I LIMITI GIURIDICI DELLA NUOVA PROPOSTA DI REGOLAMENTO SULLA *CYBERSECURITY*: I PRINCIPI DELL'UE E LE GARANZIE COSTITUZIONALI ITALIANE [*]

di Michele Trotta[**], Giuseppe Libutti[***], Sergio Santoro[****] e Giampiero Buonomo[*****]

Sommario. 1. Il quadro normativo europeo sulla *cybersecurity* nel segno della sovranità tecnologica. – 2. Il problema della base giuridica e le possibili violazioni del CSA2. – 3. Conclusioni. Il rischio di un ampio contenzioso e la necessità di un approccio multilivello.

1. Il quadro normativo europeo sulla* cybersecurity *nel segno della sovranità tecnologica. Desta non poche riflessioni la progressiva evoluzione del processo di integrazione dell'Unione europea, che dalla primiera funzione di sostegno e coordinamento delle competenze degli Stati membri, pare orientarsi verso una sempre più marcata tendenza a sostituirsi ad essi in ambiti che i Trattati riservano alla loro competenza primaria.

In questo quadro si inserisce la proposta di regolamento COM(2026) 11, noto anche come *Cyber Security Act* 2[1], il quale si inscrive nel più ampio sviluppo della disciplina europea in materia di cybersicurezza trovando il suo fondamento programmatico nei concetti di «sovranità tecnologica europea» e «sovranità digitale» elaborati negli anni dalla dottrina[2] e dalle istituzioni politiche eurounitarie[3]. Tale mutamento riflette una tendenza dell'Unione ad assumere funzioni sempre più assimilabili a quelle statuali, estendendo il proprio intervento oltre il tradizionale ambito del mercato interno fino a incidere su settori quali politica industriale, sviluppo tecnologico e sicurezza[4].

Questa dinamica segnala una nuova fase del processo di integrazione europea, caratterizzata

---

[*] *Sottoposto a referaggio.*

[**] Avvocato – Foro di Roma.

[***] Avvocato – Foro di Roma.

[****] Presidente aggiunto del Consiglio di Stato.

[*****] Consigliere parlamentare.

[1] Proposta di regolamento COM(2026) 11. Presentata dalla Commissione Europea il 20 gennaio 2026 per aggiornare e rafforzare il precedente regolamento (UE) 2019/881 (chiamato anche CSA1), da ora in poi è citata anche come CSA2.

[2] S. Couture, S. Toupin, *What does the notion of "sovereignty" mean when referring to the digital?*, New Media & Society, 2019, 21(10), 2305-2322.

[3] La sovranità digitale è stata definita in modo piuttosto vago come «Europe's ability to act independently in the digital world»: vedi T. Madiega, *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Papers). European Parliamentary Research Service, 2020.

[4] V. *Berlin Declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020*, European Commission, 2020. V. anche J. Borrell, «Perché l'autonomia strategica europea è importante», Blog dell'Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza / Vicepresidente della Commissione, 3/12/2020.

dall'adozione di strumenti regolatori potenzialmente capaci di incidere direttamente su ambiti sino ad oggi riservati agli Stati membri, come ad esempio la sicurezza[5]. Ne derivano possibili tensioni con l'attuale assetto dei Trattati, sia sotto il profilo della compatibilità giuridica, sia in termini di legittimazione democratica, in ragione della natura mista dei processi decisionali dell'Unione.

La proposta CSA2 vede la sua genesi nel percorso della strategia industriale europea e si fonda dunque su una lettura della sovranità tecnologica che trasforma esigenze economiche del mercato interno in giustificazione per interventi normativi di selezione dei partner commerciali basati su criteri di natura non esclusivamente tecnica[6] o economica, bensì orientati da valutazioni di carattere geopolitico.

Tale approccio si basa sull'assunto che la dipendenza da tecnologie extra-UE nei settori critici rappresenti un rischio per la sicurezza e la resilienza dell'Unione[7]: «in merito alla vendita di beni e servizi in certi settori come la *cybersicurezza*, ciò può comportare dipendenze tecnologiche, fughe di dati se non addirittura la perdita del dominio su tecnologie e risorse critiche o il pericolo di essere sorvegliati da soggetti non statali»[8] o da soggetti statali che – sulla scorta di un asserito utilizzo non democratico a livello interno – potrebbero utilizzare la libertà di mercato per controllare o condizionare gli affari interni dello Stato cui appartiene l'acquirente[9].

Si tratta di una questione dirimente ai fini della stessa configurazione dell'assetto costituzionale dei poteri pubblici negli odierni ordinamenti. Infatti l'influenza delle nuove tecnologie sui pubblici poteri ed i condizionamenti che esse producono sugli elementi costitutivi dello Stato, ossia il popolo, il territorio e la Sovranità, attengono alle «modalità di esercizio delle funzioni fondamentali, legislativa, giudiziaria e amministrativa»[10]. Si impone quindi estrema prudenza nell'applicare un modello unico di fonte sovranazionale, essendo ben noto il pericolo che attraverso il relativo sistema di produzione normativo si possa scavalcare la riserva di legge presente in molte Costituzioni degli Stati membri: è solo il Parlamento nazionale che può imporre determinate modalità di esercizio del potere giurisdizionale o amministrativo.

Nei rapporti sugli incidenti informatici allegati alla proposta di regolamento[11] emerge, dunque, una sostanza che non può essere indifferente al modo in cui si declina la «norma sulle fonti» contenuta nei Trattati europei: una omissione di tale rilettura critica rischierebbe di non cogliere in tempo possibili invasioni della iniziativa legislativa della Commissione dal campo della regolamentazione del mercato a quello della sicurezza che i Trattati riservano agli Stati membri.

2. Il problema della base giuridica e le possibili violazioni del CSA2. Tale evoluzione

---

[5] F. G. Burwell, K. Propp, *The European Union and the Search for Digital Sovereignty:Building "Fortress Europe" or Preparing for a New World?*, Atlantic Council Future Europe Initiative, 2020.

[6] P. Timmers, *Challenged by 'Digital Sovereignty'*, Journal of Internet Law, 2019, 23(6).

