GLI STATI MEMBRI DELL'UE AL BIVIO DELLA «TERZA VIA» DIGITALE. UNO STUDIO EMPIRICO (PARTE I)*

di Chiara Spiniello**

Sommario. 1. A proposito della «terza via» digitale europea: un'introduzione. – 2. Contenuto, metodologia e obiettivi della ricerca. – 3. Dati e tendenze nei discorsi «digitali» dei Capi di Stato. – 4. Legislazioni digitali nazionali a confronto. – 5. Una (prima) riflessione conclusiva.

1. A proposito della «terza via» digitale europea: un'introduzione. Nel dibattito sulla governance globale di Internet, l'Unione europea (UE) ha progressivamente rivendicato l'ambizione di una «terza via», un modello regolatorio capace di collocarsi tra, da un lato, l'impostazione statunitense tradizionalmente fondata su ampi margini di *private self-regulation*[1] e, dall'altro, le strategie stato-centriche promosse dai regimi autoritari, orientate alla territorializzazione della rete e al controllo governativo pervasivo delle infrastrutture digitali[2]. In questa prospettiva, la «via europea» si presenta come un tentativo di costituzionalizzare lo

* *Sottoposto a referaggio.*

** Ricercatrice post-dottorato – Zentrum für Medien-, Kommunikations- und Informationsforschung (ZeMKI).

[1] Sebbene l'attuale congiuntura storica delinei un quadro diverso – caratterizzato, da un lato, da una crescente «politicizzazione» del rapporto tra Presidenza Trump e grandi imprese tecnologiche (anche attraverso forme di interlocuzione diretta e di sostegno economico) e, dall'altro, dal riemergere ciclico di istanze di revisione delle immunità e degli obblighi delle piattaforme – la locuzione *private self-regulation* continua a descrivere efficacemente la matrice tradizionale dell'impostazione statunitense, storicamente fondata su ampi margini di regolazione privata dell'ecosistema digitale e su un intervento pubblico prevalentemente «di cornice», tendenzialmente refrattario a regimi prescrittivi *ex ante*. In tale paradigma, la definizione delle regole operative è stata a lungo affidate soprattutto al mercato e al *private ordering* (standard tecnici, codici di condotta, *terms of service* e procedure di moderazione), con lo Stato chiamato soprattutto a garantire un ambiente giuridico prevedibile, *technology-neutral* e non eccessivamente gravoso. In argomento si vedano, almeno, L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999; J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven, 2008; J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006; M.L. Mueller, *Networks and States. The Global Politics of Internet Governance*, Cambridge (MA), 2010; L. DeNardis, *The Global War for Internet Governance*, New Haven, 2014; nonché, con specifico riferimento alla tipologia dei modelli di governance, M. Santaniello, *From governance denial to state regulation: A controversy-based typology of Internet governance models*, in B. Haggart, N. Tusikov, J.A. Scholte (a cura di), *Power and Authority in Internet Governance. Return of the State?*, London and New York, 2021, 15-36.

[2] I casi cinese e russo mostrano come, in contesti autoritari, la sovranità digitale venga declinata in senso eminentemente statuale. Il potere pubblico mira a rendere il cyberspazio tecnicamente ispezionabile e giuridicamente governabile lungo linee territoriali, attraverso il controllo dei nodi infrastrutturali e dei flussi transfrontalieri, la prescrizione di obblighi su dati e fornitori e l'adozione di dispositivi normativi che legittimano censura e sorveglianza pervasive. Sul punto J. Nocetti, *Contest and conquest: Russia and global internet governance*, in *International Affairs*, 91(1), 2015, 111-130, e J.-J. Hwang, *Reframing China's Territory and Sovereignty in Cyberspace: Exploring Conceptual Territorialization and Claims of Cyber Sovereignty*, in *Issues & Studies*, 59 (4), 2023, 1-21.

Issn 2421-0528

spazio digitale, ossia di ricondurre l'esercizio del potere tecnologico entro coordinate compatibili con i diritti fondamentali e con i principi liberal-democratici[3].
Tale traiettoria segna una discontinuità rispetto alla tradizionale prudenza dell'UE in materia di Internet governance, emersa sin dai lavori del *World Summit on the Information Society* (2003-2005)[4]. Negli ultimi anni, infatti, l'approccio europeo ha conosciuto una vera e propria svolta regolatoria, alimentata sia da esigenze di policy (mercato e sicurezza, prime fra tutti) sia dalla crescente consapevolezza del ruolo giocato dalle grandi piattaforme nella distribuzione del potere digitale[5]. Questa inversione di tendenza si è tradotta, dapprima, nel ricorso a strumenti di *soft law* – raccomandazioni, dichiarazioni politiche, strategie – idonei a fissare una grammatica valoriale comune e a predisporre una cornice di orientamento per legislatori, imprese e istituzioni[6]. In tale filone rientra, emblematicamente, la «Dichiarazione europea sui diritti e i principi digitali per il decennio digitale», adottata congiuntamente da Parlamento europeo, Consiglio e Commissione il 23 gennaio 2023, la quale, pur priva di cogenza formale, ha acquisito valore significativo perché enuncia un programma politico di trasformazione digitale centrata sulla persona e, soprattutto, perché ambisce a fungere da bussola per la produzione normativa successiva[7].
In un secondo momento, tuttavia, l'UE ha intensificato la regolazione mediante atti giuridicamente vincolanti, consolidando un *corpus* normativo che – a partire dal *General Data Protection Regulation* (GDPR) – mira a incidere strutturalmente sugli assetti del mercato digitale e sulle dinamiche di potere proprie dell'ecosistema virtuale[8]. In questo processo, la giurisprudenza della Corte di Giustizia dell'Unione europea (CGUE) ha svolto una funzione propulsiva. Attraverso l'elaborazione di una tutela «robusta» della *digital privacy* e l'estensione dell'efficacia dei diritti riconosciuti dalla Carta dei diritti fondamentali, la Corte ha infatti contribuito a rafforzare la centralità dei diritti nell'ambiente digitale e, al contempo, a sollecitare una riappropriazione del ruolo di *lawmaker* da parte del legislatore europeo[9]. La

[3] Resta celebre il discorso pronunciato dal Presidente della Repubblica francese Emmanuel Macron in occasione della cerimonia inaugurale dell'*Internet Governance Forum* di Parigi del novembre 2018, in cui sollecita un «movimento di riforma» fondato su forme di regolamentazione democratica e su «nuove forme di cooperazione multilaterale», prospettando un modello alternativo tanto al paradigma della «completa autogestione» privata quanto al prototipo di controllo pubblico pervasivo associato al modello cinese. Si veda E. Macron, *Speech by M. Emmanuel Macron, President of the Republic at the Internet Governance Forum*, Unesco, Parigi, 12 novembre 2018; cfr. M. Santaniello, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, 1, 2022, spec. 50.
[4] Il *World Summit on the Information Society* (WSIS) è il processo intergovernativo promosso in sede ONU che si è svolto in due fasi (Ginevra, 2003; Tunisi, 2005) e che ha fissato principi e linee d'azione per la «società dell'informazione». In particolare, la *Tunis Agenda* ha dedicato un passaggio specifico alla *Internet governance* e ha posto le basi per la creazione dell'*Internet Governance Forum* (IGF) quale sede di confronto multilaterale e multistakeholder priva di poteri vincolanti. In argomento M. Santaniello, *From Governance Denial to State Regulation: A Controversy-Based Typology of Internet Governance Models*, cit., 15-36.
[5] Cfr. M. Santaniello, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, cit., 47-51.
[6] Cfr. C. Spiniello, *È (ancora) tempo di costituzionalismo digitale*, in *Rivista italiana di informatica e diritto*, 1, 2025, 579-599.
[7] Parlamento europeo, Consiglio, Commissione, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* (2023/C 23/01), 23 gennaio 2023.
[8] Tra i suddetti atti si annoverano, in particolare, i seguenti Regolamenti: reg. UE 2016/679 (GDPR), in GUUE, L 119, 4 maggio 2016; reg. UE 2019/881 (*Cybersecurity Act*), in GUUE, L 151, 7 giugno 2019; reg. UE 2022/868 (*Data Governance Act*), in GUUE, L 152, 3 giugno 2022; reg. UE 2022/2065 (*Digital Services Act*), in GUUE, L 277, 27 ottobre 2022; reg. UE 2022/1925 (*Digital Markets Act*), in GUUE, L 265, 12 ottobre 2022; reg. UE 2023/2854 (*Data Act*), in GUUE, L, 2023/2854, 22 dicembre 2023; reg. UE 2024/1689 (*Artificial Intelligence Act*), in GUUE, L, 12 luglio 2024; reg. UE 2024/2847 (*Cyber Resilience Act*), in GUUE, L, 20 novembre 2024.
[9] Sul ruolo propulsore della CGUE in materia digitale si vedano C. Amalfitano, F. Ferri, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. Torino, S. Zorzetto (a cura di), *La*

progressiva emersione di discipline settoriali (dalla regolazione delle piattaforme e dei mercati digitali fino alla sicurezza dei prodotti con elementi digitali e alla disciplina dell'intelligenza artificiale) risponde, così, a un disegno più ampio: dotare l'ordinamento europeo di strumenti effettivi per limitare il potere digitale e rendere azionabili le garanzie poste a presidio dei diritti fondamentali[10].

