RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0273 • articolo sottoposto a peer review • pubblicato in anteprima il 11 mag. 2026

Elisa Sorrentino – Anna Federica Spagnuolo

Cybersecurity e sovranità digitale: un modello normativo integrato

La trasformazione digitale ha riconfigurato il cyberspazio da infrastruttura tecnica a dominio funzionale dell'esercizio dei poteri pubblici e della tutela dell'interesse generale. La cybersecurity costituisce il presupposto operativo dell'ordinamento digitale e l'unico ambito dotato di una disciplina vincolante, su cui può svilupparsi una governance della sovranità digitale, ancora priva di tipizzazione giuridica e affidata a strumenti di soft law. Il lavoro analizza le principali fonti nazionali ed europee in materia di cybersicurezza e propone un modello regolatorio integrato che, attraverso parole chiave strategiche, traduce la sovranità digitale in principio giuridico operativo, intrecciando protezione delle infrastrutture con la tutela dei diritti fondamentali e il governo dell'ecosistema digitale, nell'ottica di un quadro normativo armonizzato, resiliente e multilivello.

Cybersecurity – Sovranità Digitale – Governance integrata – Diritti fondamentali

Cybersecurity and digital sovereignty: An integrated regulatory model

The digital transformation has reconfigured cyberspace from a technical infrastructure into a functional domain of the exercise of public powers and the protection of the general interest. Cybersecurity constitutes the operational premise of the digital legal order and the only domain endowed with a binding regulatory discipline, upon which a broader governance of digital sovereignty can be built, a concept still lacking legal typification and largely entrusted to soft law instruments. The paper analyzes the main national and European sources on cybersecurity and proposes an integrated regulatory model that, through strategic keywords, translates digital sovereignty into an operative legal principle, intertwining the protection of infrastructures with the safeguarding of fundamental rights and the governance of the digital ecosystem, with the objective of building a harmonized, resilient and multilevel legal framework.

Cybersecurity – Digital sovereignty – Integrated governance – Fundamental rights

A.F. Spagnuolo è tecnologo, E. Sorrentino è CTER presso l'Istituto di Informatica e Telematica del CNR, Sede di Cosenza

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambe le Autrici ed è stato parzialmente realizzato nell'ambito delle attività del progetto "SEcurity and RIghts in the CyberSpace – SERICS (PE00000014)" – Piano Nazionale di Ripresa e Resilienza MUR finanziato dall'Unione Europea – NextGenerationEU, CUP B53C22003950001

1. Introduzione

La progressiva digitalizzazione delle strutture economiche, amministrative e sociali ha profondamente riconfigurato gli equilibri istituzionali e giuridici, trasformando il cyberspazio da semplice infrastruttura tecnica a luogo strategico per l'esercizio del potere sovrano. In questo scenario, i concetti di cybersecurity[1] e sovranità digitale[2], sebbene distinti sotto il profilo definitorio, assumono un ruolo centrale, configurandosi come chiavi interpretative dell'intersezione tra tecnologia e diritto nell'ecosistema digitale. L'attuale eterogeneità del quadro normativo, a livello tanto sovranazionale quanto statuale, introduce significative discontinuità nella governance cibernetica, incidendo sul coordinamento e sull'effettività delle strategie di protezione delle infrastrutture e delle risorse digitali[3]. In questo contesto frammentato si colloca il nodo teorico centrale: la mancanza di un impianto ermeneutico adeguatamente strutturato, capace di sistematizzare in modo coerente le molteplici e crescenti articolazioni della sovranità digitale. Il presente lavoro si colloca in tale vuoto normativo e concettuale, proponendo un avanzamento metodologico che, attraverso un modello olistico, mira a ricondurre principi, funzioni e strumenti entro un'unica architettura teorica coerente.

Le fasi di mappatura e di classificazione integrata delle fonti costituiscono il presupposto metodologico di quello che definiremo modello normativo integrato, finalizzato a supportare un'organizzazione coerente dei documenti giuridico-politici più rilevanti. Questo processo analitico permette di identificare parole chiave strategiche, che agiscono come strumenti concettuali capaci di tradurre in termini concreti e operativi il concetto di sovranità digitale, fornendo una chiave interpretativa sistemica di fronte alle sfide emergenti. L'approccio proposto rappresenta l'originalità metodologica del contributo, integrando la semantica normativa nell'ordinamento digitale e delineando una visione multidimensionale della sovranità digitale, la cui articolazione dettagliata è sviluppata nei paragrafi che seguono.

2. Oltre la cybersecurity: verso una governance digitale multilivello per la sovranità digitale europea

Nell'attuale panorama digitale, la cybersecurity rappresenta un fondamento operativo imprescindibile per la protezione delle infrastrutture critiche e dei dati, costituendo il primo baluardo contro

1. Per un'analisi del concetto di cybersecurity, Taddeo 2019; Ziccardi 2019; Brighi–Chiara 2021; National Cyber Security Centre 2024.
2. Per una panoramica della letteratura in tema di sovranità digitale si rinvia all'analisi di Hummel–Braun–Tretter–Dabrock 2021. Gli autori passano in rassegna oltre seicento articoli in materia e identificano sei differenti nozioni di sovranità. Si veda ancora Hellmeier–von Scherenberg 2023. Sulla polisemia dell'espressione *sovranità digitale* si veda, inoltre, Moerel–Timmers 2021. Sul punto Bin 2013. Si veda ancora Simoncini 2017.
3. Roberts–Cowls–Casolari et al. 2021.

minacce informatiche e vulnerabilità sistemiche[4]. L'evoluzione della società digitale, tuttavia, impone l'adozione di un approccio proattivo che superi una logica meramente difensiva, affermando il principio di sovranità digitale[5], inteso come la capacità condivisa degli Stati e delle istituzioni europee di governare i propri dati, le infrastrutture e le regole dell'ecosistema digitale, promuovendo al contempo forme di maggiore tutela e coordinamento con gli attori privati e sovranazionali. La sovranità digitale, tuttavia, si configura ancora come una costruzione politica in divenire, priva di una cornice giuridica condivisa e vincolante a livello europeo. È proprio questa ambiguità[6] a renderne urgente una profonda riconfigurazione teorica e normativa, capace di ancorarla ai valori fondamentali dell'Unione europea per generare un ecosistema digitale resiliente, democratico e orientato al bene comune[7]. Il passaggio dalla cybersecurity alla sovranità digitale non si configura come un mero ampliamento di ambiti materiali, ma come una trasformazione qualitativa del modo stesso di concepire l'intervento pubblico nello spazio digitale: da funzione prevalentemente reattiva a governance strutturale, multilivello e strategica del cyberspazio[8]. Tale evoluzione impone una revisione dei presupposti teorici tradizionali, non più adeguati a descrivere l'interdipendenza tra infrastrutture, dati, potere regolatorio e diritti fondamentali[9] nello spazio digitale[10]. Lungi dal sostituirsi alla cybersecurity, la sovranità digitale ne integra e amplia i presupposti, delineando una visione del digitale in cui la protezione dei sistemi si intreccia con la valorizzazione dei principi e delle libertà costituzionali[11]. Del resto, in un contesto geopolitico profondamente mutato, caratterizzato da tensioni globali, interdipendenze tecnologiche e competizione per il controllo dei dati e delle infrastrutture strategiche, la capacità degli Stati e delle istituzioni europee di esercitare una politica digitale efficace assume una rilevanza cruciale, non solo ai fini della tutela della sicurezza nazionale e della resilienza economica[12], ma anche quale elemento per preservare l'autonomia

