territorio (Cavanillas et al., 2016; Lykourentzou et al., 2025; Wirén et al., 2019). In questi contesti, la varietà dei dati rende necessarie pratiche di virtualizzazione ed estrazione del valore, in assenza delle quali i dati rischierebbero di non essere utilizzati efficacemente o di andare persi (Cavanillas et al., 2016; Wirén et al., 2019).

La letteratura manageriale descrive questi passaggi come "virtualizzazione", o più comunemente "digitalizzazione", cioè la trasformazione e standardizzazione dei dati da fonti fisiche a digitali (Leonardi & Treem, 2020). Il concetto di "*datafication*" amplia ulteriormente la prospettiva includendo l'intero ciclo di vita dei dati fino alla creazione di nuovo valore a partire da attività in contesti reali (Cukier & Mayer-Schoenberger, 2013). Entrambi i processi dipendono dalla necessità di misurare e convertire l'attività umana o sociale in dati significativi, aumentando il volume e la diversità delle informazioni e spingendo le organizzazioni a riconsiderare i processi di raccolta e analisi (Leonardi & Treem, 2020). In questo quadro, l'*agency* umana gioca un ruolo cruciale nell'accumulazione di valore, facilitando la collezione di diversi tipi di dati provenienti da varie fonti e consentendo il loro passaggio dal mondo fisico a quello virtuale (Wirén et al., 2019). Pertanto, contesti complessi come quelli definiti *grand challenges*, sollevano nuove domande relative a meccanismi di *governance*, coordinamento degli attori e processi che favoriscono l'accumulazione, interpretazione e utilizzo dei dati (Abraham et al., 2019; Davidson et al., 2023b; Faik et al., 2020).

2.2.2. L'importanza del contesto nella costruzione della catena del valore dei dati

La letteratura manageriale ha ampiamente analizzato le sfide associate all'adozione di tecnologie basate sui dati, nonché il loro impatto sugli ambienti organizzativi e sull'azione umana in diversi settori, tra cui pubblico, manifatturiero, sanitario, retail e logistico (Åkerman et al., 2018; Cavanillas et al., 2016; Faroukhi et al., 2020; Frias-Martinez et al., 2012; Hernández-Moral et al., 2021). Solo di recente la letteratura ha rivolto una maggiore attenzione alle "*grand challenges*", ovvero problemi di rilevanza sociale come povertà, … o salvaguardia della biodiversità (Akter et al.,

2024a), accesso all'educazione, cambiamento climatico o salvaguardia della biodiversità. In questi casi estremi le sfide di gestione dei dati diventano particolarmente evidenti (Angeli et al., 2022; Davidson et al., 2023b; George et al., 2016).

Le singole organizzazioni possiedono raramente tutte le capacità e le risorse necessarie per raccogliere, analizzare o utilizzare i dati, il che genera relazioni e dipendenze con altre organizzazioni (Davidson et al., 2023b; Oliveira & Lóscio, 2018). Il coinvolgimento di più soggetti con logiche diverse comporta la formazione di complessi *network* inter-organizzativi le cui collaborazioni si basano sui dati. Questi *network* spesso presentano sfide più complesse rispetto a settori tradizionali. Nei contesti di *grand challenges*, le organizzazioni operano solitamente sul campo, raccolgono dati da fonti disperse e gestiscono campioni fisici che richiedono di essere lavorati, conservati e condivisi in base agli usi specifici (Davidson et al., 2023b; Faik et al., 2020). Queste operazioni richiedono catene del valore altamente integrate, un uso robusto di tecnologie basate sui dati, come piattaforme *cloud* e dispositivi *IoT*, e un coordinamento continuo per supportare strategie e processi decisionali basati sui dati (Akter et al., 2024b; Brous et al., 2016).

In sintesi, contesti complessi come i *grand challenges* pongono nuove domande sui meccanismi di *governance*, gestione e interpretazione dei dati tra diversi attori e tecnologie (Abraham et al., 2019; Davidson et al., 2023b; Faik et al., 2020). Questo contributo intende quindi evidenziare le principali sfide legate alla configurazione della DVC in scenari dove attività umane e tecnologie avanzate si intrecciano in un network socio-tecnico essenziale per la gestione dei dati.

3. Metodologia

3.1. Contesto empirico

Il nostro contesto empirico è il Parco Nazionale d'Abruzzo, Lazio e Molise (PNALM). Fondato nel 1922, è noto per l'elevata biodiversità e presenza di specie endemiche come l'orso marsicano. La missione del Parco è la conservazione ambientale, perseguita attraverso piani di ricerca, gestione sostenibile e iniziative culturali e turistiche. Guidato dal principio "per proteggere, bisogna conoscere", il PNALM promuove lo studio degli aspetti storici, sociali, geologici e biologici del territorio, avvalendosi della collaborazione di unità scientifiche, tecniche, di sorveglianza e partner esterni. Le attività comprendono monitoraggio, ricerca scientifica, censimenti faunistici e progetti innovativi, supportati da un ampio uso di tecnologie digitali e analogiche.

La salvaguardia dell'ambiente naturale rappresenta una sfida significativa essenziale per le dimensioni ecologiche, ricreative, culturali, economiche e scientifiche della vita umana. La raccolta estensiva di dati permette alle organizzazioni di comprendere e gestirne meglio fenomeni critici quali i cambiamenti climatici, la perdita di biodiversità, le modifiche agli ecosistemi, la salute del territorio e la qualità

dell'aria. Nonostante queste opportunità, le sfide nella gestione dei dati in questi contesti sono rilevanti. Conoscere approfonditamente questi fenomeni richiede un ampio dispiego di risorse, tecnologie digitali, strumenti analogici e collaborazioni tra attori. Esempi di tali attività includono il monitoraggio, quindi la raccolta e l'analisi sistematica di dati, i conteggi simultanei per raccogliere informazioni da più fonti, i censimenti della fauna per stimare la distribuzione delle popolazioni, la sorveglianza e l'ispezione. Il PNALM utilizza un approccio multilivello per il monitoraggio: squadre sul campo raccolgono dati per contare, seguire e valutare le specie, mentre dispositivi *IoT* come radio-collari e sensori GPS forniscono informazioni aggiuntive, successivamente condivise con enti di ricerca e istituzioni pubbliche.

Un altro esempio di attività chiave svolta dall'organizzazione riguarda la ricerca scientifica, attraverso cui il PNALM mira a ottenere una comprensione completa delle tendenze delle popolazioni o di specifici fenomeni faunistici, per migliorare di conseguenza le strategie di conservazione. Gli studi di ricerca sono spesso condotti in collaborazione con organizzazioni pubbliche e private, comprese università, ONG e altre istituzioni di ricerca. Tali studi si basano su un ampio utilizzo di tecnologie e processi legati ai dati, qui raccolti digitalmente attraverso strumenti tecnologici, tradizionalmente con metodi e strumenti analogici e sotto forma di campioni fisici. Questa varietà di fonti crea complessità che il PNALM affronta tramite una DVC progettata per integrare raccolta, gestione e condivisione dei dati, sia interna che esterna all'organizzazione.

I team di monitoraggio sono organizzati per operare sul campo in sinergia e raccogliere dati per contare, seguire i movimenti e valutare lo stato di salute delle specie. In parallelo vengono utilizzate tecnologie *IoT*, come radio-collari e altri sensori per raccogliere i tracciati GPS dei gruppi animali per arricchire la raccolta dati impiegate come fonti di informazioni più specifiche e aggiuntive. Infine, la condivisione di dati inter-organizzativa, pur essenziale per analisi avanzate e strategie di conservazione, introduce ulteriori sfide legate al coordinamento, alla standardizzazione e alle implicazioni tecnologiche.

3.1.1. Catena del valore e tecnologie digitali nel PNALM

All'interno del PNALM, le unità tecniche, scientifiche e di sorveglianza collaborano alla salvaguardia ambientale. Il PNALM configura una DVC che consente di tracciare le tendenze delle popolazioni faunistiche, tracciandone i comportamenti, le nascite, le aree chiave e i dati biologici. Questi dati supportano la ricerca, i processi decisionali, la conoscenza organizzativa e le iniziative di educazione. All'esterno, il Parco è inserito in un network di università, ONG, imprese e istituzioni con cui condivide dati, tecnologie e processi.

Le operazioni sul campo combinano tecnologie tradizionali e digitali, come radiocollari, applicazioni mobili e database, regolarmente integrati per facilitare le operazioni legate ai dati. Uno scenario tipico vede le squadre coordinate per monitorare le specie, svolgendo le attività in simultanea su territori estesi e spesso contigui, ma evitando sovrapposizioni, garantendo di conseguenza un tracciamento continuo oltre che la copertura dell'intero territorio preso in oggetto. In un territorio montano e privo di

infrastrutture, le attività richiedono attrezzature specializzate e comunicazione continua tra i team. È necessario condividere aggiornamenti in tempo reale per evitare duplicazioni e garantire un'efficace raccolta delle informazioni. Tutti i dati raccolti, come movimenti degli animali, tracciati GPS, osservazioni dirette e campioni fisici, digitali o tradizionali, vengono successivamente confrontati, archiviati e utilizzati per diversi scopi, assicurando un approccio completo al monitoraggio e alla conservazione della fauna. Poiché queste operazioni sul campo richiedono un'attenta collaborazione e il trasporto di attrezzature specializzate su terreni impervi, ogni fase della DVC è caratterizzata da sfide legate al coordinamento, ai requisiti tecnologici e tecnici, e ad altri fattori operativi. Ad esempio, i dati provenienti dai dispositivi *IoT* devono essere integrati con osservazioni meno strutturate ma ugualmente informative, standardizzati e archiviati con attenzione per evitare perdite o duplicazioni.

In sintesi, la DVC nel PNALM evidenzia la complessità di gestire dati generati da attività sul campo, interazioni uomo-macchina, tecnologie avanzate e collaborazioni esterne. La coesistenza di strumenti digitali e tradizionali combinata con la varietà delle attività complesse implicate nella salvaguardia ambientale rende la configurazione della DVC particolarmente impegnativa. Queste peculiarità giustificano e motivano un'esplorazione più approfondita di questo contesto.

3.2. Design del caso studio e raccolta dati

Abbiamo sviluppato un caso di studio per esplorare la configurazione della DVC in un contesto organizzativo caratterizzato da attività complesse sul territorio, dati altamente eterogenei, l'uso simultaneo di strumenti digitali e analogici e numerose collaborazioni con molteplici *stakeholder*. L'analisi è basata su tre principali fonti di dati: in primo luogo, abbiamo collezionato dati secondari come report e articoli riguardanti le iniziative, gli attori coinvolti, le attività e le tecnologie. In secondo luogo, abbiamo condotto 16 interviste con membri e *stakeholder* del PNALM, tra cui il Direttore, *manager*, guardiaparco, ausiliari e partner per una durata totale di 11 ore e 14 minuti. Infine, abbiamo partecipato direttamente alle attività come volontari per un periodo di 8 giorni. Durante questo tempo, abbiamo raccolto dati dettagliati attraverso osservazioni partecipanti, con particolare attenzione alle attività e alle tecnologie utilizzate. Questi dati, registrati sotto forma di *fieldnotes* e arricchiti attraverso un *out-of-the-field dictionary* (Van Maanen, 1988; Walford, 2009), ci hanno permesso una comprensione approfondita delle dinamiche organizzative e delle pratiche di gestione dei dati.

4. Data coding

La fase di codifica è stata avviata con un approccio di *open coding*, successivamente raffinato e organizzato attraverso il raggruppamento dei codici. Un *coder* è

stato coinvolto nel processo il quale ha interagito con un secondo ricercatore per aumentare l'affidabilità della codifica. Il processo di codifica è stato applicato alle diverse fonti di dati e ancorato al quadro concettuale della DVC. Abbiamo sviluppato un vocabolario per categorizzare specifiche dimensioni, attori e sfide della DVC e raggruppato i codici seguendo gli step teorici del modello.

Successivamente, utilizzando il *software NVivo*, abbiamo quantificato e analizzato la frequenza e le co-occorrenze dei codici emersi in modo da esplorare le relazioni degli stessi.

5. Content analysis

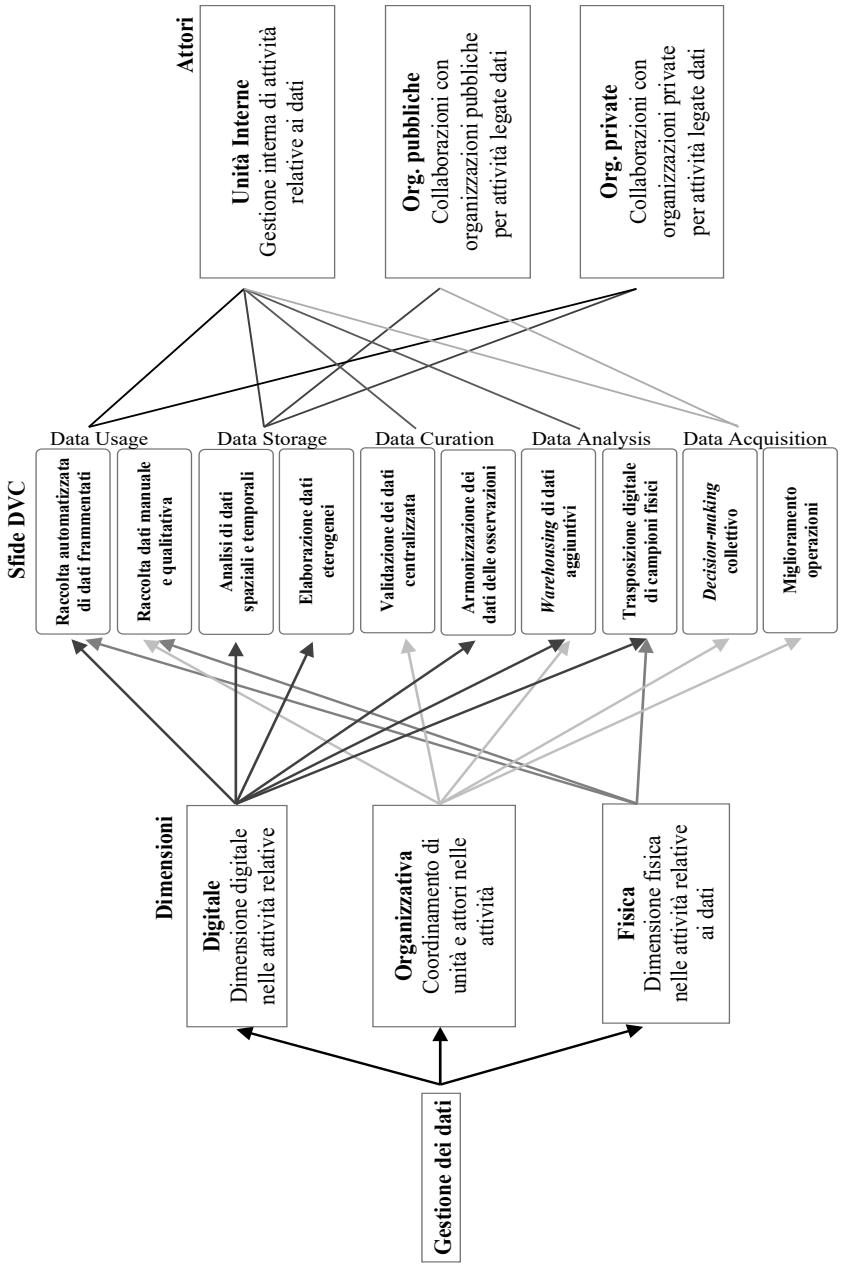
Precedente alla vera e propria analisi del contenuto (*content analysis*), analisi chiave della nostra metodologia, è stata un'analisi documentale, utile a delineare i temi principali da esplorare. Qui abbiamo sviluppato categorie concettuali individuando segmenti di testo rilevanti legati alla gestione dei dati e alle tecnologie, segmenti poi incorporati nell'analisi del contenuto vera e propria.

Questa analisi è stata svolta attraverso la selezione di parti di testo definite "nodi", aggregate poi in "temi" e successivamente raggruppate in "dimensioni". Attraverso l'analisi del contenuto, abbiamo identificato un *array* di sfide, dimensioni e attori principali coinvolti nella DVC. L'uso del software *NVivo*, in particolare della funzione *Matrix Coding Query*, ha consentito di individuare le co-occorrenze, ovvero relazioni e *pattern* tra i nodi, facilitando l'esplorazione delle relazioni tra i concetti emergenti.

6. Risultati

Abbiamo analizzato i processi di gestione dei dati e la relativa configurazione della DVC del PNALM, impiegata per supportare la grande sfida della salvaguardia ambientale attraverso la ricerca, lo studio e il monitoraggio della fauna e del territorio. I nostri risultati evidenziano un *array* di sfide su tre dimensioni differenti: tecnica, organizzativa e fisica. Questo *array* di sfide si dispiega all'interno delle dimensioni individuate e deve essere gestito nel processo di gestione dei dati lungo la DVC. Queste sfide sottolineano l'importanza di gestire l'aspetto tecnologico insieme a quello fisico e organizzativo per assicurare soluzioni efficaci, particolarmente dove unità e attori multipli gestiscono dati eterogenei e distribuiti nel territorio, ben oltre i confini organizzativi. La figura seguente illustra la configurazione di questa particolare DVC in un contesto *grand challenge*.

Figura 1. – **Configurazione della DVC in contesti *grand challenges***



6.1. Dimensione fisica

Configurare la dimensione fisica della DVC emerge come aspetto cruciale soprattutto nelle fasi di acquisizione e archiviazione dei dati. In questi passaggi la complessità deriva dalla necessità di raccogliere dati eterogenei su ampi territori, coordinando efficacemente tecnologia e attività umane. Due approcci complementari caratterizzano la raccolta: da un lato, l'uso di dispositivi *IoT* e sensori per acquisire dati quantitativi distribuiti. Dall'altro, l'arricchimento con osservazioni qualitative sul campo, ad esempio attraverso schede cartacee, telescopi o raccogliendo campioni biologici. Questa natura duale genera sfide legate alla veridicità, integrità e flessibilità dei sistemi di archiviazione, soprattutto quando i dati includono campioni fisici raccolti *off-site*. Il coordinamento tra unità organizzative e l'adeguata infrastruttura digitale risultano fondamentali per evitare perdite e duplicazioni dei dati. Come spiegato dal seguente estratto di intervista: "*utilizziamo i radio-collari GPS per tracciare e studiare i movimenti e i comportamenti [degli animali], fototrappole per aumentare le possibilità di osservare le femmine con i cuccioli … Le osservazioni vengono effettuate tramite binocoli e naturalmente cannocchiali, poiché permettono di cogliere maggiori dettagli sui comportamenti*." (estratto dall'Intervista XIII).

Nel momento in cui i dati presentano eterogeneità in numerosi aspetti, come formato e tipo, la sfida consiste nel gestirli e immagazzinarli per evitare perdite di informazioni, che potrebbero influenzare negativamente i risultati: "*Stabiliamo giorni specifici per le osservazioni simultanee … Ci sono valutazioni che vanno oltre il semplice conteggio; tramite marcature permanenti o artificiali, possiamo escludere o non escludere [se l'esemplare è stato già registrato]*." (estratto dall'Intervista I). Affrontare questa eterogeneità è essenziale per evitare problemi di standardizzazione nelle fasi successive della DVC (Wirén et al., 2019). Superare queste sfide richiede sforzi sia tecnici che organizzativi, come verrà approfondito nelle sezioni seguenti.

6.2. Dimensione digitale

Come da aspettative, la dimensione digitale evidenzia invece il ruolo centrale delle tecnologie in quasi tutte le fasi della DVC, in particolare acquisizione, analisi, cura e archiviazione. Strumenti come radio-collari GPS o GSM, *database* e *software* analitici consentono di integrare dati strutturati e non strutturati. Tuttavia, l'eterogeneità dei dati, da quelli di geolocalizzazioni a quelli dalle osservazioni qualitative, ad esempio, rende complessa l'analisi, richiedendo una stretta collaborazione tra sviluppatori e operatori sul campo per adattare i database alle esigenze reali. Ulteriori sfide emergono anche nella fase di standardizzazione: spesso si ricorre a registrazioni cartacee per controlli di qualità, correggere errori o gestire incongruenze prima della digitalizzazione. Come un intervistato ci fa notare: "*La tecnologia oggi è applicata in diversi ambiti; abbiamo progetti legati, ad esempio, al monitoraggio della fauna selvatica. I radio-collari GPS o GSM ci permettono di raccogliere e salvare questi*

dati, vedere in tempo reale cosa fanno gli animali e studiarli." (estratto dall'Intervista VI).