È in questo contesto che si afferma, negli orientamenti istituzionali, la categoria della «sovranità digitale europea». L'espressione compare inizialmente in alcuni pareri del Comitato europeo delle Regioni e del Comitato economico e sociale europeo, per poi diffondersi nei discorsi dei leader politici e nei documenti strategici dell'UE[11]. È significativo, in tal senso, che essa venga esplicitamente accostata, nella formula «*Technological Sovereignty, Security and Democracy*» (seconda Commissione von der Leyen[12]), alle categorie della sicurezza e della democrazia. Ciò è indice del fatto che, nel discorso istituzionale UE, la sovranità digitale è concepita non come obiettivo di chiusura autarchica, ma come leva di autonomia e capacità d'azione finalizzata sia alla resilienza e alla sicurezza sia alla salvaguardia dell'ordine democratico e dei diritti[13].

La *ratio* delle rivendicazioni di sovranità europee va dunque rintracciata nella necessità di ridurre forme di dipendenza strutturale da attori extra-UE – pubblici e privati – che incidono su infrastrutture, servizi e standard tecnici del digitale, con ricadute non solo economiche ma anche costituzionali[14]. Da questa angolazione, la sovranità digitale europea tende a qualificarsi come progetto «anti-sovranista», dal momento che non auspica chiusure nazionali e frammentazioni della rete, ma mira a democratizzare e costituzionalizzare Internet, soprattutto ponendo limiti effettivi al potere delle grandi piattaforme e rafforzando la capacità pubblica di governo del digitale[15]. In definitiva, l'originalità del progetto europeo si coglie nello sforzo di combinare costituzionalismo digitale e sovranità digitale, concependo lo sviluppo delle infrastrutture e dei mercati digitali, sì, come necessario, ma purché ancorato ai valori fondanti dell'Unione: solidarietà e inclusione, libertà di scelta, partecipazione, sicurezza in rete e sostenibilità, primi fra tutti.

2. Contenuto, metodologia e obiettivi della ricerca. Se gli assi portanti del discorso europeo su costituzionalismo e sovranità digitale possono essere ricostruiti nei termini sopra delineati, diviene dirimente interrogarsi sul se e in quale misura essi trovino un'effettiva corrispondenza nelle politiche e nelle strategie degli Stati Membri dell'UE. È questa la domanda di ricerca che muove il presente studio, il quale si propone – in una prospettiva di lungo periodo – di realizzare un'analisi comparata delle strategie digitali dei 27 Stati Membri dell'Unione europea, con l'obiettivo di mettere in luce convergenze, divergenze e possibili linee di frizione tra narrazione europea e declinazioni nazionali.

---

trasformazione digitale in Europa. Diritti e principi, Torino, 2024, 1-34, e G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Il diritto dell'informazione e dell'informatica*, 4-5, 2015, 779-799.

[10] M. Santaniello, *Sovranità digitale e diritti fondamentali*, cit., § 2-3.

[11] Una ricostruzione dell'impiego del termine *digital sovereignty* nel contesto europeo si rinviene in A. Alpini, *La sovranità digitale europea*, in *TIGOR. Rivista di scienze della comunicazione e di argomentazione giuridica*, 2, 2022, 144-152.

[12] Commissione europea, *Henna Virkkunen – Vicepresidente esecutiva, Technological Sovereignty, Security and Democracy*; Commissione europea, *Mission letter to Henna Virkkunen*, 1 dicembre 2024.

[13] Si vedano a riguardo i contenuti della European Commission, *A European Strategy for Data*, 2020.

[14] Cfr. E. Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini, E. Celeste, J. Quinn (a cura di), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, 2021, Oxford, 211-228.

[15] *Ibidem*.

Allo stato attuale, l'analisi si concentra su otto casi di studio (Francia, Germania, Italia, Spagna, Polonia, Danimarca, Portogallo, Romania), selezionati secondo una logica di «massima variazione»[16] così da cogliere configurazioni differenti del nesso tra sovranità, diritti e sicurezza nel contesto digitale. In concreto, ciascun caso di studio assolve a una funzione comparativa distinta, perché consente di osservare – da angolazioni differenti – come il lessico della sovranità digitale venga tradotto (o, talora, riformulato) in scelte di *policy*, strumenti di governo e priorità normative.

Francia e Germania rappresentano i due ordinamenti nei quali la sovranità digitale emerge più precocemente e con maggiore densità programmatica, anche in ragione della capacità di proiettare a livello europeo iniziative concepite come «architravi» di autonomia strategica (si pensi, in particolare, al tema del *cloud* e delle infrastrutture per la gestione dei dati). In entrambi i casi, l'interesse comparativo non risiede soltanto nell'enunciazione politica dell'obiettivo sovrano, ma nel tentativo di istituzionalizzare standard, criteri e requisiti tecnici idonei a incidere sul funzionamento del mercato digitale: in Francia, attraverso una dottrina amministrativa che orienta l'azione pubblica verso soluzioni certificate e sottoposte a requisiti rafforzati di sicurezza; in Germania, mediante strategie federali che assumono la riduzione delle dipendenze e la resilienza tecnologica come condizioni della capacità di azione statale ed europea[17].

Il caso italiano è, invece, selezionato per verificare una dinamica più sfumata: qui la sovranità digitale tende ad articolarsi lungo due linee non sempre perfettamente sovrapponibili. Da un lato, la dimensione governativa – specialmente nella stagione delle politiche di trasformazione digitale della pubblica amministrazione – privilegia un approccio centrato su architetture infrastrutturali, migrazione al *cloud*, sicurezza e interoperabilità, con un lessico in cui l'efficienza amministrativa e la modernizzazione organizzativa assumono un rilievo primario. Dall'altro lato, la dimensione «istituzionale» veicolata dal Capo dello Stato insiste con maggiore continuità sul profilo valoriale (diritti, «qualità» della democrazia, garanzie costituzionali), mettendo in luce il rischio che l'innovazione tecnologica, se non incardinata entro presìdi di legalità sostanziale, produca asimmetrie di potere e nuove vulnerabilità per la sfera pubblica. In termini comparativi, l'Italia consente dunque di osservare lo scarto

[16] Con l'espressione «massima variazione» si intende una tecnica di campionamento volta a selezionare casi tra loro marcatamente eterogenei lungo dimensioni pertinenti al fine di documentare come un medesimo fenomeno si manifesti in contesti differenti e far emergere eventuali *pattern* comuni che «attraversano» l'eterogeneità dei casi. In questa prospettiva, la scelta di Stati membri diversi per peso politico-istituzionale, collocazione geopolitica, assetti amministrativi, grado di digitalizzazione e priorità di policy risponde alla logica di ampliare la *property space* osservabile e, quindi, di cogliere configurazioni differenti del nesso tra sovranità, diritti e sicurezza digitale, chiarendo al contempo quali elementi risultino ricorrenti nonostante le differenze di contesto. La strategia si colloca nel solco delle riflessioni metodologiche sul campionamento *purposeful* e sulla selezione dei casi in studi *small-N*, dove la massimizzazione della variabilità («casi diversi») costituisce un criterio di rigore alternativo al campionamento casuale, funzionale alla costruzione di tipologie e alla generalizzazione di tipo analitico. Cfr. L.A. Palinkas et al., *Purposeful sampling for qualitative data collection and analysis in mixed method implementation research*, in *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 2015, 533-544; M.Q. Patton, *Qualitative Research and Evaluation Methods*, 3ª ed., Thousand Oaks, 2002; A. Lijphart, *Comparative Politics and the Comparative Method*, in *American Political Science Review*, 65(3), 1971, 682-693.

[17] Per una ricostruzione del discorso su sovranità e costituzionalismo digitale in Francia e Germania si faccia riferimento a C. Spiniello, *È (ancora) tempo di costituzionalismo digitale,* cit., 587-590. Sui singoli ordinamenti si vedano, inoltre, A. Desforges, *Souveraineté numérique en France: du débat polarisé aux actes dispersés*, in S. Taillat, A. Cattaruzza, D. Danet (a cura di), *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2023, 127-133; J. Pohle, T. Thorsten, *Digitale Souveränität. Von der Karriere eines einenden und doch problematischen Konzepts*, in. C. Piallat (a cura di.), *Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt*, Bielefeld, 2021, 319-340.

(eventuale) tra retorica dei diritti e capacità di traduzione in politiche pubbliche, nonché la coesistenza tra una sovranità «infrastrutturale» e una sovranità «costituzionale»[18].

