POLICY PAPERS

Fondazione CSF

DIGITALIZZAZIONE E INTEGRAZIONE: IL CONTRIBUTO BALTICO A UN'EUROPA FEDERALE

IL BEREC COME PUNTO DI PARTENZA

VERONICA SACCO

SETTEMBRE 2025

NUOVA SERIE N. 007

Veronica Sacco

veronica.sacco@uniroma3.it

Junior Fellow Fondazione CSF

Abstract

La trasformazione digitale rappresenta una sfida cruciale e un'opportunità strategica per l'Unione Europea, non più limitata all'introduzione di strumenti tecnologici, ma orientata a ridefinire la relazione tra Stato e cittadino, i diritti e le forme di partecipazione democratica. In un contesto globale dominato dalla competizione tra Stati Uniti e Cina, l'Europa si trova di fronte a una scelta: restare un mosaico di soluzioni nazionali o avanzare verso una governance digitale federale. L'esperienza dei Paesi baltici costituisce un laboratorio privilegiato. L'Estonia, in particolare, ha dimostrato come leadership politica, interoperabilità e fiducia dei cittadini possano trasformare un piccolo Stato in un pioniere globale dell'e-government: identità digitale universale, piattaforma X-Road per lo scambio sicuro dei dati, voto online e cartelle cliniche digitali hanno rafforzato efficienza e trasparenza.

Analogamente, la Lettonia ospita il BEREC, organismo che coordina i regolatori delle comunicazioni elettroniche, mentre la Lituania sviluppa soluzioni innovative in ambito fintech, blockchain e sicurezza dei dati. Tuttavia, il modello europeo rimane frammentato e intergovernativo, con rischi di inefficienza, scarsa interoperabilità e vulnerabilità cibernetiche. In questo quadro, l'esperienza baltica indica la necessità di un salto federale: la creazione di una *European Digital Agency*, evoluzione del BEREC, con poteri vincolanti in materia di standard, certificazioni e resilienza. La digitalizzazione federale europea permetterebbe di superare il digital divide, rafforzare il mercato unico e consolidare la fiducia dei cittadini, affermando al contempo l'UE come polo regolatorio globale. Come la BCE ha reso irreversibile l'integrazione economica, così un'Agenzia Digitale Europea potrebbe inaugurare la prima federazione digitale della storia.

Parole chiave: Trasformazione digitale, Baltico, Stati Baltici, Digital transformation, Digital federalism, Baltic States, e-Government, European Digital Identity (EUDI), Cybersecurity, BEREC, European Digital Agency.

Introduzione

La trasformazione digitale rappresenta una delle principali sfide e opportunità per l'Unione Europea. Non si tratta più soltanto di introdurre strumenti tecnologici, ma di ripensare la relazione tra Stato e cittadino, ridefinendo diritti, doveri e modalità di partecipazione democratica. In un contesto globale segnato dalla competizione tra grandi potenze tecnologiche – Stati Uniti e Cina *in primis* – l'Europa deve decidere se restare un mosaico di esperienze nazionali o avanzare verso un modello federale di governance digitale.

I Paesi baltici offrono un punto di osservazione privilegiato. L'indipendenza riacquistata nel 1991 li ha posti di fronte alla necessità di ricostruire quasi da zero le istituzioni pubbliche. Privi di risorse economiche comparabili a quelle dell'Europa occidentale, hanno scelto di puntare sull'innovazione digitale come strumento di efficienza, trasparenza e legittimazione politica.

La dimensione ridotta, combinata con forte volontà politica e sostegno internazionale, ha reso possibile una sperimentazione che altrove sarebbe stata più lenta e complessa. In particolare, l'esperienza estone e quella lettone possono guidare un'agenda di federalizzazione digitale europea, intesa come costruzione di un'infrastruttura comune per servizi pubblici digitali e identità elettronica.