[7] Si veda il Preambolo della proposta di regolamento CSA2.

[8] L. Marilotti, *La mano invisibile. Sicurezza nazionale e garanzia del mercato nel diritto amministrativo*, Milano, 2025.

[9] L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1, 2018, 62 ss.

[10] L. Casini, *Lo Stato taumaturgo nell'era dei big data* (doi: 10.1402/107332), il Mulino (ISSN 0027-3120), 2, 2023, 82.

[11] ENISA, *Threat Landscape 2025*. Dai dati empirici richiamati, in particolare nei rapporti ENISA, emerge che la maggior parte degli incidenti informatici deriva da vulnerabilità tecniche e comportamentali (*phishing*, *ransomware*, errori di configurazione), mentre i rischi legati alla *supply chain* risultano meno frequenti e riconducibili soprattutto a fenomeni di cyberspionaggio. Nonostante ciò, la proposta sembra privilegiare un approccio basato sulla limitazione dell'accesso al mercato per operatori stranieri quale strumento di sicurezza.

non si manifesta in modo isolato con la proposta CSA2, ma si inserisce in una traiettoria già da tempo avviata nell'ordinamento europeo, caratterizzata da una progressiva estensione dell'intervento dell'Unione in materia di cybersicurezza come si può evincere già dalle precedenti iniziative normative in materia, tra cui si rammentano le direttive NIS, la direttiva CER, il *Cyber Resilience Act*[12].

Già a questo stadio primigenio della normativa eurounitaria di settore, si presentarono necessità di contemperamento di interessi potenzialmente divergenti, come di recente ricordato da EDPB (Comitato europeo per la protezione dei dati) e EDPS (Garante europeo della protezione dei dati)[13], secondo i quali il rapporto tra protezione dei dati e sicurezza informatica è bidirezionale. Infatti, è ben vero che la sicurezza informatica contribuisce alla protezione dei dati personali limitando i rischi di accesso non autorizzato; ma si può altrettanto osservare come alcune misure di sicurezza informatica possano interferire con i diritti e le libertà delle persone, in particolare con il diritto alla vita privata e alla protezione dei dati: è quindi, opportuno adottarsi un approccio che tenga conto dei principi di necessità e proporzionalità.

In tale contesto, l'azione delle istituzioni europee si è articolata lungo due direttrici principali: da un lato, il rafforzamento della cooperazione e del monitoraggio delle criticità della cybersicurezza attraverso la creazione dell'Agenzia dell'Unione Europea per la cybersicurezza (ENISA); dall'altro, lo sviluppo del tentativo di armonizzazione tecnica mediante l'adozione di sistemi di certificazione di conformità dei componenti e dei servizi ICT (c.d. sistema europeo di certificazione ECCF) [14].

La proposta di regolamento CSA2 rappresenta tuttavia, nei propositi della Commissione, un'evoluzione qualitativa. Viene anzitutto previsto un ampliamento delle funzioni regolatorie e di coordinamento di ENISA e sono introdotti strumenti più incisivi, come l'obbligatorietà dei sistemi di certificazione – sino ad oggi adottati su base volontaria – in alcuni settori critici, come quello per le telecomunicazioni[15]. In secondo luogo sono prospettate misure restrittive sulle catene di approvvigionamento basate su criteri non tecnici rivolte, nei fatti, a limitare l'accesso al mercato europeo degli operatori stranieri provenienti da Paesi ritenuti «non sicuri».

Ciò osservato, il regolamento proposto dalla Commissione presenta numerosi profili di criticità tanto con riferimento al rispetto dei principi di attribuzione (art. 5 TUE, 114 TFUE), di proporzionalità e sussidiarietà (art. 5, par. 4, TUE), quanto con riferimento ai profili di diritto interno dei Paesi membri.

In primo luogo, il nodo centrale riguarda la base giuridica individuata nell'art. 114 TFUE, tradizionalmente utilizzato per l'armonizzazione del mercato interno. Alla luce della giurisprudenza della Corte di giustizia tale base è ritenuta legittima solo quando il mercato interno costituisce il reale centro di gravità dell'intervento. Così nella sentenza *Tobacco Advertising I* viene osservato che «interpretare tale articolo [art. 114 TFUE già art. 95 TCE] nel senso che attribuisca al legislatore comunitario una competenza generale a disciplinare il mercato interno non solo sarebbe contrario al tenore stesso delle disposizioni citate, ma sarebbe altresì incompatibile con il principio sancito all'art. 3 B del Trattato CE (divenuto art.

[12] Direttiva (UE) 2016/1148 (NIS1); Direttiva (UE) 2022/2555 (NIS2); Direttiva (UE) 2022/2557 (CER); Regolamento (EU) 2024/2847 (CRA).

[13] Cfr. il parere EDPB-EDPS 18 marzo 2026 [*Joint Opinion* 4/2026] sulla proposta della Commissione europea in merito all'introduzione del nuovo Regolamento sulla sicurezza informatica *Cybersecurity Act* 2 (CSA 2), e sulla proposta di modifica della Direttiva *Network and Information Security* 2, c.d. NIS 2 (2022/2555/UE).

[14] Si tratta di uno strumento di attestazione dell'affidabilità tecnica di un fornitore sino ad oggi utilizzato su base volontaria e disciplinato da CSA1 e NIS; v. regolamento (UE) 2019/881.

[15] Art. 110 CSA2.