La Spagna costituisce un caso peculiare, perché consente di innestare l'analisi su un ancoraggio costituzionale espresso del rapporto tra tecnologie dell'informazione e garanzie della persona: l'art. 18, c. 4, Cost. del 1978, nel prevedere un limite legislativo all'uso dell'informatica a tutela dell'onore, dell'intimità e del pieno esercizio dei diritti[19], offre infatti un punto di osservazione privilegiato sul modo in cui la dimensione dei diritti *lato sensu* possa interagire con la costruzione di strategie digitali nazionali. A ciò si aggiunge, sul piano politico-programmatico, l'elaborazione di strumenti di indirizzo che cercano di ricomporre in chiave unitaria diritti, innovazione e inclusione, con l'effetto di rendere particolarmente leggibile la tensione (e, al contempo, la complementarità) tra ambizione competitiva e grammatica costituzionale[20].

Polonia e Danimarca sono incluse per ragioni convergenti e, insieme, contrastive. In primo luogo, perché i due Paesi hanno esercitato la Presidenza del Consiglio dell'Unione europea nel 2025 (la Polonia nel semestre gennaio-giugno; la Danimarca nel semestre luglio-dicembre), offrendo due «istantanee» ravvicinate di priorità politiche europee filtrate da interessi nazionali differenti. In secondo luogo, perché consentono di confrontare due declinazioni quasi antitetiche della relazione tra digitale e Stato: la Polonia, collocata sul fianco orientale dell'Unione, tende a leggere la sovranità digitale in chiave di sicurezza (anche informativa) e protezione delle infrastrutture critiche, in un contesto in cui la dimensione geopolitica e la minaccia ibrida fungono da acceleratori di policy; la Danimarca, invece, si presta a essere assunta come caso-limite di amministrazione digitalizzata e di costruzione pragmatica di capacità pubbliche, dove la sovranità tecnologica si manifesta soprattutto come governo efficace di servizi, identità digitale, dati e sicurezza, con un'impronta marcatamente *problem-solving*[21].

La Romania completa il campione con una funzione eminentemente «stress test»: la sua collocazione strategica sul confine orientale dell'Unione, unita alla fragilità che può derivare dall'intreccio tra polarizzazione politica e comunicazione digitale, rende il caso particolarmente istruttivo per analizzare la sovranità digitale come risposta a rischi sistemici. In questa prospettiva, la vicenda elettorale del 2024-2025 – segnata dall'annullamento giudiziario del processo presidenziale e dalla successiva ripetizione delle elezioni sullo sfondo di accuse di interferenze e campagne di disinformazione veicolate tramite piattaforme digitali[22] – mostra in modo paradigmatico come la dimensione digitale incida non soltanto

[18] Cfr. C. Spiniello, *È (ancora) tempo di costituzionalismo digitale,* cit., 590-592.

[19] Precisamente, l'art. 18, c. 4, Cost. stabilisce che «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Un commento al suddetto precetto è stato proposto, tra gli altri, da B. S. L. Toro, *El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas*, in *Revista de la Facultad de Derecho y Ciencias Políticas*, 77, 1987, 107-146.

[20] A partire dal luglio 2021, l'ordinamento spagnolo si è infatti dotato della *Carta de Derechos Digitales*, documento di indirizzo promosso dal *Ministerio de Asuntos Económicos y Transformación Digital* ed elaborato mediante un percorso partecipativo con il coinvolgimento di un gruppo multidisciplinare di esperti. La Carta sistematizza, in chiave «proiettiva», diritti e libertà già riconosciuti nell'ordinamento e ne esplicita alcune declinazioni nel contesto tecnologico; quanto al valore giuridico, è espressamente qualificata come atto non normativo e non vincolante, privo di immediata cogenza, ma destinato a orientare politiche pubbliche e possibili futuri interventi legislativi. Cfr. Gobierno de España, *Carta de Derechos Digitales*, luglio 2021.

[21] In argomento R. F. Jørgensen, *Data and rights in the digital welfare state: the case of Denmark,* in *Information, Communication & Society*, 1, 2023, 123-138.

[22] Hanno trattato l'argomento C. Spiniello, *La seconda volta non si scorda mai. Note a margine sulle elezioni presidenziali rumene 2024-2025*, in *Federalismi.it*, 24, 2025, 263-270; F. Rosa, *L'annullamento delle elezioni presidenziali in Romania*

sull'economia o sull'amministrazione, ma sul cuore stesso della competizione democratica e della fiducia istituzionale.

Il Portogallo, infine, è rilevante perché permette di osservare una declinazione della transizione digitale nella quale acquistano particolare centralità le politiche per le competenze, inclusione e modernizzazione, in un quadro che ambisce a combinare competitività e coesione. Inoltre, la partecipazione – insieme a Italia e Spagna – alla rete «COTEC Europa»[23] consente di mettere a fuoco un livello di circolazione delle idee (tra istituzioni rappresentative e attori dell'innovazione) che, pur non traducendosi automaticamente in normazione, contribuisce a strutturare un vocabolario pubblico sulla sovranità tecnologica e sui suoi presupposti industriali, sociali e valoriali.

Quanto alle fonti, lo studio si concentra (I) sui discorsi dei Capi di Stato, intesi come sedi di elaborazione e legittimazione pubblica dei concetti-chiave, e (II) sulle leggi «digitali» adottate e tuttora vigenti nel medesimo arco temporale considerato per l'analisi discorsiva, ossia dal 2019 al primo semestre del 2025, così da concentrarsi su scelte già consolidate ed escludere, per quanto possibile, progetti di legge o iniziative ancora *in itinere*. La selezione del 2019 come anno di avvio risponde a una ragione sostanziale: è in tale tornante che la nozione di «sovranità digitale» conosce una marcata crescita di visibilità nel lessico politico-istituzionale europeo e, progressivamente, in quello nazionale, divenendo categoria operativa per la costruzione di strategie e priorità[24].

L'analisi combina metodi qualitativi e quantitativi, in una prospettiva interdisciplinare giuridico-politologica: da un lato, una ricognizione giuridica delle principali soluzioni normative adottate; dall'altro, una *content analysis* dei discorsi istituzionali, volta a rilevare frequenze, co-occorrenze e cornici argomentative ricorrenti. L'obiettivo finale è duplice. Ricostruire una mappa comparativa delle strategie digitali nazionali e, sulla base di essa, proporre una prima tipologia delle principali declinazioni della sovranità digitale negli Stati Membri, valutandone la compatibilità – o la tensione – rispetto al progetto europeo di «terza via» digitale.

3. Dati e Tendenze nei discorsi «digitali» dei Capi di Stato. Non è possibile procedere all'illustrazione dei dati emersi dall'analisi dei discorsi «digitali»[25] dei Capi di Stato senza

---

e la difficile difesa della democrazia, in *Federalismi.it*, 15, 2025, 53-75; B. Selejan-Gutan, *The Second Round that Wasn't: Why The Romanian Constitutional Court Annulled the Presidential Elections*, in *VerfBlog*, 7 dicembre 2024.

[23] «COTEC Europa» è la rete trilaterale che riunisce le organizzazioni COTEC di Italia, Spagna e Portogallo, creata per favorire cooperazione e confronto su ricerca, innovazione e competitività, con l'obiettivo di incidere sull'agenda politica europea (in particolare nello spazio euro-mediterraneo) attraverso proposte, iniziative comuni e momenti istituzionali di dialogo.

[24] Di contro, la scelta di arrestare l'osservazione al primo semestre 2025 risponde, anzitutto, a un'esigenza di omogeneità e chiusura del *corpus*: sia i discorsi dei Capi di Stato sia la legislazione «digitale» sono stati raccolti, verificati e codificati entro una finestra temporale definita, così da evitare un aggiornamento «a scorrimento» che avrebbe compromesso la comparabilità tra ordinamenti (non tutti adottano atti con la medesima frequenza) e avrebbe incluso fonti ancora non stabilizzate.