4. Si veda Guarda 2008; Faini 2018; Brighi–Chiara 2021; Di Corinto 2022; Ponti 2024; Resta 2024.
5. Si veda Cardone 2025.
6. Palladino 2023. L'esigenza di definire in modo preciso ed entro parametri normativi ben delineati il concetto di sovranità digitale nasce proprio dall'ambiguità che questo termine porta con sé e dalle conseguenze che genera. Infatti, come evidenzia Palladino la nozione di sovranità nel cyberspazio si presenta intrinsecamente ambivalente: da un lato, si rifà alla tradizionale sovranità territoriale, che attribuisce agli Stati controllo esclusivo su infrastrutture e dati all'interno dei confini nazionali; dall'altro lato, emerge una concezione post-territoriale che sposta il quadro verso autonomia e potere di governo sui flussi digitali indipendentemente dal territorio fisico. Questa doppia interpretazione determina tensioni normative e geopolitiche, sovrapposizioni e conflitti di giurisdizione, confermando quanto sia necessario stabilire definizioni chiare e condivise per evitare derive e ambiguità nel governo del cyberspazio.
7. Rodotà 2021.
8. Si veda Santaniello 2022, che evidenzia come la sovranità digitale sia una risposta strategica alle sfide poste dalla globalizzazione delle tecnologie e dalla necessità di tutelare i diritti digitali fondamentali. Si veda ancora Sorrentino–Spagnuolo 2024, che sottolineano la necessità di implementare misure legislative che garantiscano la sicurezza delle infrastrutture e dei dati, nel pieno rispetto dei diritti fondamentali, evidenziando la sovranità digitale come nuova frontiera della governance statale sulle risorse critiche digitali. Si veda ancora De Rosa 2021; Gatti 2019.
9. Mangiameli 2023; Custers 2022.
10. Longo 2023.
11. Spiniello 2025, che esamina come il costituzionalismo digitale, inteso come radicamento dei diritti e principi costituzionali nel contesto digitale, starebbe evolvendo insieme all'idea di sovranità digitale nell'Ue e negli ordinamenti nazionali.
12. In questo scenario, la regolazione della datasfera, intesa come lo spazio digitale dove si generano, transitano e si accumulano dati, diventa "una delle nuove frontiere del potere statale, che si esercita su una dimensione immateriale ma non per questo meno strategica". Si veda Zeno-Zencovich 2018.

strategica in un mondo sempre più interconnesso. La crescente dipendenza da soluzioni tecnologiche sovranazionali aumenta l'esposizione di governi, imprese e cittadini a rischi rilevanti, tra cui violazioni dei dati personali, attacchi a settori critici (energia, trasporti, sanità), squilibri informativi e concentrazioni monopolistiche[13]. Un governo responsabile e consapevole dell'ecosistema digitale richiede, dunque, l'elaborazione di un quadro teorico integrato, ancora mancante, e la definizione di un modello normativo organico, in grado di armonizzare norme e regole tecniche e di dare piena attuazione al principio di sovranità digitale. Nonostante il progressivo rafforzamento del quadro regolatorio europeo e nazionale, permane difatti un divario significativo. Mentre la cybersecurity dispone ormai di un impianto normativo rafforzato, la sovranità digitale resta ancora affidata prevalentemente a strumenti di soft law[14], linee guida e dichiarazioni politiche non vincolanti[15] che riflettono la complessità e la mutevolezza delle trasformazioni in atto[16]. Questa asimmetria non costituisce un mero squilibrio tecnico, ma segnala l'assenza di una grammatica normativa comune, capace di integrare le diverse dimensioni dell'ordinamento digitale segnato tuttora da una serie di interventi settoriali e privi di un disegno unitario[17] capace di assicurarne la coerenza complessiva (a

13. In altri termini la protezione dei dati personali assume ormai una dimensione transnazionale, nella quale "gli ordinamenti nazionali appaiono spesso inadeguati a fronteggiare le sfide poste dalla globalizzazione digitale". Si veda Resta–Zeno-Zencovich 2016.

14. I principali riferimenti sono: Commissione europea, *Analisi comparativa dei progressi dell'iniziativa eEurope 2002*, 5 febbraio 2002, doc. COM (2002) 62; Comitato delle Regioni, *Parere sulla Comunicazione della Commissione – Sicurezza delle reti e sicurezza dell'informazione: Proposta di un approccio strategico europeo*, 3 maggio 2002; Commissione europea, *Comunicazione sulla strategia dell'UE per l'Unione della sicurezza*, 24 luglio 2020, doc. COM (2020) 605; Consiglio dell'Unione europea, *Conclusioni del Consiglio – Plasmare il futuro digitale dell'Europa*, 9 giugno 2020; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, 2 dicembre 2020; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale*, 22 marzo 2021; Consiglio dell'Unione europea, *Conclusioni del Consiglio – Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio*, 8 ottobre 2021; Commissione europea, Alto Rappresentante dell'Unione, *Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale*, 2021, doc. JOIN (2021) 14; Parlamento europeo, *Risoluzione sulla strategia UE per la cibersicurezza*, 10 giugno 2021, doc. 2020/2667(RSP); Consiglio dell'Unione europea, *Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica*, 23 maggio 2022; Consiglio dell'Unione europea, *Conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride*, 2022; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla sicurezza delle catene di approvvigionamento delle TIC*, 17 ottobre 2022; Commissione europea, *European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers*, 15 gennaio 2024.

15. Tra i documenti non vincolanti vi sono: Von der Leyen U., *Discorso sullo stato dell'Unione,* Parlamento europeo, Strasburgo, 16 settembre 2020, doc. SPEECH/20/1655; Ministri UE e EFTA, *Tallinn Declaration on eGovernment*, Conferenza ministeriale sull'eGovernment, Tallinn, 6 ottobre 2017; Merkel A., *Speech at the Annual Meeting of the World Economic Forum*, Davos, 23 gennaio 2020; Macron E., intervento a VivaTech, Parigi, 16-19 giugno 2021. Il discorso di Von der Leyen (2020), pur rilevante per aver posto in primo piano l'autonomia tecnologica dell'Unione europea e la necessità di una maggiore sovranità digitale rispetto agli Stati Uniti e alla Cina, non ha la forza di un atto normativo. Allo stesso modo, anche la Dichiarazione di Tallinn (2017), pur sottolineando l'importanza della sicurezza cibernetica e dell'autonomia digitale, non crea obblighi legali per gli Stati membri.