5 CE – oggi art. 5 TUE), secondo cui le competenze della Comunità sono competenze di attribuzione»[16].
Il CSA2, invece, sembra perseguire obiettivi ulteriori, legati alla sicurezza tecnologica e alla sovranità strategica, introducendo strumenti che incidono direttamente sulla selezione dei fornitori e sull'accesso al mercato sulla base di criteri non tecnici.
In particolare, il nuovo sistema di certificazione ECCF (Titolo III della proposta) evolve da strumento neutrale di conformità tecnica di un dispositivo tecnologico a meccanismo potenzialmente selettivo di affidabilità di un fornitore basato su criteri di sicurezza, come risulta in particolare dal combinato disposto degli artt. 85 e 100[17].
Parimenti estranee a criteri tecnici appaiono le norme sulla catena di approvvigionamento (Titolo IV della proposta) le quali attribuiscono alla Commissione poteri incisivi come quello di designare un Paese terzo come fonte di problemi sulla sicurezza (art. 100) e di escludere dai settori critici del mercato (NIS2, All. I e II) gli operatori da esso provenienti o ad esso in qualche modo connessi (su tutti art. 103). Trattasi dunque di un potere di valutazione geopolitica che potrebbe risolversi nella introduzione di barriere di accesso al mercato europeo per fornitori di dispositivi o di servizi in ragione della loro riconducibilità a Paesi privi di requisiti di affidabilità variamente definiti, tra cui spicca quanto a genericità quello dell'assenza di meccanismi di controllo «indipendenti e democratici» (cfr. art. 100, par. 1, lett. *a)-e)*).
Ciò accentuerebbe inevitabilmente quello slittamento dalla logica del mercato interno, propria del perimetro stabilito dall'art. 114 TFUE, ad una logica di sicurezza basata su valutazioni di carattere geopolitico, che era stata già rilevata nelle precedenti iniziative eurounitarie in materia di cibersicurezza[18], ma che risulta ancor più caratterizzare la proposta di regolamento in commento. Corollario ne è il rischio di violazione del principio di attribuzione sancito dai Trattati con la possibile invadenza delle competenze degli Stati membri.
A tali criticità si aggiungono ulteriori profili di illegittimità afferenti al rispetto dei principi di proporzionalità e sussidiarietà prescritti dall'art. 5, par. 4, TUE.
Sotto il profilo della proporzionalità, le misure appaiono eccessive rispetto agli obiettivi perseguiti, in quanto basate su criteri non direttamente correlati ai rischi tecnici e sostituibili con strumenti meno restrittivi[19]. È stato sottolineato, infatti, come dai rapporti richiamati nel Preambolo si evinca che i principali incidenti siano riconducibili al *Phishing*, al *Ransomware* e ai *malware*, e dunque dipendano da vulnerabilità in gran parte comportamentali o di cattiva configurazione dei sistemi, non attribuibili all'affidabilità dei fornitori dei dispositivi ICT[20].
Né i problemi rappresentati dalla riscontrata arretratezza tecnologica delle reti informative

[16] Corte di giustizia dell'Unione europea, sent. 5 ottobre 2000, causa C-376/98, *Tobacco Advertising I*, § 83. Vedi anche, sempre della Corte di Giustizia: sent. 13 luglio 1995, causa C-350/92, *Spagna/Consiglio*, § 35; sent. 9 ottobre 2001, causa C-377/98, *Paesi Bassi/Parlamento e Consiglio*, § 15; sent. 10 dicembre 2002, causa C-491/01, *British American Tobacco (Investments) e Imperial Tobacco*, § 61; sent. 14 dicembre 2004, causa C-434/2002, *Arnold André*, § 31; sent. 9 settembre 2001, causa C-198/2001, *Swedish Match*, § 30; sent. 12 luglio 2005, cause riunite C-154/04 e C-155/04, *Alliance for Natural Health e a.*, § 29.
[17] Le aperture a fattori non puramente tecnici si riscontrano nel combinato disposto di cui all'art. 85 e all'art. 100, par. 4, lett. *c)* e *d)*) che esclude i fornitori ad alto rischio - individuati secondo le procedure di cui al Titolo IV - dalla possibilità di diventare organismi di valutazione della conformità accreditati ai sensi del Titolo III.
[18] Sara Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, I Post di AISDUE, III (2021), aisdue.eu Sezione «Atti convegni AISDUE», 5, 20 dicembre 2021 Annali AISDUE, ISSN 2723-9969.
[19] Sul bilanciamento tra gli oneri imposti e i benefici perseguiti v. *ex multis* Corte di giustizia dell'Unione europea, sent. 13 novembre 1990, causa C-331/88, *Fedesa*, § 13; Corte di giustizia, sent. 8 giugno 2010, causa C-58/08, Vodafone, § 51.
[20] ENISA *Threat Landscape 2025*, cit.

europee, e dalla loro conseguente vulnerabilità, sembrano essere riconducibili alla inaffidabilità dei fornitori stranieri, quanto al contrario al basso livello degli investimenti delle aziende europee[21].

Quanto alla sussidiarietà, non risulta dimostrato che un intervento così centralizzato sia necessario rispetto alle competenze e agli strumenti già disponibili a livello nazionale e nell'ambito della cooperazione prevista dalla NIS2. Un esempio su tutti è rappresentato dall'esperienza d'Oltralpe sull'utilizzo con efficacia dello strumento dell'azione speciale, comunemente indicata con l'espressione *golden share*, che fa parte dell'arsenale giuridico adottato al fine di completare il controllo sugli *asset* strategici combinando strumenti di polizia amministrativa con quelli di tipo societario[22].

Ulteriori possibili violazioni potrebbero riscontrarsi con riferimento alle libertà del mercato interno (artt. 34–36 TFUE), in quanto le restrizioni fondate sull'origine dei fornitori possono configurare misure di effetto equivalente e discriminazioni indirette[23]. Infine, rilevanti questioni di compatibilità si pongono con la Carta dei diritti fondamentali dell'Unione europea, la quale, come noto, è stata resa giuridicamente vincolante per le istituzioni UE e per gli Stati membri quando attuano il diritto unionale ai sensi dell'art. 6 del Trattato sull'Unione europea (TUE). Essa contiene previsioni a tutela della libertà di impresa (art. 16), del diritto di proprietà (art. 17) e del principio di non discriminazione (artt. 20 e 21) la cui compressione può essere giustificata solamente nel rispetto del principio di proporzionalità come statuito dalla costante giurisprudenza della Corte di Giustizia dell'Unione europea[24].

Analoghi dubbi emergono, ancorché con riferimento all'applicazione della normativa UE negli Stati Membri, rispetto ai principi sanciti dalla Convenzione europea dei diritti dell'uomo (CEDU). Ciò con particolare riguardo al diritto di proprietà e al divieto di discriminazione, nonché alla libertà d'impresa così come ricavati dalla giurisprudenza della Corte europea dei diritti dell'uomo in applicazione dell'art. 1 del primo Protocollo addizionale e dell'art. 14 della Convenzione.