[25] Per «discorso digitale» si intende, in questa sede, un intervento ufficiale del Capo di Stato (o del Sovrano) nel quale le questioni digitali costituiscono l'oggetto principale o comunque prevalente (e non un mero riferimento incidentale). Il *corpus* complessivo include 77 discorsi (gennaio 2019–giugno 2025), raccolti sui siti istituzionali delle Presidenze/Case Reali e sottoposti a codifica semantico-tematica. In particolare, per l'Italia si è fatto riferimento all'Archivio dei discorsi del Quirinale; per la Germania alla sezione *Reden* del *Bundespräsidialamt*; per la Francia ai discorsi dell'*Élysée*; per la Polonia al portale ufficiale del *Prezydent Rzeczypospolitej Polskiej*; per il Portogallo al sito della *Presidência da República Portuguesa*; per la Romania al portale della *Preşedinţia României*; per la Spagna ai discorsi della *Casa de S.M. el Rey*; per la Danimarca ai discorsi ufficiali della Casa Reale danese (*Kongehuset*). Ove disponibili, sono state utilizzate le versioni integrali pubblicate online e i relativi archivi cronologici.

premettere due ordini di considerazioni, l'una di carattere istituzionale e l'altra, più trasversale, relativa al grado di democraticità dei sistemi politici considerati. In primo luogo, l'indagine riguarda Paesi dell'Unione europea accomunati dall'appartenenza ad un ordinamento sovranazionale fondato sullo Stato di diritto, ma contraddistinti da forme di governo e figure di vertice profondamente eterogenee. Repubbliche parlamentari, sistemi semi-presidenziali e monarchie parlamentari rientrano nel novero dei casi analizzati, incidendo in maniera diretta sul perimetro dei poteri, sul tasso di esposizione pubblica e, di riflesso, sulla stessa «densità discorsiva» dei rispettivi Capi di Stato in materia digitale. Tale variabilità istituzionale non è un semplice dato formale; essa rende metodologicamente necessario contestualizzare i risultati quantitativi, distinguendo quanto dipende dall'«attivismo comunicativo» del singolo e quanto, invece, discende da un ruolo costituzionale strutturalmente più o meno idoneo a farsi luogo di elaborazione simbolica, indirizzo valoriale o, nei casi più incisivi, impulso politico[26]. La comparazione qui proposta, pertanto, non assume i Capi di Stato come figure funzionalmente omogenee sotto il profilo dei poteri costituzionali, né intende sovrapporre ordinamenti nei quali il vertice statale svolge funzioni profondamente diverse. L'omogeneità del raffronto va piuttosto rinvenuta sul piano dell'oggetto discorsivo considerato: dichiarazioni pubbliche, messaggi istituzionali e interventi ufficiali nei quali la massima figura rappresentativa dello Stato contribuisce, con intensità e modalità variabili, alla costruzione del lessico pubblico della trasformazione digitale. In questa prospettiva, i discorsi dei Capi di Stato non vengono utilizzati per misurare direttamente l'indirizzo politico dei rispettivi ordinamenti, bensì per cogliere se, quando e attraverso quali categorie il digitale venga tematizzato al livello più alto della rappresentazione istituzionale nazionale[27].

In secondo luogo, pur non rappresentando l'oggetto centrale della ricerca, la «qualità» della democrazia dei sistemi esaminati costituisce una variabile di contesto non eludibile, soprattutto quando l'analisi investe temi – come sovranità digitale, sicurezza, dati personali,

[26] Sul ruolo del Capo di Stato nel diritto comparato europeo si veda F. Clementi, *Garante o governante? La figura del Capo dello Stato nella recente esperienza dei Paesi dell'Unione europea a regime repubblicano*, in *Diritto pubblico comparato ed europeo - Rivista trimestrale*, 3, 2016, 617-638. Più in generale, per un inquadramento sistemico della figura presidenziale si vedano, a titolo esemplificativo, L. Elia, *Governo (forme di)*, in *Enciclopedia del diritto*, vol. XIX, Milano, 1970; C. Mortati, *Le forme di governo*, Padova, 1973; G.U. Rescigno, *Forme di Stato e forme di governo (diritto costituzionale)*, in *Enciclopedia giuridica Treccani*, vol. XIV, Roma, 1989; C. Pinelli, *Forme di Stato e forme di governo*, Napoli, 2006.

[27] La scelta di mantenere nel campione figure istituzionali non perfettamente sovrapponibili risponde, dunque, ad una precisa opzione metodologica. È evidente che, in una prospettiva di micro-comparazione strettamente funzionale, il raffronto tra il Presidente rumeno, eletto direttamente dai cittadini e titolare di un ruolo incisivo nell'architettura dell'esecutivo, il Presidente della Repubblica italiana, organo di garanzia eletto dal Parlamento in seduta comune, e il Re di Spagna, figura di rappresentazione simbolica dell'unità e della permanenza dello Stato, presenterebbe limiti significativi. Tali differenze incidono non solo sull'ampiezza dei poteri formalmente attribuiti, ma anche sul perimetro dell'esternazione pubblica, sul grado di libertà comunicativa e sulla legittimazione ad intervenire su temi politicamente sensibili. L'analisi qui proposta, tuttavia, non mira a comparare l'esercizio di poteri costituzionali omogenei, né a inferire dai discorsi presidenziali o monarchici l'indirizzo politico complessivo dei singoli ordinamenti. Essa assume invece i discorsi dei Capi di Stato come materiali privilegiati per osservare la dimensione simbolico-rappresentativa della trasformazione digitale: vale a dire il modo in cui il digitale entra, o non entra, nel linguaggio pubblico delle figure poste al vertice della rappresentanza statale. In questa prospettiva, la diversità dei ruoli non costituisce un vizio del campione, ma una variabile esplicativa da rendere visibile nell'interpretazione dei risultati. La comparazione opera quindi non tra funzioni costituzionali equivalenti, ma tra modalità differenziate di tematizzazione istituzionale del digitale. Ne consegue che i risultati quantitativi non sono assunti come indicatori immediatamente comparabili di attenzione politica o di maturità normativa, bensì come tracce discorsive da leggere alla luce della forma di governo, della posizione del Capo dello Stato, del grado di esposizione pubblica della carica e del contesto democratico-istituzionale di ciascun ordinamento.

intelligenza artificiale – che implicano, in modo spesso conflittuale, bilanciamenti tra efficienza statale e garanzie, tra interessi strategici e diritti fondamentali. In base alla tipologia *Regimes of the World* (RoW) impiegata dal *V-Dem Institute* (*Democracy Report 2025*)[28], il campione include, da un lato, Stati qualificati come *liberal democracies* (nei quali le elezioni competitive si accompagnano a solidi *checks and balances*, tutela delle libertà civili e primato del diritto) e, dall'altro, Stati qualificati come *electoral democracies* (nei quali, pur in presenza di elezioni, le garanzie istituzionali risultano comparativamente più deboli)[29].

Passando alle variabili istituzionali, il campione comprende due repubbliche parlamentari, nelle quali il Capo dello Stato tende (con intensità diverse) a svolgere una funzione di garanzia e rappresentanza: la Germania e l'Italia. A queste si affiancano quattro sistemi semi-presidenziali: la Francia (nel modello archetipico della V Repubblica) e tre casi che, pur condividendo la presenza di un Presidente eletto e di un Governo responsabile di fronte al Parlamento, presentano assetti di «seconda generazione» e traiettorie politiche differenziate (Polonia, Portogallo e Romania). Infine, due monarchie parlamentari – Spagna e Danimarca – completano il quadro; qui, l'intervento del Sovrano si colloca prevalentemente sul terreno simbolico e valoriale, ma ciò non esclude che, specie in determinati contesti, i discorsi reali divengano cassa di risonanza di priorità nazionali e preoccupazioni collettive legate alla digitalizzazione. Questa eterogeneità – com'è ovvio – implica diverse configurazioni della comunicazione istituzionale. Dove il Presidente dispone di maggiore capacità di indirizzo (o opera entro un sistema altamente personalizzato), la dimensione digitale tende ad essere più frequentemente tematizzata; dove, al contrario, il ruolo è più notarile o cerimoniale, la produzione discorsiva può risultare più rarefatta, pur non necessariamente meno significativa sul piano qualitativo. Proprio per questa ragione, i dati relativi alla frequenza e alla distribuzione dei riferimenti al digitale non possono essere letti isolatamente, ma devono essere interpretati alla luce della posizione costituzionale del Capo dello Stato nel rispettivo ordinamento. La minore occorrenza di riferimenti al digitale nei discorsi di un Sovrano parlamentare o di un Presidente con funzioni prevalentemente di garanzia non indica, di per sé, una minore rilevanza del tema nell'ordinamento considerato; segnala, piuttosto, che quel tema trova verosimilmente altri canali istituzionali di elaborazione. Simmetricamente, una maggiore frequenza di riferimenti nei discorsi di un Presidente politicamente più esposto non può essere automaticamente assunta come indice di una più avanzata cultura costituzionale del digitale, ma va ricondotta anche alla diversa conformazione del ruolo presidenziale e del sistema politico-costituzionale di riferimento.

Nel periodo considerato (2019-prima metà del 2025), la variabile «continuità al vertice» ha inciso in modo non trascurabile. Nelle repubbliche analizzate, la presenza di Capi di Stato riconfermati per un secondo mandato consecutivo[30] ha favorito – almeno potenzialmente –

[28] Pubblicato annualmente dal *V-Dem Institute* dell'Università di Göteborg, il *Global Democracy Index Report* è uno dei più autorevoli e completi strumenti di analisi comparata della qualità delle democrazie nel mondo.

[29] In particolare, secondo la classificazione RoW, nel 2024 Danimarca, Germania, Spagna, Francia e Italia sono qualificati come *liberal democracies* (LD), mentre Portogallo, Polonia e Romania rientrano tra le *electoral democracies* (rispettivamente ED+, ED, ED). L'uso dei segni +/– segnala, secondo il report, un possibile margine di oscillazione della stima, dal momento che il Paese si colloca a ridosso della soglia tra le due categorie, sicché una variazione minima dell'indicatore potrebbe comportarne la riclassificazione, ragione per cui il Portogallo figura come ED+. Cfr. M. Nord, D. Altman, F. Angiolillo, T. Fernandes, A. Good God, S.I. Lindberg, *Democracy Report 2025: 25 Years of Autocratization - Democracy Trumped?,* Gothenburg, 2025, Table 1 e Box 3.