16. Lo sviluppo tecnologico delle società contemporanee ha avuto un notevole impatto sulle figure giuridiche tradizionali e sulla identificazione di nuovi diritti. Si veda a tal proposito Faralli 2018.

17. Le principali normative sovranazionali sull'argomento includono: Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA); Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e

titolo esemplificativo: tutela dei dati personali, identità digitale[18], mercato unico[19], sicurezza informatica[20] e contrasto al cybercrime[21]). Sebbene la competenza sovrana sulle infrastrutture e

che abroga il regolamento (CE) n. 460/2004; Accordo interistituzionale tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea per l'istituzione di una squadra di pronto intervento informatico (CERT-UE) permanente, 2018; Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

18. Le principali normative sovranazionali sull'argomento includono: Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS); Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR); Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati; Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio, del 14 luglio 2021, relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE ai fini della lotta contro gli abusi sessuali online sui minori; Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati (Data Governance Act); Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act); EDPB, *Guidelines 9/2022 on personal data breach notification under GDPR*, Version 2.0, adottate il 28 marzo 2023; Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act).
19. Le principali normative sovranazionali sull'argomento includono: Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni; Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (ePrivacy); Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche; Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale (Digital Markets Act – DMA); Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali (Digital Services Act – DSA).
20. Le principali normative sovranazionali sull'argomento includono: Commissione europea, Alto Rappresentante dell'Unione, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, 7 febbraio 2013, doc. JOIN (2013) 1, Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS1); Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (Cybersecurity Act); Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2); Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (DORA); Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio; Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, recante misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione; Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (Cyber Resilience Act).
21. Le principali normative sovranazionali sull'argomento includono: Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce

sulla sicurezza[22] resti formalmente attribuita agli Stati membri, l'Unione europea esercita un ruolo di coordinamento strategico che ne rivela l'intrinseca ambivalenza, non una mera armonizzazione tecnica ma autentica riconfigurazione del locus del potere sovrano nello spazio digitale. Iniziative come la *Bussola Digitale 2030*[23] tracciano un orizzonte normativo volto alla costruzione di un ecosistema digitale resiliente, etico e competitivo, ma la loro efficacia rimane sospesa, perché la sovranità digitale europea esige non soltanto resilienza tecnica, ma anche una cooperazione fondata su fiducia ontologica tra gli Stati, interoperabilità strutturale e una governance partecipativa, capace di incarnare principi fondamentali in pratiche operative evitando che essi si riducano a mera retorica istituzionale. Sul piano nazionale, questa dinamica genera una frattura concettuale profonda, poiché la tensione tra sovranità statale e imperativi europei non si limita a produrre frammentazione normativa, ma mette in luce la crisi ontologica del paradigma giuridico tradizionale, ormai incapace di integrare coerentemente la *datasfera* con valori costituzionali e diritti fondamentali[24]. La digitalizzazione, infatti, erode la storica territorialità della sovranità, rivelando l'insufficienza dei modelli statocentrici di fronte a flussi transnazionali di dati e infrastrutture interconnesse[25]. Anche il nostro Paese, pur avendo adottato norme strategiche[26], recepito normative europee[27] e disposizioni

la decisione quadro 2005/222/GAI del Consiglio; Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi; Direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio; Consiglio europeo, *Conclusioni del Consiglio europeo sulla rete giudiziaria europea per la criminalità informatica*, 2016; Consiglio europeo, *Conclusioni del Consiglio europeo sulle attività informatiche dolose*, 2018; Consiglio dell'Unione europea, *Quadro strategico dell'UE in materia di ciberdifesa*, aggiornamento 2018.

22. Parlamento europeo, *Lo Stato di diritto nell'ordinamento giuridico dell'Unione europea*, EPRS/Servizio Ricerca del Parlamento europeo, PE 745.685, luglio 2023. Questo studio è parte di un progetto più ampio di diritto comparato. Analizza il principio dello Stato di diritto come valore fondamentale dell'Unione europea, sancito nel Trattato sull'Unione Europea (TUE) e declinato in numerose fonti normative vincolanti e non vincolanti. Il documento illustra i meccanismi preventivi e repressivi volti a garantire il rispetto dello Stato di diritto da parte degli Stati membri, inclusa la procedura prevista dall'articolo 7 TUE in caso di violazioni gravi. Viene inoltre evidenziata la complessità semantica della nozione di Stato di diritto e le prospettive di sviluppo legate a una sua interpretazione evolutiva. Lo studio sottolinea come il rispetto dello Stato di diritto sia intrinsecamente connesso alla democrazia e ai diritti fondamentali, garantendo che tutti i poteri pubblici operino entro i limiti della legge, sotto il controllo di organi giurisdizionali indipendenti e imparziali. Inoltre, la relazione annuale della Commissione europea sullo Stato di diritto (2023) fornisce una valutazione aggiornata della situazione nei singoli Stati membri, evidenziando le sfide e le misure adottate per assicurare il rispetto del principio nei diversi ordinamenti nazionali (Commissione europea, *Relazione annuale sullo Stato di diritto 2023*, Bruxelles, 5 luglio 2023, doc. SWD (2023) 812). Per approfondimenti si veda Crespi 2024.
23. Commissione europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, Bruxelles, 9 marzo 2021, doc. COM (2021) 118.
24. Si veda Catanzariti 2024; De Gregorio–Radu 2022.
25. Pierucci 2025; Chander–Sun 2023.
26. In Italia, le principali norme di indirizzo strategico includono: Presidenza del Consiglio dei Ministri, D.P.C.M. 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*; mPresidenza del Consiglio dei Ministri, D.P.C.M. 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*.
27. Le principali norme italiane di recepimento direttive e regolamenti europei: Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; Decreto

trasversali[28], definito assetti organizzativi e istituzionali[29], resta intrappolato in una frammentazione strutturale che rivela l'insufficienza esistenziale degli approcci settoriali e la mancanza di un coordinamento efficace sin dalla fase progettuale.