Analizzare dati dispersi ed eterogenei rappresenta una sfida significativa nel nostro contesto; per questo motivo, dati strutturati e non strutturati vengono combinati prima dell'analisi per estrarre informazioni approfondite. Infatti, gestire tale eterogeneità diventa essenziale: "*Incrociamo dati spaziali e temporali e, dato che possono verificarsi errori, il nostro obiettivo è ridurli al minimo ...*" (estratto dall'Intervista I). Se da un lato le tecnologie forniscono ricchi dati quantitativi, le osservazioni qualitative richiedono maggior impegno umano, a causa delle difficoltà nel raccogliere informazioni limitate ma preziose nel paesaggio naturale. Come evidenziato da un *intervistato:* "*Spesso preferiamo richiedere schede cartacee e poi modifichiamo i database secondo necessità. Questo permette di identificare errori, duplicati o altri errori direttamente sulla scheda.*" (estratto dall'Intervista I).

6.3. Dimensione organizzativa

La dimensione organizzativa si manifesta soprattutto nelle attività sul campo, dove il coordinamento tra squadre risulta essenziale per evitare sovrapposizioni e garantire copertura completa del territorio. Le sfide principali riguardano la pianificazione delle operazioni, lo scambio in tempo reale di informazioni e la successiva validazione centralizzata dei dati, gestita in prevalenza dall'area scientifica. In questa fase, i processi di condivisione e i momenti di confronto, come *meeting* e riunioni, supportano l'integrità del flusso di informazioni e favoriscono decisioni operative e strategiche. L'obiettivo ultimo è attuare un *management* adattivo, caratterizzato da un miglioramento continuo delle pratiche tramite analisi dei dati raccolti, modelli predittivi e aggiustamenti delle strategie. Come espresso da un intervistato: "*Svolgiamo valutazioni che vanno oltre il semplice conteggio. Su alcune specie realizziamo conteggi in simultanea per ottenere informazioni utili e monitorare specifici animali, come le unità riproduttive.*" (estratto dall'Intervista I).

La necessità di arricchire i dati attraverso interventi dell'uomo crea un *layer* aggiuntivo di complessità che dev'essere gestito per un'efficace gestione dei dati. Per condurre quindi attività basate sui dati, le organizzazioni devono attuare meccanismi di coordinamento, di scambio di informazioni e valutazioni collettive definendo attori e ruoli lungo gli step della DVC. Nel nostro caso, l'area scientifica riceve e gestisce i dati, supportando le fasi successive per estrarne valore. Durante il loro utilizzo, vengono implementati meccanismi di coinvolgimento dei membri dell'organizzazione, con riunioni come strumento di coordinamento per decisioni strategiche e operative: "*Alla fine del campionamento, raccogliamo tutti i dati, li memorizziamo nel database e iniziamo ad elaborarli*" – "*gli incontri hanno diverse funzioni: non solo per informare, ma anche per far sentire tutti i partecipanti coinvolti e capire le difficoltà, ...*" (estratti dall'intervista I).

In conclusione, la dimensione organizzativa svolge un ruolo di collegamento tra le dimensioni tecniche e fisiche, garantendo il coordinamento tra unità e membri.

Superare le sfide organizzative lungo la DVC significa assicurare una corretta gestione dei dati in tutto il processo, supportare le operazioni, facilitare la condivisione delle informazioni, allocare i compiti in modo efficiente e coinvolgere i membri nei processi decisionali e di miglioramento.

6.4. Attori

Infine, il ruolo degli attori esterni si rivela decisivo. Le collaborazioni tra pubblico e privato permettono di superare limiti tecnologici e gestionali, potenziando le capacità interne. Gli enti pubblici contribuiscono soprattutto all'analisi genetica e all'uso dei dati per lo sviluppo di *policy*, mentre i *partner* privati forniscono tecnologie e supporto nelle fasi di acquisizione e analisi. Queste collaborazioni rafforzano la capacità dell'organizzazione di affrontare la crescente complessità, mantenendo al contempo il controllo interno delle risorse e del processo decisionale: "*la tecnologia oggi è applicata in vari ambiti ...*". L'intervistato ha poi proseguito spiegando: "*Monitoriamo i segni di presenza, raccogliamo campioni e li inviamo 'all'Agenzia Pubblica' (anonimizzata), che si occupa delle analisi genetiche ... Questo è un progetto in cui la tecnologia potrebbe sembrare marginale, ma in realtà fa davvero la differenza. Senza analisi genetiche o radio-collari satellitari, si perderebbe ovviamente un'intera serie di informazioni.*" (estratto dall'Intervista IV).

D'altro canto, un membro intervistato di un'azienda privata partner del PNALM ha dichiarato: "*Noi forniamo la tecnologia. Poi, sono loro a effettuare l'analisi dei dati, valutare la situazione e svolgere le analisi incrociate e statistiche ...*". (estratto dall'intervista XIV). In generale, questi risultati evidenziano il ruolo cruciale delle *partnership* pubbliche e private, che permettono al PNALM di affrontare la crescente complessità dei dati, cercando competenze e tecnologie al di fuori dei propri confini organizzativi, pur mantenendo il pieno controllo delle proprie risorse.

7. Discussione e Conclusioni

Le organizzazioni sfruttano il progressivo sviluppo delle tecnologie basate sui dati per comprendere più profondamente il proprio contesto operativo e adattarsi alle sue crescenti sfide, soprattutto nei contesti complessi come quelli definiti *grand challenges* (Akter et al., 2024b; Davidson et al., 2023b). Al fine di ottenere vantaggi maggiori e sfruttare il potenziale dei dati, queste organizzazioni devono essere in grado di raccoglierli, condividerli e gestirli in modo efficace. Attraverso il *framework* DVC abbiamo analizzato questi processi, dalla raccolta dei dati all'impatto generato dal loro utilizzo e ridefinito ruoli, relazioni e risorse nella sua configurazione (Curry & Ojo, 2020; Oliveira & Lóscio, 2018).

7.1. Contributi alla letteratura sulla catena del valore dei dati

Configurare la DVC in contesti *grand challenges* caratterizzati da frequenti attività *off-site* e molteplici attori con logiche e obiettivi spesso divergenti richiede alle organizzazioni particolare attenzione (Curry & Ojo, 2020; Davidson et al., 2023a, 2023b). Il nostro contributo evidenzia come le organizzazioni, in questi contesti, orchestrino le tre dimensioni emerse nella nostra analisi, interconnesse nella gestione della DVC: la dimensione fisica, che riguarda le caratteristiche spaziali del contesto operativo; tecnica, che include sistemi e strumenti digitali, piattaforme e elaborazione; e organizzativa, che garantisce il coordinamento tra unità interne e partner esterni attraverso assegnazione di ruoli, compiti, condivisione e comunicazione *real-time.* Mentre studi precedenti si sono concentrati su una singola dimensione della DVC, ad esempio quella tecnica (Åkerman et al., 2018; Curry, 2016; De Simone et al., 2023; Hernández-Moral et al., 2021; Watch, 2017), questo studio approfondisce la nostra comprensione di come le organizzazioni gestiscono sfide multidimensionali derivanti da contesti in cui le operazioni umane e la tecnologia interagiscono continuamente, influenzandosi reciprocamente lungo l'intera DVC. Il nostro caso di studio mostra come una gestione integrata di queste dimensioni sia fondamentale per evitare perdite di informazioni, inefficienze e criticità operative. Estendiamo quindi la visione lineare della DVC a favore di un modello più interconnesso e sfaccettato, evidenziando l'importanza della gestione adattiva e dell'integrazione tra dimensioni fisiche, tecniche e organizzative per ottenere valore dai dati e garantire operazioni efficaci in contesti complessi.

Il nostro secondo contributo riguarda la crescente complessità dei dati che spinge le organizzazioni a ricercare e favorire collaborazioni con attori pubblici e privati. Queste collaborazioni agiscono infatti come catalizzatori, permettendo un maggiore sviluppo di progetti innovativi, implementazioni tecnologiche e analisi avanzate. Tali collaborazioni favoriscono la nascita di ecosistemi di dati, promuovendo sinergie intersettoriali, favorendo una creazione congiunta di valore, un'innovazione sostenibile e molteplici collaborazioni a lungo termine basate sui dati (Adner & Kapoor, 2010, 2016; Cennamo & Santalo, 2018; Jacobides et al., 2018; Cavanillas et al., 2016).

In sintesi, emerge l'importanza fondamentale di una corretta configurazione di ruoli (attori interni, pubblici e privati) e dimensioni (fisica, tecnica e organizzativa) della catena del valore dei dati specifica per i contesti di *grand challenges* (Akter et al., 2024a; Angeli et al., 2022; Ferraro et al., 2015; Gümüsay et al., 2022). Il nostro contributo evidenzia l'importanza di un approccio multidimensionale e collaborativo, in cui è cruciale coordinare efficacemente le attività in tempo reale, bilanciare l'apporto di input da tecnologie digitali e attività umane per favorire la collaborazione tra unità interne e ricercare collaborazioni esterne per ampliare le capacità tecnologiche e analitiche. In conclusione, questo approccio integrato consente quindi alle organizzazioni di dimostrarsi preparate ad affrontare sfide sempre più complesse che richiedono approcci innovativi e il coinvolgimento continuo di diversi attori su più livelli che massimizzano il valore dei dati e favoriscono le iniziative relative a progetti innovativi e necessari.

7.2. Implicazioni per practitioner

Le sfide individuate rappresentano un utile riferimento per *manager* e professionisti nella configurazione e gestione della DVC. Esse forniscono indicazioni pratiche per pianificare azioni mirate a estrarre valore dai dati. In particolare, l'integrazione di fonti digitali e tradizionali presenta criticità che non possono essere risolte solo con la tecnologia: occorrono anche adeguate soluzioni organizzative. La dimensione organizzativa, infatti, agisce da ponte tra attività tecniche e umane, e richiede meccanismi di coordinamento in tempo reale come riunioni o piattaforme digitali condivise per favorire l'allineamento di unità e processi. Un'efficace gestione della DVC richiede quindi non solo strumenti adeguati, ma anche l'orchestrazione di logistica, sistemi tecnici e processi organizzativi. Inoltre, le collaborazioni pubblico-private risultano fondamentali per arricchire competenze e strumenti, favorendo la creazione di ecosistemi di dati capaci di generare innovazione collettiva e favorire nuove opportunità. Queste collaborazioni sono fondamentali per configurare un ecosistema di dati robusto che permetta di creare valore dagli stessi.

7.3. Implicazioni organizzative

Nel contesto della tutela ambientale, la gestione dei dati consente alle organizzazioni di migliorare l'impatto delle proprie attività e la comprensione del loro ambiente operativo. Raccolta e archiviazione sono le due fasi della DVC maggiormente legate alla dimensione fisica e possono essere rafforzate tramite automatizzazione, per esempio tramite *IoT* e integrazione di nuove fonti di dati, riducendo il carico di lavoro umano. Parallelamente, meccanismi di coordinamento potenziano la collaborazione tra unità e la condivisione delle conoscenze, soprattutto durante le attività sul campo. Un approccio di *management* adattivo permette di trasformare i dati in una vera e propria risorsa strategica. I dati diventano così strumenti per attivare cicli di *feedback*, orientare le decisioni e favorire un continuo apprendimento organizzativo.

7.4. Limiti

I limiti di questo studio riguardano, in primo luogo, la sua generalizzabilità, essendo basato su un singolo caso di studio. Replicare questa metodologia in contesti differenti potrebbe rafforzare la solidità dei suoi risultati, consentendo di individuare ulteriori *pattern* e migliorandone i contributi (Yin, 2003). In secondo luogo, sebbene il framework della DVC fornisca solide basi concettuali, le sfide individuate sono strettamente legate alle sue fasi. Sebbene questo approccio offra una visione strutturata, può portare a un'eccessiva enfasi su alcune sfide a discapito di altre. In terzo luogo, questo lavoro aggrega sfide che potrebbero essere rilevanti anche in altri

contesti *grand challenges* enfatizzando maggiormente la prospettiva inter-organizzativa, esaminando così la configurazione della DVC in una logica di ecosistema (Curry & Ojo, 2020; Oliveira & Lóscio, 2018).

Messaggi chiave:

- Nei contesti di *grand challenges*, le organizzazioni devono ripensare la configurazione della catena del valore dei dati (DVC) considerando tre dimensioni: fisica, digitale e organizzativa.
- La gestione dei dati richiede un coordinamento socio-tecnico, in cui attività umane e tecnologie si intrecciano in modo complementare e continuativo.
- I dati generano valore strategico quando il loro potenziale è riconosciuto all'interno di ecosistemi collaborativi che ampliano capacità, risorse e conoscenze delle organizzazioni.

Bibliografia

Abraham, R., Schneider, J. & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. In *International Journal of Information Management* (Vol. 49, 424-438). Elsevier Ltd. https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

Adner, R. & Kapoor, R. (2010). Value creation in innovation ecosystems: How the structure of technological interdependence affects firm performance in new technology generations. *Strategic Management Journal*, *31*(3), 306-333. https://doi.org/10.1002/smj.821.

Adner, R. & Kapoor, R. (2016). Innovation ecosystems and the pace of substitution: Re-examining technology S-curves. *Strategic Management Journal*, *37*(4), 625-648. https://doi.org/10.1002/smj.2363.

Adner, R. & Levinthal, D.A. (2002). The emergence of emerging technologies. In *California Management Review* (Vol. 45, Issue 1, 50-66). Haas School of Business. https://doi.org/10.2307/41166153.

Åkerman, M., Lundgren, C., Bärring, M., Folkesson, M., Berggren, V., Stahre, J., Engström, U. & Friis, M. (2018). Challenges Building a Data Value Chain to Enable Data-Driven Decisions: A Predictive Maintenance Case in 5G-Enabled Manufacturing. *Procedia Manufacturing*, *17*, 411-418. https://doi.org/10.1016/j.promfg.2018.10.064.

Akter, S., Hossain, M.A., Hani, U., Vrontis, D., Thrassou, A. & Arslan, A. (2024a). Addressing the grand challenges of poverty with data-driven creative service offerings. *Journal of Product Innovation Management*, *41*(2), 236-266. https://doi.org/10.1111/jpim.12679.

Akter, S., Hossain, M.A., Hani, U., Vrontis, D., Thrassou, A. & Arslan, A. (2024b). Addressing the grand challenges of poverty with data-driven creative service offerings. *Journal of Product Innovation Management*, *41*(2), 236-266. https://doi.org/10.1111/jpim.12679.

Angeli, F., Metz, A. & Raab, J. (2022). *Organizing for Sustainable Development; Addressing the Grand Challenges*.

Brous, P., Janssen, M. & Vilminko-Heikkinen, R. (2016). Coordinating decision-making in data management activities: A systematic review of data governance principles. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9820 LNCS*, 115-125. https://doi.org/10.1007/978-3-319-44421-5_9.

Brynjolfsson, E. & McElheran, K. (2016). The rapid adoption of data-driven decision-making. *American Economic Review*, *106*(5), 133-139. https://doi.org/10.1257/aer.p20161016.

Cavanillas, J.M., Curry, E. & Wahlster, W. (2016). *New Horizons for a Data-Driven Economy A Roadmap for Usage and Exploitation of Big Data in Europe*.

Cennamo, C. & Santalo, J. (2018). *Generativity Tension and Value Creation in Platform Ecosystems*. https://ssrn.com/abstract=3289574.

Cohen, B., Amorós, J.E. & Lundy, L. (2017). The generative potential of emerging technology to support startups and new ecosystems. In *Business Horizons* (Vol. 60, Issue 6, 741-745). Elsevier Ltd. https://doi.org/10.1016/j.bushor.2017.06.004.

Constantiou, I.D. & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. *Journal of Information Technology*, *30*(1), 44-57. https://doi.org/10.1057/jit.2014.17.

Cukier, K. & Mayer-Schoenberger, V. (2013). The Rise of Big Data: How It's Changing the Way We Think About the World. *Foreign Affairs*, *92*(3), 28-40.

Curry, E. (2016). The big data value chain: Definitions, concepts, and theoretical approaches. In *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe* (29-37). Springer International Publishing. https://doi.org/10.1007/978-3-319-21569-3_3.

Curry, E. & Ojo, A. (2020). Enabling Knowledge Flows in an Intelligent Systems Data Ecosystem. In *Real-time Linked Dataspaces* (15-43). Springer International Publishing. https://doi.org/10.1007/978-3-030-29665-0_2.

Curry, E., Scerri, S. & Tuikka, T. (2022). *Data Spaces Design, Deployment and Future Directions*.

Davidson, E., Wessel, L., Winter, J.S. & Winter, S. (2023a). Future directions for scholarship on data governance, digital innovation, and grand challenges. *Information and Organization*, *33*(1). https://doi.org/10.1016/j.infoandorg.2023.100454.

Davidson, E., Wessel, L., Winter, J.S. & Winter, S. (2023b). Future directions for scholarship on data governance, digital innovation, and grand challenges. *Information and Organization*, *33*(1). https://doi.org/10.1016/j.infoandorg.2023.100454.

De Simone, C., Ceci, F. & Alaimo, C. (2023). *Data Ecosystem and Data Value Chain: An Exploration of Drones Technology Applications* (203-218). https://doi.org/10.1007/978-3-031-15770-7_13.

Dosi, G. (1982). Technological paradigms and technological trajectories. A suggested interpretation of the determinants and directions of technical change. *Research Policy*.

Faik, I., Barrett, M. & Oborn, E. (2020). How Information Technology Matters In Societal Change: An Affordance-based Institutional Logics Perspective. *MIS Quarterly: Management Information Systems*, *44*(3), 1143-1176. https://doi.org/10.25300/MISQ/2020/14193.

Faroukhi, A.Z., El Alaoui, I., Gahi, Y. & Amine, A. (2020). Big data monetization throughout Big Data Value Chain: a comprehensive review. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-019-0281-5.

Ferraro, F., Etzion, D. & Gehman, J. (2015). Tackling Grand Challenges Pragmatically:

Robust Action Revisited. *Organization Studies*, *36*(3), 363-390. https://doi.org/10.1177/0170840614563742.

Frias-Martinez, V., Soguero, C. & Frias-Martinez, E. (2012). Estimation of urban commuting patterns using cellphone network data. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 9-16. https://doi.org/10.1145/2346496.2346499.

George, G., Howard-Grenville, J., Joshi, A. & Tihanyi, L. (2016). Understanding and tackling societal grand challenges through management research. *Academy of Management Journal*, *59*(6), 1880–1895. https://doi.org/10.5465/amj.2016.4007.

Gümüsay, A., Marti, E., Trittin-Ulbrich, H. & Wickert, C. (2022). *Organizing for Societal Grand Challenges* (Emerald Publishing, Trans.; Vol. 79). Research in the Sociology of Organizations.

Hernández-Moral, G., Mulero-Palencia, S., Serna-González, V.I., Rodríguez-Alonso, C., Sanz-Jimeno, R., Marinakis, V., Dimitropoulos, N., Mylona, Z., Antonucci, D. & Doukas, H. (2021). Big data value chain: Multiple perspectives for the built environment. In *Energies* (Vol. 14, Issue 15). MDPI AG. https://doi.org/10.3390/en14154624.

Jacobides, M.G., Cennamo, C. & Gawer, A. (2018). Towards a Theory of Ecosystems. In *Strategic Management Journal* (Vol. 39).

Kapoor, R. & Teece, D.J. (2021). Three faces of technology's value creation: Emerging, enabling, embedding. In *Strategy Science* (Vol. 6, Issue 1, 1-4). INFORMS Inst.for Operations Res.and the Management Sciences. https://doi.org/10.1287/STSC.2021.0124.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N. & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211047576.

Leonardi, P.M. & Treem, J.W. (2020). Behavioral Visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, *41*(12), 1601-1625. https://doi.org/10.1177/0170840620970728.

Lykourentzou, M.A., Apostolopoulos, N., Dabić, M., Liargovas, P. & Tekavčič, M. (2025). Assessing the role of human factor in digital transformation projects: A systematic literature review and research agenda. *Technology in Society*, *82*. https://doi.org/10.1016/j.techsoc.2025.102934.

Marchesani, F. (2023). Digital Implementation in the Smart City Ecosystem. In *The Global Smart City* (p. 217). Emerald Publishing Limited.

Martijn, N., Hulstijn, J., De Bruijne, M. & Tan, Y.-H. (2015). Determining the Effects of Data Governance on the Performance and Compliance of Enterprises in the Logistics and Retail Sector. *Open and Big Data Management and Innovation*, 454-466. https://doi.org/10.1007/978-3-319-25013-7_37.

McAfee, A. & Brynjolfsson, E. (2012). Big Data: The Management of Revolution. *Harvard Business Review*.

Oliveira, M.I.S. & Lóscio, B.F. (2018, May 30). What is a data ecosystem? *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3209281.3209335.

Orlandi, F., Attard, J., Ponce Rodriguez, A. & Daniel Ibáñez González, L. (2016). *Elements of a Data Value Chain Strategy*.

Porter, M.E. & Heppelmann, J.E. (2015). How Smart, Connected Products Are Transforming Companies. *Harvard Business Review*.

Rayport, J.F. & Sviokla, J. (1995). Exploiting the virtual value chain. *Harvard Business Review*.

Redman, T.C. (2008). *Data Driven: Profiting from Your Most Important Business Asset*. Harvard Business Press.