[30] Il Presidente italiano Sergio Mattarella ha svolto il suo primo mandato tra il 2015 e il 2022, per essere poi rieletto – il 29 gennaio di quello stesso anno – per la seconda volta. Il Presidente tedesco Frank-Walter Steinmeier, in carica dal 19 marzo 2017, è stato rieletto il 13 febbraio 2022, per il suo secondo mandato, iniziato il 19 marzo del medesimo anno. Il Presidente francese Emmanuel Macron, per la prima volta in carica dal 2017 al 2022, sta svolgendo il suo secondo mandato dopo la rielezione del 24 aprile 2022. Il Presidente polacco

una maggiore coerenza tematica e la sedimentazione di cornici interpretative riconoscibili nel tempo. Ciò vale, in particolare, per quei casi in cui la dimensione digitale è stata progressivamente incorporata in un repertorio discorsivo stabile (si pensi alla ricorrenza di categorie come diritti, dignità, sicurezza, sovranità, inclusione). Nondimeno, la continuità formale non sempre coincide con una linearità sostanziale: in taluni casi, fattori geopolitici (guerra in Ucraina), *shock* tecnologici (accelerazione dell'IA generativa) o tensioni interne hanno prodotto cambi di accento e slittamenti semantici anche in assenza di avvicendamenti al vertice. Per quanto concerne, invece, i regimi monarchici se la Spagna ha visto una continuità nel regno di Re Filippo VI, il cui ruolo simbolico e rappresentativo si è rafforzato nel tempo anche rispetto alla questione digitale; la Danimarca, al contrario, ha vissuto nel gennaio 2024 un passaggio epocale, con l'abdicazione della Regina Margherita II e l'ascesa al trono del Re Federico X, cui ha fatto seguito un rinnovamento del registro discorsivo e dei temi affrontati.

Venendo ai dati quantitativi, l'analisi del *corpus* evidenzia una disomogeneità marcata nel numero di interventi esplicitamente dedicati – in via esclusiva o prevalente – a temi digitali. La maggiore frequenza si registra nel caso italiano, dove il Presidente della Repubblica ha pronunciato 16 interventi riconducibili al perimetro digitale, delineando, nel complesso, una sorta di agenda presidenziale che intreccia innovazione e garanzie costituzionali, trasformazione tecnologica e diritti fondamentali. Seguono la Francia con 13 interventi e la Spagna con 11, mentre Germania e Polonia registrano 9 discorsi ciascuna; Danimarca e Portogallo si attestano a 7, e la Romania chiude la serie con 5. Tale distribuzione non può essere letta in chiave meramente «numerica». Essa riflette, infatti e congiuntamente, la diversa centralità che la questione digitale assume nelle strategie nazionali; la diversa capacità (o scelta) del Capo dello Stato di tematizzare pubblicamente tali questioni; la diversa collocazione costituzionale delle figure analizzate, che condiziona il grado di intervento nei dibattiti politici e, in generale, l'ampiezza dei registri ammissibili.

Sul piano qualitativo, la codifica semantico-tematica consente di individuare, nel campione, alcune linee di tendenza che attraversano i casi nazionali, senza appiattirne le specificità. In primo luogo, emerge una polarità tra un lessico orientato ai diritti e uno orientato alla sovranità/sicurezza. Nei discorsi di Italia e Spagna la transizione digitale è frequentemente incardinata in una riflessione giuridico-costituzionale: l'innovazione tecnologica è presentata come spazio di opportunità, ma anche come terreno nel quale riaffermare – e aggiornare – il nucleo dei diritti fondamentali, la «qualità» della partecipazione democratica, la necessità di inclusione e la prevenzione di nuove forme di diseguaglianza (*digital divide*, asimmetrie informative, marginalizzazione sociale). In questi casi, l'argomento «diritti digitali» funge da criterio ordinatore, più che da semplice tema tra gli altri, e tende a collocare l'azione pubblica

Andrzej Duda ha svolto il suo doppio mandato tra agosto 2015 e giugno 2025, con un rinnovo intervento nel 2020. Il Presidente portoghese Marcelo Rebelo de Sousa ha esercitato il suo mandato senza soluzione di continuità per l'intero arco temporale considerato, essendo stato eletto per la prima volta nel 2016 e successivamente riconfermato nel 2021. Il Presidente rumeno Klaus Iohannis è stato in carica dal 21 dicembre 2014 al 12 febbraio 2025. Il suo secondo mandato (iniziato nel 2019) si è protratto per alcuni mesi dopo la data ufficiale di termine (dicembre 2024), a causa del già citato annullamento da parte della Corte costituzionale rumena delle elezioni presidenziali del 2024 per sospette interferenze esterne. Nel periodo successivo, le funzioni presidenziali sono state temporaneamente esercitate da Ilie Bolojan, in qualità di Presidente *ad interim*. La successiva tornata elettorale ha portato all'elezione di Nicușor Dan, entrato ufficialmente in carica nel maggio 2025. Considerata la brevità del periodo trascorso dall'inizio del suo mandato, il nuovo Presidente non è stato incluso nell'analisi comparativa finora condotta.

Tale dato – più in generale – apre ad un'interessante riflessione sul tema della riconferma presidenziale (in Europa e nel mondo), la quale pur non trovando opportuno spazio di sviluppo in questa sede è indubbiamente stimolante per l'elaborazione di una ulteriore linea di ricerca.

entro un orizzonte assiologico che richiama, in modo più o meno esplicito, la funzione di garanzia del vertice istituzionale.

In secondo luogo, Francia e Polonia si distinguono per l'uso ricorrente della categoria di «sovranità digitale», ma con declinazioni differenti. In Francia, la sovranità è spesso articolata su un doppio livello: nazionale e, soprattutto, europeo. La retorica presidenziale tende a leggere la sovranità tecnologica come presupposto dell'autonomia strategica dell'Unione europea e della capacità di proteggere cittadini e imprese all'interno di un mercato globale dominato da attori extra-UE. In Polonia, invece, la sovranità è più frequentemente ricondotta a un registro domestico e difensivo: controllo delle infrastrutture critiche, resilienza, sicurezza nazionale, protezione da influenze esterne. Qui, l'evoluzione diacronica appare particolarmente significativa. Nel passaggio dal 2019 al 2025 si osserva, infatti, uno slittamento dalla narrazione entusiastica dell'innovazione globale (con richiami al «modello» statunitense) verso rivendicazioni più assertive di sovranità tecnologica nazionale, coerenti con un contesto regionale segnato da minacce ibride e con una più generale securitizzazione del digitale.

In terzo luogo, il caso tedesco mostra un'interessante asimmetria tra ruolo del Paese nel discorso europeo sulla sovranità digitale e limitata esposizione del Capo dello Stato sul tema. Ciò è in parte spiegabile alla luce della natura prevalentemente rappresentativa della funzione presidenziale in Germania[31]; tuttavia, anche nel *corpus* ristretto, il Presidente federale insiste con regolarità su un'idea di «democratizzazione delle tecnologie», intesa come esigenza di accesso equo, controllo pubblico degli effetti sociali dell'innovazione e protezione dello spazio democratico da manipolazioni e disinformazione. Ne deriva un profilo discorsivo meno centrato sulla sovranità in senso stretto e più orientato alla dimensione sociale e democratica della trasformazione digitale.

In quarto luogo, Portogallo e, in misura parzialmente diversa, la Spagna convergono su una lettura della transizione digitale come leva di giustizia sociale e strumento di rafforzamento dello Stato di diritto. Nei discorsi portoghesi, la digitalizzazione è spesso associata a categorie quali inclusione, coesione e uguaglianza sostanziale: l'innovazione viene rappresentata come opportunità solo se accompagnata da politiche capaci di evitare una «dualizzazione» della società tra inclusi ed esclusi, tra competenze digitali e marginalità tecnologica. Tale registro – pur con peculiarità nazionali – dialoga con quello spagnolo, dove l'enfasi sulla dimensione sociale della digitalizzazione si intreccia con l'idea di una transizione eticamente orientata, anche nel contesto di reti transnazionali (come COTEC) che promuovono innovazione e competitività nello spazio euro-mediterraneo.

Nei regimi monarchici, infine, la dimensione digitale assume contorni peculiari. In Spagna, il Re tende ad integrare l'innovazione in un discorso sulla modernizzazione economica e sulla coesione sociale, valorizzando le opportunità offerte dalle tecnologie per istruzione, mercato del lavoro e competitività. In Danimarca, i messaggi della Regina Margherita II hanno incluso solo episodicamente riferimenti al digitale, con un tono prevalentemente simbolico; tuttavia, come detto, il passaggio al Re Federico X ha coinciso con un'evoluzione sensibile del registro discorsivo, segnato da maggiore attenzione a sostenibilità tecnologica, educazione digitale, modernizzazione amministrativa e – più spesso rispetto agli altri casi – ai rischi e alle prospettive legati all'intelligenza artificiale. Tale dinamica suggerisce che, anche in contesti a forte simbolismo istituzionale, la trasformazione digitale può diventare un tema «abilitante» per ridefinire, in chiave contemporanea, la funzione rappresentativa del vertice dello Stato.