3. Mappatura e classificazione delle fonti giuridiche e strategiche della cybersicurezza e della sovranità digitale

Alla luce delle criticità concettuali e normative fin qui analizzate, si è ipotizzata la costruzione di un modello normativo integrato per la gestione regolatoria della sicurezza cibernetica e della sovranità digitale. Tale modello funge da strumento operativo capace di tradurre la sovranità digitale da mera nozione teorica a principio giuridico pienamente efficace. La sua definizione presuppone una cornice metodologica rigorosa, volta a garantire coerenza concettuale, concretezza normativa e replicabilità analitica, superando le discontinuità generate dalla frammentazione regolatoria vigente. Il percorso metodologico si sviluppa in due momenti sequenziali e complementari: una prima fase di mappatura sistemica delle fonti normative e strategiche, seguita da una fase di classificazione interpretativa. La trasparenza e la chiarezza dei criteri organizzativi assicurano la replicabilità del metodo e ne consolidano il valore come strumento per l'elaborazione di soluzioni regolatorie innovative. La selezione delle fonti ha privilegiato atti dotati di efficacia giuridica vincolante o di comprovata rilevanza strategica per la definizione delle politiche digitali a livello europeo e nazionale, delineando un corpus analitico coerente. Documenti settoriali o atti tecnici di peso normativo limitato sono stati esclusi, al fine di concentrare l'analisi su strumenti capaci di orientare concretamente le scelte regolatorie e di costituire un fondamento solido per il modello stesso. L'approccio metodologico è dinamico e multilivello, in grado di integrare prospettive differenti e di far emergere interdipendenze, priorità strategiche e relazioni tra norme e principi. In questo quadro, la mappatura svolge la funzione di fondamento analitico, fornendo le basi per l'elaborazione di modelli giuridici coerenti, integrati e resilienti, in grado di tradurre concetti complessi in strumenti operativi concretamente applicabili. La successiva fase di classificazione interpretativa si muove lungo due binari complementari. Il primo raggruppa tre categorie tematiche: rischio, minacce e attori coinvolti, al fine di cogliere la logica sostanziale sottesa alle norme. Il secondo si fonda sul rango giuridico e sulla natura delle fonti, graduando

legislativo 8 novembre 2021, n. 207, Norme di attuazione del regolamento (UE) 2019/881 relativo all'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (Cybersecurity Act); Decreto legislativo 4 settembre 2024, n. 134, Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, in GU Serie Generale n. 223 del 23 settembre 2024; Decreto legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

28. In Italia, le principali norme complementari e trasversali sono: Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo 10 agosto 2018, n. 101; Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (CAD); Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici; AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026*, Roma, 2024; AGID, *Linee guida per l'adozione di intelligenza artificiale nella pubblica amministrazione,* Versione 1.0, 14 febbraio 2025 (in consultazione).
29. Le principali norme organizzative e istitutive italiane sono: Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (PSNC); Legge 18 novembre 2019, n. 133, Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica; Presidenza del Consiglio dei Ministri, D.P.C.M. 30 luglio 2020, n. 131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105; Decreto-legge 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

l'influenza delle diverse disposizioni e consentendo di ricostruire gerarchie, interazioni e relazioni di forza tra strumenti normativi. Nel dettaglio, il procedimento di mappatura e analisi si è concretizzato in tre passaggi distinti: (1) identificazione e selezione delle fonti pertinenti; (2) estrazione delle componenti semantiche rilevanti; (3) aggregazione delle ricorrenze all'interno di una tassonomia tematico giuridica. Pur caratterizzato da sistematicità e rigorosità, il metodo riconosce un limite intrinseco nella continua evoluzione del quadro regolatorio e strategico che mantiene inevitabilmente aperto il perimetro delle fonti, richiedendo aggiornamenti e interpretazioni costanti.

Sulla base della classificazione interpretativa, il corpus delle fonti è stato organizzato secondo una partizione funzionale che distingue due ambiti principali: da un lato, le fonti relative alla cybersicurezza, focalizzate sulla protezione di dati, sistemi e infrastrutture critiche; dall'altro, le fonti pertinenti alla sovranità digitale, orientate all'autonomia strategica e al controllo delle tecnologie e dei flussi informativi. Questa distinzione non mira a separare rigidamente le due dimensioni, ma a facilitare l'analisi delle interdipendenze tra sicurezza e governance digitale, evidenziando come scelte normative apparentemente settoriali contribuiscano a costruire un quadro unitario di sovranità digitale e resilienza cibernetica. La classificazione interpretativa, articolata lungo i due assi analitici precedentemente delineati, consente di scomporre la complessità del sistema regolatorio in componenti strutturate e interconnesse, offrendo una visione sistemica anche in contesti ad alta densità normativa[30]. In questo quadro, le tre categorie tematiche – rischio[31], minaccia[32] e attori[33] – assumono il ruolo di chiavi interpretative trasversali, capaci di collegare la dimensione tecnica a quella normativa e di trasformare concetti astratti in criteri analitici. In particolare, la categoria del rischio assume un ruolo centrale, identificando vulnerabilità[34] e orientando interventi

30. Sorrentino–Spagnuolo 2024.

31. In un ecosistema digitale estremamente complesso e in rapida trasformazione è fondamentale adottare approcci dinamici e adattivi per valutare il rischio cyber. La continua evoluzione delle minacce e delle tecnologie richiede di "ricostruire i contorni" di questo ecosistema in modo continuo, per comprendere le interdipendenze tra gli asset digitali, le nuove vulnerabilità e le superfici di attacco emergenti. Solo con una visione sistemica e aggiornata è possibile garantire efficacemente la sicurezza e la resilienza delle infrastrutture digitali. Si veda Commissione europea 2024. Il report della Commissione europea (2024) mette in evidenza come la sovranità digitale nell'Unione europea richieda una comprensione profonda e aggiornata dell'intero ecosistema digitale, caratterizzato da continui cambiamenti tecnologici, geopolitici e di minacce informatiche. Per garantire l'autonomia strategica e la sicurezza, è fondamentale ricostruire in modo dinamico e costante i contorni di questo ecosistema, identificando nuove vulnerabilità, rischi emergenti e interdipendenze critiche tra infrastrutture, fornitori e tecnologie. Questa necessità nasce dall'evoluzione continua delle tecnologie digitali e dalle minacce sofisticate che mettono a rischio la resilienza e la protezione degli asset digitali europei. In particolare, il report insiste sull'importanza di adottare strategie flessibili, cicliche e sistemiche di valutazione e gestione dei rischi, così da mantenere un controllo efficace sulla complessità in rapido mutamento dell'ecosistema digitale.

32. Nel contesto della governance digitale, il concetto di minaccia si riferisce alle evoluzioni continue delle minacce informatiche sofisticate, che caratterizzano l'ecosistema digitale in rapido mutamento, richiedendo strategie di monitoraggio dinamico per identificare interdipendenze critiche e superfici di attacco emergenti. Si veda a tal proposito Abo Mhara–Abdulrahman–Baroud 2024; El-Shrouk 2023; Ahmed 2022.

33. La categoria degli attori nella governance digitale si articola in un modello multistakeholder inclusivo, comprendente governi, imprese, associazioni non governative, istituti di ricerca, organizzazioni intergovernative, società civile, cittadini e altri stakeholder, i quali collaborano in modo condiviso per definire policy digitali evolute. Tale approccio decentralizzato e privo di gerarchie rigide integra enti pubblici come Agenzia per l'Italia Digitale (AgID), Agenzia per la Cybersicurezza Nazionale (ACN) e Garante privacy, oltre a figure professionali dedicate alla transizione digitale. Si veda Baldazzini–Bottos–Danna et al. 2024; Pliauškaitė 2024; Millard 2023.

34. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024. July 2023 to June 2024*. Il rapporto fornisce un'analisi dettagliata delle minacce emergenti nel panorama europeo, sottolineando la

normativi mirati alla tutela delle infrastrutture, dei dati personali e della privacy degli utenti. Si tratta di un criterio dinamico, capace di guidare proporzionalità, adeguatezza e responsabilità dell'azione normativa; in tal senso il General Data Protection Regulation (GDPR)[35] rappresenta un riferimento paradigmatico, collegando sicurezza dei dati, valutazione del rischio e responsabilità normativa[36]. La categoria della minaccia costituisce la materializzazione operativa del rischio, includendo eventi dannosi, dolosi o accidentali, interni o esterni, che possono compromettere l'integrità, la disponibilità o la riservatezza dei sistemi. L'analisi delle minacce evidenzia la necessità di strumenti normativi flessibili e adattabili, in grado di rispondere alla natura mutevole degli attacchi. Infine, la categoria degli attori consente di comprendere la distribuzione policentrica delle responsabilità, evidenziando come ruoli e competenze siano intrecciati a livello nazionale, sovranazionale e transnazionale. Il livello giuridico, diversamente dalle categorie tematiche che collegano la logica sostanziale delle norme, si concentra sull'ordinamento sistematico delle fonti secondo la loro forza cogente e il potenziale impatto strategico. Questo approccio permette di distinguere con chiarezza le fonti che, pur differenziandosi per grado di vincolatività, contribuiscono in maniera determinante a regolare e orientare le politiche digitali[37], offrendo un quadro coerente e integrato per l'interpretazione e l'applicazione delle norme. Nella fase applicativa, la distinzione tra forza giuridica formale e impatto sostanziale è stata applicata in modo sistematico alla classificazione delle fonti. Le fonti vincolanti (regolamenti, direttive e norme primarie) sono state identificate come strumenti dotati di potere cogente immediato, capaci di orientare direttamente le politiche pubbliche. In parallelo, i documenti di soft law, comprese strategie, linee guida e dichiarazioni politiche, sono stati considerati fonti a impatto sostanziale, il cui valore risiede nella capacità di indirizzare decisioni regolatorie, modellare comportamenti istituzionali e orientare l'interpretazione delle norme cogenti. Questa doppia lettura consente di costruire una mappa normativa multilivello, in cui forza formale e influenza sostanziale delle fonti vengono trattate come variabili interconnesse. Attraverso questo approccio, il modello permette di mettere in relazione fonti eterogenee, evidenziando come norme vincolanti e indicazioni strategiche, pur differenziandosi per natura e grado di vincolatività, contribuiscano congiuntamente a definire un quadro unitario di sovranità digitale e resilienza cibernetica. In tale prospettiva, il panorama nazionale di cybersecurity e governance digitale si prospetta come un percorso evolutivo, in cui strumenti fondativi e interventi più recenti concorrono a delineare un'architettura regolatoria sempre più integrata e interconnessa, capace di coniugare coerenza normativa, tutela dei diritti fondamentali e orientamento strategico. A questo schema sistemico si innesta il complesso apparato normativo nazionale, in cui la legge 18 novembre 2019, n. 133[38], istitutiva del Perimetro di sicurezza nazionale cibernetica, assume il ruolo di fondamento strutturale, definendo responsabilità istituzionali, procedure di vigilanza e requisiti di protezione per reti, sistemi e servizi di rilevanza strategica. Su questa base si colloca il recepimento della Direttiva (UE) 2022/2555 (NIS2) [39], recepita con il d.lgs. 4 settembre 2024, n. 138[40], che estende la platea dei soggetti "essenziali" e "importanti", innalza gli standard di gestione del rischio, chiarisce il

natura dinamica e interconnessa delle minacce cyber, e la necessità di un approccio integrato per la loro gestione.

35. Regolamento (UE) 2016/679.
36. *Ibidem*. Si veda Gonçalves 2019.
37. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024. July 2023 to June 2024*. Si veda ancora Nodehi–Berisha–Da Silva et al. 2024.
38. Legge 18 novembre 2019, n. 133.
39. Direttiva (UE) 2022/2555 (NIS2).
40. Decreto legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

regime di responsabilità e abroga contestualmente il d.lgs. 65/2018[41], attuativo della precedente Direttiva NIS (UE) 2016/1148[42], segnando il passaggio verso un modello regolatorio più ampio, uniforme e coordinato. In questa prospettiva, la NIS1 mantiene valore ricostruttivo quale primo tentativo europeo di armonizzazione in materia di sicurezza delle reti e dei sistemi informativi, ma è la NIS2 a determinare un effettivo salto qualitativo, rafforzando la resilienza digitale[43] complessiva e ponendo l'accento su interoperabilità, continuità operativa, coordinamento nella gestione degli incidenti[44] e omogeneità degli standard nazionali, in un'ottica di coesione tra gli Stati membri e di consolidamento della capacità di risposta comune. Parallelamente, la legge 23 settembre 2025, n. 132[45], in armonia con il Regolamento UE 2024/1689 (AI Act), istituisce un quadro organico per l'intelligenza artificiale, attribuendo all'Agenzia per l'Italia Digitale (AgID) e all'Agenzia per la Cybersicurezza Nazionale (ACN) compiti precisi di vigilanza, autorizzazione, monitoraggio e sanzione degli usi dell'intelligenza artificiale, con particolare attenzione a sicurezza, trasparenza, tutela dei diritti fondamentali e protezione dei dati. L'insieme di queste norme testimonia come il sistema nazionale stia assumendo una configurazione integrata e stratificata, in cui la protezione delle infrastrutture critiche, la gestione dei rischi informatici e la regolazione delle tecnologie emergenti non siano ambiti separati, ma componenti interconnesse di una governance digitale complessa.

Il livello giuridico internazionale costituisce la cornice entro cui le norme e gli standard acquisiscono forza e significato, delineando i confini entro cui le politiche nazionali possono essere coerentemente orientate. Standard riconosciuti globalmente, quali ISO/IEC 27001[46] e il NIST Cybersecurity Framework[47], svolgono una funzione metodologica di orientamento, definendo pratiche di gestione del rischio condivise e interoperabili. La versione 2.0 del NIST (2024), articolata nelle funzioni Governare, Identificare, Proteggere, Rilevare, Rispondere e Recuperare[48], offre una struttura flessibile, facilmente raccordabile tanto agli strumenti normativi vincolanti, quali regolamenti e direttive europee, quanto agli atti di soft law.