Nella disamina delle implicazioni dell'art. 1 del primo Protocollo addizionale alla CEDU[25], la Corte europea dei diritti umani da tempo ha affermato la necessità che l'ingerenza dello Stato nel godimento del diritto di proprietà può avvenire solo in seguito ad un *fair balance* tra «esigenze di interesse generale e l'imperativo di salvaguardia dei diritti fondamentali dell'individuo»[26]. Segnatamente, la Corte di Strasburgo ha rilevato che l'art. 1 del Protocollo addizionale non si limita alla proprietà in senso stretto, ma comprende anche interessi

[21] Nel Rapporto Draghi sulla competitività UE del 2024 si sottolinea, specialmente con riferimento alle telecomunicazioni, che le problematiche del mercato europeo sono riconducibili alla frammentazione degli operatori e ad un basso livello degli investimenti (v. M. Draghi, *The future of European competitiveness Part B*, In-depth analysis and recommendations, 2024, § 3.1, 68).

[22] Nella modulazione di questi poteri, alcuni Stati esteri dispongono di strumenti contrattuali particolarmente incisivi – quali i *proxy agreements* in USA – che consentono una rigorosa separazione delle informazioni strategiche (v. S. Clavel et D. Chekroun, *Golden share (action spécifique) et contrôle des investissements étrangers: vers une gouvernance de la sécurité économique?*, Dalloz actualité, 13 mars 2026).

[23] Tale principio, elaborato sin dalla giurisprudenza Dassonville, è stato ulteriormente sviluppato nella sentenza Cassis de Dijon e costituisce uno dei pilastri del mercato interno.

[24] V., tra le altre, della Corte di Giustizia dell'Unione Europea: sent. 22 gennaio 2013, C-283/11, *Sky Österreich GmbH v ORF*; sent. 3 settembre 2008, cause riunite C-402/05 P e C-415/05, *P.Kadi and Al Barakaat v Council and Commission*; Grande Sezione, sent. 2 settembre 2020, cause riunite C-724/18 e C-727/18, *Cali Apartments*; sent. 26 aprile 2022, C-401/19, *Polonia c. Parlamento e Consiglio*; sent. 16 luglio 2020, C-311/18, *Schrems II*.

[25] In cui si legge, tra l'altro, che «nessuno può essere privato della sua proprietà se non per causa di pubblica utilità e nelle condizioni previste dalla legge e dai principi generali del diritto internazionale». Per una disamina della genesi del testo e della lettura datane, v. F. Buonomo, *La tutela della proprietà dinanzi alla Corte europea dei diritti dell'uomo*, Milano, 2005.

[26] Si veda al riguardo Corte EDU, sent. 5 gennaio 2000, *Beyeler c. Italia* (merito), § 107.

patrimoniali, attività economiche e aspettative legittime di natura economica, quali licenze, autorizzazioni e accesso al mercato[27].

Il 19 marzo 2026, le conclusioni dell'Avvocata generale nella causa C-354/24 (caso *Elisa Eesti*) dinanzi alla Corte di giustizia dell'Unione europea, non si sono distanziate da questa lettura, nella disamina della corrispondente norma della Carta di Nizza[28]. E tuttavia l'Avvocata generale Ćapeta ha rilevato che una restrizione relativa all'uso di *hardware* e *software* – a causa del rischio che tali apparecchiature rappresentano per la sicurezza dell'Unione e degli Stati membri – costituisce non già una privazione della proprietà, bensì una limitazione dell'uso di tali beni, ai sensi dell'art. 17, par. 1, Carta di Nizza. In un simile caso, una società non ha, in linea di principio, diritto all'indennità, salvo che il giudice nazionale ritenga che l'onere derivante da tale tipo di restrizione sia sproporzionato rispetto alla necessità perseguita[29]. Per verificare la sussistenza di detta proporzionalità i giudici analizzano i mezzi impiegati dallo Stato nel caso di specie: non c'è dubbio che faranno lo stesso nel caso Elisa Eesti, in attesa della cui definizione sarebbe prudente, per il legislatore europeo, non accelerare i tempi dell'adozione del regolamento CSA-2.

Sebbene la distinzione fatta dall'Avvocata generale Ćapeta richiami quella tra atti ablatori ed atti conformativi della proprietà della giurisprudenza nostrana[30], proprio per questo non si dovrebbe dimenticare che l'art. 53 CEDU reca un meccanismo di salvaguardia del «livello più alto di tutela» recato a livello di Stati membri: vi si stabilisce, infatti, che nulla nella Carta deve essere interpretato come limitativo dei diritti riconosciuti dalle costituzioni nazionali, dalla Convenzione europea dei diritti dell'uomo o da altre fonti di diritto internazionale.

Sotto tale aspetto, dunque, vanno viste le norme previste dal CSA2 – e dunque le previsioni nazionali che vi darebbero attuazione – che potrebbero determinare l'esclusione di operatori economici da segmenti rilevanti del mercato europeo (ad esempio infrastrutture critiche o servizi digitali essenziali), impattando su tali interessi patrimoniali e configurando una possibile privazione sostanziale del valore economico dell'attività, assimilabile a una forma di interferenza nel diritto di proprietà.

La migliore dottrina[31], sul punto, nota che quando si invoca apoditticamente la protezione della sicurezza nazionale può derivare un danno alle imprese, a partire dalla perdita della possibilità di ottenere uno sviluppo proficuo dell'attività economica fino al caso del blocco di un investimento o di un acquisto di beni e servizi economicamente vantaggiosi. Tutto ciò avviene mediante l'esercizio di poteri autoritativi espressi in varie forme: «a causa dell'esercizio dei *golden powers* o delle prescrizioni sulla resilienza e sulla cybersicurezza»[32] possono scaturire danni in conseguenza dell'esclusione da una competizione e dalla perdita

---

[27] Corte europea dei diritti dell'uomo, sent. 7 giugno 2012, *Centro Europa 7 S.r.l. e Di Stefano c. Italia* (2012).