[31] In argomento G. Uhl, *Das Staatsoberhaupt in der deutschen Verfassungsgeschichte. Die Bürden des Bundespräsidenten*, in *GWP-Gesellschaft. Wirtschaft. Politik*, 2, 2012, 23-24.

Quanto alla Romania, la limitata numerosità degli interventi si accompagna ad un profilo tematico relativamente omogeneo. Ivi, la digitalizzazione è presentata soprattutto come strumento di ammodernamento istituzionale (efficienza, trasparenza, integrità), più che come campo di conflitto valoriale tra diritti, sicurezza e sovranità. Ciò non implica assenza di rilevanza politica, ma segnala una specifica traiettoria discorsiva, in cui il digitale è prevalentemente inscritto nel quadro del rafforzamento delle capacità amministrative e delle istituzioni, in un contesto nazionale e regionale segnato da tensioni geopolitiche e da crescente centralità della dimensione tecnologica nei processi politico-istituzionali interni.
Nel complesso, l'analisi comparata mostra un crescente protagonismo dei Presidenti della Repubblica e dei Sovrani nella costruzione delle narrative pubbliche sulla digitalizzazione. Tale protagonismo resta, per definizione, in larga parte simbolico, dal momento che non sostituisce la funzione di indirizzo e decisione attribuita agli organi di governo, né può garantire di per sé una traduzione normativa coerente. Tuttavia, è indubbio che i Capi di Stato svolgano un ruolo non trascurabile nel definire le cornici valoriali entro cui la transizione digitale viene presentata ai cittadini. Ora come spazio di tutela e aggiornamento dei diritti, ora come terreno di sicurezza e sovranità, ora come politica di inclusione e coesione, ora come leva di efficienza amministrativa.

4. Legislazioni digitali nazionali a confronto. Per ricostruire in modo più solido le traiettorie nazionali della digitalizzazione, accanto ai discorsi dei Capi di Stato si è reso necessario lavorare su un secondo *corpus* di fonti: gli atti normativi nazionali adottati tra il 2019 e il primo semestre del 2025 e tuttora vigenti, selezionati in modo da includere soltanto misure dotate di forza giuridica vincolante (leggi in senso proprio e atti aventi forza di legge)[32], ed escludere invece strategie, piani, linee guida e, più in generale, documenti di *policy* non cogenti. Una simile delimitazione – che inevitabilmente «taglia fuori» una parte significativa dell'azione pubblica sul digitale, spesso veicolata da atti amministrativi e documenti programmatici – è tuttavia funzionale a isolare quelle scelte che il legislatore ha ritenuto meritevoli di traduzione in precetti giuridici immediatamente operativi, e che quindi rivelano, più di altre, le priorità effettive dei sistemi politici in esame.
Ne deriva un'analisi che, in questa fase, non ambisce a comparare nel merito ogni singola disciplina[33], ma mira a una prima sistematizzazione per ambiti, così da individuare (I) i settori in cui si registra una convergenza più marcata, (II) le aree in cui persistono divergenze strutturali, (III) le dinamiche temporali che segnalano «accelerazioni» o «svolte» legislative.
Un primo elemento di contesto, decisivo per comprendere la fisionomia del *corpus*, è il vincolo europeo come fattore di omogeneizzazione selettiva. La produzione normativa nazionale, infatti, tende a concentrarsi soprattutto sull'attuazione di direttive e sull'adeguamento organizzativo richiesto dall'evoluzione dell'*acquis* (in particolare in materia di sicurezza delle reti e dei sistemi informativi) nonché sulla predisposizione di capacità amministrative e

[32] Il *corpus* normativo è composto da 51 atti di rango primario adottati tra gennaio 2019 e giugno 2025 e vigenti alla data del 30 giugno 2025. La ricognizione è stata effettuata tramite consultazione delle banche dati ufficiali e delle Gazzette nazionali: per la Francia, *Journal officiel* e portale *Légifrance*; per la Germania, *Bundesgesetzblatt* e portale federale *Gesetze im Internet*; per l'Italia, *Normattiva* e *Gazzetta Ufficiale*; per la Spagna, *Boletín Oficial del Estado*; per la Danimarca, banca dati *Retsinformation*; per la Polonia, *Dziennik Ustaw* e sistema ISAP; per il Portogallo, *Diário da República Eletrónico*; per la Romania, *Monitorul Oficial* e portali istituzionali di legislazione. Per ciascun atto sono stati annotati estremi, data, oggetto e ambito materiale (cybersecurity, e-government/servizi pubblici, dati e infrastrutture, diritti digitali), verificandone la vigenza mediante i testi consolidati disponibili sui suddetti repertori

[33] Un'eventuale comparazione contenutistica – anche rispetto alla cornice della strategia digitale europea – potrà rappresentare un naturale sviluppo di ricerca futuro.

infrastrutturali funzionali ai nuovi obblighi e standard europei[34]. Questo «effetto cornice» – contrariamente a quello sarebbe naturale aspettarsi – non produce, però, una convergenza uniforme. Mentre, infatti, in alcuni settori (si pensi alla *cybersecurity*) le fonti europee stimolano interventi nazionali relativamente omogenei quanto a obiettivi, pur con differenze di tecnica normativa e di governance; in altri ambiti il diritto dell'Unione lascia spazio a scelte nazionali più idiosincratiche, specie quando si tratta di assetti istituzionali interni, architetture di controllo, opzioni di centralizzazione amministrativa o modulazioni del bilanciamento tra efficienza, sicurezza e garanzie.

In parallelo, la pandemia da COVID-19 ha operato come catalizzatore, trasformando la digitalizzazione dei servizi pubblici da obiettivo programmatico a urgenza amministrativa, con effetti visibili, seppure diseguali, anche sul piano legislativo. Tuttavia, la «accelerazione pandemica» non si è tradotta ovunque in un incremento lineare di leggi, producendo talora norme cornice (o correttivi) destinate ad abilitare procedure digitali e canali telematici, altre volte, spingendo verso la concentrazione di competenze e la costruzione di infrastrutture nazionali e lasciando ai livelli amministrativi il compito di rendere effettiva la transizione.

Sotto il profilo tematico, il primo asse comparativo – e, al tempo stesso, il terreno di maggiore convergenza – è indubbiamente la sicurezza digitale (*cybersecurity*) e, più in generale, la tendenza alla securitizzazione del digitale. Pur con tecniche normative differenti, gli ordinamenti esaminati hanno rafforzato (o riordinato) gli obblighi relativi alla protezione delle infrastrutture critiche, delle filiere tecnologiche sensibili e delle pubbliche amministrazioni. Qui la convergenza è forte non tanto perché identiche siano le soluzioni, quanto perché condivisa è l'idea di fondo. La dipendenza tecnologica e la vulnerabilità delle reti sono percepite, cioè, come rischi sistemici, che investono insieme continuità dei servizi essenziali, sicurezza nazionale e fiducia dei cittadini nella capacità dello Stato di assicurare protezione in un dominio permeato da attori privati e interdipendenze transnazionali. Ad esempio, in Italia, tale direttrice si manifesta in modo emblematico sia nel consolidamento del perimetro di sicurezza nazionale cibernetica, sia nell'istituzione dell'Agenzia per la cybersicurezza nazionale, con conseguente riorganizzazione di competenze e funzioni di prevenzione e risposta agli incidenti[35]. In Germania, la stessa traiettoria emerge nel potenziamento del quadro di sicurezza per sistemi informatici e operatori rilevanti e, più in generale, nella progressiva istituzionalizzazione di apparati e strumenti dedicati alla sicurezza informatica, spesso letta anche come presupposto della sovranità tecnologica[36]. In Romania, il «nodo sicurezza» tende a intrecciarsi in modo particolarmente evidente con la dimensione geopolitica e con la protezione delle infrastrutture e delle reti di nuova generazione, nonché con l'esigenza di irrobustire capacità di difesa cibernetica in un contesto regionale caratterizzato da vulnerabilità e pressioni esterne[37].

---

[34] Per un inquadramento della disciplina relativa all'efficacia degli atti dell'Unione europea negli ordinamenti interni, si vedano, tra gli Altri, R. Adam, A. Tizzano, *Manuale di diritto dell'Unione europea*, Torino, 2024; U. Villani, *Istituzioni di diritto dell'Unione europea*, Bari, 2024; G. Tesauro, *Manuale di diritto dell'Unione europea*, vol. I, IV ed., Napoli, 2023; P. Craig, G. de Búrca, *EU Law: Text, Cases, and Materials*, Oxford, 2020; D. Chalmers, G. Davies, G. Monti, *European Union Law: Text and Materials*, Cambridge, 2019.