Schreiber, M. & Metternich, J. (2022). Data Value Chains in Manufacturing: Data-based Process Transparency through Traceability and Process Mining. *Procedia CIRP*, *107*, 629-634. https://doi.org/10.1016/j.procir.2022.05.037.

Van Maanen, J. (1988). *Tales of the field on Writing Ethnography*.

Walford, G. (2009). The practice of writing ethnographic fieldnotes. *Ethnography and Education*, *4*(2), 117-130. https://doi.org/10.1080/17457820902972713.

Watch, O.D. (2017). *The data value chain: moving from production to impact*.

Wirén, M., Mäntymäki, M. & Najmul Islam, A. (2019). Big Data Value Chain: Making Sense of the Challenges. *Digital Transformation for a Sustainable Society in the 21st Century*, 125-137. https://doi.org/10.1007/978-3-030-29374-1_11.

Wu, T., Xu, W. & Kung, C.C. (2025). The impact of data elements on urban sustainable development: Evidence from the big data policy in China. *Technology in Society*, *81*. https://doi.org/10.1016/j.techsoc.2024.102800.

Yin, K.R. (2003). *Designing Case Studies Research*.

Zhang, Q., Huang, T., Zhu, Y. & Qiu, M. (2013). A case study of sensor data collection and analysis in smart city: Provenance in smart food supply chain. *International Journal of Distributed Sensor Networks*, *2013*. https://doi.org/10.1155/2013/382132.

Parte 3
La creazione di nuove pratiche di governance dei dati

Le sfide alla data governance per favorire audit e monitoraggio continuo nella gestione del rischio di terze parti: il caso della cybersecurity

Alessandra Di Giacomo [*] **e Paolo Spagnoletti** [**]

Abstract: L'intensificarsi della pressione normativa in materia di privacy e sicurezza dei dati ha posto le piccole e medie imprese (PMI) di fronte a sfide di conformità di crescente complessità, rendendo inadeguati i tradizionali approcci all'audit, basati su controlli manuali e verifiche periodiche. Le recenti regolamentazioni europee – dal Regolamento generale sulla protezione dei dati (GDPR) alla Direttiva 2022/2555 (NIS2) – richiedono infatti un monitoraggio continuo della conformità normativa e l'estensione delle verifiche lungo l'intera catena del valore, includendo l'ecosistema delle terze parti. Questo studio esamina il potenziale trasformativo dell'Intelligenza Artificiale Agentica nei processi di audit, quale catalizzatore per la transizione da modelli reattivi a paradigmi predittivi e autoadattivi. Attraverso un'analisi della letteratura, della normativa e degli standard di riferimento si evidenziano le criticità di data governance da risolvere per favorire la diffusione di sistemi multi-agente che possano automatizzare il rilevamento delle vulnerabilità, semplificare le valutazioni di conformità e gestire proattivamente i rischi associati alle terze parti attraverso la suddivisione automatica degli obiettivi e il coordinamento dinamico.

Parole chiave: Compliance, Audit, Intelligenza Artificiale Agentica, Third Party Risk Management (TPRM).

1. Introduzione

Nell'attuale economia digitale e globalizzata, le organizzazioni operano in ecosistemi caratterizzati da interconnessione strutturale e crescente dipendenza da

[*] Alessandra Di Giacomo (✉)
Dipartimento di Diritto e Impresa, Università Luiss, Italia.
E-mail: adigiacomo@luiss.it

[**] Paolo Spagnoletti (✉)
Dipartimento di Business and Management, Università Luiss, Italia.
E-mail: pspagnoletti@luiss.it

DOI: 10.82018/9791221165456-9

fornitori esterni. L'esternalizzazione di funzioni, processi e attività rappresenta una leva strutturale per incrementare l'efficienza operativa, contenere i costi e accedere a competenze specialistiche. Parallelamente, essa comporta un'inevitabile espansione dei confini organizzativi, che introduce nuove aree di vulnerabilità e rende imprescindibile l'adozione di approcci sistematici di gestione del rischio. In questo scenario, le piccole e medie imprese (PMI) devono confrontarsi con obblighi stringenti di conformità a normative consolidate in materia di protezione dei dati e sicurezza informatica (Oluoha et al., 2023), nonché con standard internazionali emergenti che rafforzano ulteriormente i requisiti di governance digitale. Il quadro normativo europeo è infatti intriso di vari regolamenti e direttive: la direttiva sulla sicurezza delle reti e dell'informazione (NIS) (direttiva (UE) 2016/1148) e la sua versione riveduta, la direttiva (UE) 2022/2555 (NIS 2) relativa a norme comuni per la sicurezza delle reti e dell'informazione; il Regolamento generale sulla protezione dei dati (GDPR) (Regolamento (UE) 2016/679) sulla privacy, la protezione dei dati e l'obbligo di notifica delle violazioni dei dati; il Regolamento sulla cybersicurezza (Regolamento (UE) 2019/881) sul quadro per l'istituzione di un sistema di certificazione a livello dell'UE in materia di cibersicurezza; e molte altre normative specifiche del settore. Questa stratificazione normativa non solo accresce i rischi legali e operativi, ma impone anche un notevole onere sulle risorse aziendali. Le normative vigenti, infatti, estendono gli obblighi regolamentari oltre i confini organizzativi tradizionali, coinvolgendo direttamente l'intero ecosistema di terze parti (Jacobisides et al., 2018; Adner, 2017). Il concetto di 'terza parte' assume, in questo contesto, una connotazione particolarmente estensiva, includendo qualsiasi persona fisica o giuridica, esterna all'organizzazione e con cui questa intrattiene, o potrebbe intrattenere, relazioni commerciali o di collaborazione. Questa definizione ricomprende, dunque, non soltanto la rete di fornitori diretti e indiretti (le cosiddette "quarte parti") e la clientela, ma si estende a una costellazione più vasta di attori: partner strategici, concessionari, sponsor e intermediari di varia natura. Tale ampiezza definitoria comporta implicazioni operative significative per la gestione della compliance, poiché obbliga le organizzazioni a sviluppare sistemi di monitoraggio e controllo capaci di abbracciare l'intera rete di relazioni aziendali. Di conseguenza, i team di *compliance* sono impegnati in modo crescente nell'interpretazione delle normative, nella personalizzazione di politiche e controlli e nella conduzione di audit frequenti.

Gli audit di cybersicurezza, consistenti in valutazioni approfondite dei sistemi informativi di un'organizzazione, con particolare attenzione alle politiche di sicurezza, ai controlli implementati e alla conformità agli standard normativi, rappresentano uno strumento cruciale per identificare le vulnerabilità, valutare l'efficacia dei controlli di sicurezza e garantire la conformità ai requisiti normativi e agli standard di settore. Tuttavia, gli approcci tradizionali all'audit – fondati su procedure manuali, controlli periodici e verifiche spesso frammentarie (Fantoni et al. 2021) – si rivelano lenti, onerosi e inadeguati a sostenere la rapidità e la complessità del panorama normativo contemporaneo, soprattutto quando tali controlli devono estendersi lungo ecosistemi articolati di terze e quarte parti. Questo lavoro esplora le prospettive di integrazione dell'intelligenza artificiale agentica nei processi di valutazione della

conformità normativa e nella ricerca di vulnerabilità negli ecosistemi di business (Jacobisides et al., 2018; Adner, 2017; Ajiga, Ayanponle e Okatta, 2022; Francis Onotole et al., 2022; Ilori et al., 2022). I sistemi agentici di intelligenza artificiale rappresentano una classe emergente di architetture intelligenti in cui più agenti specializzati collaborano per raggiungere obiettivi complessi utilizzando il ragionamento collaborativo e la pianificazione in più fasi (Sapkota et al., 2025). L'intelligenza artificiale agentica promette maggiore autonomia, capacità di ragionamento e adattabilità alle procedure aziendali, consentendo valutazioni dinamiche del rischio ed esecuzione automatizzata dell'audit interno. Questi sistemi possono identificare autonomamente anomalie, monitorare deviazioni dai protocolli di conformità e avviare azioni correttive senza richiedere una supervisione costante da parte dell'uomo (Hosseini & Seilani, 2025). Tuttavia, lo sviluppo e l'integrazione di soluzioni di intelligenza artificiale agentica negli ecosistemi di business risultano problematici per via delle difficoltà di distribuzione delle attività di data governance necessarie al funzionamento dei sistemi multi-agente, che richiedono un continuo allineamento con gli obiettivi delle parti coinvolte.

Il presente capitolo analizza criticamente la letteratura sulla gestione del rischio di terze parti, sulle pratiche di audit e sui recenti sviluppi nei sistemi di IA agentica, per rispondere alla seguente domanda di ricerca: in che modo la data governance può favorire l'audit e il monitoraggio continuo basato su sistemi multi-agente?

Benefici e ostacoli individuati con l'analisi della letteratura sono applicati al caso della gestione del rischio cyber in un ecosistema di business per problematizzare il fenomeno e identificare possibili aree di intervento per futuri studi empirici.

2. Il rischio legato alle terze parti

Nell'attuale economia interconnessa e globalizzata, la gestione del rischio associato alle terze parti (Third Party Risk Management – TPRM) è divenuta una priorità strategica per le piccole e medie imprese (OECD, 2018; Associazione Italiana Internal Auditors, 2019). Se da un lato il ricorso a supply chain sempre più ampie e articolate costituisce un fattore imprescindibile per accrescere la produttività, ridurre i costi operativi, ottimizzare l'efficienza dei processi ed espandere i mercati di riferimento, dall'altro espone le organizzazioni a rischi crescenti e diversificati.

Le relazioni con fornitori, partner e altri attori esterni implicano spesso l'accesso a informazioni privilegiate – come i dati dei clienti, i sistemi interni o asset critici – trasformando tali soggetti in potenziali vettori di vulnerabilità e punti di ingresso privilegiati per incidenti di sicurezza. Le imprese che limitano le proprie strategie di protezione esclusivamente ai confini organizzativi tradizionali, trascurando di estendere controlli rigorosi e misure preventive alle terze e quarte parti, si espongono inevitabilmente a violazioni e compromissioni della sicurezza. I rischi associati alla gestione delle terze parti dipendono da una serie articolata di potenziali minacce, tra

cui violazioni dei dati, attacchi alla catena di approvvigionamento e inadempienze normative, ciascuna con le proprie implicazioni per la sicurezza, la reputazione e la continuità operativa (Adama & Okeke, 2024; Popoola et al., 2024).

Le violazioni dei dati rappresentano uno dei rischi più diffusi associati ai fornitori terzi. Tali violazioni possono verificarsi quando i fornitori non adottano adeguate misure di sicurezza, consentendo accessi non autorizzati a informazioni sensibili. Le conseguenze possono essere gravi, con perdite finanziarie, danni reputazionali e implicazioni legali. Per questo motivo, è fondamentale che le organizzazioni si assicurino che i propri fornitori rispettino rigorosi standard di protezione dei dati e adottino controlli di sicurezza efficaci, al fine di ridurre il rischio di violazioni e minimizzare l'esposizione a potenziali incidenti (Ilori et al., 2024).

Dall'altro lato, le PMI devono implementare misure volte a mitigare l'impatto qualora una violazione dovesse comunque verificarsi. In questa prospettiva, assumono particolare rilevanza la predisposizione di controlli post-incident, quali sistemi di rilevazione degli incidenti, sistemi di condivisione delle informazioni, sistemi di training; nonché l'attivazione di coperture assicurative cyber o sugli errori dei soggetti apicali, che consentono la riduzione dell'impatto economico.

Un ulteriore rischio rilevante è rappresentato dagli attacchi alla supply chain. Essi sfruttano vulnerabilità presenti lungo la catena di fornitura per ottenere accesso non autorizzato ai sistemi o ai dati aziendali (Benjamin, Amajuoyi & Adeusi, 2024). Compromettendo un fornitore di fiducia, gli aggressori possono infiltrarsi nella rete dell'organizzazione e lanciare attacchi sofisticati, come infezioni da malware, esfiltrazioni di dati o furti d'identità (c.d. impersonificazione). Le conseguenze di un attacco riuscito alla supply chain possono essere devastanti per l'organizzazione colpita, causando gravi interruzioni operative e perdite economiche. Di conseguenza, le organizzazioni devono condurre valutazioni approfondite e periodiche dei rischi associati ai propri partner e implementare controlli di sicurezza robusti per mitigare tali minacce.

Anche le carenze in materia di conformità normativa rappresentano un fattore critico nei rapporti con i fornitori. In molti casi, le organizzazioni affidano a soggetti esterni l'esecuzione di attività importanti e processi critici. Questi soggetti esterni sono vincolati a stringenti requisiti regolatori derivanti da normative settoriali, standard internazionali e framework di compliance complessi. Il mancato rispetto di tali obblighi normativi da parte dei fornitori può determinare l'esposizione dell'organizzazione committente a sanzioni amministrative, penalità pecuniarie e contenziosi legali. Diviene, dunque, imprescindibile che le imprese verifichino con rigore la piena conformità dei propri partner alle normative vigenti, agli standard settoriali di riferimento e alle best practice internazionali, al fine di mitigare efficacemente i rischi connessi a inadempienze di natura regolatoria e preservare la propria reputazione istituzionale.

L'impatto complessivo derivante da questi rischi interconnessi può essere particolarmente rilevante. Oltre ai danni finanziari e reputazionali connessi a violazioni dei dati, attacchi informatici o mancanze di compliance, le organizzazioni possono subire gravi disfunzioni operative, una perdita significativa della fiducia da parte di

clienti e stakeholder, nonché un'esposizione a responsabilità giuridiche. È pertanto fondamentale adottare un approccio strutturato, sistematico e proattivo alla gestione del rischio di terze parti, attraverso l'implementazione di un solido framework di risk management, l'esecuzione regolare di audit e valutazioni di conformità e la promozione di una cultura organizzativa fortemente orientata alla sicurezza, alla trasparenza operativa e alla compliance normativa.

3. L'identificazione e la gestione del rischio associato alle terze parti

Il complesso delle attività attraverso cui un'organizzazione – sia essa un'impresa privata o un ente pubblico – identifica, valuta, gestisce e monitora i rischi derivanti dalle relazioni con controparti esterne è comunemente definito Third Party Risk Management (TPRM). Tale disciplina si colloca all'interno dell'alveo più ampio del risk management aziendale, e ne recepisce i principi fondanti così come delineati, tra gli altri, dallo standard internazionale ISO 31000. In analogia ai processi strutturati di gestione del rischio, anche il Third Party Risk Management si articola in un insieme coordinato di fasi metodologicamente distinte, ma strettamente interconnesse:

1. Identificazione del rischio/i: In questa fase preliminare, l'organizzazione procede all'individuazione delle terze parti rilevanti, nonché alla mappatura preliminare dei rischi potenzialmente associati a ciascuna di esse. Parallelamente, viene formalmente definito il risk appetite, ovvero il livello di rischio che l'organizzazione è disposta a tollerare in coerenza con la propria strategia, struttura operativa e obblighi normativi.
2. Valutazione del rischio/i e classificazione delle terze parti: I rischi identificati vengono sottoposti a un processo rigoroso di analisi quantitativa e/o qualitativa finalizzato alla misurazione della loro probabilità di accadimento e del potenziale impatto sull'organizzazione. Sulla base degli esiti di tale valutazione, le controparti vengono classificate secondo un profilo di rischio differenziato (ad esempio: basso, medio, alto), funzionale alla definizione di livelli di controllo differenziati.
3. Gestione e mitigazione del rischio: In base al livello di rischio attribuito a ciascuna terza parte, l'organizzazione implementa misure proporzionate e mirate di mitigazione. Tali interventi possono comprendere l'introduzione di clausole contrattuali stringenti; l'esecuzione di attività di due diligence rafforzata; l'adozione di misure correttive o, nei casi più critici, la cessazione del rapporto contrattuale, con eventuale notifica agli organi di vigilanza competenti.
4. Monitoraggio nel continuo: La gestione del rischio non si esaurisce nella fase iniziale, ma richiede un'attività costante di sorveglianza sull'evoluzione del profilo di rischio delle controparti. Il monitoraggio continuo è indispensabile per intercettare tempestivamente eventuali variazioni (organizzative, economico-finanziarie, normative) che siano in grado di modificare il livello di esposizione

dell'organizzazione. La frequenza e l'intensità di tale attività sono definite da policy interne basate su una valutazione dinamica del rischio.

Sebbene applicabile a diverse tipologie di rischio – inclusi quelli finanziari, operativi, tecnologici e di continuità operativa – il TPRM trova la sua maggiore rilevanza nella gestione dei rischi di compliance. In tale ambito, l'assenza di presidi adeguati nei rapporti con terze parti può tradursi in sanzioni amministrative o penali, ammende pecuniarie, danni economici rilevanti, pregiudizi reputazionali e compromissione del posizionamento sul mercato.

4. Audit di cybersicurezza risk-based e il potenziamento derivante dalle nuove tecnologie

Nel panorama in continua evoluzione della cybersecurity, le pratiche di auditing hanno subito trasformazioni profonde e significative, spinte dalla complessità degli ambienti digitali e dalle nuove minacce emergenti. Questo cambiamento ha catalizzato il progressivo passaggio da approcci all'audit tradizionali, orientati principalmente alla verifica della compliance normativa, a metodologie più dinamiche, agili e strategicamente focalizzate sulla valutazione continua del rischio e sulla resilienza organizzativa.

Le organizzazioni sono oggi chiamate non solo a rispettare rigorosamente i requisiti normativi, ma anche ad anticipare e gestire i rischi emergenti, allineando le proprie strategie di sicurezza informatica agli obiettivi complessivi di business. Tale trasformazione è resa necessaria dal bisogno di un monitoraggio continuo e dall'integrazione strategica di tecnologie innovative nei processi di verifica, che hanno portato all'affermazione di diverse metodologie chiave nell'auditing della cybersecurity (Tiwari & Debnath, 2017). L'auditing basato sul rischio è divenuto un principio cardine delle pratiche di audit moderne. A differenza dei metodi tradizionali, che applicano un livello uniforme di controllo su tutti gli asset, l'auditing risk-based consente alle organizzazioni di concentrare le risorse sulle aree a maggiore esposizione potenziale e impatto per il business. Come precedentemente evidenziato, questa metodologia inizia con una valutazione approfondita dei rischi, che prevede l'identificazione degli asset critici, la valutazione delle vulnerabilità e la mappatura dei potenziali vettori di minaccia (Antunes et al., 2022). Focalizzando gli audit sulle aree ad alto rischio, le organizzazioni possono ottimizzare l'allocazione delle risorse, massimizzare l'efficacia delle verifiche condotte e allineare i propri sforzi di cybersecurity agli obiettivi strategici (Aliyu et al., 2020; Sabillón, 2022). Questo approccio non solo aumenta la rilevanza degli audit, ma supporta anche la compliance con framework come il NIST Cybersecurity Framework e con regolamenti quali il GDPR, che pongono l'accento sulla gestione del rischio e sulle misure di protezione contro le violazioni della privacy (Adiloğlu & Güngör, 2019; Diamantopoulou, Tsohou & Karyda, 2020).

Accanto a questo approccio orientato al rischio e alla prioritizzazione strategica, stanno guadagnando terreno i sistemi di auditing e monitoraggio continuo. In un contesto in cui le minacce informatiche possono emergere rapidamente, evolversi in tempo reale e propagarsi attraverso reti distribuite con velocità esponenziale, i cicli di audit tradizionali non sono più sufficienti né adeguati a garantire una protezione efficace e tempestiva.

L'auditing continuo incorpora capacità avanzate di analisi dei dati e monitoraggio in tempo reale, permettendo alle organizzazioni di rilevare immediatamente anomalie e violazioni delle policy (Drivas et al., 2020; Rahman et al., 2021). Sfruttando tecnologie avanzate, le organizzazioni possono mantenere un quadro costantemente aggiornato del proprio stato di compliance e dell'efficacia dei controlli, migliorando nettamente la capacità di risposta a eventi minacciosi (National Cybersecurity Strategies, 2021).

A tal fine, parte della letteratura (Anuar, 2023; Ganapathy et al., 2023; Mohammed, 2023) prospetta l'utilizzo di soluzioni tecnologiche avanzate basate sull'intelligenza artificiale (IA). Essa, infatti, consentirebbe di porre rimedio alle carenze umane, offrendo notevoli opportunità di monitoraggio, automatizzando il rilevamento delle minacce, la gestione delle vulnerabilità e la valutazione della conformità normativa in contesti regolatori complessi e dinamici.