[28] Advocate General's Opinion in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*, §127: «Dalla giurisprudenza della Corte risulta inoltre che la tutela conferita dall'articolo 17, paragrafo 1, della Carta è ampia e comprende, oltre ai beni aventi un valore economico, gli interessi connessi allo sfruttamento di una licenza o di un'autorizzazione d'uso».

[29] Advocate General's Opinion in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*, §130 («in tal caso, il ricorrente non ha, in linea di principio, diritto all'indennità») e § 131: «ciò premesso, la limitazione dell'uso dei beni è possibile solo nella misura in cui sia necessaria per l'interesse generale. Ai fini della presente causa, tale valutazione sarà simile a quella richiesta per giustificare un'ingerenza nella libertà di fornire reti e servizi di comunicazione elettronica» ai sensi dell'articolo 12, paragrafo 1, della direttiva (UE) 2018/1972 (codice europeo delle comunicazioni elettroniche).

[30] Sorta con la sentenza della Corte costituzionale n. 55/1968, l'evoluzione dottrinaria è narrata con dovizie da C. Tucciarelli, *Vincoli conformativi e sostanzialmente espropriativi. Appunti* in occasione del corso «Urbanistica ed espropriazione per pubblica utilità - Corso di formazione per Magistrati amministrativi di nuova nomina», organizzato dall'Ufficio studi e formazione della Giustizia amministrativa (10 luglio 2023).

[31] L. Marilotti, *La mano invisibile. Sicurezza nazionale e garanzia del mercato nel diritto amministrativo*, cit., Milano, 2025.

[32] *Ibidem*.

di commesse pubbliche anche di elevato valore, ma anche a seguito dell'imposizione di «oneri di sicurezza eccessivamente gravosi». Le conseguenze potrebbero essere paragonabili «a un vero e proprio ergastolo imprenditoriale laddove un imprenditore sia privato *sine die* dei requisiti per poter operare in certe sezioni di mercato (come quelle della difesa e della sicurezza caratterizzate da uno stretto legame con il committente pubblico) o si veda congelati i propri *assets*»[33].

Quella dell' «ergastolo dell'imprenditore» è tutt'altro che una formula icastica: «tutti questi danni possono indebolire l'operatore colpito a livelli tali da poterne comportare anche la definitiva uscita dal mercato o il fallimento, con l'aggiunta che uno stesso operatore economico può essere soggetto passivo di più di questi poteri contemporaneamente, come ad esempio laddove si vedesse revocata l'abilitazione di sicurezza e fosse destinatario di prescrizioni o divieti connessi ai *golden powers*, alla resilienza dei soggetti critici o alla cybersicurezza»[34]. Si tratta di «prescrizioni, obblighi e interventi» che possono comportare «un aumento esponenziale dell'onerosità dell'attività economica» fino a provocare «addirittura l'uscita dal mercato dell'operatore» [35]: ecco perché la procedura che definisce i requisiti rappresenta una sede di potenziale, pesantissima compressione della libera competizione[36]. Anche quando è concessa la ricorribilità giurisdizionale contro le misure restrittive in concreto subìte, essa sposta in avanti l'effettività della partecipazione e del contraddittorio degli operatori economici incisi dai poteri, che non hanno una sede partecipativa nel procedimento amministrativo in merito alla definizione delle concrete misure.

La letteratura più recente già si è soffermata sulle modalità con cui gli Stati Uniti possono «azzoppare» lo sviluppo di partner commerciali esteri con argomenti di sicurezza nazionale[37].

Le preoccupazioni espresse, al medesimo riguardo, dal Parlamento europeo nella Risoluzione del 12 marzo 2019[38], sfidano la differenza tra *occasio* e *ratio legis*: il conseguente orientamento della Commissione – volto ad introitare nei requisiti di accesso la «selezione» degli operatori ammessi al mercato europeo – legittima il dubbio in ordine alla «incertezza su quale sia lo scopo prevalente dell'atto amministrativo»[39].

In altre parole nel sistema proposto dal CSA2, la qualificazione di determinati fornitori come «ad alto rischio» appare strettamente correlata, almeno in alcuni casi, al Paese di origine dell'operatore o al sistema politico-giuridico di appartenenza, così aprendo all'adozione di misure generalizzate e non individualizzate che rischiano di non superare un vaglio di legittimità condotto sulla base della Convenzione EDU e della Costituzione italiana.

È ben vero che «non tutti gli atti amministrativi che impongono un onere o incidono sui diritti o sugli interessi dei privati devono essere considerati 'sanzioni': tali atti possono perseguire una pluralità di finalità, tra cui la tutela dell'interesse pubblico e delle politiche pubbliche, la protezione della collettività da un pericolo imminente (per la salute pubblica, la qualità dell'ambiente, la sicurezza dell'occupazione, ecc.) mediante misure preventive»[40], e la finalità punitiva può essere assente o marginale. Ma è anche possibile osservare che le

[33] *Ibidem*.
[34] *Ibidem*.
[35] *Ibidem*.
[36] Il mercato interno, di cui all'articolo 3, paragrafo 3, TUE, comporta che la concorrenza non sia falsata: cfr. Protocollo n. 27 sul mercato interno e sulla concorrenza, allegato ai Trattati.
[37] A. Aresu, *Lo Stato nella competizione tecnologica*, il Mulino, 2, 2023, 87-88.
[38] P8_TA (2019)0156, § 2.
[39] CM(91)3 - European Committee on Legal Co-operation (CDCJ) - 54th meeting (Strasbourg, 3 - 7 December 1990) - Meeting report, 10/01/1991, citato dalla ReNEUAL 2.0 (*The Pan-European General Principles on Administrative Sanctions*).
[40] *Ibidem*.

conclusioni prospettate dall'avvocata generale nell'ordinamento euro-unitario attenevano a decisioni amministrative estoni riguardanti «una richiesta di autorizzazione all'uso di taluni hardware e software nella fornitura di reti e servizi di comunicazione elettronica (…) accolta solo parzialmente e limitatamente alla durata massima prevista» dalla normativa nazionale[41]. Nel caso estone si è dunque rilevato che «le decisioni impugnate rappresentano una limitazione dell'uso della proprietà della ricorrente ai sensi dell'articolo 17, paragrafo 1, terza frase, della Carta» proprio perché al momento della loro emanazione l'azienda già operava e, quindi, si è concluso «non sussisteva alcuna ingerenza sul contenuto essenziale di tale proprietà»[42].