[35] L. 18 novembre 2019, n. 133, *Conversione in legge, con modificazioni, del d.l. 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, in G.U., Serie gen., n. 272, 20 novembre 2019; d.l. 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*, in G.U., Serie gen., n. 140, 14 giugno 2021, conv. con modif. in l. 4 agosto 2021, n. 109, in G.U., Serie gen., n. 185, 4 agosto 2021.

[36] *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (*IT-Sicherheitsgesetz 2.0*), 18 maggio 2021, in BGBl. I, 2021, Nr. 25, 27 maggio 2021, 1122 ss.

[37] *Legea nr. 163 din 11 iunie 2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G*, in *Monitorul Oficial*, nr. 590, 11 giugno 2021; *Legea nr. 58 din 14*

Un secondo asse – quantitativamente rilevante e qualitativamente rivelatore delle priorità nazionali – riguarda la digitalizzazione della pubblica amministrazione e la trasformazione delle modalità di interazione tra Stato e cittadini (*e-government*, identità digitale, accesso ai servizi, comunicazioni ufficiali, interoperabilità). Qui la scelta di positivizzare in legge requisiti tecnici e standard organizzativi non è uniforme, ma resta correlata al grado di «maturità» digitale preesistente, alla struttura amministrativa (centralizzata o composita), alla disponibilità di infrastrutture abilitanti e alla propensione dei legislatori a «normativizzare» processi che altrove restano affidati a regolazione tecnica o a prassi amministrative. In alcuni casi, l'obiettivo è rendere effettivo un diritto (o un'aspettativa) all'accesso digitale ai servizi; in altri, la priorità è garantire la continuità e l'affidabilità del canale telematico quale modalità ordinaria di relazione con l'amministrazione, con conseguenti questioni di inclusione, di tutela delle categorie vulnerabili e di compatibilità tra automatizzazione procedimentale e garanzie partecipative. Nel caso tedesco, per esempio, la traiettoria passa per interventi che puntano a rendere effettivo l'accesso digitale ai servizi pubblici e a costruire basi dati interoperabili, anche in funzione del principio *digital by default* e della riduzione delle dipendenze tecnologiche nella pubblica amministrazione federale[38]. In Polonia, un indicatore significativo della medesima direttrice è la disciplina delle consegne elettroniche quale modalità di comunicazione ufficiale, con un ampliamento progressivo dei soggetti tenuti ad avvalersi del canale digitale, segno di una scelta legislativa orientata alla «normalizzazione» giuridica della comunicazione telematica nei rapporti con le istituzioni[39]. In Danimarca – spesso considerata un termine di paragone, per l'elevato livello di digitalizzazione amministrativa – la centralità dell'identità digitale come infrastruttura abilitante del *digital welfare state* rende particolarmente istruttivo osservare come il legislatore consolidi, nel tempo, regole, responsabilità e standard di affidabilità dei sistemi di accesso ai servizi pubblici digitali[40].

Un terzo asse riguarda la regolazione dello spazio digitale in chiave di ordine pubblico, tutela degli utenti e responsabilizzazione degli attori online. Si tratta di un ambito che, nel contesto europeo, tende sempre più a dialogare (e talora ad entrare in competizione) con la disciplina sovranazionale – soprattutto laddove si incida su piattaforme, contenuti e servizi intermediari – e nel quale i legislatori nazionali si muovono spesso lungo un crinale delicato, ossia rafforzare la protezione (di minori, consumatori, vittime di illeciti *online*) senza compromettere coerenza e primato del diritto dell'Unione e senza sovrapporre regimi che rischiano di produrre frammentazione. In Francia, la l. del 21 maggio 2024 (c.d. SREN)[41] costituisce un riferimento centrale, poiché interviene su più fronti (protezione in rete, poteri regolatori, contrasto a fenomeni illeciti *online*), mostrando come la sicurezza possa tradursi anche in un ampliamento degli strumenti di intervento pubblico nello spazio digitale; al contempo, parte della dottrina ne ha evidenziato limiti di sistematicità e una marcata tecnicità,

---

martie 2023 privind securitatea ş i apărarea cibernetică a României, precum ş i pentru modificarea ş i completarea unor acte normative, in *Monitorul Oficial*, nr. 214, 15 marzo 2023.

[38] *Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze* (*Registermodernisierungsgesetz* - RegMoG), 28 marzo 2021, in BGBl. I, 2021, 591 ss.; *Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen* (*Onlinezugangsgesetz* – OZG), 14 agosto 2017, in BGBl. I, 2017, 3122.

[39] *Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych*, in Dz.U., 2020, poz. 2320. Tala disciplina prevede, in particolare, un'applicazione progressiva mediante disposizioni transitorie e scaglionamento degli obblighi per categorie di soggetti.

[40] *Bekendtgørelse af lov om MitID og NemLog-in*, LBK nr. 333, 19 marzo 2025 (testo consolidato della *Lov* nr. 783, 4 maggio 2021, come modificata, tra l'altro, dalla *Lov* nr. 1559, 12 dicembre 2023).

[41] L.n. 449/2024, *visant à sécuriser et à réguler l'espace numérique* (c.d. SREN), in JORF, n. 0117, 22 maggio 2024 (NOR: ECOI2309270L).

specie là dove la disciplina nazionale finisce per ricalcare opzioni già tracciate a livello europeo[42]. In Spagna, invece, la legislazione del periodo considerato appare meno orientata alla costruzione di un catalogo vincolante di diritti digitali in senso stretto e più concentrata su settori regolati, mentre la già ricordata *Carta dei diritti digitali* resta, per espressa qualificazione istituzionale, documento di indirizzo privo di forza vincolante.

Infine, un quarto asse – spesso sottotraccia, ma cruciale per leggere le tensioni tra integrazione europea e autonomia strategica – concerne dati e infrastrutture (*cloud* pubblico, governance del dato, filiere tecnologiche, requisiti di affidabilità dei fornitori). Qui la dimensione «sovranità» tende a emergere non tanto in formule dichiarative, quanto in scelte normative che incidono su controllo, sicurezza, requisiti di localizzazione o di certificazione, regole di *procurement* e architetture di gestione del dato pubblico. È però proprio in questo punto che la scelta metodologica di escludere fonti non cogenti pesa maggiormente. Molte decisioni strategiche su infrastrutture e dati, infatti, transitano per strategie nazionali, atti amministrativi, bandi e strumenti di finanziamento, che non sempre si traducono immediatamente in leggi. Ne consegue un risultato comparativo non banale: la sovranità digitale può essere fortemente evocata nella retorica politica e nei documenti programmatici, ma rimanere «meno visibile» nel *corpus* legislativo, oppure apparire in forme indirette (regole di sicurezza e di affidabilità) più che come proclamazione esplicita.

Nel complesso, il confronto tra legislazioni nazionali restituisce almeno tre evidenze trasversali. Primo, la *cybersecurity* opera come minimo comun denominatore e come «porta d'ingresso» privilegiata della sovranità tecnologica nelle normative interne, perché consente di legare immediatamente digitale, rischio e responsabilità pubblica. Secondo, l'*e-government* e l'identità digitale funzionano da moltiplicatori di capacità statale, ma con intensità e tecniche di positivizzazione molto differenti; dove l'amministrazione è già strutturalmente digitalizzata, la legge tende a consolidare e rifinire; dove invece la transizione è ancora incompleta, la legge spesso interviene come strumento di accelerazione, ma la sua efficacia dipende dalla capacità attuativa. Terzo, la dimensione dei diritti digitali, fuori dall'alveo della protezione dei dati personali, fatica a tradursi in strumenti legislativi vincolanti, con una frequente divaricazione tra retoriche costituzionali, carte/manifesti non cogenti e produzione normativa effettiva (dinamica che, nella comparazione, emerge con particolare nettezza nei casi in cui i diritti sono molto presenti nella narrazione istituzionale ma meno nella legislazione «dura»). Su questo sfondo, la «terza via» europea sembra essere recepita dagli Stati Membri in modo selettivo: là dove il digitale è letto come questione di sicurezza e resilienza, l'intervento legislativo tende a essere più rapido e strutturato; là dove è letto primariamente come questione di diritti (in senso lato), la traduzione in norme vincolanti risulta – almeno entro il perimetro temporale considerato – più intermittente e frammentaria.

5. Una (prima) riflessione conclusiva. Il confronto tra i due insiemi di fonti esaminati – i discorsi dei Capi di Stato e la legislazione «digitale» nazionale vigente – consente di formulare alcune riflessioni conclusive che, pur rimanendo inevitabilmente provvisorie, perché legate a un segmento temporale delimitato e a un fenomeno in rapida trasformazione, risultano comunque sufficienti a mettere in luce un profilo di fondo. La traduzione nazionale della «terza via» europea appare allo stato attuale selettiva, asimmetrica e, in taluni casi, strutturalmente sbilanciata a favore delle categorie di sovranità e sicurezza, mentre il lessico e l'architettura dei diritti faticano a consolidarsi in un diritto positivo coerente.