5. Le promesse dell'intelligenza artificiale agentica per l'audit e il monitoraggio continuo

L'intelligenza artificiale (IA) si è evoluta da semplice strumento computazionale a forza trasformativa che sta rimodellando settori, economie e società. L'integrazione dell'IA in vari ambiti ha generato incrementi significativi di efficienza, velocità operativa e automazione, spingendo le organizzazioni a implementare rapidamente soluzioni basate su tale tecnologia per ottenere vantaggi competitivi strategici (Hosseini et al., 2025). Tuttavia, i modelli di IA tradizionali sono tipicamente sviluppati per compiti specifici e mancano dell'autonomia necessaria per adattarsi in modo dinamico a contesti complessi e mutevoli. Questa limitazione ha catalizzato l'interesse verso un paradigma innovativo denominato IA agentica, una categoria di sistemi di IA in grado di prendere decisioni in modo indipendente, interagire con l'ambiente e ottimizzare i processi senza l'intervento umano diretto. L'IA agentica rappresenta un progresso sostanziale rispetto agli agenti di IA tradizionali, poiché integra funzionalità avanzate come l'autoapprendimento, l'adattabilità in tempo reale e la collaborazione multi-agente, consentendo di affrontare scenari caratterizzati da incertezza, interdipendenze e variabilità continua. Questi sistemi sono composti da agenti modulari, ciascuno dei quali ha il compito di svolgere un sottocomponente distinto di un obiettivo più ampio e coordinati tramite un orchestratore centralizzato o un protocollo decentralizzato (Borghoff et al., 2025; Hughes et al., 2025).

A differenza di altre forme di IA, spesso vincolate da rigide linee guida operative, i sistemi agentici sono progettati per integrare un certo grado di razionalità, che consente loro di ragionare e adattarsi in modo autonomo ai diversi contesti, perseguendo gli obiettivi per cui sono stati progettati. Un ulteriore elemento qualificante dell'IA agentica è la sua tendenza intrinseca a potenziare progressivamente le proprie funzioni per affrontare ostacoli inattesi e situazioni non lineari. Proprio per questa ragione, essa viene sempre più spesso considerata come un punto di riferimento per applicazioni che richiedono non solo efficienza operativa, ma anche capacità di interazione avanzata, come accade nel caso dei dispositivi autonomi di nuova generazione, dei robot collaborativi impiegati nelle catene produttive e nei servizi, nonché dei sistemi interattivi di supporto decisionale utilizzati in ambiti critici quali la sanità e la finanza.

La crescente esigenza di soluzioni in grado di gestire processi complessi, distribuiti e caratterizzati da elevata dinamicità ha contribuito ad alimentare un interesse diffuso verso l'IA agentica, specialmente in quei settori che mostrano un potenziale significativo di automazione avanzata e che necessitano di tecnologie capaci di bilanciare autonomia e controllo. Pur fondandosi sugli stessi principi costitutivi dell'IA classica, l'IA agentica amplia la gamma dei risultati ottenibili introducendo elementi di azione indipendente adattiva, capaci di ridurre la dipendenza da input esterni e di incrementare la capacità di auto-organizzazione. Dunque, nell'ecosistema complessivo dell'intelligenza artificiale, l'IA agentica si colloca in una posizione intermedia tra le tecnologie puramente reattive e rigidamente basate su regole e le concezioni più avanzate di intelligenza artificiale, svolgendo la funzione essenziale di abilitare un processo decisionale autonomo entro confini o strutture definiti. Questa posizione unica mette in risalto la capacità dell'IA agentica di adattarsi a scenari in cui rapidità decisionale, gestione di obiettivi di lungo periodo e apprendimento continuo rappresentano requisiti fondamentali per affrontare i problemi (Acharya et al., 2025).

Tra i principali ambiti di applicazione delle architetture multi-agente, l'audit in ambito di cybersicurezza rappresenta un caso d'uso particolarmente rilevante per il valore strategico che tali sistemi possono offrire. In particolare, il monitoraggio continuo delle controparti esterne – elemento cruciale nei modelli di gestione del rischio operativo e di conformità – risulta oggi imprescindibile per mitigare l'esposizione a minacce derivanti da terze parti, in un contesto normativo caratterizzato da elevata dinamicità e crescente complessità. In questo scenario, le architetture multi-agente si configurano come una soluzione tecnologica avanzata, capace di supportare audit distribuiti attraverso la cooperazione di agenti autonomi dotati di capacità di percezione e adattamento. Questi sistemi permettono di implementare meccanismi di controllo proattivo e predittivo migliorando l'efficacia dei processi di valutazione della conformità e abilitando forme di auditing continuo e contestuale rispetto all'evoluzione del rischio.

Infatti, la natura collaborativa e modulare dei sistemi multi-agente consente di scomporre obiettivi di controllo complessi in sotto-attività affidate a unità specializzate, capaci di operare in modo asincrono e in tempo reale. Questo approccio supera i limiti degli audit periodici e centralizzati, migliorando sia l'efficienza sia l'accuratezza

delle verifiche di conformità (Yaseen et al., 2022; Abouelyazid et al., 2019). Gli agenti possono così monitorare in modo continuo l'allineamento delle terze parti a specifici requisiti regolatori o a standard di settore intercettando eventuali deviazioni, proponendo azioni correttive e documentando automaticamente le evidenze di audit. Un ulteriore valore risiede nella capacità degli agenti di interagire con l'ambiente, apprendere dai dati e adattarsi ai mutamenti del contesto normativo o operativo. Ciò consente di mantenere aggiornati i criteri di valutazione e i modelli di rischio, riducendo il ricorso a interventi manuali e rafforzando la resilienza dell'intero sistema di controllo.

In definitiva, l'adozione di architetture multi-agente nell'audit di cybersicurezza non si limita a potenziare l'efficacia dei controlli di compliance, ma contribuisce a trasformare l'intero processo da funzione essenzialmente reattiva a sistema proattivo e predittivo. Tale evoluzione, resa possibile dall'integrazione di capacità autonome e intelligenti, conferisce alle organizzazioni un vantaggio strategico nel governo del rischio, rafforzando la loro capacità di operare con resilienza e trasparenza in un ecosistema regolatorio sempre più esigente e fluido.

6. Le sfide per la data governance negli audit di cybersicurezza

L'evoluzione verso sistemi di IA agentica sta ridefinendo in modo sostanziale il paradigma della data governance, ponendo al centro del dibattito non più la dimensione puramente tecnologica dei modelli, ma la capacità delle organizzazioni di governare in modo affidabile e trasparente l'intero ciclo di vita del dato. In questa prospettiva, il dato non rappresenta semplicemente la materia prima dei processi algoritmici, ma diventa l'oggetto stesso della responsabilità organizzativa e il fondamento della fiducia nei sistemi di intelligenza artificiale (Sugureddy, 2023). Il tradizionale approccio *model-centric*, incentrato sull'ottimizzazione dell'architettura algoritmica, sta progressivamente lasciando spazio a una prospettiva *data-centric*, che riconosce nella qualità, nella provenienza e nella corretta gestione dei dati i fattori determinanti del successo e dell'affidabilità dei sistemi di intelligenza artificiale.

Questa trasformazione assume una rilevanza particolare nel contesto degli audit di cybersicurezza, nei quali la solidità, la tracciabilità e la verificabilità dei dati costituiscono la base di ogni processo di verifica, controllo o certificazione. Gli ecosistemi digitali contemporanei si caratterizzano per la presenza di flussi informativi dinamici, interconnessi e multi sorgente, all'interno dei quali agenti intelligenti autonomi – capaci di osservare, apprendere e agire – partecipano direttamente alla generazione, elaborazione e validazione dei dati.

In questo scenario, il ciclo di vita del dato – dalla raccolta all'integrazione, dalla trasformazione alla migrazione – diventa il punto nevralgico in cui l'automazione agentica può, da un lato, rafforzare la coerenza e la tracciabilità dei processi, ma dall'altro introdurre nuovi rischi legati alla perdita di controllo, alla distorsione

informativa e all'uso improprio di informazioni sensibili. La governance dei dati si trova così ad affrontare sfide derivanti dalla dinamicità dei flussi informativi, dalla molteplicità delle fonti e dalla crescente autonomia delle entità computazionali. L'effettiva capacità della data governance di supportare i sistemi di intelligenza artificiale agentica dipende dalla presenza di un insieme di condizioni strutturali e tecnico-organizzative che ne consentano l'integrazione nei processi di controllo e di gestione del rischio. Strutturalmente, la governance dei dati si esercita attraverso politiche, incentivi e meccanismi sanzionatori volti a promuovere una cultura organizzativa in cui i dati siano trattati come una risorsa strategica, e i comportamenti che ne favoriscono o ne compromettono la corretta gestione siano rispettivamente premiati o sanzionati.

Tra le funzioni chiave della governance dei dati rientrano: la standardizzazione dei dati, ovvero la creazione di metadati per favorire l'integrazione e l'interpretazione coerente dei dataset; l'attribuzione di responsabilità e procedure decisionali per la gestione e la qualità dei dati; il monitoraggio dell'utilizzo dei dati, e la supervisione dei sistemi di gestione dei dati lungo tutto il loro ciclo di vita (Janssen et al., 2020).

7. Discussione e conclusioni

L'attuale configurazione della data governance e della cybersecurity nelle organizzazioni è attraversata da una trasformazione strutturale che segna la transizione da un modello di compliance prevalentemente reattivo ad un paradigma proattivo e predittivo. La moltiplicazione degli obblighi normativi e la loro estensione lungo l'intera catena del valore hanno reso evidente come la conformità non possa più essere ridotta a un mero adempimento regolatorio, bensì debba essere concepita quale meccanismo abilitante per la resilienza organizzativa e la continuità operativa. In tale prospettiva, la gestione della compliance estesa alle terze parti rappresenta un perno strategico, in quanto l'esposizione ai rischi cyber e regolatori non si arresta ai confini giuridici dell'impresa, ma si propaga a tutto l'ecosistema di attori interconnessi.

Il Third Party Risk Management (TPRM) si pone come disciplina cardine di questa riconfigurazione, articolandosi non soltanto come processo di identificazione, valutazione e mitigazione dei rischi esterni, ma come dispositivo metodologico che consente di riallineare il rapporto tra impresa e terze parti a criteri di responsabilità condivisa e trasparenza. La sua natura ciclica e adattiva garantisce la possibilità di calibrare i presidi in funzione della criticità delle relazioni esterne, introducendo un approccio graduato e proporzionato al livello di esposizione. Ciononostante, l'implementazione di un Third Party Risk Management realmente efficace risulta limitata dai vincoli dei tradizionali strumenti di audit, fondati su logiche di verifica periodica, controlli ex post e forte dipendenza dall'intervento umano. Tale impostazione, pur consolidata nella prassi, si rivela oggi intrinsecamente inefficiente in un contesto caratterizzato da minacce dinamiche, cicli di innovazione tecnologica accelerati e un contesto regolatorio in costante evoluzione.

L'affermazione dell'audit risk-based e del monitoraggio continuo rappresenta dunque un punto di svolta. Il primo consente di superare l'omogeneità dei controlli, concentrando risorse e attenzioni sugli asset a più elevato impatto strategico e normativo; il secondo traduce la compliance in un processo ininterrotto, capace di rilevare in tempo reale deviazioni, anomalie e potenziali vulnerabilità.

In questo scenario, l'avvento dell'intelligenza artificiale agentica costituisce il catalizzatore tecnologico di maggiore impatto. A differenza delle soluzioni di intelligenza artificiale tradizionale, caratterizzate da specializzazione e rigidità algoritmica, i sistemi agentici introducono elementi di autonomia decisionale, apprendimento incrementale e cooperazione multi-agente. Le architetture agentiche sono progettate per scomporre obiettivi complessi in sotto-attività modulari, assegnandole ad agenti specializzati in grado di operare in parallelo e coordinarsi secondo logiche distribuite. Questo consente di trasformare radicalmente i processi di audit: non più sequenze lineari e centralizzate, ma reti dinamiche e adattive, capaci di monitorare simultaneamente fornitori critici, recepire modifiche normative, aggiornare metriche di rischio e produrre in autonomia report strutturati per organismi interni ed autorità di vigilanza.

La capacità degli agenti di interagire con l'ambiente operativo, apprendere da flussi informativi eterogenei e rimodulare le proprie strategie in funzione di contesti mutevoli rende possibile la costruzione di un sistema di audit predittivo, resiliente e auto adattivo.

Resta, tuttavia, la consapevolezza che l'integrazione di sistemi di intelligenza artificiale agentica nei contesti inter-organizzativi ponga sfide significative. Infatti, nonostante essa offra un potenziale trasformativo nei processi aziendali, i costi di implementazione elevati, la complessità tecnologica e le problematiche legate alla gestione dei dati, ne rallentano l'adozione diffusa. Ed infatti la frammentazione delle fonti informative, l'eterogeneità dei formati e delle politiche di accesso ai dati, nonché l'assenza di standard condivisi di qualità e interoperabilità, limitano la capacità degli agenti di operare in modo coordinato e affidabile lungo l'intera catena del valore. Inoltre, la scarsa maturità digitale delle PMI (Boccardelli et al., 2007; Oldemeyer et al., 2024) e la limitata disponibilità di dati (EIB, 2023) costituiscono ostacoli significativi agli investimenti in questo ambito. A questi elementi si aggiunge l'incertezza derivante da un quadro normativo in continua evoluzione, che varia considerevolmente tra settori industriali e casi d'uso (Cohen et al., 2023), creando sfide nella mitigazione dei rischi emergenti e nelle garanzie di conformità (Spagnoletti and Volpentesta, 2024).

Messaggi chiave:

- Dimostra come l'Intelligenza Artificiale Agentica e le architetture multi-agente abilitino l'automazione dei processi di audit di conformità.
- Evidenzia la transizione dagli audit periodici e reattivi a un paradigma di auditing continuo, basato sul rischio e di natura predittiva.

- Fornisce un quadro concettuale e tecnico che illustra come gli agenti autonomi orientati agli obiettivi possano rafforzare la trasparenza della governance, la gestione del rischio delle terze parti e la resilienza organizzativa negli ecosistemi digitali interconnessi.

Bibliografia

Abouelyazid, M. & Xiang, C. (2019). Architectures for AI integration in next-generation cloud infrastructure, development, security, and management. *International Journal of Information and Cybersecurity*, *3*(1), 1-19.

Acharya, D.B., Kuppan, K. & Divya, B. (2025). Agentic AI: Autonomous intelligence for complex goals – a comprehensive survey. *IEEEc Access*.

Adama, H.E. & Okeke, C.D. (2024). Digital transformation as a catalyst for business model innovation: A critical review of impact and implementation strategies. *Magna Scientia Advanced Research and Reviews*, *10*(2), 256-264. https://doi.org/10.30574/msarr.2024.10.2.0066.

Adiloğlu, B. & Güngör, N. (2019). Investigation of increasing technology use and digitalization in auditing. *Pressacademia*, *9*(9), 20-23. https://doi.org/10.17261/pressacademia.2019.1058.

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management*, *43*(1), 39-58.

Ajiga, D., Ayanponle, L. & Okatta, C.G. (2022). AI-powered HR analytics: Transforming workforce optimization and decision-making. *International Journal of Science and Research Archive*, *5*(2), 338-346.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., et al. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

Antunes, M., Maximiano, M. & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences*, *12*(9), 4102. https://doi.org/10.3390/app12094102.

Anuar, N.B. (2023). The role of AI in GDPR compliance and data protection auditing. *Multidisciplinary Innovations & Research Analysis*, *4*(4), 1-15.

Associazione Italiana Internal Auditors. (2019). *Top Risk 2020 secondo i CAE Europei.* https://www.aiiaweb.it/sondaggio-i-top-risk-del-2020-secondo-i-cae-europei.

Benjamin, L.B., Amajuoyi, P. & Adeusi, K.B. (2024). Marketing, communication, banking, and Fintech: Personalization in Fintech marketing, enhancing customer communication for financial inclusion. *International Journal of Management & Entrepreneurship Research*, *6(*5), 1687-1701.

Boccardelli, P., Fontana, F. & Manzocchi, S. (2007). *La diffusione dell'ICT nelle piccole e medie imprese*. Luiss University Press, Rome.

Borghoff, U.M., Bottoni, P. & Pareschi, R. (2025). Human-artificial interaction in the age of agentic AI: A system-theoretical approach. *Frontiers in Human Dynamics*, *7*, 1579166.

Cohen, G.I., Evgeniou, T. & Husovec, M. (2023). Navigating the new risks and regulatory challenges of GenAI. *Harvard Business Review*, *1-4.* https://hbr.org/2023/11/navigating-the-new-risks-and-regulatory-challenges-of-genai.

Diamantopoulou, V., Tsohou, A. & Karyda, M. (2020). From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls. *Information and Computer Security*, *28*(4), 645-662. https://doi.org/10.1108/ICS-01-2020-0004.

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A. & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* (1641-1646). IEEE. https://doi.org/10.1109/COMPSAC48688.2020.00-20.

European Investment Bank (EIB) (2023). *Digitalisation of SMEs in Italy.* https://www.eib.org/attachments/thematic/digitalisation_of_smes_in_italy_summary_en.pdf.

Fantoni, G., Al-Zubaidi, S.Q., Coli, E. & Mazzei, D. (2021). Automating the process of method-time-measurement. *International Journal of Productivity and Performance Management*, *70*(4), 958-982.

Francis Onotole, E., Ogunyankinnu, T., Adeoye, Y., Osunkanmibi, A.A., Aipoh, G. & Egbemhenghe, J. (2022). The Role of Generative AI in developing new Supply Chain Strategies-Future Trends and Innovations. *International Journal of Supply Chain Management*, *11*(4), 325-338.

Ganapathy, V. (2023). AI in auditing: A comprehensive review of applications, benefits and challenges. *Shodh Sari – An International Multidisciplinary Journal*, *2*(4), 328-343.

Hosseini, S. & Seilani, H. (2025). The role of agentic AI in shaping a smart future: A systematic review. *Array*, 26, 100399.

Hughes, L., Dwivedi, Y.K., Malik, T., Shawosh, M., Albashrawi, M.A., Jeon, I., Dutot, V., Appanderanda, M., Crick, T. & De', R. (2025). AI agents and agentic systems: A multi-expert analysis. *Journal of Computer Information Systems*, 1-29.

Ilori, O., Lawal, C.I., Friday, S.C., Isibor, N.J. & Chukwuma-Eke, E.C. (2022). Cybersecurity auditing in the digital age: A review of methodologies and regulatory implications. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 174-187.

Ilori, O., Nwosu, N.T. & Naiho, H.N.N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews, 22*(3), 213-224.

Jacobides, M.G., Cennamo, C. & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255-2276.

Janssen, M., Brous, P., Estevez, E., Barbosa, L.S. & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government information quarterly*, *37*(3), 101493.

Mohammed, A. (2023). Elevating cybersecurity audits: How AI is shaping compliance and threat detection. *Aitoz Multidisciplinary Review*, *2*(1), 35-43.

OECD (2018). *OECD due diligence guidance for responsible business conduct*. https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf.

Oldemeyer L., Jede A., Teuteberg F., "Investigation of Artificial Intelligence in SMEs: A Systematic Review of the State of the Art and the Main Implementation Challenges", *Management Review Quarterly*, 2024, https://doi.org/10.1007/s11301-024-00405-4.

Oluoha, O., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V. & Orieno, O. (2023). A privacy-first framework for data protection and compliance assurance in digital ecosystems. *Iconic Research and Engineering Journals*, *7*(4), 620-646.

Popoola, O.A., Adama, H.E., Okeke, C.D. & Akinoso, A.E. (2024). Conceptualizing agile development in digital transformations: Theoretical foundations and practical applications.

Engineering Science & Technology Journal, *5*(4), 1524-1541. https://doi.org/10.51594/estj/v5i4.1080.

Rahman, F., Putri, G., Wulandari, D., Pratama, D. & Permadi, E. (2021). Auditing in the digital era: Challenges and opportunities for auditor. *Golden Ratio of Auditing Research*, *1*(2), 86-98. https://doi.org/10.52970/grar.v1i2.367*.

Sabillon, R. (2022). Audits in Cybersecurity. In I. Management Association (Ed.), *Research Anthology on Business Aspects of Cybersecurity* (pp. 1-18). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-3698-1.ch001.

Sapkota, R., Roumeliotis, K.I. & Karkee, M. (2025). AI agents vs. agentic AI: A conceptual taxonomy, applications and challenges. *arXiv preprint arXiv:2505.10468*.

Spagnoletti, P. & Volpentesta, T. (2024). Intelligenza artificiale generativa nelle piccole e medie imprese: Evidenze empiriche nel contesto italiano. *Rivista di Politica Economica*, *2*, 113-130.

Sugureddy, A.R. (2023). AI-driven solutions for robust data governance: A focus on generative AI applications. *Journal ID*, *6202*, 8020.

Tiwari, R. & Debnath, J. (2017). Forensic accounting: A blend of knowledge. *Journal of Financial Regulation and Compliance*, *25*(1), 73-85. https://doi.org/10.1108/jfrc-05-2016-0043.

Yaseen, A. (2022). Accelerating the SOC: Achieve greater efficiency with AI-driven automation. *International Journal of Responsible Artificial Intelligence*, *12*(1), 1-19.