L'interesse dell'UE per questo traguardo è evidente. Nel 2021 la Commissione ha adottato il *Digital Compass 2030*, fissando obiettivi ambiziosi: almeno l'80% della popolazione con competenze digitali di base; connettività a banda larga ovunque; 5G in tutti i centri abitati; accesso online a tutti i principali servizi pubblici. Parallelamente sono stati approvati *Digital Services Act* e *Digital Markets Act* (regole per servizi digitali e piattaforme dominanti), il *Data Governance Act* (per la condivisione dei dati in sicurezza) e avviata la sperimentazione dell'*European Digital Identity Wallet* per consentire ai cittadini l'accesso transfrontaliero ai servizi con un'identità digitale unica. A questo quadro si è aggiunto l'AI Act, che pone standard europei sull'intelligenza artificiale.

Nonostante tali progressi, il modello europeo resta essenzialmente intergovernativo. Gli Stati membri conservano ampi margini di autonomia, con il rischio di soluzioni frammentate, poco interoperabili e non scalabili. L'assenza di un'istituzione centrale forte indebolisce la capacità dell'UE di competere a livello globale e di proteggere i cittadini da minacce cibernetiche sempre più sofisticate. Le sfide sono interconnesse: frammentazione normativa e tecnica, che limita la mobilità dei cittadini e la fluidità del mercato unico; *cybersecurity* disomogenea, che espone l'Unione a minacce esterne e interne; *digital divide* tra regioni e gruppi sociali, con rischio di nuove forme di esclusione; fiducia democratica a rischio se mancano privacy, trasparenza e sicurezza (anche per l'adozione dell'e-ID europea).

Lezioni dal Baltico

In questo panorama, il Baltico propone una via per “fare ordine”. L’Estonia è il caso emblematico di come una scelta politica consapevole possa trasformare un piccolo Stato in laboratorio globale di innovazione digitale. Negli anni immediatamente successivi all’indipendenza le risorse erano scarse e la macchina statale andava ricostruita. La leadership di Lennart Meri e la visione promossa da Toomas Hendrik Ilves con il programma *Tiigrihüpe* (Tiger Leap) segnarono una svolta: bypassare la modernizzazione analogica e puntare da subito su internet, pagamenti elettronici e telefonia mobile[1]. L’idea di fondo era chiara: uno Stato troppo piccolo per una burocrazia estesa doveva cercare efficienza, trasparenza e competitività attraverso il digitale.

Entro due anni dal lancio del programma, tutte le scuole erano connesse a internet, segno che la digitalizzazione era anche investimento educativo e generazionale.

Nel 2002 l’Estonia introdusse l’identità digitale universale, utilizzabile per operazioni bancarie, fiscali e accesso ai servizi pubblici. A sostegno, la piattaforma X-Road – sviluppata già nel 1996 a seguito di un grave *data leak* – ha reso possibile la circolazione sicura e interoperabile dei dati tra istituzioni e privati, grazie alla cifratura end-to-end e al superamento dei silos informativi; varianti del modello sono state adottate in oltre venti Paesi, dalla Finlandia alla Colombia[2].

L’identità digitale ha rafforzato anche la partecipazione civica. Nel 2005 l’Estonia ha introdotto il voto online; nel 2019 oltre metà dell’elettorato ha votato in rete. La piattaforma Rahvaalgatus, collegata all’e-ID, consente iniziative civiche digitali che, superate 1000 firme certificate, devono essere discusse dal Parlamento.

Dal 2008 tutte le cartelle cliniche sono digitali; circa 200.000 cittadini hanno donato il proprio DNA alla biobanca nazionale, abilitando ricerca e screening personalizzati con strumenti di IA. Ciò ha migliorato i servizi e aperto nuovi spazi per la collaborazione scientifica e industriale[3].

Accanto ai successi, emergono fragilità: la dipendenza dal digitale espone a rischi considerevoli. Nel 2024 un attacco hacker ha colpito quasi metà della popolazione adulta, con furto di milioni di dati personali e sanitari. La lezione estone è duplice: leadership, rapidità di esecuzione e fiducia dei cittadini sono decisive; ma occorre resilienza continua per evitare vulnerabilità sistemiche. Non a caso, la celebre frase di Meri — “*time threatens to become a scarce resource. We must count the weeks and months*” — riassume la filosofia che ha guidato la trasformazione: trattare il tempo come risorsa scarsa da capitalizzare con l’innovazione[4].

Lezioni dal Baltico

Per l'UE, la lezione è anch'essa duplice: replicare interoperabilità e fiducia facendo dell'e-ID e dell'*e-government* strumenti federali; evitare al contempo la dipendenza da un unico modello, costruendo sistemi resilienti, diversificati e sicuri.