Diversamente, nel caso che ci occupa, la proposta della Commissione anticiperebbe alla fase di determinazione dei requisiti il vaglio amministrativo in ordine alle caratteristiche di sicurezza richieste: il riferimento principale è l'art. 74 della proposta di regolamento, che disciplina l'elaborazione dei *European cybersecurity certification schemes* da parte dell'ENISA, nonché alle successive norme che portano alla loro adozione successiva da parte della Commissione mediante atti di esecuzione. È in quella sede che la Commissione definisce *ex ante* i requisiti, i criteri di valutazione, i livelli di *assurance* e le caratteristiche di sicurezza richieste ai prodotti/servizi ICT: il relativo effetto, contemplato dall'art. 85, costituisce quanto meno un'alterazione della concorrenza quando introduce il livello «high» a favore del candidato che soddisfa questi *compliance requirements*. Ma, più in generale, va segnalato che l'effetto è assai più dirompente per coloro che non rientrano in nessuno dei livelli («*basic*», «*substantial*» o «*high*») imposto dagli *schemes*: il vaglio amministrativo viene anticipato dalla fase del singolo certificato alla fase di determinazione dei requisiti dello schema. Ciò significherebbe rendere apodittico l'inserimento in albi o elenchi e sfuggire proprio a quel controllo giurisdizionale in concreto che l'Avvocata generale Ćapeta voleva far salvo[43].

Se quindi si versa nel caso di «*sanctions by another name*»[44], occorre applicare il principio di tipicità che, nel diritto amministrativo sanzionatorio, è accolto nel nostro ordinamento sin dal d.P.R. n. 689/1981, ma che discende dal criterio di determinatezza e prevedibilità imposto dalla CEDU[45]. Soprattutto, l'applicazione del test dei «criteri Engel» della CEDU[46] renderebbe estremamente problematica una misura afflittiva che si basa su status, ruolo o appartenenza e che presume una responsabilità – dell'ente collettivo, della società o dell'individuo[47] – senza verifica concreta.

Adottando ancor di più la prospettiva del diritto interno, e segnatamente dell'ordinamento italiano, le considerazioni sulle criticità della proposta CSA2 in relazione alla CEDU

[41] Advocate General's Opinion in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*, § 128.

[42] Di conseguenza, «la ricorrente non ne è stata privata»: Advocate General's Opinion in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*, § 129.

[43] Advocate General's Opinion in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*, § 115: «Qualora, come nel caso di specie, vi sia una convergenza tra gli interessi in materia di sicurezza di cui trattasi a livello dell'Unione e a livello nazionale, un giudice nazionale può anche prendere in considerazione – nell'ambito del controllo giurisdizionale della misura di cui trattasi – le valutazioni dei rischi effettuate dalle istituzioni e dagli organi dell'Unione nonché da organi nazionali».

[44] W. Steenbruggen, F. Sickinghe, *The CSA2's ICT Supply Chain Framework: Necessary Reform or Legal Overreach?*, Bird&Bird, Mar 17, 2026.

[45] Corte europea dei diritti dell'uomo, sent. 26 aprile 1979, *Sunday Times c. Regno Unito*, §§ 49 ss.

[46] Corte europea dei diritti dell'uomo, *ex multis*: sent. 8 giugno 1976, *Engel e altri contro Paesi Bassi*; sent. 21 febbraio 1984, *Öztürk contro Germania*; sent. 1° febbraio 2005, *Ziliberberg contro Moldavia*. Con la sentenza n. 43 del 2017, la Corte costituzionale italiana ne ha riconosciuta la rilevanza, al fine di evitare l'effetto di sottrarre gli illeciti alle garanzie sostanziali assicurate dagli artt. 6 e 7 della CEDU, il che «trascina, dunque, con sé tutte e soltanto le garanzie previste dalle pertinenti disposizioni della Convenzione, come elaborate dalla Corte di Strasburgo».

[47] Il modello offerto da Corte di Giustizia UE nel 2008, con la sentenza *Kadi* cit., rende estremamente problematico il metodo delle selezioni «a monte», imposto senza rispetto del contraddittorio e della difesa.

potrebbero acquistare rilievo alla luce dell'art. 117 della Costituzione, norma che obbliga il legislatore italiano e le istituzioni a tutti i livelli a rispettare non solo i principi stabiliti dalla Carta ma anche i vincoli derivanti dagli obblighi internazionali.
Così, nel sistema delineato dalla Corte costituzionale con le sentenze n. 348/2007 e n. 349/2007 e ribadito con la sentenza n. 120/2018 il giudice nazionale è chiamato a svolgere un ruolo centrale nel garantire il rispetto dell'art. 117 della Costituzione e dunque della CEDU, dando perciò attuazione a quel controllo giurisdizionale effettivo sulle decisioni incidenti sui diritti civili che attribuisce proprio ai principi sanciti dalla CEDU, e per quanto d'interesse a quelli affermati dal richiamato art. 1, Prot. n. 1 e art. 14 della Convenzione, una funzione di parametro interposto di legittimità costituzionale[48].
Del resto, anche non volendo prendere in considerazione alcuna convenzione internazionale, i suddetti principi sono pienamente condivisi dalla Costituzione italiana, la quale ha quale valore fondante il divieto di ogni discriminazione sancito dall'art. 3, e tutela la libertà di iniziativa economica privata ai sensi dell'art. 41.
Sono principi, questi, che non vincolano solo il legislatore ma che permeano l'azione a tutti i livelli dei poteri dello Stato, ivi inclusa la funzione amministrativa: essa deve essere improntata al principio di legalità, proporzionalità e di ragionevolezza, risultando dunque vietate tutte quelle disposizioni di carattere restrittivo o discriminatorio prive di adeguato bilanciamento con altri valori della Carta.
Da questo punto di vista, il meccanismo previsto dal CSA2 appare problematico in quanto è stato osservato che potrebbe portare all'esclusione di determinati fornitori da segmenti significativi del mercato. Una limitazione basata su motivazioni che, se fossero ritenute generiche, predittive e insufficientemente individualizzate, creerebbe un'evidente tensione non solo con l'art. 41 e con l'art. 3 Cost., ma anche con i principi di buon andamento e di imparzialità[49] che regolano l'attività amministrativa[50].
Laddove l'accesso alle infrastrutture critiche o ai servizi digitali essenziali fosse limitato non a causa di comportamenti specifici, carenze comprovate o vulnerabilità tecniche concrete, ma piuttosto in ragione di considerazioni generali legate all'origine, alla dipendenza strategica o alle caratteristiche del sistema giuridico e politico di un paese terzo, come vorrebbe il combinato disposto degli artt. 100 e 103 della proposta di regolamento, la misura scaturente rischierebbe di eccedere i valori fondanti dell'ordinamento italiano[51].
Emblematico è il caso che potrebbe prospettarsi ove in applicazione dell'art. 100 del CSA2