Orchestrare la data governance inter-organizzativa: pratiche, insight e ruoli

Niloofar Kazemargi [*] e Federica Ceci [**]

Abstract: Pur ampiamente riconosciuti come asset strategico per innovazione, produzione, posizionamento e crescita, i dati sostengono decisioni efficaci solo quando sono governati mediante pratiche, definite data governance, che allineano ruoli, responsabilità, standard e modalità d'uso, definendo in modo esplicito chi fa cosa, quando e con quali informazioni. L'attenzione degli studiosi si è concentrata soprattutto sul livello intra-organizzativo, mentre risulta ancora poco chiaro come la data governance si configura quando sono coinvolte imprese che collaborano per condividere, utilizzare ed estrarre valore dai dati. Attraverso un case study qualitativo dimostriamo come la data governance emerga direttamente dalle interazioni fra i vari attori e si struttura intorni a tre dimensioni interconnesse: *data practice* (definizione/creazione/accesso), *data insight* (rappresentazioni per il decision-making) e *data value* (confini fluidi del valore). Queste dimensioni sono co-costruite attraverso accordi, adattamenti di processi e co-progettazione di interfacce. Discutiamo infine i contributi teorici e le implicazioni manageriali e di policy, sottolineando la natura dinamica e relazionale negli ecosistemi collaborative.

Parole chiave: Data governance, Ecosistemi di dati, Collaborazione inter-organizzativa, Piattaforme dati, Data Value Chain.

1. Introduzione

Manager, studiosi ed esperti di innovazione concordano che oggi i dati costituiscono un asset strategico per le imprese sotto ogni punto di vista: innovazione, produzione, posizionamento nel mercato, coordinamento operativo e crescita. Altrettanto condiviso è che la loro trasformazione in decisioni efficaci non è un'attività

[*] Niloofar Kazemargi (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: niloofar.kazemargi@unich.it

[**] Federica Ceci (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: federica.ceci@unich.it

DOI: 10.82018/9791221165456-10

semplice o immediata. Essa, infatti, richiede pratiche di data governance capaci di allineare ruoli, responsabilità, standard e modalità d'uso, regole e ruoli. Le definizioni classiche descrivono la data governance come allocazione di *decision right* e *accountability* lungo i processi informativi [1] – ovvero chi può fare cosa, con quali informazioni, metodi e in quali circostanze – e identificano ruoli tipici (*data owner*, *data producer*, *data consumer*, *data governance leader*) (Abraham, Schneider & vom Brocke, 2019; Jarvenpaa & Essén, 2023). Questo impianto concettuale ha trovato terreno fertile nel perimetro intra-organizzativo, dove policy, procedure e architetture definiscono la proprietà del dato, le responsabilità di qualità e le condizioni di accesso. Tuttavia, la creazione di valore avviene sempre più oltre i confini di una singola organizzazione, all'interno di ecosistemi in cui attori eterogenei co-producono, integrano e riusano dati. In tali contesti la natura del dato modulare, riusabile, e ricombinabile accentua tensioni e opportunità: i processi che funzionano internamente non sono automaticamente trasferibili; le metriche di qualità, i dizionari, i livelli di granularità e le finestre temporali di aggiornamento devono essere negoziati fra organizzazioni con priorità, tempi e vincoli differenti. Ne discende l'esigenza di spostare l'attenzione dal perimetro della singola impresa al livello inter-organizzativo (Abraham et al., 2019; Davidson, Wessel, Winter & Winter, 2023; Jagals & Karger, 2021), interrogandosi su come le interazioni tra attori plasmino scelte operative (definizioni, accessi, cadenze di aggiornamento), assetti decisionali (chi decide cosa e quando) e assetti informativi (come i dati vengono rappresentati e resi fruibili per le decisioni). Da questo punto di vista, la sfida non riguarda soltanto la compliance o l'adozione di un framework normativo, ma la capacità di orchestrazione tra organizzazioni: occorre integrare standard tecnici e semantici, definire interfacce e modalità di integrazione (API, formati, metadati), stabilire regimi di qualità e livelli di servizi che riducano ambiguità e ritardi informativi. La data governance si configura allora come un processo dinamico che combina regole formali e pratiche, emergenti dall'uso quotidiano e dall'adattamento reciproco. In questo scenario, il ruolo dei diversi attori, i.e. grandi imprese, PMI tecnologiche, fornitori di piattaforme, non è meramente esecutivo: ciascuno contribuisce a costruire meccanismi di coordinamento che rendono le informazioni effettivamente utilizzabili e utili nelle decisioni.

Muovendo da un caso qualitativo su una PMI e due grandi imprese manifatturiere clienti della stessa, il capitolo vuole rispondere alla seguente domanda: in che modo le interazioni inter-organizzative influenzano le pratiche di data governance? Dai nostri dati emergono tre dimensioni, i.e. *data practice*, *data insight* e *data value*, che vengono negoziate e rese operative attraverso accordi, routine e strumenti condivisi. In particolare, le *data practice* riguardano la definizione, la creazione e l'accesso ai dati (chi produce cosa, con quale granularità e con quali cadenze); i *data insighs* attengono alle rappresentazioni che rendono i dati azionabili (quali viste, per quali attori, con quali metriche e soglie); il *data value* concerne i benefici realizzati e la loro evoluzione nel tempo, poiché lo scope d'uso si amplia con la maturità

[1] https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.

organizzativa e l'innovazione tecnologica. Considerate lungo la Data Value Chain, queste dimensioni non sono step isolati, ma snodi interdipendenti: decisioni prese su una dimensione (p.es. la frequenza di aggiornamento) condizionano ciò che è possibile vedere e decidere sulle altre (p.es. tempestività dei report, capacità predittiva, ritorno operativo). La ricerca mostra, inoltre, che l'efficacia della data governance non dipende unicamente dall'introduzione di strumenti o policy, ma dalla qualità della relazione e dalla capacità di apprendimento congiunto: protocolli di qualità, dizionari condivisi, cicli di revisione dei report e regole d'accesso si consolidano attraverso iterazioni ripetute, in cui esigenze operative e vincoli tecnici vengono progressivamente armonizzati. In tal senso, la governance appare meno come un esito "disegnato a tavolino" e più come una tessitura relazionale che allinea responsabilità, routine e rappresentazioni, abilitando la trasformazione dei dati in decisioni coerenti con obiettivi comuni.

2. Rassegna della letteratura

2.1. Gli ecosistemi di dati

Gli ecosistemi di dati sono definiti come "reti socio-tecniche complesse nelle quali gli attori interagiscono e collaborano per trovare, archiviare, pubblicare, consumare o riusare dati, oltre che per promuovere l'innovazione, creare valore e supportare nuovi business" (Oliveira, Lóscio & Lima, 2019, p. 590). In tali ecosistemi, il valore emerge dal fatto che un gruppo di attori produce o fornisce dati ed altri attori li consumano (Janssen, Charalabidis & Zuiderwijk, 2012). Questa divisione dei ruoli rende centrali i meccanismi di coordinamento, gli standard semantici e le procedure di qualità che consentono il passaggio dai dati grezzi a usi effettivi in contesti organizzativi differenti. La letteratura distingue gli ecosistemi di dati in base alla struttura di governance: *mercato*, *gerarchia*, *a rete* o *a bazaar* (Lis & Otto, 2021). Nel *mercato*, lo scambio di dati è regolato da prezzi, contratti e da coordinamento leggero tra attori relativamente autonomi. La *gerarchia* concentra diritti decisionali e regole in un soggetto centrale (es. il proprietario della piattaforma), con controllo top-down su accessi, standard e qualità. La governance a *rete* si fonda su relazioni bilanciate fra partner: decisioni e standard emergono da coordinamento reciproco, accordi di lungo periodo e fiducia inter-organizzativa. Il *bazaar* richiama logiche comunitarie e auto-organizzate (vicine all'open source/open data): l'ingresso è aperto, le regole sono pubbliche e l'evoluzione degli standard avviene in modo partecipativo. Questi archetipi non sono esclusivi: nella pratica possono co-esistere nello stesso ecosistema, variando per asset, fasi del ciclo di vita e potere degli attori. La tipologia incide sul modo in cui si prendono decisioni, si allocano diritti e si distribuiscono incentivi. Un'ulteriore dimensione riguarda il grado di apertura. Negli ecosistemi aperti qualunque attore può aderire e utilizzare i dati senza particolari vincoli;

l'obiettivo principale è spesso la trasparenza e il supporto al decision-making pubblico o diffuso. Al contrario, negli ecosistemi di dati chiusi solo attori selezionati sono autorizzati ad accedere e utilizzare i dati (Gelhaar, Groß & Otto, 2021; Janssen et al., 2012). Ne deriva che la scelta di apertura o chiusura condiziona le politiche di qualità, le licenze, la privacy e i meccanismi di controllo.

Un'ulteriore distinzione riguarda l'infrastruttura. Alcuni ecosistemi si appoggiano a infrastrutture proprietarie, gestite e possedute da un attore (ad es. piattaforme social) (Alaimo, Kallinikos & Valderrama, 2020). In questo caso l'attore centrale definisce stack tecnologico, formati, interfacce e ciclo di vita dei dati: ne derivano tempi di adozione più rapidi, integrazione verticale e un'unica cabina di regia su sicurezza, scalabilità e qualità. In cambio, gli altri partecipanti accettano maggiore lock-in tecnologico e contrattuale, minore portabilità degli asset informativi e una posizione negoziale asimmetrica sulle API, sul versioning degli schemi e sugli SLA. Altri ecosistemi adottano infrastrutture distribuite per memorizzare, processare e scambiare dati (ad es., federazioni, *data mesh*, *data space*) (Gelhaar & Otto, 2020). Qui l'interoperabilità è perseguita con standard aperti, metadati condivisi e contratti di dati fra domini; i dati possono rimanere presso i titolari (*data sovereignty*), riducendo rischi di concentrazione e favorendo resilienza. Il rovescio della medaglia è un maggiore costo di coordinamento: occorre allineare identità e accessi, cataloghi e ontologie, politiche di qualità, osservabilità end-to-end e meccanismi di conformità (ad es., residenza dei dati, minimizzazione). Performance e coerenza dipendono dall'accordo su frequenze di aggiornamento, latenze accettabili e priorità di sincronizzazione.

In entrambi i modelli, l'infrastruttura non è neutra: abilita e insieme vincola formati, interfacce, tempi e modi d'uso lungo la filiera dei dati. Scelte architetturali, come cloud vs edge; API sincrone (REST/GraphQL) vs asincrone (event streaming); gestione degli schemi (registry) e del *versioning*; cifratura in transito/a riposo; tecniche di pseudonimizzazione/anonimizzazione; containerizzazione per la portabilità per citarne alcune, hanno effetti diretti su: interoperabilità (quanto è semplice integrare nuove fonti/servizi); lock-in (dipendenza da *vendor* o protocolli proprietari); sostenibilità (costi di esercizio, efficienza energetica, riuso); governance (chi controlla accessi, cambi di schema, priorità di calcolo); affidabilità (monitoraggio, audit trail, ripristino, continuità operativa). Scegliere l'infrastruttura significa disegnare il campo di gioco della governance: chi detiene il controllo del piano tecnologico influenza i diritti decisionali, la qualità realizzabile, i tempi di aggiornamento e, in ultima analisi, la capacità dell'ecosistema di generare valore dai dati.

2.2. Data governance

La data governance è comunemente definita come "un sistema di diritti decisionali e responsabilità per i processi informativi, eseguito secondo modelli concordati che descrivono chi può intraprendere quali azioni, con quali informazioni, quando,

in quali circostanze e con quali metodi" (Khatri & Brown, 2010). Gli studi precedenti si sono concentrati su: (i) allocazione dei *decision right* e (ii) meccanismi per allineare attività e obiettivi organizzativi. Numerosi contributi propongono framework per garantire che le decisioni sui dati siano coerenti con obiettivi e strategie (Gregory, Kaganer, Henfridsson & Ruch, 2018; Tiwana, Konsynski & Venkatraman, 2013), introducendo ruoli distinti, ad esempio data governance leader, *data owner*, *data producer*, *data consumer* e chiarendone responsabilità e interazioni (Abraham et al., 2019; Jarvenpaa & Essén, 2023).

La ricerca ha guardato soprattutto al livello organizzativo (Abraham et al., 2019), ossia a come una singola impresa gestisca i propri asset informativi. Tuttavia, la crescente dipendenza da condivisione e accesso ai dati dentro e fuori i confini aziendali spinge a spostare il baricentro dalla governance "interna" a quella ecosistemica (Abraham et al., 2019; Jagals & Karger, 2021a). I framework esistenti, pur offrendo spunti per i contesti inter-organizzativi, non coprono pienamente le sfide poste da eterogeneità degli attori, complessità dei flussi e dinamiche negoziali tipiche della collaborazione sui dati (Lis & Otto, 2021). Solo di recente sono emersi studi comparativi che analizzano empiricamente i meccanismi di governance in diversi ecosistemi di dati (Micheli, Ponti, Craglia & Berti Suman, 2020). Quando dati e decisioni attraversano confini organizzativi, la governance richiede coordinamento su più assi: definizioni e semantiche (dizionari dati, gerarchie, granularità); qualità e cadenze (criteri, controlli, frequenze di aggiornamento/lettura); accessi e diritti (chi vede cosa, quando e con quali vincoli); rappresentazioni (formati, viste e indicatori rilevanti per stakeholder diversi). In questo scenario, le logiche di governance pensate per una singola organizzazione sono necessarie ma non sufficienti: occorrono meccanismi inter-organizzativi che riducano ambiguità semantiche, gestiscano le dipendenze temporali e diano accountability condivisa sulle decisioni che si basano sui dati. Da qui l'interesse per un approccio ecosistemico, capace di leggere relazioni, infrastrutture e regole come parti di un medesimo sistema socio-tecnico.

Un recente filone di ricerca ha interpretato i dati come artefatti digitali con proprietà peculiari (modularità, plasticità, riusabilità) e ha ampliato la comprensione della governance oltre i modelli top-down. In questa prospettiva, la governance dipende dal lavoro situato sui dati, cioè *data curation*, gestione di metadati, procedure di qualità, svolto dagli attori che quotidianamente producono, trasformano e utilizzano i dati (Parmiggiani & Grisot, 2020). Tali scelte bottom-up influiscono in modo decisivo su ciò che i dati "possono" fare in pratica: quali viste sono realmente utili, quali standard risultano adottabili, quali routine risultano sostenibili. Nonostante questi avanzamenti, sappiamo ancora poco su come la natura dei dati (la loro malleabilità, ri-combinabilità e dipendenza dall'uso) modelli la data governance a livello di ecosistema. Colmare questo vuoto empirico e teorico significa osservare in situ come gli attori negozino definizioni, qualità e accessi, e come tali negoziazioni si traducano in rappresentazioni e valore condiviso. È precisamente in questa direzione che si colloca il nostro contributo empirico.

3. Contesto e metodo

Per rispondere a come la collaborazione inter-organizzativa plasmi la data governance, abbiamo svolto una analisi qualitativa basata su studio di caso(Pan & Tan, 2011). Questo approccio ci ha consentito di approfondire la dimensione relazionale della gestione dei dati a livello inter-organizzativo. Abbiamo studiato un fornitore di piattaforme digitali, di seguito indicato come DigitalONE. Fondata nel 2005, DigitalONE è una piccola impresa specializzata nella trasformazione Industry 4.0 per la manifattura e la supply chain.

DigitalONE costituisce un caso adatto per indagare la data governance in assetti inter-organizzativi poiché presenta condizioni tecniche e organizzative che mettono alla prova i meccanismi di coordinamento tra attori. Il prodotto principale di DigitalONE è la ONE platform, una piattaforma per la gestione di dati con una struttura modulare ed end-to-end. Questa piattaforma attraversa più domini funzionali (demand management, production planning, manutenzione predittiva) e integra fonti di dati eterogenee, quali sistemi ERP (es. SAP), sensori e open data, caratterizzate da semantiche, granularità e latenze differenti. Tale eterogeneità richiede la negoziazione inter-organizzativa di definizioni (dizionari e gerarchie), qualità (criteri e controlli), accessi (ruoli, finestre temporali, policy di sicurezza) e rappresentazioni (viste e indicatori per stakeholder molteplici), evidenziando come la governance emerga nella pratica quotidiana più che da un disegno esclusivamente top-down. Inoltre, la modularità consente un'osservazione longitudinale degli effetti di retroazione lungo la Data Value Chain: decisioni prese a monte (ad es., frequenze di aggiornamento o versioning degli schemi) incidono sulla fruibilità delle visualizzazioni, sull'adozione e, in ultima analisi, sul valore realizzato. La dimensione PMI del fornitore, infine, favorisce cicli iterativi di specifica-prototipo-revisione e una più diretta visibilità del "lavoro dei dati" (curation, metadati, procedure di qualità), rendendo osservabili i processi di orchestrazione e le dinamiche bottom-up che, nei contesti gerarchici più complessi, tendono a rimanere meno trasparenti.

La ricerca empirica ha utilizzato dati primari e dati secondari. I dati primari comprendono interviste e osservazioni sul campo; i dati secondari includono siti web aziendali e blog post. In totale, abbiamo condotto 8 interviste con dipendenti della DigitalONE e con i clienti della stessa. La durata media delle interviste è stata di 40 minuti. L'analisi dei dati è iniziata in parallelo alla raccolta. Abbiamo adottato un approccio qualitativo induttivo (Myers, 2019) articolato in tre fasi. Primo, abbiamo svolto un open coding delle interviste per identificare i codici del primo ordine, attenendoci il più possibile al linguaggio degli informatori o a brevi descrizioni strettamente aderenti ai dati (Glaser & Strauss, 1967). Secondo, abbiamo effettuato un confronto costante tra i codici del primo ordine per far emergere codici di secondo ordine, ossia temi più ampi in grado di catturare significati sottostanti e connessioni nei dati. Infine, abbiamo aggregato i codici di secondo ordine in temi complessivi, che costituiscono l'esito finale del processo di analisi.

4. Analisi e Risultati

L'esame congiunto di interviste e osservazioni sul campo mette in evidenza tre nuclei tematici tra loro interdipendenti, *data practice*, *data insight* e *data value*, attraverso i quali si osserva come la data governance prenda forma nelle interazioni tra organizzazioni. Nelle sezioni che seguono discutiamo ciascun nucleo, mostrando come le scelte su definizione/creazione/accesso ai dati sostengano le rappresentazioni utili per decidere e, per questa via, contribuiscano alla generazione di valore lungo la Data Value Chain.

Data practice. Per *data practice* intendiamo i modi situati di definire, creare e accedere ai dati tra organizzazioni. L'implementazione di ONEplatform non è un plug-and-play: richiede revisione delle pratiche esistenti, allineamento di gerarchie e granularità dei dati, definizione dei punti di produzione del dato, aggiornamenti e controlli qualità. Senza *master data* solidi, integrazione adeguata e processi di aggiornamento precisi, anche il "miglior" software non produce risultati soddisfacenti: è la gestione dei dati a determinare il successo dell'investimento. Queste scelte sono negoziate tra fornitore e cliente, con effetti su routine operative e responsabilità diffuse. Tre evidenze spiccano. Primo, la definizione dei dati (non solo la loro selezione) richiede spesso di concordare gerarchie e granularità per garantirne coerenza e uso. Secondo, la creazione dei dati è un processo dinamico che coinvolge livelli manageriali e operativi: l'introduzione di nuove routine richiede change management e meccanismi di controllo della qualità. Terzo, l'accesso ai dati e il quando leggerli vanno concordati per evitare asimmetrie e versioni multiple: si definiscono tempi e frequenze di aggiornamento e lettura, incluse policy per strumenti esterni/API per tutelare prestazioni e sicurezza. Un intervistato ha raccontato:

> "*Le organizzazioni pensano che adottando un nuovo tool di mercato risolveranno tutti i problemi, senza considerare la revisione dei processi operativi e del modello. Noi abbiamo scelto lo strumento di DigitalONE perché consente di personalizzare. Non era una black box che colleghi e usi. Ci permette di riflettere su dove produrre i dati e prendere decisioni sui dati. Molte organizzazioni invece commettono l'errore di fidarsi ciecamente di un software/tool e poi si accorgono che il software non funziona, e incolpano i fornitori. Non è il software, è la gestione dei dati in quanto tale. Se non ho i master data, un buon livello di integrazione, se non gestisco i dati, se non ho processi precisi di aggiornamento, anche adottando il miglior software i risultati non saranno soddisfacenti. Senza rivedere i processi sui dati, l'investimento non ha successo. Dobbiamo ripensare la gestione dei dati*".

Le *data practice* sono state modellate e influenzate dalle interazioni inter-organizzative, poiché DigitalONE e i clienti hanno dovuto negoziare e concordare la definizione, la creazione e l'accesso ai dati. In primo luogo, gli informatori hanno sottolineato più volte che spesso è necessario coordinarsi con il fornitore non solo per identificare i dati rilevanti per un progetto specifico, ma anche per definirli. Nella

definizione dei dati, gli informatori hanno evidenziato la necessità di sedersi insieme e concordare formalmente sia la gerarchia sia la granularità dei dati. Hanno inoltre osservato che, mentre i dati generati dai sensori seguono misurazioni standardizzate e predefinite, per altre tipologie di dati operativi sono necessari accordi sulle definizioni:

> "*La raccolta di dati direttamente da una macchina è la parte più semplice; definisco i parametri che voglio tenere sotto controllo e stabilisco frequenza e unità di misura dei dati che desidero raccogliere. Ma non è lo stesso per altri dati necessari alla pianificazione. Devo definire, per esempio, la domanda del cliente*".