[42] Così P. Mouron, *La loi visant à sécuriser et réguler l'espace numérique est promulguée*, in *Revue européenne des médias et du numérique*, 67-70, 2024, 35-39.

Issn 2421-0528

In primo luogo, emerge un disallineamento tra retorica istituzionale e tecniche legislative. Nei discorsi pubblici – specie nei contesti in cui il Capo dello Stato può fare leva su un ruolo simbolico capace di orientare il lessico valoriale del dibattito – la trasformazione digitale viene frequentemente inquadrata come questione di democrazia costituzionale: limiti ai poteri privati, salvaguardia della libertà, inclusione, protezione della persona e responsabilità degli attori tecnologici. In tale cornice, i riferimenti alla necessità di evitare nuove forme di soggezione (pubblica o privata) e di garantire un «controllo democratico» sugli ecosistemi digitali si presentano come elementi ricorrenti, in linea con l'impostazione europea che collega, in modo esplicito, sovranità tecnologica, sicurezza e valori democratici.

Sul piano normativo, al contrario, la traiettoria appare più circoscritta e meno ricettiva della componente propriamente costituzionalista. Le leggi nazionali del periodo considerato tendono a concentrarsi, con maggiore densità e continuità, su (a) *cybersecurity*, protezione delle infrastrutture critiche e costruzione di capacità statali di prevenzione e risposta; (b) digitalizzazione amministrativa e infrastrutture abilitanti; (c) misure settoriali di regolazione o ordine pubblico digitale, spesso con una logica reattiva. Ne deriva una divaricazione non solo quantitativa (più norme su sicurezza e apparati; meno norme su diritti «oltre» la protezione dei dati), ma anche qualitativa. Mentre la securitizzazione produce dispositivi giuridicamente robusti e istituzionalmente «visibili», la tutela dei diritti digitali – intesa come libertà sostanziali, non discriminazione algoritmica, trasparenza e garanzie procedurali effettive – resta spesso confinata a richiami di principio o a strumenti non vincolanti, senza approdare a un catalogo legislativo organico.

In secondo luogo, l'esito della comparazione suggerisce che la categoria della «sovranità digitale» opera, negli ordinamenti nazionali, come concetto «ponte» ma anche come potenziale fattore di ambiguità. Da un lato, essa consente di legittimare – in modo politicamente spendibile – investimenti pubblici, scelte industriali e requisiti di affidabilità delle filiere (dati, *cloud*, reti). Dall'altro, proprio la forza evocativa della sovranità rischia di favorire un'osmosi semantica tra il progetto europeo (che ambisce a combinare sovranità e diritti) e posture più strettamente sovraniste o difensive, in cui la sicurezza tende a divenire la chiave interpretativa dominante dell'intera agenda digitale[43].

In terzo luogo, la lettura congiunta delle fonti consente di inserire una variabile che, nel campo digitale, è spesso sottovalutata ma decisiva: la «qualità» della democrazia del contesto istituzionale come condizione abilitante (o, al contrario, come vincolo) della traduzione dei principi in garanzie. Senza assumere in modo meccanico un nesso causale, i principali indicatori comparativi evidenziano, nel campione, uno spettro significativo. Stati con livelli elevati di democrazia liberale (come Danimarca, Francia, Germania, e – su valori comunque alti – Spagna, Portogallo e Italia) e contesti più fragili o più esposti a dinamiche di erosione (in particolare Polonia e Romania). Questa eterogeneità incide sulla «capacità di diritti» dell'ordinamento digitale, ossia sulla probabilità che misure di sicurezza e modernizzazione amministrativa vengano accompagnate da architetture di *accountability*, controlli indipendenti, garanzie procedurali e spazi di partecipazione. In altri termini, la sovranità tecnologica può essere costruita come sovranità democratica (diritti come limiti e come condizioni dell'innovazione) oppure come sovranità prevalentemente amministrativa (efficienza e controllo come criteri guida): la differenza, spesso, è data dal grado di istituzionalizzazione dei contro-poteri e dalla resilienza dello Stato di diritto.

In quarto luogo, l'analisi mette in luce una frizione verticale – non sempre esplicita, ma crescente – tra il livello europeo e quello statale. L'Unione europea ha progressivamente costruito un impianto regolativo che, almeno nelle sue intenzioni, non si limita a «mettere

[43] Sul punto E. Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, cit., 211-228.

ordine» nel mercato digitale, ma mira a predisporre limiti e responsabilità per i poteri privati e a preservare l'ordinamento democratico nell'ecosistema digitale, innestando la logica della tutela dei diritti nella disciplina delle piattaforme e dei servizi. Al livello statale, invece, l'adeguamento tende spesso a manifestarsi come costruzione di capacità amministrative e di sicurezza funzionali agli obblighi europei e come intervento settoriale su infrastrutture e procedure, più che come sviluppo di un diritto nazionale dei diritti digitali coerente con la cornice valoriale dell'Unione. Il paradosso che ne discende è che, mentre il diritto europeo spinge – almeno in parte – verso forme di *accountability* democratica delle architetture digitali, molte legislazioni nazionali, pur pienamente legittime e spesso necessarie, appaiono ancora principalmente orientate a rispondere a esigenze di protezione ed efficienza, lasciando sullo sfondo la questione della positivizzazione dei diritti digitali in senso forte.

Tali evidenze consentono una valutazione più mirata del rischio evocato sin dall'avvio del contributo, ossia che la sovranità digitale divenga la categoria egemone, capace di assorbire o marginalizzare la dimensione costituzionalista anziché integrarla. Il rischio è tutt'altro che teorico. Se la sovranità viene costruita in chiave soprattutto securitaria, l'esito più verosimile è l'espansione di poteri, apparati e logiche tecnocratiche, accompagnata da un indebolimento degli spazi partecipativi e delle garanzie. Se, invece, la sovranità è intesa come capacità pubblica orientata ai diritti, la sicurezza può essere ricondotta alla funzione di strumento al servizio dello Stato costituzionale, e non assunta come suo surrogato. È su questo crinale che si misura la tenuta della «terza via» europea, non tanto nella quantità di norme prodotte, quanto nella capacità di assicurare che innovazione e resilienza digitale non siano perseguite a detrimento delle garanzie, ma attraverso garanzie.

In conclusione, il periodo 2019-primo semestre 2025 restituisce l'immagine di un'Unione europea che tenta di istituzionalizzare una «terza via» tra autoregolazione privata e controllo statale pervasivo, e Stati membri che recepiscono tale impulso in modo diseguale, apparendo essi più pronti a legiferare dove il digitale è percepito come rischio e meno attenti a tradurre in norme vincolanti la parte più innovativa del progetto europeo, quella che mira a fare del digitale un terreno di espansione – e non di contrazione – dei diritti e della democrazia costituzionale. Resta allora aperta la questione di fondo: la sovranità digitale europea riuscirà a mantenersi, nella prassi multilivello, come sovranità «con» i diritti e a non a costruirsi, invece, in opposizione, «contro», gli stessi diritti?

Abstract. Il contributo indaga se e in che misura gli assi del discorso dell'Unione europea su sovranità digitale e costituzionalismo digitale trovino corrispondenza nelle strategie degli Stati membri dell'UE. L'analisi comparata si concentra su otto casi (Francia, Germania, Italia, Spagna, Polonia, Danimarca, Portogallo, Romania), selezionati secondo un criterio di «massima variazione». Il disegno di ricerca combina due *corpus* di dati (entrambi ricompresi nell'orizzonte temporale 2019-primo semestre 2025): i discorsi politici dei Capi di Stato e gli atti legislativi nazionali «digitali», sottoposti a codifica semantico-tematica e sistematizzazione per ambiti materiali. I risultati mostrano una convergenza robusta su sicurezza e resilienza, mentre la dimensione dei diritti fatica a tradursi in norme vincolanti. Ne emerge un recepimento selettivo della «terza via» europea: più avanzato sul versante securitario-tecnologico, più disomogeneo su garanzie e *accountability* democratiche.

Abstract. This paper examines whether, and to what extent, the key pillars of the European Union discourse on digital sovereignty and digital constitutionalism are reflected in the strategies of EU Member States. The comparative analysis focuses on eight cases (France, Germany, Italy, Spain, Poland, Denmark, Portugal, Romania), selected according to a «maximum variation» criterion. The research design combines two datasets (both within the

2019-first half of 2025 time frame): Heads of State political speeches and national «digital» legislative acts, analysed through semantic-thematic coding and mapped across substantive policy domains. The findings show strong convergence around security and resilience, whereas the rights dimension struggles to crystallise into binding rules. Overall, the EU «third way» is internalised selectively: more advanced on the securitised-technological front, and more uneven with regard to safeguards and democratic accountability.

Parole chiave. Sovranità digitale – Costituzionalismo digitale – Unione europea – Stati membri UE – analisi comparata.

Key words. Digital sovereignty – Digital constitutionalism – European Union – EU Member States – Comparative analysis.