A tale dimensione si affianca il profilo dell'origine delle fonti e del loro impatto sistemico. L'impianto normativo europeo si struttura in atti sovranazionali che definiscono standard e logiche di intervento in materia digitale, cui si aggiungono strumenti nazionali che recepiscono e implementano le priorità europee, contribuendo alla costruzione di un quadro regolamentare sempre più coeso e integrato[49]. L'analisi deve inoltre

41. Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
42. Direttiva (UE) 2016/1148.
43. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025, October 2025*.
44. La Direttiva NIS2 impone una governance strutturata e responsabilità dirette agli organi aziendali, spostando il baricentro della sicurezza cyber dal tecnico al gestionale, con l'obbligo di gestione agile, proattiva e trasparente del rischio informatico. Per approfondimenti si veda Agenda Digitale 2025; ICT Security Magazine 2025; Netribe Group 2025; SS Group 2024.
45. Legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale.
46. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), *Information Security Management Systems – Requirements* (ISO/IEC 27001:2022/Amd 1:2024), Geneva, February 2024.
47. National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024, ultima versione del Framework che aggiorna e rafforza l'approccio risk-based alla cybersecurity.
48. Edwards 2024.
49. European Commission 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, COM (2025) 290, Brussels, 2025. Il Rapporto sottolinea l'importanza strategica della sovranità digitale e la necessità di una governance integrata a livello europeo. Tuttavia, rimangono rilevanti lacune normative e una predominanza di linee guida e strategie rispetto a norme vincolanti e armonizzate, riflettendo così lo stato ancora in evoluzione della disciplina.

considerare l'influenza di iniziative come GAIA-X[50] e di fonti esterne all'ordinamento dell'Unione come il Cloud Act statunitense[51], che intervengono sulla definizione dei requisiti di sicurezza e sovranità dei dati, sull'elaborazione di standard di interoperabilità e sulle strategie di localizzazione, incidendo così sulla configurazione dello spazio europeo della sovranità digitale. Considerata nella sua interezza, questa complessa architettura dischiude un ordine normativo dinamico in cui le interazioni, le continuità e le tensioni tra i diversi piani non si risolvono in semplici sovrapposizioni, ma compongono un paradigma sistemico di natura evolutiva. In tale orizzonte, perfettamente coerente con l'impianto metodologico delineato, si manifesta la *ratio essendi* di un equilibrio rigoroso tra fonti cogenti, strumenti di soft law, vincoli giuridici e direttive strategiche.

4. Parole chiave per una governance europea della sovranità digitale

L'analisi metodologica condotta nei paragrafi precedenti, dalla mappatura sistematica delle fonti, alla classificazione interpretativa lungo assi tematici e giuridici, fino all'articolazione multilivello delle norme cogenti e degli strumenti di soft law, ha messo in luce la complessità e le interdipendenze dell'ecosistema normativo europeo e nazionale, offrendo le basi per la costruzione di un modello normativo integrato. Come abbiamo già osservato, mentre la cybersecurity è ampiamente regolamentata da un quadro normativo consolidato, la sovranità digitale, pur essendo al centro del dibattito politico e strategico europeo, rimane una nozione sfuggente, priva di un inquadramento normativo esaustivo che ne definisca chiaramente presupposti, finalità e implicazioni operative[52]. Da qui la necessità di isolare termini chiave capaci di sintetizzare la complessità del quadro regolatorio europeo e nazionale. Le parole chiave non sono semplici etichette ma rappresentano nodi concettuali, in cui si condensano principi, tensioni normative e orientamenti strategici, permettendo di tradurre la sovranità digitale da nozione teorica a strumento operativo. Proprio l'assenza di una definizione unitaria, infatti, genera una frizione sistemica che ostacola l'armonizzazione delle discipline vigenti in materia di sicurezza informatica, protezione dei dati e governance delle infrastrutture critiche, complicando la gestione delle minacce digitali e rallentando l'emersione di un'autonomia tecnologica pienamente coerente con i principi del diritto internazionale[53]. In questo contesto, l'individuazione dei termini ricorrenti si configura come esito naturale della metodologia comparativa e sistematica adottata divenendo uno strumento interpretativo capace di collegare l'elaborazione teorica alla prassi decisionale.

In particolare, la ricorrenza dei termini è stata accertata mediante un'analisi sistematica non solo quantitativa, ma anche qualitativa, capace di cogliere il loro peso semantico all'interno dei contesti d'uso. L'annotazione manuale, adottata come scelta metodologica consapevole, ha permesso di intercettare nessi concettuali, sfumature lessicali e impliciti normativi che gli strumenti automatizzati tendono a elidere, trasformando ciò che potrebbe apparire come un limite operativo in un vero punto di forza ermeneutico. La manualità, lungi dall'essere un retaggio pre-analitico, diviene la condizione previa, consentendo di valutare non soltanto che cosa ricorre, ma come e perché.

Dal processo analitico, così condotto, emergono tre assi interpretativi, capaci di chiarire la trama concettuale prevalente nelle fonti esaminate e di offrire chiavi di lettura stabili senza ridurre la complessità del fenomeno. La loro validità teorica è confermata dalla letteratura scientifica di settore che, pur non avendo orientato la selezione o condizionato la classificazione dei documenti, ha validato *a posteriori* i risultati ottenuti.

Si è definita come prima area concettuale quella della *Autonomia Tecnologica e della Resilienza*

50. European Cloud Federation 2022, *GAIA-X: A Federated Data Infrastructure for Europe*, Brussels, 2022. Progetto europeo per la creazione di un'infrastruttura cloud sicura e autonoma.
51. U.S. Congress 2018, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. 115-141, Division V, 23 marzo 2018, Normativa statunitense che ha influenzato il dibattito europeo sulla protezione dei dati.
52. European Commission 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, COM (2025) 290, Brussels, 2025.
53. Guerra 2025.

Strategica, comprendente termini quali "autonomia tecnologica", "resilienza" e "infrastrutture critiche". Tale area è rafforzata e valorizzata dalla Dichiarazione europea sui diritti e principi digitali[54], che offre un quadro valoriale human-centric finalizzato a guidare l'attuazione dell'*open autonomy*[55] promosso dalla Commissione europea e riconosciuto nei principali documenti strategici comunitari.

La seconda area concettuale, denominata *Controllo Normativo e Infrastrutturale*, incorpora concetti quali "sicurezza cibernetica", "protezione dei dati" e "regolamentazione delle piattaforme digitali" riflettendo l'esigenza di strumenti giuridici chiari ed efficaci[56]. La definizione di quest'asse segue l'evoluzione normativa europea (GDPR, DSA, DMA, NIS2), in cui la sovranità digitale si configura come capacità regolatoria dello Stato sulle architetture digitali, sui flussi informativi e sulle piattaforme medesime.

La terza area, infine, denominata *Diritti Fondamentali e Partecipazione Democratica*, include concetti come "diritti digitali", "giustizia algoritmica", "partecipazione democratica" e "solidarietà internazionale". Questa dimensione mette in evidenza l'intreccio tra politiche tecnologiche e valori costituzionali[57].