In secondo luogo, gli informatori hanno sottolineato l'importanza della fase di creazione dei dati contestualmente all'implementazione di una nuova soluzione digitale. La creazione dei dati è risultata un processo dinamico che implica coordinamento continuo. Essa ha richiesto tempo e impegno significativi non solo a livello manageriale ma anche operativo:

> "*È un percorso che intraprendiamo insieme: fornitori di software, fornitori IT e noi. Siamo parte di questo sistema. Siamo noi a creare i dati, in momenti diversi e di tipologie diverse, e il software aiuta a gestire e facilitare le attività*".

Dopo aver concordato quali dati creare e come, è diventato necessario che le persone all'interno dell'organizzazione adattassero le routine quotidiane per allineare le proprie pratiche sui dati. Da un lato, ciò ha comportato uno sforzo di modifica dei processi e delle routine esistenti per garantire che i dati fossero inseriti in modo accurato e coerente. Dall'altro, è stato necessario definire meccanismi di controllo e monitoraggio della qualità dei dati. Gli individui hanno assunto una responsabilità più ampia nel determinare come, quando e quali dati registrare, a conferma del ruolo decisivo delle pratiche umane nella creazione dei dati. Questo ha mostrato che la qualità dei dati non è solo una questione tecnica, ma dipende anche dai comportamenti e dalle pratiche individuali nelle operazioni quotidiane:

> "*Nella manifattura, considerate che lavoriamo con persone impegnate sulle linee produttive: operatori che per anni hanno lavorato sempre nello stesso modo; ora si va da loro e si dice 'no, prima devi inserire i dati e poi svolgere le altre attività', come passaggio logico, oppure 'ora devi effettuare il log-in e completare alcune attività sui sistemi' mentre prima usavano documenti cartacei. Nella pianificazione si lavora con personale d'ufficio, con contesti, specializzazioni e dinamiche diverse. Ma anche lì serve change management: ogni ufficio ha le proprie routine e i propri processi, alcuni corretti, altri meno*".

Un altro aspetto cruciale ha riguardato l'accesso ai dati, cioè chi può accedere ai dati e quando. Sebbene i dati vengano mantenuti aggiornati nei sistemi, è stato necessario un accordo su quando leggerli per assicurare un'integrazione efficace:

"*Per esempio, i dati del cliente: se tre persone usano Excel e prelevano i dati da SAP in momenti diversi, quei dati diventano un problema perché ognuno poi formula le proprie considerazioni su una base informativa evidentemente diversa. Che cosa facciamo in questi casi? Nell'analisi iniziale concordiamo con gli stakeholder le tempistiche: ogni quanto, a che ora e con quale frequenza i dati devono essere aggiornati*".

Parallelamente, gli informatori hanno menzionato alcuni casi in cui determinati clienti preferivano usare strumenti analitici esterni. L'accesso ai dati doveva quindi essere concordato formalmente, con regole chiare sulla forma, la struttura e l'ampiezza dei dati da condividere. Dovevano essere definite politiche per l'uso di API esterne, inclusi limiti alla frequenza delle chiamate ai dati, per proteggere le prestazioni del sistema e mantenere la sicurezza. Per esempio, l'accesso poteva essere limitato a non più di una volta all'ora, tre volte al giorno o una volta alla settimana.

Data insight. Per *data insight* intendiamo le pratiche attraverso cui i dati diventano conoscenza azionabile e sono comunicati/impiegati nelle decisioni. Un modulo della piattaforma offre visualizzazioni e report in tempo reale; tuttavia, gli standard report raramente bastano: i team co-progettano report ad hoc con cicli iterativi di specifica-prototipo-revisione, per rispondere alle esigenze di stakeholder eterogenei. Questo lavoro porta a un cambiamento comportamentale: si passa da slide statiche a grafici e report real-time per monitorare priorità, avanzamento e costi, integrando l'uso dell'informazione nelle routine manageriali quotidiane. La lezione è duplice: a) gli insight richiedono alignment tra limiti tecnologici, logiche organizzative e formati informativi; b) l'efficacia decisionale dipende dalla rilevanza contestuale (chi vede cosa, quando e perché). In generale, i report standard si sono rivelati spesso insufficienti per i clienti, che richiedevano report personalizzati per rispondere a esigenze diversificate. Ciò ha richiesto interazioni costanti e un investimento di tempo e impegno a livello inter-organizzativo per comprendere e identificare i bisogni:

"*I report standard non sono sufficienti rispetto alle esigenze. Creiamo report ad hoc insieme ai clienti. Il cliente presenta un bisogno, noi proponiamo soluzioni e poi ci sono innumerevoli revisioni. Abbiamo investito molto tempo per soddisfare le richieste non solo di un gruppo, ma anche di diverse figure all'interno dell'azienda cliente. È stata una parte fondamentale. Ricordo molte riunioni dedicate a layout, proposte, 'ok, possiamo farlo così', ma è sempre un'attività che svolgiamo insieme*".

I *data insight* hanno richiesto un'attenta considerazione sia dei limiti tecnologici dello strumento sia delle specifiche esigenze degli stakeholder nei vari dipartimenti. Ciò ha comportato l'adattamento delle informazioni per allinearle ad aspettative, priorità e realtà operative delle diverse unità organizzative. Gli insight sono stati effettivamente sfruttati nelle decisioni solo quando hanno risposto alle esigenze e alle preoccupazioni eterogenee di tali dipartimenti. Ne è derivato un cambiamento comportamentale nell'uso delle informazioni: invece di affidarsi a presentazioni statiche nelle riunioni, i manager hanno utilizzato con crescente frequenza grafici e report in

tempo reale per ottenere visibilità sulle operazioni quotidiane. Queste rappresentazioni aggiornate hanno consentito di monitorare le priorità produttive, tracciare l'avanzamento e controllare i costi in modo più efficace, incorporando pratiche di decision-making data-driven nelle attività manageriali di routine.

Data value. Per *data value* intendiamo i benefici percepiti e realizzati dall'uso dei dati. Nel caso studiato, i confini del valore sono fluidi: l'avanzamento delle tecnologie (inclusa l'AI) introduce nuove funzionalità e *value proposition*; parallelamente, i clienti maturano capacità d'uso e ridefiniscono aspettative, generando domanda di innovazione continua. In pratica, lo scope d'uso dei dati non è definito ex ante: emerge interattivamente. Ne deriva che il valore si co-costruisce lungo la Data Value Chain, attraverso rilasci incrementali, sperimentazione e aggiustamenti alle priorità operative. La governance efficace include meccanismi di revisione periodica dello scope e di prioritizzazione delle feature coerenti con la maturità d'uso. Questo ha contribuito a rimodulare le aspettative e, di conseguenza, a generare una domanda più elevata di innovazione continua:

> "*Il nostro mondo non finisce mai: siamo sempre in innovazione continua, quindi ci sono sempre novità che per fortuna arrivano; non so, dal disporre di uno strumento che consente la previsione della domanda all'aggiunta di nuovi algoritmi di intelligenza artificiale che supportano i dati. C'è sempre un'evoluzione, e lo stesso vale per la pianificazione della produzione o per l'intera supply chain. La collaborazione, finché il cliente ne sente il bisogno, non ha fine perché camminiamo di pari passo con l'innovazione*".

Non tutte le funzionalità erano definite ex ante e, in alcuni casi, DigitalONE ha sviluppato nuove soluzioni sulla base delle esigenze del cliente emerse durante il progetto. In altre parole, lo scope dell'uso dei dati non era stabilito a priori, ma si è evoluto ed è emerso lungo l'interazione. Un informatore ha fornito un esempio:

> "*Durante il Covid c'era grande attenzione sulle forniture, in particolare dalla Cina; in quel periodo ci è stato chiesto di creare un modulo ad hoc molto focalizzato sul lato fornitore, in cui fosse possibile simulare scenari e stimare la fattibilità dei piani in base a diversi scenari di approvvigionamento dei componenti, soprattutto dall'Est, dall'Asia. È un caso in cui il cliente ci ha chiesto una soluzione e noi abbiamo rilasciato gradualmente nuove funzionalità. Abbiamo sviluppato e proposto la soluzione al cliente; se il cliente ritiene la feature interessante, avviamo con lui la fase di analisi. Il cliente può presentarsi con un nuovo bisogno e noi sviluppiamo e rilasciamo nuove funzionalità*".

Dall'analisi emerge che la data governance inter-organizzativa non è un esito statico né interamente prescrivibile, ma una pratica in continua evoluzione, negoziata nelle interazioni tra i diversi attori. Tre dimensioni interrelate ne articolano lo svolgersi: le *data practice*, che descrivono i modi situati e condivisi con cui i dati vengono definiti, creati e resi accessibili attraverso i confini organizzativi, spesso richiedendo la riconfigurazione di routine e responsabilità esistenti; i *data insight*, che riguardano la trasformazione dei dati in conoscenza fruibile per le decisioni e

sottolineano la co-progettazione di rappresentazioni aderenti ai bisogni dei vari stakeholder; il *data value*, che cattura la natura progressiva ed emergente della creazione di valore, via via che clienti e fornitori ridefiniscono scopi e usi dei dati al mutare delle priorità. Considerate congiuntamente, queste dimensioni mostrano una governance dinamica e relazionale, radicata nel contesto socio-tecnico della collaborazione: decisioni su definizioni, qualità e accessi abilitano insight appropriati, gli insight sostengono l'adozione e l'impatto operativo, e i risultati ottenuti retroagiscono sulle pratiche, rilanciando l'allineamento lungo la Data Value Chain. Una sintesi è riportata nella Tabella 1.

Tabella 1. – Sintesi dei costrutti chiave

Dimensione	Definizione	Come emerge	Insight chiave
Data Practice	Modi situati di definire, creare e accedere ai dati tra organizzazioni.	Attraverso negoziazione e coordinamento di routine, ruoli e vincoli tecnici.	La data governance dipende da definizioni condivise, workflow adattati e meccanismi di accesso concordati.
Data Insight	Trasformazione dei dati in conoscenza azionabile per le decisioni.	Tramite co-design iterativo di report e strumenti, calibrati sui bisogni degli stakeholder.	La generazione di insight richiede allineamento tra rappresentazioni dei dati e logiche/usi organizzativi.
Data Value	Benefici percepiti e realizzati derivanti dall'uso dei dati.	Attraverso collaborazione continua, sperimentazione ed evoluzione delle aspettative dei clienti.	Il valore non è predefinito, ma co-costruito ed evolve nel tempo con innovazione e maturità d'uso.

5. Discussione: la governance come processo dinamico e relazionale

Recentemente molti contributi scientifici si sono concentrati sul livello operativo, con l'obiettivo di far emergere le pratiche di data governance (Benfeldt, 2020; Monteiro & Parmiggiani, 2019; Parmiggiani & Grisot, 2020). Con questo studio intendiamo contribuire a tale filone disvelando le pratiche di data governance a livello inter-organizzativo. Sulla base del caso esaminato, offriamo nuovi elementi interpretativi: la data governance non coincide con l'adozione di un framework statico, poiché l'oggetto stesso della governance presenta una natura intrinsecamente evolutiva. Di conseguenza, le interazioni tra organizzazioni risultano determinanti nel plasmare regole, routine e strumenti; la governance complessiva emerge come esito co-modellato dalle diverse parti coinvolte, più che come applicazione unidirezionale di

principi astratti. In questa prospettiva abbiamo identificato tre componenti della data governance, i.e. *data practice*, *data insight* e *data value*, che, considerate congiuntamente, delineano un circuito ricorsivo di configurazione e apprendimento. Le *data practice* riguardano i modi situati e negoziati con cui i dati sono definiti, creati, qualificati e resi accessibili oltre i confini organizzativi; esse richiedono spesso la riconfigurazione di responsabilità e processi, nonché accordi su semantiche, granularità, cadenze di aggiornamento e finestre di lettura. I *data insight* concernono la trasformazione dei dati in rappresentazioni utili per decidere; qui la co-progettazione di report, indicatori e visualizzazioni consente di allineare i formati informativi alle logiche e ai fabbisogni dei diversi stakeholder, favorendo l'adozione e l'uso effettivo. Il *data value* cattura, infine, la natura progressiva della creazione di valore: lo scope di utilizzo si amplia con la maturità d'uso, le funzionalità vengono ri-prioritizzate in base alle esigenze emergenti e l'impatto operativo si consolida nel tempo, anche in reazione a shock esterni o innovazioni tecnologiche.

L'analisi mostra che queste tre componenti non si succedono in modo lineare, ma operano iterativamente per integrare culture organizzative eterogenee, allineare una visione condivisa che comprende la definizione degli obiettivi generali e dello scope di progetto, e affrontare le tensioni tipiche dei progetti data-driven (disallineamenti semantici, trade-off tra performance e sicurezza, vincoli infrastrutturali). Ne deriva la necessità di superare concezioni statiche e top-down della data governance e di adottare, invece, una lettura dinamica e relazionale, che riconosce come la governance si dispieghi attraverso interazioni situate tra gli attori. Evidenziando i ruoli di *data practice*, *data insight* e *data value*, il nostro studio sottolinea l'importanza di negoziazione continua, adattamento reciproco e allineamento contestuale: è questo lavoro di coordinamento, più che la mera conformità a un modello predefinito, a determinare la capacità delle organizzazioni di tradurre i dati in decisioni e risultati lungo la Data Value Chain.

La nostra analisi offre contributi significativi alla comprensione della data governance. Il lavoro si inserisce nella letteratura sugli ecosistemi di data governance intrecciando la prospettiva sulle dimensioni organizzative (Winter & Davidson, 2017) in tre direzioni. Primo, integra ed estende gli studi che si concentrano sulle pratiche a livello d'impresa (Benfeldt, 2020; Monteiro & Parmiggiani, 2019; Parmiggiani & Grisot, 2020), mostrando come tali pratiche si dispieghino nell'inter-organizzativo. In secondo luogo, amplia la comprensione di pratiche che spesso restano invisibili, dalle quali tuttavia dipende in modo critico l'impiego efficace di strumenti analitici e di intelligenza artificiale (van den Broek, 2025). Senza *data practice*, *data insight* e *data value* anche le tecnologie più avanzate non sono in grado di generare valore. In terzo luogo, il nostro studio mette in evidenza il ruolo attivo delle PMI nella formazione degli ecosistemi di dati e nella configurazione della data governance. Il caso mostra come le caratteristiche strutturali e la flessibilità delle piccole imprese consentano modalità di ingaggio differenti con le aziende clienti, offrendo soluzioni personalizzate, tarate sulle esigenze e aspettative specifiche, invece di affidarsi a proposte standardizzate.

Sul piano manageriale, proponiamo una lettura granulare delle pratiche di data governance a livello inter-organizzativo, utile a orientare scelte progettuali e

operative. Le evidenze suggeriscono di rendere esplicita l'architettura dei diritti decisionali lungo l'intera Data Value Chain, dalla definizione alla creazione, dall'accesso alla rappresentazione, e di incorporarla negli accordi contrattuali e negli SLA, così da allineare aspettative, tempi e responsabilità. La rappresentazione dell'informazione andrebbe governata tramite cicli brevi di co-progettazione e revisione, con dashboard e report differenziati per profilo d'uso e integrati nei momenti decisionali; al contempo, andrebbero previsti meccanismi di gestione del cambiamento, formazione mirata alla *data literacy* e metriche di adozione che misurino l'effettivo impatto sulle decisioni. Per cogliere i benefici dei dati, le imprese che implementano soluzioni digitali dovrebbero considerare la governance come un processo iterativo. Nei rapporti tra PMI e grandi organizzazioni, l'efficacia deriva dalla chiarezza dei ruoli e da spazi strutturati di coordinamento: comitati di indirizzo congiunti, percorsi di escalation, sandbox per prototipazione rapida e regole trasparenti su proprietà intellettuale e riuso dei componenti favoriscono la personalizzazione senza perdere controllo e tracciabilità. Una governance orientata al contesto, che combina *decision right* formalizzati, pratiche di qualità incorporate nelle routine, co-design delle rappresentazioni e monitoraggio continuo, aumenta la probabilità di trasformare i dati in decisioni tempestive e, quindi, in valore realizzato lungo la Data Value Chain.

Messaggi chiave:

- La governance è co-modellata dai diversi attori e si configura come un processo evolutivo di adattamento reciproco.
- La ricerca identifica tre dimensioni ricorsive e intrecciate (cioè *data practice*, *data insight* e *data value*) che operano iterativamente per integrare culture organizzative e allineare obiettivi condivisi.
- È importante esplicitare i diritti decisionali lungo la Data Value Chain, adottare cicli brevi di co-design e monitoraggio e integrare la governance nei meccanismi contrattuali e nei processi di decision-making.

Bibliografia

Abraham, R., Schneider, J. & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*(July), 424-438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

Alaimo, C., Kallinikos, J. & Valderrama, E. (2020). Platforms as service ecosystems: Lessons from social media. *Journal of Information Technology*, *35*(1), 25-48.

Benfeldt, O. (2020). *Polycentric governance of organizational data ventures: An organizing logic for data governance in the digital era.* Aalborg Universitetsforlag.

Davidson, E., Wessel, L., Winter, J.S. & Winter, S. (2023). Future directions for scholarship on data governance, digital innovation, and grand challenges. *Information and Organization*, *33*(1), 100454. https://doi.org/10.1016/j.infoandorg.2023.100454.

Gelhaar, J., Groß, T. & Otto, B. (2021). A taxonomy for data ecosystems. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 6113-6122. https://doi.org/10.24251/hicss.2021.739.

Gelhaar, J. & Otto, B. (2020). Challenges in the emergence of data ecosystems. *Proceedings of the 24th Pacific Asia Conference on Information Systems*.

Glaser, B. & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research. New Brunswick, NJ: Aldine Transaction. New Brunswick, NJ: Aldine Transaction.* LWW.

Gregory, R.W., Kaganer, E., Henfridsson, O. & Ruch, T.J. (2018). It consumerization and the transformation of it governance. *MIS Quarterly: Management Information Systems*, *42*(4), 1225-1253. https://doi.org/10.25300/MISQ/2018/13703.

Jagals, M. & Karger, E. (2021a). Inter-organisational data governance: A literature review. *ECIS 2021 Research Papers*, (June), 1-19. Retrieved from https://aisel.aisnet.org/ecis2021_rp/57.

Jagals, M. & Karger, E. (2021b). Inter-Organizational Data Governance : A Literature Review. *European Conference on Information Systems (ECIS 2021)*. Retrieved from https://aisel.aisnet.org/ecis2021_rp/57.

Janssen, M., Charalabidis, Y. & Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. *Information Systems Management*, *29*(4), 258-268.

Jarvenpaa, S.L. & Essén, A. (2023). Data sustainability: Data governance in data infrastructures across technological and human generations. *Information and Organization*, *33*(1). https://doi.org/10.1016/j.infoandorg.2023.100449.

Khatri, V. & Brown, C.V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148-152. https://doi.org/10.1145/1629175.1629210.

Lis, D. & Otto, B. (2021). Towards a taxonomy of ecosystem data governance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 6067-6076. https://doi.org/10.24251/hicss.2021.733.

Micheli, M., Ponti, M., Craglia, M. & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data and Society*, *7*(2). https://doi.org/10.1177/2053951720948087.

Monteiro, E. & Parmiggiani, E. (2019). Synthetic knowing: The politics of the internet of things. *ArXiv Preprint ArXiv:1903.00663*.

Myers, M.D. (2019). *Qualitative research in business and management*.

Oliveira, M.I.S., Lóscio, B.F. & Lima, G. de F.B. (2019). *Investigations into Data Ecosystems: a systematic mapping study*. *Knowledge and Information Systems* (Vol. 61). Springer, London. https://doi.org/10.1007/s10115-018-1323-6.

Pan, S.L. & Tan, B. (2011). Demystifying case research: A structured – pragmatic – situational (SPS) approach to conducting case studies. *Information and Organization*, *21*(3), 161-176.

Parmiggiani, E. & Grisot, M. (2020). Data Curation as Governance Practice. *Scandinavian Journal of Information Systems*, *32*(1), 1-38.

Tiwana, A., Konsynski, B. & Venkatraman, N. (2013). Special Issue: Information Technology and Organizational Governance: The IT Governance Cube. *Journal of Management Information Systems*, *30*(3), 7-12. https://doi.org/10.2753/mis0742-1222300301.

van den Broek, E. (2025). Unpacking AI at work: Data work, knowledge work, and values work. *Information and Organization*, *35*(3), 100584. https://doi.org/10.1016/j.infoandorg.2025.100584.

Winter, J.S. & Davidson, E. (2017). *Investigating values in personal health data governance models*.