[48] Nel sistema delineato dalla Corte costituzionale con le sentenze n. 348 e n. 349 del 2007 - e ribadito con la richiamata sentenza n. 120 del 2018 - il giudice nazionale è chiamato a svolgere un ruolo centrale nel garantire il rispetto dell'art. 117 della Costituzione e dunque della CEDU, dando così attuazione a quel controllo giurisdizionale effettivo sulle decisioni incidenti sui diritti civili di cui si è più volte sottolineata l'indispensabilità. Vedi, tra l'altro, M. Bignami, *Le gemelle crescono in salute: la confisca urbanistica tra costituzione, CEDU e diritto vivente*, in *Diritto penale contemporaneo*, 2, 2015, 293.
[49] V. legge n. 241/1990. La sua ricaduta, in termini di tutela del cittadino, è evidenziata da Corte costituzionale, sent. n. 104/2017, Considerato in diritto, § 2.9, secondo cui «la disciplina del giusto procedimento, specie dopo l'entrata in vigore della legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi), come modificata dalla legge 11 febbraio 2005, n. 15, per cui il destinatario dell'atto deve essere informato dell'avvio del procedimento, avere la possibilità di intervenire a propria difesa, ottenere un provvedimento motivato, adire un giudice».
[50] Sulla applicazione effettuata dalla Corte costituzionale degli artt. 3 e 41 della Costituzione si veda la sent.n. 84 del 2017. Sulle restrizioni all'attività economica - e sulla necessità che siano non discriminatorie, proporzionate, giustificate da interessi pubblici reali - v. anche Corte costituzionale, sent. n. 104/2014.
[51] È il caso che si potrebbe prospettare ove trovassero piena applicazione l'art. 85, l'art. 100 e l'art. 103 della CSA2. L'art. 111 addirittura prevede che i fornitori di reti di comunicazione elettronica mobili, fisse e satellitari non possono utilizzare, installare o integrare in alcuna forma componenti ICT o componenti che li includano, se provenienti da fornitori ad alto rischio, nel funzionamento delle risorse ICT fondamentali.

una amministrazione approvasse un bando di gara per un appalto pubblico in conformità con le direttive 2014/24/UE e 2014/25/UE inserendovi una norma di carattere escludente per quegli operatori qualificati come ad alto rischio dalla Commissione. Potrebbe derivarne un possibile contenzioso dinanzi alla giurisdizione amministrativa e, nella ipotesi di accertamento della natura discriminatoria della disposizione, l'atto amministrativo potrebbe essere annullato, dare luogo ad un sindacato di costituzionalità ovvero ad una questione pregiudiziale dinanzi alla CGUE[52].

A ben vedere, infatti, le sopra esposte preoccupazioni possono essere inquadrate, sebbene in modo più indiretto, in termini di limiti costituzionali al trasferimento e all'esercizio dei poteri nell'ambito dell'ordinamento giuridico europeo: pur riconoscendo il primato del diritto dell'Unione, l'ordinamento italiano non esclude la possibilità per la Corte Costituzione di sindacare gli atti dell'Unione qualora essi producano una violazione dei principi fondamentali dell'ordinamento giuridico interno[53].

Anche sotto tale profilo si può concludere che un uso eccessivamente estensivo dell'art. 114 TFUE e la introduzione di meccanismi di esclusione – basati su motivazioni discriminatorie – potrebbero innescare tensioni sistemiche all'interno del sistema multilivello di *governance* europea: il rischio è, da un lato, alterare l'equilibrio delle competenze tra Unione e ordinamento interno, e dall'altro produrre una compressione di principi costituzionalmente protetti[54].

3. Conclusioni. Il rischio di un ampio contenzioso e la necessità di un approccio multilivello. All'esito dell'analisi svolta, il quadro normativo europeo in materia di cybersicurezza appare caratterizzato da un processo di rafforzamento della c.d. sovranità tecnologica dell'Unione, intesa quale capacità di governare autonomamente le infrastrutture digitali e di garantire la sicurezza del mercato interno. In tale prospettiva, le iniziative normative adottate e proposte evidenziano come l'Unione stia facendo ampio ricorso alle proprie competenze, in particolare a quelle fondate sull'art. 114 TFUE, al fine di promuovere l'utilizzo di tecnologie sviluppate all'interno dello spazio europeo, proteggere i settori economici critici e mitigare i rischi derivanti da minacce informatiche sempre più pervasive[55].

Tuttavia, questo processo di integrazione normativa non è privo di criticità. L'uso estensivo della base giuridica del mercato interno solleva, infatti, rilevanti interrogativi in ordine al rispetto dei principi di attribuzione, proporzionalità e sussidiarietà, che delimitano l'esercizio delle competenze dell'Unione.

Anche quando il *Cybersecurity Act* ha reso l'ENISA il pilastro della cybersicurezza europea, pur senza sostituire le agenzie nazionali, la dottrina giudicò ciò «in linea con il principio di sussidiarietà», ma ricordò anche che «il Senato francese si è opposto nel 2017 all'attribuzione

---

[52] *Ex multis* si veda Consiglio di Stato, Ad. Plen., 25 febbraio 2014, n. 9.