L'analisi sistematica delle parole chiave, organizzate nei tre assi interpretativi, non serve solo a chiarirne il significato lessicale, ma diventa uno strumento capace di interpretare e anticipare l'evoluzione del panorama normativo attorno al concetto di sovranità digitale. I termini emergenti funzionano come nodi concettuali in grado di svolgere una duplice funzione: chiariscono i concetti e indicano i possibili sviluppi normativi, integrando sicurezza, autonomia tecnologica e tutela dei diritti traducendo un concetto frammentato e ambiguo in principio guida per una nuova architettura giuridica[58].

Attraverso questa prospettiva, il *Digital constitutionalism*[59] appare come il traguardo teleologico verso cui tende la regolazione della sovranità digitale. Non è una realtà già compiuta, ma un progetto normativo e istituzionale che trasla nell'ecosistema digitale i valori fondanti del costituzionalismo tradizionale (tutela dei diritti fondamentali, separazione dei poteri, limiti all'autorità e garanzie democratiche). In questo modo contribuisce a modellare strumenti, processi e responsabilità[60].

5. Conclusioni

L'analisi condotta ha evidenziato che per affrontare in modo efficace le sfide poste da un ecosistema digitale globale, in continua evoluzione e sempre

54. Parlamento europeo, Consiglio europeo, Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, 2023/C 23/01. La Dichiarazione punta a stabilire un quadro costituzionale per la società digitale. Come altre iniziative simili, punta ad aggiornare le norme costituzionali per rispondere alle sfide imposte dalla rivoluzione digitale, mettendo in evidenza i diritti e i principi che devono guidare gli attori europei durante questa trasformazione.
55. Il concetto di *open strategic autonomy* è stato introdotto dalla Commissione europea nel 2021 nella *Trade Policy Strategy* per sottolineare la necessità di rendere l'apertura commerciale compatibile con la sua autonomia. Da giugno 2023 l'Ue si è concentrata sullo sviluppo di una *Economic Security Strategy*, al fine di integrare politiche economiche e commerciali incentrate sull'autonomia strategica aperta, sicurezza energetica ed economica, resilienza della catena di approvvigionamento agli shock esterni e riduzione del rischio.
56. Fratini–Hine–Novelli et al. 2024. Il testo offre una mappatura critica dei diversi modelli di sovranità digitale (statale, dei diritti, di mercato), utile per situare il proprio modello interpretativo.
57. Amoretti–Santaniello 2024.
58. Floridi 2020. L'autore fornisce un approfondimento accademico sul ruolo della razionalizzazione normativa nella costruzione della sovranità digitale.
59. Il *Digital constitutionalism* può essere definito come un insieme di principi, strumenti e iniziative volti a trasferire i valori fondamentali del costituzionalismo nell'ambiente digitale, attraverso norme, codici, dichiarazioni e policy che organizzano la governance di Internet e delle infrastrutture digitali, pur senza costituire un corpus normativo unitario e codificato. Si veda a tal proposito Celeste 2021; Celeste 2019; Redeker–Gill–Gasser 2018.
60. De Gregorio–Radu 2022.

più esposto a minacce informatiche sofisticate, è necessario un quadro giuridico solido, coerente e integrato. In tale contesto, la sistematizzazione delle fonti normative e l'individuazione di parole chiave strategiche non si configurano come un esercizio meramente classificatorio, ma divengono un passaggio interpretativo essenziale per guidare l'elaborazione di strategie normative in grado di coniugare sicurezza, innovazione e tutela dei diritti fondamentali. Il modello normativo integrato articola la sovranità digitale lungo i tre assi interpretativi (Autonomia Tecnologica e Resilienza Strategica, Controllo Normativo e Infrastrutturale, Diritti Fondamentali e Partecipazione Democratica), da cui emergono le parole chiave come nodi concettuali che offrono una lente privilegiata per interpretare l'attuale quadro normativo e anticiparne le possibili evoluzioni, trasformando concetti frammentati in strumenti progettuali capaci di tracciare traiettorie normative future. La sovranità digitale, intesa come capacità di esercitare un controllo autonomo, responsabile e democraticamente legittimato sulle risorse digitali, costituisce la naturale evoluzione del paradigma della cybersecurity. Essa non si limita alla difesa da minacce esterne, ma si estende alla gestione proattiva di infrastrutture critiche, dati sensibili, algoritmi decisionali e piattaforme strategiche, assumendo una rilevanza concreta e immediata nell'architettura costituzionale degli Stati e nell'equilibrio tra potere pubblico, mercato e cittadini. Il bilanciamento tra autonomia tecnologica, sicurezza cibernetica e tutela dei diritti fondamentali emerge come una delle sfide più complesse e decisive del nostro tempo, soprattutto in un contesto segnato da crescenti interdipendenze geopolitiche e da una competizione globale per il controllo delle tecnologie strategiche che rischiano di minare le basi del vivere democratico. La piena operatività di questo paradigma richiede il rafforzamento delle infrastrutture critiche, l'adozione di una cultura di responsabilità digitale e la promozione di trasparenza e inclusività regolativa guidando la costruzione di strumenti e processi volti ad armonizzare innovazione, sicurezza e protezione dei diritti fondamentali.

Riferimenti bibliografici

M.A.O. Abo Mhara, A.A.A. Abdulrahman, A.A.S. Baroud (2024), *Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage*, in "The International Journal of Electrical Engineering and Sustainability (IJEES)", vol. 2, 2024, n. 4

Agenda Digitale (2025), *Nis2, come adeguarsi ai nuovi obblighi cyber: i punti chiave*, in "Agenda Digitale", 2025

S. Ahmed (2022), *A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age*, in "Journal of Cybersecurity & Information Management", vol. 10, 2022, n. 2

F. Amoretti, M. Santaniello (2024), *Sovranità e costituzionalismo digitale*, in "Tecnologia, Politica, Società", 2024

A. Baldazzini, G. Bottos, R. Danna, E. Desiata, F. Nasi, O. Palmini, A. Venieri (2024), *La governance del digitale in Italia. Innovazione, democraticità e sviluppo sociale*", Nous Media, 2024

R. Bin (2013), *La sovranità nazionale e la sua erosione*, in A. Pugiotto (a cura di), "Per una consapevole cultura costituzionale. Lezioni magistrali", Jovene Editore, 2013

R. Brighi, P.G. Chiara (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "federalismi.it", 2021, n. 21

M. Cardone (2025), *Punti di Vista sulla sovranità digitale – Difendere il cyberspazio: la nuova frontiera della sovranità digitale*, in "IRPA – Osservatorio sullo Stato Digitale", 21 marzo 2025