Costruire ponti digitali: le competenze di *systems integration* nelle pubbliche amministrazioni

Niloofar Kazemargi [*] e Federica Ceci [**]

Abstract: Le scelte relative alle infrastrutture dati incidono in modo determinante sulla generazione di valore, tanto nelle imprese quanto nel settore pubblico. In sistemi complessi che integrano fonti eterogenee, un ruolo centrale è svolto dall'interoperabilità dei dati, intesa come competenza di integrare e far circolare senza soluzione di continuità le informazioni all'interno di infrastrutture distribuite. Nonostante gli ingenti investimenti nella trasformazione digitale, molte amministrazioni locali faticano a garantire tale interoperabilità tra sistemi eterogenei, pur essendo essa la chiave per offrire servizi all'avanguardia ai cittadini. Il presente studio esamina come una pubblica amministrazione possa assicurarla pur avvalendosi di un insieme variegato di fornitori di servizi e infrastrutture. Dall'analisi di un caso qualitativo emergono due tensioni ricorrenti: i vincoli del procurement in un mercato frammentato e "a silos" e il bilanciamento tra sistemi legacy e soluzioni orientate al futuro. I risultati mostrano che l'interoperabilità è una competenza collettiva sostenuta da ruoli distribuiti: la pubblica amministrazione come coordinatore, i regolatori come facilitatori e i fornitori come contributori.

Parole chiave: Infrastrutture digitali, System integration, Data governance, Ecosistemi digitali.

1. Introduzione

La trasformazione digitale sta rimodellando il modo in cui le amministrazioni pubbliche operano, erogano servizi e interagiscono con i cittadini. Oltre la mera adozione di tecnologie, essa implica la riconfigurazione degli assetti istituzionali, dei processi e delle dinamiche inter-organizzative. Al cuore di questa trasformazione

[*] Niloofar Kazemargi (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: niloofar.kazemargi@unich.it

[**] Federica Ceci (✉)
Dipartimento di Economia Aziendale, Università "G. d'Annunzio" Chieti-Pescara, Italia.
E-mail: federica.ceci@unich.it

DOI: 10.82018/9791221165456-11

si collocano le infrastrutture digitali, concepite come sistemi socio-tecnici in evoluzione che abilitano l'integrazione di tecnologie, attori e servizi eterogenei (Henfridsson & Bygstad, 2013; Tilson et al., 2010). La loro efficacia dipende non solo dagli aspetti tecnici, ma anche dalla capacità di supportare l'interoperabilità e la collaborazione oltre i confini organizzativi.

L'interoperabilità, ossia la competenza di sistemi eterogenei di scambiare, interpretare e utilizzare in modo efficace le informazioni (IEEE, 2002), è un abilitatore chiave della creazione di valore nel settore pubblico (Nambisan et al., 2017). Tuttavia, la disponibilità di standard di interoperabilità non conduce automaticamente alla creazione di valore, poiché le organizzazioni devono affrontare diverse "tensioni" sui dati (Kazemargi et al., 2023; Spagnoletti et al., 2025). In particolare, le organizzazioni, incluse le amministrazioni pubbliche, spesso faticano a garantire elevati livelli di interoperabilità a causa di sistemi informativi frammentati, retaggi storici, strutture a silos e piattaforme incompatibili (Hodapp and Hanelt, 2022; Otjacques et al. 2007). Queste barriere minano frequentemente il potenziale della trasformazione digitale. Pur essendo la dimensione tecnica essenziale, l'interoperabilità implica anche allineamento organizzativo (Kadadi et al., 2014; Pagano et al., 2013). In ecosistemi pubblici multilivello, raggiungere tale allineamento richiede governance condivisa, coordinamento istituzionale e sviluppo di competenze nel tempo (Bozkurt et al., 2022; Ceci & Davies, 2024). Considerando l'interoperabilità come un esito, ci basiamo sulle competenze di *system integration*, definite come l'abilità di connettere sistemi, armonizzare i flussi di dati e orchestrare servizi digitali, per sottolinearne l'importanza in questo scenario (Zhao & Xia 2014).

La letteratura esistente ha spesso enfatizzato approcci top-down, focalizzati su strategie nazionali e standardizzazione (Dinçkol et al., 2023; Hodapp and Hanelt 2022), trascurando come tali competenze di *system integration* si sviluppino in pratica a livello locale. Poiché le infrastrutture digitali nel settore pubblico sono sempre più co-prodotte con fornitori privati e altri stakeholder, è necessario esplorare come coordinamento, governance e innovazione evolvano sul campo. Questo studio affronta tale lacuna chiedendosi: come emerge la competenza di *system integration* nelle amministrazioni pubbliche locali che sviluppano infrastrutture digitali? Per rispondere a questa domanda, abbiamo studiato il Comune, un'amministrazione di medie dimensioni dell'Italia centrale con elevata maturità digitale. Il coinvolgimento di Pescara in iniziative digitali nazionali, la collaborazione attiva con fornitori IT privati e la riorganizzazione istituzionale in corso (per fusione con comuni limitrofi) offrono un contesto convincente per osservare come le competenze di *system integration* vengano negoziate e costruite. Questo studio contribuisce alla letteratura su infrastrutture digitali, interoperabilità e innovazione nel settore pubblico facendo emergere ruoli, processi e pratiche tra gli attori per conseguire infrastrutture interoperabili e accrescere la creazione di valore per il pubblico. Invece di trattare la *system integration* come un semplice esito di policy, evidenziamo come essa emerga attraverso coordinamento adattivo, negoziazione situata e agenzia distribuita.

2. Stato dell'arte della letteratura

2.1. Innovazione digitale, interoperabilità e infrastruttura digitale

L'innovazione digitale si riferisce all'"uso della tecnologia digitale durante il processo di innovazione [oppure] in parte o interamente, all'esito dell'innovazione" (Nambisan et al., 2017, 224). Requisito principale per poter utilizzare le tecnologie digitali nei processi innovativi e realizzare i benefici attesi è l'interoperabilità (Hodapp & Hanelt, 2022), definita come la competenza di due o più sistemi di scambiare informazioni e comprendere le informazioni scambiate (IEEE, 2002). Senza interoperabilità i dati restano intrappolati in silos tecnici e organizzativi, con costi di coordinamento elevati, ridondanze, errori di scambio e ritardi decisionali. L'interoperabilità (a livello sintattico, semantico e organizzativo) consente invece di: (i) riusare e comporre servizi e dataset eterogenei; (ii) garantire qualità, tracciabilità e sicurezza dei flussi informativi; (iii) scalare soluzioni su più unità e territori; (iv) evitare lock-in tecnologici e ridurre i costi di integrazione; (v) abilitare analitiche e AI su basi dati affidabili (principi FAIR) e servizi in tempo reale orientati all'utente.

Nelle amministrazioni pubbliche, l'innovazione digitale non è soltanto tecnologica, ma anche profondamente istituzionale e infrastrutturale. La sua efficacia dipende dalla competenza delle infrastrutture digitali di supportare la collaborazione inter-organizzativa, lo scambio informativo senza soluzione di continuità e la scalabilità dei servizi oltre i confini organizzativi e territoriali (Bygstad et al., 2022; Tilson et al., 2010). In questo contesto, l'interoperabilità svolge un ruolo fondativo. Essa comprende dimensioni tecniche e organizzative e consente ad attori eterogenei di interagire e co-creare valore negli ecosistemi digitali (Kadadi et al., 2014; Pagano et al., 2013). Riducendo la frammentazione e favorendo competenza integrative, l'interoperabilità risulta dall'allineamento di standard, processi e logiche istituzionali. aspetto particolarmente cruciale in ambienti altamente regolati come le amministrazioni pubbliche locali (Bozkurt et al., 2022; Ceci & Davies, 2024). Infatti, in ambito pubblico, l'interoperabilità spesso di traduce in processi "end-to-end" tra enti, migliore coordinamento istituzionale e maggiore competenza di generare valore pubblico a parità di risorse, obiettivi difficilmente raggiungibili con standard chiusi o piattaforme non interoperabili.

Perché queste condizioni abilitanti si traducano in risultati concreti e sostenibili, occorre rivolgere l'attenzione all'infrastruttura digitale che le sorregge. Le infrastrutture digitali forniscono l'ossatura socio-tecnica dell'innovazione. Non sono statiche, ma evolvono dinamicamente attraverso interazioni complesse tra tecnologie, standard e routine istituzionali. Hanseth e Lyytinen (2010) descrivono questa condizione come una sfida di complessità dinamica, in cui la soluzione di un problema genera spesso nuove interdipendenze ed effetti inattesi. La loro teoria del design sottolinea la necessità di principi generativi, come modularità, adattabilità ed evoluzione guidata dagli utenti, per gestire la tensione tra flessibilità e controllo. Henfridsson e Bygstad (2013) ampliano tale prospettiva identificando i meccanismi generativi

attraverso cui le infrastrutture digitali evolvono. Mostrano come la crescita infrastrutturale derivi da un'interazione ricorsiva tra progettazione architetturale e agenzia organizzativa, in cui nuovi componenti (ad es., servizi, standard, piattaforme) si stratificano su sistemi esistenti, dando luogo a competenza emergenti e a usi inediti. Questa prospettiva riconcettualizza l'infrastruttura, da fondazione statica a risorsa generativa in continua riconfigurazione.

La crescita infrastrutturale si fonda dunque su tattiche specifiche, quali stratificazione (*layering*), collegamento (*bridging*) e arricchimento (*enrichment*), che devono essere sostenute da componenti interoperabili e da adeguati meccanismi di governance (Koutsikouri et al., 2018). La governance diventa quindi cruciale quando più attori co-sviluppano o co-detengono parti dell'infrastruttura. Studi recenti enfatizzano modelli di governance ibridi e decentrati che bilanciano apertura, coordinamento e controllo (Chen et al., 2022; O'Mahony & Karp, 2020). Ciò è particolarmente rilevante negli ecosistemi del settore pubblico, dove le infrastrutture devono servire una platea eterogenea di stakeholder nel rispetto di vincoli legali e di accountability (Gubser et al., 2023).

2.2. La *System Integration* come lente strategica e operativa

La Systems Integration è riconosciuta come una competenza centrale per le organizzazioni che operano in ambienti complessi e ad alta intensità di dati. Originariamente radicata nell'ingegneria dei sistemi e in grandi progetti militari (Hobday et al. 2005), la *system integration* si è evoluta in una funzione manageriale strategica che consente il coordinamento di sottosistemi tecnologici, organizzativi e umani per fornire soluzioni integrate. Questa evoluzione riflette un più ampio passaggio dal mero coordinamento tecnico all'orchestrazione di processi inter-organizzativi in condizioni di incertezza e complessità (Whyte & Davies 2021). La letteratura contemporanea identifica la *system integration* come una competenza dinamica (Hobday et al., 2005; Teece et al., 1997), essenziale per gestire le crescenti interdipendenze tra architetture modulari, infrastrutture digitali e componenti di servizio (Davies et al., 2007). Le competenze di *system integration* variano da un coordinamento gerarchico stretto ad assetti più adattivi e debolmente accoppiati, a seconda dell'ampiezza del sistema e della novità tecnologica (Madni & Sievers, 2014).

Il ruolo centrale dell'impresa verticalmente integrata si è sfumato, dando luogo a forme organizzative ibride (Davies et al., 2007). Tradizionalmente, i "*systems seller*" verticalmente integrati progettavano, producevano ed erogavano internamente tutti i componenti e i servizi chiave, offrendo soluzioni end-to-end tramite tecnologie e interfacce proprietarie. Tuttavia, poiché la domanda dei clienti si è spostata verso soluzioni più complesse e personalizzate, spesso oltre la portata di una singola impresa, questo modello si è rivelato sempre meno adeguato. In risposta, molte imprese si sono riconfigurate come "*system integrator*", coordinando una rete di partner esterni, fornitori e service provider per assemblare offerte integrate. Eppure, il passaggio da *system seller* a *system integrator* non è stato lineare né assoluto: la maggior parte delle imprese ha sviluppato modelli organizzativi ibridi che combinano

selettivamente competenza interne con componenti in outsourcing, bilanciando controllo e flessibilità. Ad esempio, un'impresa può mantenere il controllo proprietario sull'architettura core del sistema o sulle funzionalità a contatto con il cliente, esternalizzando moduli non core o servizi specialistici. Questa ibridazione riflette non solo scelte strategiche in tema di risorse e competenza, ma anche la crescente modularità e interoperabilità delle tecnologie, che facilitano l'integrazione di elementi eterogenei in sistemi coerenti. Inoltre, i modelli ibridi consentono alle imprese di riconfigurare dinamicamente le reti di valore in risposta all'evoluzione tecnologica, ai cambiamenti regolatori e al feedback dei clienti, caratteristica essenziale in mercati ad alta velocità come telecomunicazioni, aerospazio e servizi IT.

L'emergere di forme organizzative ibride suggerisce che le competenze di *system integration* non sono più confinate alle funzioni ingegneristiche interne, ma risultano incorporate nell'architettura organizzativa, coinvolgendo dimensioni strategiche, operative e relazionali. Per gestire l'integrazione nei sistemi informativi in senso stretto, sono stati sviluppati strumenti concettuali che consentono ad attori funzionali e tecnici di modellare e allineare i requisiti di integrazione tra piattaforme e domini (Purao et al., 2018). Tali modelli risultano sempre più necessari poiché le sfide di integrazione non sono più meramente tecniche, ma riguardano confini di conoscenza, frammentazione della proprietà dei dati e interoperabilità di piattaforma (ad es., SIRE-ML per le semantiche di integrazione; ArchiMate per la struttura a livello *enterprise*; BPMN e UML per la modellazione di processi e interazioni; Capella/ARCADIA per il co-design architetturale).

A livello di progetto, la SI coinvolge dimensioni sia strutturali sia processuali. In grandi iniziative infrastrutturali come Crossrail e CERN, l'integrazione richiede non solo compatibilità tecnica, ma anche governance dell'informazione sugli asset e del cambiamento nel tempo, soprattutto in contesti "big data" (Whyte et al., 2016). Questi progetti mostrano come le pratiche di SI siano influenzate dalle tradizioni del *configuration management*, adattandosi al contempo a ambienti più agili e *data-rich*. Lavori recenti collocano tali sfide entro ecosistemi digitali più ampi, in cui l'integrazione dei dati è centrale per la creazione di valore e il posizionamento competitivo (Ceci & Davies, 2024). In tali ecosistemi, le competenze di *system integration* sostengono l'orchestrazione dei flussi di dati, l'interoperabilità inter-organizzativa e l'abilitazione dell'innovazione. Il passaggio da sistemi standalone a infrastrutture digitali interconnesse amplifica il bisogno di competenza di SI raffinate, in grado di attraversare confini organizzativi e tecnologici.

3. Metodo di ricerca

3.1 Contesto empirico

Per rispondere alla domanda di ricerca abbiamo condotto uno studio di caso qualitativo (Eisenhardt & Graebner, 2007). Il caso scelto è il Comune, un'amministrazione di medie dimensioni situata nell'Italia centrale. Il Comune è stato selezionato

per la sua rilevanza strategica nel panorama italiano della trasformazione digitale: figura con continuità tra le prime dieci città più digitalizzate secondo lo Smart City Ranking italiano e rappresenta un esempio di amministrazione locale attivamente impegnata nell'innovazione digitale. Di recente, il Comune ha ricevuto finanziamenti mirati nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) a sostegno dei processi di modernizzazione e digitalizzazione. Oltre alle iniziative PNRR, è parallelamente coinvolto in altri progetti digitali orientati alle infrastrutture. Questi sviluppi hanno posizionato il Comune come un hub di sperimentazione nella co-progettazione di servizi pubblici digitali.

Una caratteristica distintiva del caso è la forte collaborazione pubblico–privato: la maggior parte dei progetti di sviluppo software è stata esternalizzata, tramite procedure di gara pubblica, a imprese private che forniscono soluzioni digitali sia "on-premises" sia cloud. Ciò ha favorito un'interazione continua e strutturata tra amministrazione locale e attori del settore privato. Inoltre, il Comune opera entro un quadro regolatorio multilivello, che richiede allineamento con gli standard di governance digitale nazionali ed europei, rispondendo al contempo a bisogni e mandati specifici del contesto. Un ulteriore livello di complessità è introdotto dal processo di fusione amministrativa con due Comuni limitrofi, il cui completamento è previsto entro il 2027. Tale processo espanderà significativamente la popolazione, da 130.000 a circa 200.000 abitanti, e ridisegnerà governance e assetto urbano dell'area sotto la nuova identità di "Nuova Pescara". La combinazione di transizione istituzionale, conformità regolatoria e maturità digitale rende questo caso particolarmente adatto a esplorare come infrastrutture digitali e interoperabilità evolvano in contesti dinamici e complessi. Consideriamo pertanto il Comune un caso rappresentativo della complessità socio-tecnica e giuridica riscontrabile in altre amministrazioni locali.

In linea con la pianificazione strategica delineata a livello di macro-aree dal Sindaco, il Comune ha avviato ufficialmente diversi progetti. Queste iniziative sono coerenti con la visione e le priorità dell'amministrazione e mirano a migliorare i processi decisionali, i servizi pubblici e l'innovazione in tutto il territorio comunale. Ogni progetto costituisce una risposta mirata agli obiettivi chiave definiti in fase di pianificazione strategica. Grazie ai finanziamenti nazionali, il Comune ha colto l'opportunità di modernizzare infrastrutture e architetture in modo sicuro e centrato sul cittadino. In linea con la direzione strategica, il Comune ha avviato quattro progetti principali. Il primo è la migrazione al cloud, che prevede la transizione dei sistemi legacy e degli archivi dati verso ambienti cloud sicuri e scalabili, con l'obiettivo di migliorare accessibilità, efficienza e resilienza. Il secondo riguarda l'interoperabilità dei dati a livello nazionale, volta a garantire che i sistemi locali comunichino e condividano informazioni senza soluzione di continuità con le piattaforme nazionali, favorendo servizi pubblici integrati e un'attuazione più coerente delle politiche. Il terzo progetto è il rafforzamento della cybersecurity, finalizzato a proteggere i dati sensibili, assicurare la conformità alle normative sulla protezione dei dati e consolidare la fiducia dei cittadini nei sistemi digitali. Infine, il quarto progetto è dedicato ai servizi digitali centrati sul cittadino, con la progettazione ed erogazione di servizi

intuitivi, accessibili e calibrati sui bisogni reali degli utenti, ponendo particolare attenzione all'esperienza d'uso e all'inclusività.

3.2. Raccolta e analisi dei dati

La ricerca si basa su fonti primarie e secondarie. I dati primari sono stati raccolti tramite interviste semi-strutturate con attori chiave coinvolti nella creazione dell'infrastruttura digitale: informatori del Comune di Pescara con ruoli e responsabilità su digitalizzazione, sistemi informativi, sicurezza, appalti pubblici, nonché informatori del settore privato che forniscono soluzioni digitali alla pubblica amministrazione. La raccolta è avvenuta in due round: il primo con il Comune (gennaio 2023-aprile 2024); il secondo con Comune e principali fornitori di servizi (febbraio 2025-maggio 2025). In totale, abbiamo condotto 38 interviste con dipendenti del Comune di Pescara e dei suoi fornitori. In media, le interviste sono durate 60 minuti. I dati secondari comprendono informazioni tratte da siti web aziendali e comunicati stampa. L'analisi dei dati è iniziata in parallelo alla raccolta. Abbiamo adottato un approccio qualitativo induttivo (Myers, 2019) articolato in tre fasi. Primo, open coding delle interviste per identificare i codici di primo livello, attenendoci al linguaggio degli informatori o a brevi descrizioni strettamente aderenti ai dati (Glaser & Strauss 1967). Secondo, confronto costante dei codici di primo livello per derivare codici di secondo livello, rappresentativi di temi più ampi e delle connessioni sottostanti. Terzo, sviluppo di temi aggregati a partire dai codici di secondo livello.

4. Risultati

4.1. L'emergere delle competenze di *system integration*

Il Comune ha ricevuto mandati e programmi dal Governo italiano, in particolare nell'ambito del PNRR, per la digitalizzazione e l'innovazione nei Comuni. I progetti in corso comprendono undici iniziative PNRR, dalla migrazione al cloud all'implementazione di servizi digitali, attualmente in diverse fasi di avanzamento. Inoltre, il Dipartimento IT gestisce ulteriori interventi di digitalizzazione a supporto delle operazioni di routine dell'ente. Tali progetti presentano aree di sovrapposizione, scambi informativi e, soprattutto, stringenti esigenze di interoperabilità. Per assicurare l'interoperabilità tra iniziative eterogenee è necessaria una competenza specifica, aggiuntiva rispetto a quelle già presenti nell'amministrazione: la competenza di *system integration*, ossia la capacità di attivare sforzi coordinati su dati, strumenti IT e servizi per abilitare l'innovazione digitale. L'emergere di questa competenza si è manifestato lungo due direttrici principali: (i) il procurement in un mercato frammentato in silos e (ii) l'integrazione tra sistemi legacy e soluzioni orientate al futuro.