Da qui tre possibili percorsi:

1. **coordinamento soft** (raccomandazioni UE, piena autonomia nazionale: flessibilità ma maggiore frammentazione);
2. **modello ibrido** (standard tecnici comuni con attuazione nazionale: equilibrio tra unità e sovranità, ma possibili divergenze applicative);
3. **federalizzazione piena** (istituzione di un'Agenzia Digitale Europea con poteri vincolanti su standard, certificazioni e monitoraggio). È questa terza via che appare necessaria per garantire coerenza, efficienza e fiducia.

Il BEREC: un buon punto di partenza

Un precedente rilevante è il *Body of European Regulators for Electronic Communications* (BEREC), istituito nel 2009 e operativo dal 2010, con sede a Riga. BEREC coordina i regolatori nazionali delle comunicazioni elettroniche, garantendo coerenza nell'applicazione delle regole del mercato unico digitale. Nel tempo si è affermato come punto di riferimento per gli Stati membri, lavorando in stretto coordinamento con Commissione e Parlamento, ma mantenendo indipendenza tecnica. Composto dalle NRAs (autorità nazionali di regolazione), ha sviluppato una metodologia di lavoro consensuale e multilivello che armonizza le regole rispettando le diversità locali.

In un contesto di crescente complessità geopolitica e tecnologica, questa esperienza dimostra l'efficacia della cooperazione regolatoria, ma anche il bisogno di poteri più incisivi e centralizzati.

Con la *Draft Strategy 2026–2030* (BoR (25) 80), BEREC delinea cinque priorità che costituiscono una vera roadmap tecnico-politica per l'Europa digitale:

1. **Connettività e Mercato Unico Digitale:** VHCN, migrazione a 5G Standalone, avvio del 6G, resilienza dei cavi sottomarini e integrazione delle NTN (LEO e Device-to-Device) per un'Europa connessa, autonoma e competitiva.
2. **Ecosistemi aperti e competitivi:** contrasto alle concentrazioni di potere dei CAPs (CDN, data center, cavi proprietari) e garanzia di level playing field tra telco e piattaforme.
3. **Diritti degli utenti:** aggiornamento di open internet, tutele su QoS e slicing, trasparenza, misure anti-frode e protezione da pratiche manipolative e rischi AI.
4. **Sostenibilità, sicurezza e resilienza:** reti a basse emissioni, approccio zero-trust, cooperazione con ENISA e attuazione della direttiva NIS, con attenzione al contesto geopolitico.
5. **Capacità istituzionali e regolazione data-driven:** cooperazione con ETSI, Eurostat, EU SPA, ITU e OECD, armonizzazione della raccolta dati e passaggio a un approccio proattivo.

Il BEREC: un buon punto di partenza

Questa traiettoria suggerisce l'evoluzione del BEREC verso una European Digital Agency dotata di poteri vincolanti in materia di interoperabilità, sicurezza, certificazioni e standardizzazione – un percorso analogo a quello dall'IME alla BCE: da coordinamento tecnico a istituzione federale con poteri diretti e indipendenti. La nuova Agenzia potrebbe ispirarsi al modello BEREC (o integrarlo), ampliandone il perimetro oltre le comunicazioni elettroniche a identità digitale europea, interoperabilità dei servizi pubblici, gestione dei dati e resilienza cibernetica. La localizzazione nei Paesi baltici – con BEREC a Riga e il NATO *Cooperative Cyber Defence Centre* a Tallinn – rafforzerebbe il ruolo della regione come hub digitale e di sicurezza dell'UE.

Il contributo baltico è quindi cruciale: Estonia: digitalizzazione come pilastro della cittadinanza democratica; Lettonia: resilienza delle infrastrutture critiche e sede del BEREC; Lituania: integrazione tra innovazione (*fintech, blockchain, AI*) e sicurezza dei dati.

Queste esperienze possono confluire in un *Baltic–EU Digital Lab*, hub europeo di sperimentazione e formazione per lo scambio di competenze e l'adozione di buone pratiche negli altri Stati membri. La collocazione geografica e istituzionale del Baltico ne fa già oggi un polo strategico euro-atlantico: oltre a BEREC a Riga e al centro NATO a Tallinn, Vilnius ospita il *NATO Energy Security Centre*. Questo network rende la regione una cerniera UE–NATO capace di guidare la costruzione di una resilienza ibrida europea.