M. Catanzariti (2024), *Disconnecting sovereignty: how data fragmentation reshapes the law*, Springer Nature, 2024

E. Celeste (2021), *Digital constitutionalism: mapping the constitutional response to digital technology's challenge*, in "Direitos Fundamentais & Justiça", 2021, n. 45

E. Celeste (2019), *Digital constitutionalism: a new systematic theorisation*, in "International Review of Law, Computers & Technology", vol. 33, 2019, n. 1

A. Chander, H. Sun (a cura di) (2023), *Data Sovereignty: From the Digital Silk Road to the Return of the State,* Oxford University Press, 2023

Commissione europea (2024), *State of the Digital Decade 2024*, COM (2024) 400, Bruxelles, 2024

S. Crespi (2024), *La protezione dello Stato di diritto nel sistema dell'Unione europea*, in "Eurojus.it", 2024, n. 2

B. Custers (2022), *New digital rights: Imagining additional fundamental rights for the digital era*, in "Computer Law & Security Review", vol. 44, 2022

G. De Gregorio, R. Radu (2022), *Digital constitutionalism in the new era of Internet governance*, in "International Journal of Law and Information Technology", vol. 30, 2022, n. 1

P. De Rosa (2021), *Concetto di Stato e nuove tecnologie. Quale ruolo per lo Stato nello spazio digitale?,* in "Media Laws", Law and Media WPS n. 1/2021

A. Di Corinto (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1

J. Edwards (2024), *A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice*, John Wiley & Sons, 2024

A. El-Shrouk (2023), *Comprehensive cybersecurity review: Modern threats and innovative defense approaches*, in "International Journal of Computers and Informatics (Zagazig University)", 2023, n. 1

F. Faini (2018), *Dati, informazioni e società digitale: il cambiamento nei confini del diritto*, in R. De Giorgi (a cura di), "Limiti del diritto. Prospettive di riflessione e analisi", Pensa MultiMedia, 2018

C. Faralli (2018), *Diritto, diritti e nuove tecnologie*, Editoriale Scientifica, 2018

L. Floridi (2020), *The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU*, in "Philosophy & Technology", vol. 33, 2020, n. 3

S. Fratini, E. Hine, C. Novelli, H. Roberts, L. Floridi (2024), *Digital sovereignty: A descriptive analysis and a critical evaluation of existing models*, in "Digital Society", vol. 3, 2024, n. 3

A. Gatti (2019), *Istituzioni e anarchia nella rete. I paradigmi tradizionali della sovranità alla prova di internet*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 3

M.E. Gonçalves (2019), *The risk-based approach under the new EU data protection regulation: a critical perspective*, in "Journal of Risk Research", vol. 23, 2019, n. 2

P. Guarda (2008), *Data Protection, Information Privacy and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in "Ciberspazio e diritto", vol. 9, 2008, n. 1

M. Guerra (2025), *Le prospettive di collaborazione tra Autorità indipendenti nell'era digitale*, in "Rivista italiana di informatica e diritto", 2025, n. 1

M. Hellmeier, F. von Scherenberg (2023), *A delimitation of data sovereignty from digital and technological sovereignty*, in "ECIS 2023 Research Papers", 306, 2023

P. Hummel, M. Braun, M. Tretter, P. Dabrock (2021), *Data sovereignty: A review*, in "Big Data & Society", vol. 8, 2021, n. 1

ICT Security Magazine (2025), *NIS2 e oltre: la cybersicurezza diventa governance aziendale*, in "ICT Security Magazine", 3 dicembre 2025

E. Longo (2023), *La ricerca di un'antropologia costituzionale della società digitale*, in "Rivista italiana di informatica e diritto", 2023, n. 2

S. Mangiameli (2023), *La sovranità digitale*, in A.C. Amato, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023

J. Millard (2023), *Impact of Digital Transformation on Public Governance*, Publications Office of the European Union, 2023

E.M.L. Moerel, P. Timmers (2021), *Reflections on Digital Sovereignty*, in "EU Cyber Direct, Research in Focus series", 2021

National Cyber Security Centre (2024), *NCSC Annual Review 2024*, in National Cyber Security Centre (NCSC), 2024

Netribe Group (2025), *Direttiva NIS2: nuove responsabilità cybersecurity degli imprenditori*, in Netribe Group, 22 aprile 2025

N.R. Nodehi, F Berisha, L Da Silva, Z Pourzolfaghar, M Helfert (2024), *Integrating Cybersecurity, Data Sovereignty and Trustworthiness in Agri-data Sharing Environments: A Conceptual Framework*, in "2024 Cyber Research Conference – Ireland (Cyber-RCI)", Carlow, Ireland, 2024

N. Palladino (2023), *The Ambiguity of Digital Sovereignty between Territorialization of the Cyberspace, Extraterritorial Claims and Digital Rights: Analysing Data Transfer Policies in EU, US and China*, in giga-net.org, 2023

F. Pierucci (2025), *Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace*, in "Digital Society", vol. 4, 2025, n. 1

L. Pliauškaitė (2024), *Digital Governance in Europe: A Stakeholder Map of European Institutions and Regulators*, in iapp.org, 2024

B. Ponti (2024), *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in "Rivista italiana di informatica e diritto", 2024, n. 2

D. Redeker, L. Gill, U. Gasser (2018), *Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights*, in "International Communication Gazette", vol. 80, 2018, n. 4

F. Resta (2024), *Cybersicurezza e protezione dati: un rapporto ambivalente*, in "Rivista italiana di informatica e diritto", 2024, n. 2

G. Resta, V. Zeno-Zencovich (a cura di) (2016), *La Protezione Transnazionale dei Dati Personali*, RomaTrE-Press, 2016

H. Roberts, J. Cowls, F. Casolari, J. Morley, M. Taddeo, L. Floridi (2021), *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in SSRN, 2021

S. Rodotà (2021), *Tecnologie e diritti*, il Mulino, 2021

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance,* in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Simoncini (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), "Diritti e libertà in internet", Mondadori Education, 2017

E. Sorrentino, A.F. Spagnuolo (2024), *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in "Rivista italiana di informatica e diritto", 2024, n. 2

C. Spiniello (2025), *È (ancora) tempo di costituzionalismo digitale*, in "Rivista italiana di informatica e diritto", 2025, n. 1

SS Group (2024), *La Direttiva NIS2: Nuove Regole per la Cybersecurity e la Responsabilità Aziendale*, in SSG Scai Solution Group, 19 aprile 2024

M. Taddeo (2019), *Is cybersecurity a public good?*, in "Minds and Machines", vol. 29, 2019, n. 3

V. Zeno-Zencovich (2018), *La "datasfera". Regole giuridiche per il mondo digitale parallelo*, in L. Scaffardi (a cura di), "I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale", Giappichelli, 2018

G. Ziccardi (2019), *La Cybersecurity nel quadro tecnologico (e politico) attuale*, in G. Ziccardi, P. Perri (a cura di), "Tecnologia e Diritto", III, Giuffrè, 2019