4.1.1. Procurement in un mercato frammentato in silos

Dalle interviste è emerso che il mercato della pubblica amministrazione in Italia è altamente chiuso e frammentato. Numerosi fornitori IT offrono soluzioni proprietarie, con conseguente bassa interoperabilità. Lo scambio dati raramente è fluido: tra fornitori o sistemi gestionali diversi avveniva tipicamente tramite processi manuali (ad es., file CSV o TXT). La carenza di standardizzazione e automazione lasciava al Comune di Pescara l'onere di esportare e importare i dati, creando un ulteriore carico e imponendo la negoziazione di nuovi accordi contrattuali con i fornitori coinvolti. Inoltre, i processi di approvvigionamento del Comune di Pescara ricadono nelle normative sugli appalti pubblici, che spesso limitano l'affidamento ripetuto agli stessi fornitori. Per promuovere la concorrenza ed evitare monopoli e *lock-in*, il Comune è tenuto a ruotare periodicamente i fornitori. Se i servizi provenienti da un unico fornitore si integrano con facilità, l'acquisizione di servizi digitali da un insieme eterogeneo di supplier (internazionali, nazionali e locali) ha creato sfide quotidiane, sia tecniche sia legali. La rotazione dei fornitori è appropriata quando le applicazioni gestiscono silos informativi isolati; tuttavia, poiché il Comune mirava a un modello più *data-centric*, tali regole hanno reso l'integrazione più difficile. Mantenere l'integrazione durante la rotazione richiede un coordinamento aggiuntivo.

4.1.2. Legacy vs approccio orientato al futuro

L'infrastruttura digitale esistente del Comune di Pescara è intrinsecamente complessa, essendosi sviluppata ed evoluta nel tempo attraverso precedenti procedure di appalto pubblico. Gli informatori hanno sottolineato la necessità di ulteriori sforzi di coordinamento tra i progetti finanziati e i sistemi *legacy*, un compito impegnativo. Nell'acquisire un nuovo servizio IT, il Comune deve considerare l'integrazione sin dalla fase di design fino alla fase di gara. Requisito essenziale è che ogni nuovo servizio fosse interoperabile con i sistemi legacy, i quali contengono dati e routine di valore. Garantire la loro interoperabilità con i nuovi servizi è cruciale per mantenere la continuità operativa. Il Comune segue la pianificazione strategica delineata a livello di macro-area dal Sindaco: gli obiettivi sono definiti e poi declinati in risultati operativi, su cui si concentrano sforzi e investimenti. Per raggiungerli, tuttavia, il Comune può contare solo su progetti approvati e finanziati, limitando la flessibilità nel perseguire obiettivi di lungo periodo. Ne consegue che la *system integration* è essenziale non solo per i sistemi *legacy* ancora operativi in molte pubbliche amministrazioni, ma anche per le soluzioni innovative. Molti nuovi servizi sfruttano infatti intelligenza artificiale, data analytics e piattaforme: i servizi acquisiti devono poter essere integrati, ad esempio tramite API standardizzate.

4.2. Una competenza collettiva di *system integration*

4.2.1. Coordinamento dell'interoperabilità

Per coordinare efficacemente i progetti e garantire l'interoperabilità, il Comune ha dovuto ampliare le proprie competenze. Sono stati reclutati diversi esperti in

sistemi informativi (ad es., data management). Il team di nuova costituzione ha riunito saperi diversificati, tecnici e legali. Il team ha svolto un ruolo cruciale nel coordinare l'allineamento tra sistemi legacy e nuovi servizi digitali. Questo approccio multidisciplinare ha consentito un'elevata interoperabilità, riducendo al contempo i rischi legali e migliorando la conformità ai framework di interoperabilità nazionali ed europei, fondamentali per la sostenibilità di lungo periodo dell'infrastruttura digitale del Comune di Pescara. Il team ha permesso al Comune di Pescara di definire requisiti minimi per i fornitori. Mentre il team era responsabile della definizione ex ante degli Service Level Agreement (SLA), una commissione dedicata, composta da esperti tecnici e legali, ha avuto un ruolo chiave nella selezione del fornitore più idoneo sulla base di criteri di valutazione predefiniti. Oltre alla definizione dei requisiti minimi, un ulteriore strumento efficace nelle mani del Comune di Pescara è stato l'inserimento e l'applicazione di penali legate all'interoperabilità nei contratti. L'esplicitazione e l'enforcement di tali penali hanno favorito maggiore interoperabilità in ecosistemi digitali complessi e la consegna di servizi pubblici efficaci. Inoltre, negli ultimi capitolati di gara il Comune ha imposto esplicitamente a tutti i partecipanti l'uso e la fornitura di *web service* e API, includendo l'integrazione non solo con basi dati nazionali e internazionali ma anche con fornitori terzi, promuovendo così un approccio standardizzato e onnicomprensivo all'interoperabilità tra molteplici stakeholder.

4.2.2. Facilitazione dell'interoperabilità

I dati raccolti evidenziano l'importante ruolo svolto dagli organismi regolatori nel facilitare l'interoperabilità nelle infrastrutture della pubblica amministrazione. Negli ultimi anni, attraverso l'istituzione di framework, linee guida e obblighi, gli organismi nazionali ed europei hanno cercato di sostenere gli enti locali nella creazione di infrastrutture digitali interoperabili. In assenza di tali interventi regolatori, sarebbe ricaduto sul Comune di Pescara l'onere continuo di negoziare termini e condizioni con i fornitori, sfida non banale, soprattutto con provider di grandi dimensioni e internazionali. Un esempio nel contesto italiano è la Piattaforma Digitale Nazionale Dati (PDND), che abilita lo scambio sicuro, standardizzato ed efficiente di dati e servizi tra amministrazioni pubbliche e loro fornitori tecnologici. Anche i bandi PNRR incorporano una prospettiva più ampia: lo sforzo è estendere l'interoperabilità non solo a livello locale, ma all'intera pubblica amministrazione, includendo società *in house* e partner/fornitori terzi. Un altro esempio riguarda la governance dei requisiti di cybersecurity nelle amministrazioni. Il Comune rientra nel campo di applicazione della Direttiva NIS2, che impone standard stringenti di sicurezza e operatività per le infrastrutture pubbliche critiche. La NIS2 incoraggia l'adozione di strumenti e applicazioni open-source, favorendo livelli più elevati di interoperabilità. Di conseguenza, le pubbliche amministrazioni non sono solo responsabili del rispetto dei requisiti di sicurezza internamente, ma sono chiamate a estendere tali obblighi anche ai fornitori tecnologici e ai partner terzi. I partecipanti hanno sottolineato che tali iniziative regolatorie non solo fissano le basi legali e tecniche necessarie, ma promuovono anche una cultura della responsabilità nell'ecosistema digitale pubblico.

4.2.3. Contributo all'interoperabilità

Sebbene le iniziative delle pubbliche amministrazioni e i framework regolatori promuovano sempre più sistemi interoperabili, il Comune ha riscontrato resistenze in fase attuativa da parte di alcuni fornitori. La resistenza non derivava da mancanza di intenzione nell'adottare i principi di interoperabilità o da scarsa comprensione tecnica, ma dalla poca convenienza a collaborare con altri provider per preservare posizioni commerciali e competitive. Altri fornitori, invece, hanno abbracciato volontariamente i principi di interoperabilità. In assenza di obblighi contrattuali, alcuni hanno adottato standard aperti e formati dati noti nelle proprie soluzioni, consentendo livelli più elevati di interoperabilità. Un esempio menzionato da un fornitore è l'uso del General Transit Feed Specification (GTFS), formato open standardizzato per gli orari del trasporto pubblico e le informazioni geografiche associate. Queste pratiche volontarie contribuiscono all'interoperabilità della pubblica amministrazione. Tali fornitori riconoscono i trend di mercato e il quadro regolatorio e, sviluppando soluzioni interoperabili, ottengono vantaggi reputazionali. Questi casi mostrano che, sebbene l'*enforcement* regolatorio resti cruciale, approcci bottom-up da parte dei fornitori possono condurre a livelli più elevati di interoperabilità.

5. Discussione

I risultati mostrano l'importanza della competenza di *system integration* anche per le pubbliche amministrazioni al fine di creare valore pubblico di lungo periodo attraverso le tecnologie digitali. Il bisogno di questa competenza è alimentato da vari fattori tra loro interconnessi. Primo, in un mercato frammentato in cui i fornitori offrono infrastrutture digitali eterogenee, le amministrazioni pubbliche devono garantire l'interoperabilità tra nuovi servizi e sistemi *legacy* sviluppati nel tempo. Non si tratta di un compito semplice, poiché le pubbliche amministrazioni devono conformarsi a policy e cornici regolatorie relative ai processi di procurement pubblico. Tali regole introducono spesso ulteriore complessità mentre si tenta di bilanciare i requisiti tecnici di interoperabilità con principi di equità, trasparenza e concorrenza. Secondo, i risultati evidenziano che l'interoperabilità non riguarda soltanto la gestione delle infrastrutture *legacy*, ancora ampiamente diffuse nelle pubbliche amministrazioni, ma investe la progettazione e la modellazione della futura infrastruttura digitale che deve essere ad alta interoperabilità. Con l'attenzione crescente a digitalizzazione e innovazione nel settore pubblico, nonché con le scelte di allocazione delle risorse e i mandati conseguenti, questa competenza è essenziale per affrontare i problemi di interoperabilità che ostacolano l'innovazione digitale. Essa va oltre le soluzioni meramente tecniche e richiede ulteriori sforzi di coordinamento e assetti collaborativi tra una pluralità di attori.

La prima parte dei risultati spiega perché sta emergendo la competenza di integrazione dei sistemi, ovvero come risposta al procurement in un mercato a silos e

alla tensione tra legacy e soluzioni orientate al futuro. La seconda parte dell'analisi affronta come tale competenza venga sviluppata nella pratica. I risultati mostrano che lo sviluppo di competenze è collettivo, coinvolgendo attori con ruoli distinti di coordinatori, facilitatori e contributori.

Inoltre, identifichiamo competenze specifiche e processi per ciascun attore. Le amministrazioni pubbliche devono acquisire non solo expertise tecniche, ma anche competenze legali e di governance strategica per gestire i vincoli del procurement, negoziare con molteplici fornitori e coordinare progetti complessi multi-attore. Ai fornitori di servizi è richiesto un allineamento crescente ai requisiti di interoperabilità e la conformità a framework regolatori in evoluzione. Per definire linee guida sull'interoperabilità, stabilire regole di gara ed imporre i meccanismi di compliance, gli organismi regolatori necessitano di competenze avanzate e costantemente aggiornate che riflettano sia le opportunità correnti sia le minacce future delle tecnologie digitali. Ciò include non solo conoscenze tecniche (ad es., standard, API, protocolli dati), ma anche una comprensione strategica dell'infrastruttura digitale delle pubbliche amministrazioni e di come l'evoluzione tecnologica possa rimodellare in futuro gli ecosistemi digitali pubblici. Riteniamo che tali risultati siano generalizzabili oltre lo specifico contesto studiato, poiché il panorama tecnologico e i mercati dei servizi per le amministrazioni pubbliche sono in continua evoluzione. Anche se linee guida e framework per l'interoperabilità si aggiornano e si evolvono, la sfida dell'interoperabilità è destinata a persistere a causa del rapido ritmo del cambiamento tecnologico.

6. Conclusioni

La letteratura esistente sull'interoperabilità ha identificato diversi antecedenti dei bassi livelli di interoperabilità (Hodapp & Hanelt, 2022), ma ha dedicato minore attenzione a tali sfide in contesti altamente regolati come le amministrazioni pubbliche. In questi ambienti, le organizzazioni pubbliche devono rispettare stringenti normative sugli appalti e quadri istituzionali che spesso vincolano le scelte tecnologiche e limitano la capacità di integrazione flessibile dei sistemi. Inoltre, molte pubbliche amministrazioni non dispongono delle risorse interne e delle competenze specialistiche necessarie per sviluppare o gestire soluzioni digitali in-house, rendendo gli sforzi di interoperabilità fortemente dipendenti da fornitori esterni. Questo studio contribuisce alla letteratura su *system integration* e interoperabilità, mettendo in luce pratiche, processi e responsabilità attraverso cui l'interoperabilità viene conseguita nelle infrastrutture digitali pubbliche. Mentre la ricerca precedente ha enfatizzato la standardizzazione come abilitatore chiave (Dinçkol et al., 2023; Hodapp & Hanelt, 2022), i nostri risultati, adottando una prospettiva di *system integration* (Davies et al., 2007; Hobday et al., 2005; Prencipe et al., 2003; Whyte & Davies, 2021), rivelano che raggiungere l'interoperabilità va ben oltre l'adozione formale di standard tecnici (Spagnoletti et al., 2025). Sono necessari sforzi di coordinamento nelle

negoziazioni contrattuali, nelle pratiche di procurement, negli strumenti di enforcement della conformità e, in alcuni casi, clausole penali per indurre l'interoperabilità tra i fornitori tecnologici. Evidenziamo anche la natura intrinsecamente multidisciplinare di tali processi, che richiedono competenze legali, tecniche e manageriali distribuite tra attori pubblici e privati, a riprova della difficoltà nel conseguire l'interoperabilità (Ceci & Davies, 2024; Madni & Sievers, 2014). Inoltre, mostriamo che l'interoperabilità è un fenomeno a livello di ecosistema (Hodapp & Hanelt, 2022), plasmato da ruoli e responsabilità distribuite tra molteplici stakeholder. In tal senso, le amministrazioni pubbliche non sono consumatori passivi, ma svolgono un ruolo di coordinamento definendo requisiti e imponendo obblighi di integrazione. Contestualmente, alcuni fornitori mostrano un impegno proattivo e volontario adottando standard aperti, API e architetture interoperabili.

In sintesi, questo studio estende il dibattito sull'interoperabilità mostrando come essa possa essere conseguita come esito delle competenze di *system integration* in contesti regolati, e rivelando l'intreccio di pratiche contrattuali, tecniche e organizzative che abilitano l'integrazione in infrastrutture digitali frammentate. Queste intuizioni restano rilevanti mentre i framework regolatori e i paesaggi tecnologici continuano a evolvere, dato il persistente bisogno di strategie di interoperabilità a livello di sistema nella trasformazione digitale del settore pubblico.

Messaggi chiave:

- L'interoperabilità nelle infrastrutture digitali pubbliche non deriva solo dall'adozione formale di standard tecnici, ma da pratiche complesse di integrazione sistemica.
- Raggiungere l'interoperabilità richiede competenze legali, tecniche e manageriali. Le PA assumono un ruolo attivo.
- L'interoperabilità efficace abilita nuove forme di creazione di valore pubblico.

Bibliografia

Bozkurt, Y., Rossmann, A. & Pervez, Z. (2022). A Literature Review of Data Governance and Its Applicability to Smart Cities. *Proceedings of the Annual Hawaii International Conference on System Sciences* (2022-Janua), 2680-2689. doi: https://doi.org/10.24251/hicss.2022.333.

Bygstad, B., Iden, J. & Øvrelid, E. (2022). The Emergence of a National Collaborative Digital Ecosystem. A Study of One-Citizen-One-Health-Record in Norway. In *Norsk IKT-Konferanse for Forskning Og Utdanning*.

Ceci, F. & Davies, A. (2024). A Systems Integration View on Data Ecosystems. In *Digital (Eco) Systems and Societal Challenges: New Scenarios for Organizing*, Springer, 375-389.

Chen, L., Tong, T.W., Tang, S. & Han, N. (2022). Governance and Design of Digital Platforms: A Review and Future Research Directions on a Meta-Organization. *Journal of Management* (Vol. 48). (https://doi.org/10.1177/01492063211045023).

Davies, A., Brady, T. & Hobday, M. (2007). Organizing for Solutions: Systems Seller vs. Systems Integrator. *Industrial Marketing Management* (36:2), Elsevier, 183-193.

Dinçkol, D., Ozcan, P. & Zachariadis, M. (2023). Regulatory Standards and Consequences for Industry Architecture: The Case of UK Open Banking. *Research Policy* (52:6), Elsevier B.V., 104760. (https://doi.org/10.1016/j.respol.2023.104760).

Eisenhardt, K.M., and Graebner, M.E. (2007). Theory Building From Cases: Opportunities and Challenges. *Academy of Management Journal* (50:1), (A.M. Huberman and M.B. Miles, eds.), Academy of Management, 25-32. (https://doi.org/10.1002/job.).

Glaser, B., and Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New Brunswick, NJ: Aldine Transaction. New Brunswick, NJ: Aldine Transaction., LWW.

Gubser, R., Schulte-Althoff, M., Heinemann, N., Pohle, J. & Fürstenau, D. (2023). Data Governance Strategies for Data Platforms – A Multiple Case Study in Nursing Care. *ECIS 2023: European Conference on Information Systems*. (https://aisel.aisnet.org/ecis 2023_rip/50).

Hanseth, O. & Lyytinen, K. (2010). Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet. *Journal of Information Technology* (25:1), Springer, 1-19. (https://doi.org/10.1057/jit.2009.19).

Henfridsson, O. & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. *MIS Quarterly* (37:3), 907-931.

Hobday, M., Davies, A. & Prencipe, A. (2005). Systems Integration: A Core Capability of the Modern Corporation. *Industrial and Corporate Change* (14:6), Oxford University Press, 1109-1143.

Hodapp, D. & Hanelt, A. (2022). Interoperability in the Era of Digital Innovation: An Information Systems Research Agenda. *Journal of Information Technology* (0:0), 1-21. (https://doi.org/10.1177/02683962211064304).

IEEE (2002). *Terminology of Software Engineering*, Standard Glossary of Software Engineering Terminology. Piscataway, NJ: IEEE; 2002.

Kadadi, A., Agrawal, R., Nyamful, C. & Atiq, R. (2014). Challenges of Data Integration and Interoperability in Big Data. *2014 IEEE International Conference on Big Data (Big Data)*, IEEE, 38-40.

Kazemargi, N., Spagnoletti, P., Constantinides, P. & Prencipe, P. (2023). Data Control Coordination in Cloud-Based Ecosystems. In C. Cennamo, G.B. Dagnino & F. Zhu (Eds.), *Handbook of Research on Digital Strategy*. Edward Elgar.

Koutsikouri, D., Lindgren, R., Henfridsson, O. & Rudmark, D. (2018). Extending Digital Infrastructures: A Typology of Growth Tactic. *Journal of Association for Information Systems* (19:10), Association for Information Systems, 1001-1019.

Madni, A.M. & Sievers, M. (2014). Systems Integration: Key Perspectives, Experiences, and Callenges. *Systems Engineering* (17:1), Wiley Online Library, 37-51.

Myers, M.D. 2019. *Qualitative Research in Business and Management*, SAGE publications Ltd.

Nambisan, S., Lyytinen, K., Majchrzak, A. & Song, M. (2017). Digital Innovation Management : Reinventing Innovation Management Research in a Digital World. *MIS Quarterly* (41:1), 223-238. (https://doi.org/10.25300/MISQ/2017/41).

O'Mahony, S., and Karp, R. (2020). From Proprietary to Collective Governance: How Platform Participant Strategies Adapt. *Strategic Management Journal*, 1-33. (https://onlinelibrary.wiley.com/doi/abs/10.1002/smj.3150).

Otjacques, B., Hitzelberger, P. & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems* (23:4), 29-51. (https://doi.org/10.2753/MIS0742-1222230403).

Pagano, P., Candela, L. & Castelli, D. (2013). Data Interoperability. *Data Science Journal* (12), CODATA, GRDI19-GRDI25.

Prencipe, A., Davies, A. & Hobday, M. (2003). *The Business of Systems Integration*, OUP Oxford.

Purao, S., Bolloju, N. & Tan, C.-H. (2018). A Modeling Language for Conceptual Design of Systems Integration Solutions. *ACM Transactions on Management Information Systems (TMIS)* (9:2), ACM New York, NY, USA, 1-25.

Spagnoletti, P., Kazemargi, N., Constantinides, P. & Prencipe, A. (2025). Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors. *Journal of the Association for Information Systems*, 26, 1-33.

Teece, D. J., Pisano, G. & Shuen, A. (1997). Dynamic Capabilities and Strategic Management. *Strategic Management Journal* (18:7), Wiley Online Library, 509-533.

Tilson, D., Lyytinen, K. & Sørensen, C. (2010). Digital Infrastructures: The Missing IS Research Agenda. Research Commentary. *Information Systems Research* (21:4), 748-759.

Whyte, J. & Davies, A. (2021). Reframing Systems Integration: A Process Perspective on Projects. *Project Management Journal* (52:3), SAGE Publications Sage CA: Los Angeles, CA, 237-249.

Whyte, J., Stasis, A. & Lindkvist, C. (2016). Managing Change in the Delivery of Complex Projects: Configuration Management, Asset Information and 'Big Data. *International Journal of Project Management* (34:2), Elsevier, 339-351.

Zhao, K. & Xia, M. (2014). Forming Interoperability through Interorganizational Systems Standards. *Journal of Management Information Systems* (30:4), 269-298. (https://doi.org/10.2753/MIS0742-1222300410).

Finito di stampare nel mese di gennaio 2026
nella Stampatre s.r.l. di Torino
Via Bologna, 220