Accanto a infrastrutture e servizi, la federazione digitale deve includere politiche sociali e formative: alfabetizzazione digitale, riduzione del digital divide, sostegno alle fasce vulnerabili e incentivi alla formazione dei lavoratori. Nei sistemi scolastici di Estonia, Lettonia e Lituania, la digitalizzazione è integrata sin dalle prime fasi: robotica educativa, programmazione e pensiero computazionale già nella scuola primaria.

Ciò riduce il divario generazionale, rende la popolazione più resiliente all'innovazione e rafforza il capitale umano necessario a un ecosistema competitivo, alimentando start-up, centri di ricerca e partnership pubblico-private. Non sorprende che Tallinn e Riga siano oggi hub tecnologici in grado di attrarre investimenti e sviluppare soluzioni replicabili su scala europea.

Guardando avanti, l'UE deve anche dotarsi di una strategia federale di resilienza cibernetica: cloud sovrano europeo, sistemi di allerta precoce, capacità condivise di risposta agli incidenti e esercitazioni congiunte regolari.

La digitalizzazione non è più un'opzione ma una necessità strategica. I Paesi baltici hanno dimostrato che la tecnologia può rafforzare democrazia, trasparenza e qualità dei servizi. L'UE ha ora l'opportunità di fare un salto di qualità, passando da un modello frammentato a una vera federazione digitale. La creazione di una *European Digital Agency*, naturale evoluzione del BEREC, non sarebbe un mero esercizio tecnico, ma un atto politico costituente:

- all'interno, eliminerebbe la frammentazione, rafforzando il Mercato Unico Digitale e la fiducia dei cittadini;
- all'esterno, affermerebbe l'Europa come polo regolatorio globale, capace di competere con Stati Uniti e Cina.

Come la BCE ha reso irreversibile l'integrazione economica, così un'Agenzia Digitale Europea renderebbe irreversibile l'integrazione politica del XXI secolo, dando vita alla prima federazione digitale della storia. L'alternativa è restare un mosaico di iniziative nazionali; la scelta federale, invece, consoliderebbe autonomia strategica, coesione e legittimità democratica dell'Unione.

Una possibile Road Map

Priorità	Azione chiave	Strumenti UE	Scadenze indicative	Responsabili	Esito atteso entro 2030
Identità digitale unica	Diffusione dell'European Digital Identity Wallet (EUDI)	eIDAS 2	2025–2026: roll-out cittadino/PA	Stati membri, Commissione, (futura) EDA	Accesso transfrontaliero ai servizi pubblici/privati
Interoperabilità PA	Modelli dati comuni, API e principio "once-only"	Interoperable Europe Act	2025–2027: piani nazionali e implementazione	Stati/PA, Commissione	Pratiche online valide in tutta l'UE senza re-upload
Connettività gigabit	VHCN, 5G SA (verso 6G), permessi più rapidi	Gigabit Infrastructure Act	Da 11/2025: applicazione; 2027–2028: upgrade rete	Stati, regolatori (BEREC)	5G in tutti i centri abitati; fibra diffusa
Sicurezza & resilienza	Baseline comune, certificazioni, zero-trust	NIS2, CRA, DORA, EUCC/ENISA	2026: NIS2 a regime; 2027–2028: certificazioni	Stati, ENISA, autorità settoriali	Prodotti/servizi "secure-by-design", meno incidenti
Mercati & dati	Enforcement piattaforme; spazi dati settoriali	DSA, DMA, Data Act, DGA	2025–2027: enforcement e data spaces	Commissione, autorità nazionali	Concorrenza leale, riuso dati pubblici/privati
Capacità federali	Creare una European Digital Agency	Evoluzione da BEREC	2025: proposta; 2026: operatività iniziale	Parlamento, Consiglio, Commissione	Standard unici, certificazioni, audit UE
Baltic–EU Digital Lab	Formazione, interoperabilità, cyber-esercitazioni	Best practice EE/LV/LT + NATO COE	2026: avvio hub regionale	Stati baltici, Commissione/EDA	Soluzioni scalabili e maggiore resilienza

Abbreviazioni
EDA = European Digital Agency (proposta)
VHCN = Very High-Capacity Networks
5G SA = 5G Standalone
CRA = Cyber Resilience Act
DGA = Data Governance Act
DORA = Reg. resilienza operativa digitale finanza

In breve, L'Europa può diventare una federazione digitale in cinque passi principali, tutti già previsti in realtà dalle norme UE più recenti.

1 **Un'unica identità digitale per entrare ovunque**
Ogni cittadino/impresa usa il *Digital Identity Wallet* (EUDI) per accedere a servizi pubblici e privati in qualunque Paese UE. È il cuore della riforma eIDAS 2: meno password, più servizi transfrontalieri, più fiducia.

2 **Servizi pubblici che "parlano la stessa lingua"**
Con l'*Interoperable Europe Act* la PA progetta servizi e dati compatibili fin dall'inizio (modelli dati comuni, API condivise, principio *once only*). Così un certificato emesso in uno Stato funziona subito negli altri.

Una possibile Road Map

3 **Reti veloci dappertutto**
Perché tutto giri, servono fibra e 5G “standalone” ovunque. Il *Gigabit Infrastructure Act* semplifica scavi, permessi e condivisione di infrastrutture per arrivarci prima.
Sicurezza come standard, non come optional

4 **Sicurezza come standard, non come optional**
Regole comuni contro gli attacchi: NIS2 per i settori essenziali, *Cyber Resilience Act* per prodotti digitali più sicuri, DORA per la finanza, e un AI Act che impone valutazioni del rischio dove serve.

5 **Mercati equi e dati che circolano**
DSA e DMA tengono in riga i grandi intermediari digitali; *Data Act e Data Governance Act* sbloccano l’uso dei dati (pubblici/privati) in modo equo e sicuro.

Non sprecare per non rimanere indietro

Risulta importante non sprecare quello che già abbiamo, ovvero è fondamentale sfruttare quello che già funziona; guardiamo dunque al BEREC (l’agenzia che coordina i regolatori TLC, con sede a Riga) è un modello pronto da “potenziare”. La sua Strategia 2026–2030 (bozza) va proprio in quella direzione: connettività gigabit, mercati aperti, diritti utenti, resilienza e raccolta dati migliore. Da qui può nascere, per evoluzione, una *European Digital Agency* con poteri chiari su standard, certificazioni e monitoraggio.

Rimanere indietro nella trasformazione digitale ha un costo economico misurabile: la frammentazione riduce produttività e crescita, mentre un’integrazione ambiziosa genera benefici significativi per il PIL europeo[5]. In un mercato globale sempre più competitivo, capitali e talenti convergono dove trovano regole chiare, tempi rapidi e capacità di calcolo accessibile; se l’UE non accelera su standard comuni e adozione, la convenienza si sposta altrove[7].

Il rischio è che il divario di competenze e l’uso dell’IA nelle imprese — soprattutto nelle PMI — si cristallizzino: oggi poco più della metà dei cittadini possiede competenze digitali di base e l’adozione di IA resta contenuta[7].

Sul piano infrastrutturale, non basta “coprire” il territorio: conta l’uso effettivo di 5G/5GSA e l’integrazione con reti fisse ad altissima capacità; dove l’adozione è bassa rallentano automazione, IoT e servizi a bassa latenza[8]. In parallelo, il profilo di rischio cyber aumenta e senza resilienza la fiducia dei cittadini vacilla: gli attacchi ransomware e i grandi furti di dati — come il caso estone nel settore farmacie — mostrano quanto rapidamente possa erodersi la legittimità dell’identità e dei servizi digitali[9]. Per evitare un’Europa “a velocità diverse”, serve un coordinamento federale che definisca standard, certificazioni e audit comuni, seguendo la traiettoria già tracciata da BEREC e sostenuta dai nuovi quadri regolatori sull’interoperabilità e sulla sicurezza dei prodotti digitali[10].

Conclusioni

Il Baltico insegna che la digitalizzazione funziona quando si combinano leadership politica, progettazione *interoperable-by-design*, fiducia dei cittadini e resilienza. L'Estonia lo mostra da vent'anni: identità digitale universale, scambio dati sicuro con *X-Road/X-tee*, servizi *once only* e persino voto online su larga scala — non un vezzo tecnologico, ma un modo per rendere lo Stato più vicino, trasparente ed efficiente[11]. La lezione è duplice: il digitale può rafforzare la democrazia e la qualità dei servizi, ma senza cyber-igiene continua e architetture zero-trust la fiducia si rompe in fretta, come ricorda il grande furto dati nel settore farmacie nel 2024[12].

Lettonia e Lituania completano il quadro: Riga ospita BEREC, prova che il coordinamento regolatorio europeo può essere concreto e incisivo; Vilnius e Tallinn sono nodi euro-atlantici per la sicurezza e l'energia, utili a esercitazioni congiunte e risposta agli incidenti. Portare questa esperienza a livello UE significa passare da un mosaico di iniziative a una federazione digitale: standard comuni, certificazioni e audit europei, con un coordinamento centrale forte sul modello BEREC, evolvendo verso una European Digital Agency. È la via più rapida per trasformare gli obiettivi della Digital Decade in risultati misurabili, evitando il "costo del non-Europa" e consolidando autonomia strategica, crescita e fiducia dei cittadini[13].

Note

[1]Moody O. (2025), *Baltic The Future of Europe*, Murray, p. 33.

[2]Idem, p. 34.

[3]Idem, p. 35.

[4]Idem, p 27.

[5]European Parliamentary Research Service (EPRS). (2023). *The cost of non-Europe in the Single Market (digital chapter)*. https://www.europarl.europa.eu/thinktank

[6]European Commission. (2024). *State of the Digital Decade 2024 report*. https://digital-strategy.ec.europa.eu

[7]Eurostat. (2024a). *Individuals' level of digital skills (Statistics Explained*). *https://ec.europa.eu/eurostat/statistics-explained/*;
Eurostat. (2024b). *Artificial intelligence use by enterprises (Statistics Explained)*. https://ec.europa.eu/eurostat/statistics-explained/

[8]European 5G Observatory. (2024). *Quarterly report*. *https://5gobservatory.eu/*;
European Parliament & Council. (2024d). *Regulation (EU) 2024/1309 (Gigabit Infrastructure Act)*. https://eur-lex.europa.eu/eli/reg/2024/1309/oj/eng

[9]ENISA. (2024). *ENISA Threat Landscape 2024*. *https://www.enisa.europa.eu/publications*

[10]BEREC. (2025). *Public consultation on the draft BEREC Strategy 2026–2030*. *https://www.berec.europa.eu/en/public-consultations-calls-for-inputs/public-consultation-on-the-draft-berec-strategy-2026-2030*;
European Parliament & Council. (2024b). *Regulation (EU) 2024/903 (Interoperable Europe Act)*. https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng;
European Parliament & Council. (2024c). *Regulation (EU) 2024/2847 (Cyber Resilience Act)*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[11]Drechsler, W. (2018). *Digital governance and post-Soviet transformation: The Estonian case;*
e-Governance Academy. (2023). *Digital transformation in the Baltic States*;
Madise, Ü., & Vinkel, P. (2020). *Internet voting in Estonia: From local to European elections*.

[12]Tiirmaa-Klaar, H. (2022). *Cybersecurity policy in the EU and the Baltics*;
ERR News. (2024, April 3). *Cybercriminals steal data of around 700,000 Apotheka pharmacy customers*. https://news.err.ee/1609302096/cybercriminals-steal-data-of-around-700-000-apotheka-pharmacy-customers

[13]BEREC. (2025). *Public consultation on the draft BEREC Strategy 2026–2030*. https://www.berec.europa.eu/en/public-consultations-calls-for-inputs/public-consultation-on-the-draft-berec-strategy-2026-2030;
European Parliamentary Research Service (EPRS). (2023). *The cost of non-Europe in the Single Market (digital chapter)*. https://www.europarl.europa.eu/thinktank

POLICY PAPERS

Fondazione CSF

SETTEMBRE 2025

NUOVA SERIE N. 007

Fondazione CSF
Piazza Vincenzo Arbarello 8
10122 Torino
Tel.+39 011 15630 890
www.fondazionecsf.it