[53] La Corte costituzionale, a partire dalla sent. n. 183/1973 (Frontini), ha infatti affermato che il trasferimento di competenze all'ordinamento europeo trova fondamento nell'art. 11 Cost., ma è subordinato al rispetto dei principi fondamentali dell'ordinamento e dei diritti inviolabili della persona. Tale impo stazione è stata sviluppata attraverso la teoria dei c.d. controlimiti, che costituiscono una clausola di salvaguardia dell'identità costituzionale nazionale. Nella successiva giurisprudenza – dalla sentenza n. 170/1984 (Granital) fino alle più recenti decisioni Taricco (sentt. nn. 24/2017 e 115/2018) – la Corte ha progressivamente consolidato un modello di integrazione aperta ma condizionata, nel quale il primato del diritto dell'Unione trova il proprio fondamento nella Costituzione e incontra un limite nei principi supremi dell'ordinamento. In tale prospettiva, pur privilegiando il dialogo con la Corte di giustizia attraverso il rinvio pregiudiziale, la Corte costituzionale non ha escluso in linea di principio la possibilità di sindacare gli atti dell'Unione qualora essi incidano su tali principi.

[54] V. A., Schmidt, M. Wood, *Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance*. Public Administration, 2019, 97(4), 727–740.

[55] M. Taddeo, *Deterrence by Norms to Stop Interstate Cyber Attacks*, Minds and Machines, 2017, 27(3), 387-392.

di poteri investigativi all'ENISA proprio per rispetto di tale principio»[56].
In particolare, la crescente centralizzazione delle politiche di cybersicurezza e il possibile innalzamento di barriere di ingresso a fornitori extra-UE rischiano di avere, anzitutto, ripercussioni economiche sulle medesime aziende europee, non più libere di avvalersi delle componenti ICT più efficienti e più convenienti. In secondo luogo, c'è il pericolo di incidere sulla capacità degli Stati membri di fronteggiare autonomamente le sfide tecnologiche, in un settore che presenta forti implicazioni strategiche e di sicurezza nazionale.
Il rischio che dalla introduzione delle norme previste dal CSA2 si sviluppi un ampio contenzioso è dunque realistico. Anzitutto con riferimento al possibile rimedio rappresentato dall'art. 263 TFUE attivabile dagli Stati membri o dal Parlamento ove dovesse riscontrarsi un uso distorto dell'art. 114 TFUE e dunque un vizio di competenza. In secondo luogo, ancor più rilevante dalla prospettiva degli operatori economici è il rimedio previsto dall'art. 267 TFUE il quale, come noto, consiste nel rinvio pregiudiziale dinanzi alla Corte di giustizia dell'Unione europea attivabile in via incidentale nel corso di una controversia pendente presso una giurisdizione domestica.
Non da ultimo un ulteriore livello di tutela deriva dal sistema dei diritti fondamentali, quale risultante dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione europea dei diritti dell'uomo. È stato osservato come le misure del CSA2 potrebbero incidere su libertà di impresa, diritto di proprietà e principio di non discriminazione ed essere sottoposte al sindacato del giudice nazionale e, in ultima istanza, della Corte EDU.
Nel sistema italiano, è stato evidenziato come eventuali violazioni dei diritti convenzionali possono rilevare anche attraverso l'art. 117 Cost., che impone il rispetto degli obblighi internazionali. Ciò consente, in via mediata, un controllo di compatibilità costituzionale delle norme interne di attuazione del diritto dell'Unione. Detto controllo incidentale può altresì avvenire anche ai sensi dell'art. 3 e art. 41 della Costituzione ove le misure introdotte dal CSA2 dovessero risolversi in una lesione non giustificata del principio di uguaglianza e in una compressione della libertà di impresa non adeguatamente bilanciata dagli obiettivi effettivamente perseguiti. Un controllo che, in astratto, potrebbe addirittura estendersi ad un vaglio di costituzionalità delle norme UE ove le stesse si trovassero in antinomia con i principi fondamentali dell'ordinamento interno.
In tale contesto, il modello europeo sembra allontanarsi dall'attuale sistema multilivello, nel quale il ruolo dell'Unione si affianca – senza sostituirsi integralmente – a quello degli ordinamenti nazionali che rimangono però il perno centrale delle politiche industriali e in materia di sicurezza, secondo una prospettiva maggiormente compatibile con l'attuale formulazione dei Trattati e probabilmente più rispettosa delle specificità e dei contesti nazionali.
Il caso italiano, da questo punto di vista, appare emblematico: pur in assenza di grandi operatori globali nel settore digitale, il sistema nazionale si caratterizza per un tessuto dinamico di piccole e medie imprese e per un quadro normativo avanzato, che include strumenti quali il perimetro di sicurezza nazionale cibernetica[57] e i poteri speciali (*golden*

[56] A. Deprau, *L'Union européenne face à la cybermenace: une stratégie de régulation à l'épreuve des souverainetés nationales* , Cahiers de Conflits 2024/3 Juillet-septembre, 7, 3-10.
[57] In particolare, con il d.l. n. 82/2021 è stata istituita l'Agenzia per la cybersicurezza nazionale (ACN), quale autorità centrale responsabile del coordinamento delle politiche di sicurezza informatica e dell'attuazione delle strategie nazionali, in linea con gli obblighi derivanti dalla direttiva NIS 2. A ciò si affianca il c.d. Perimetro di sicurezza nazionale cibernetica (d.l. n. 105/2019), che individua soggetti pubblici e privati operanti in settori strategici e impone specifici obblighi di sicurezza e notifica degli incidenti.

power)[58].
Alla luce di tali considerazioni, il rafforzamento della sovranità tecnologica europea non può essere interpretato in termini meramente centralizzatori, ma richiede un equilibrio tra livello unionale e livello nazionale. La soluzione sembra rinvenibile in un approccio realmente multilivello, fondato su forme di cooperazione orizzontale e sull'individuazione di strumenti normativi adeguati alla natura transnazionale dei fenomeni digitali.

Abstract. Il testo esamina i limiti giuridici della proposta di Regolamento europeo sulla cybersicurezza COM(2026) 11 (CSA2), collocandola nel più ampio processo evolutivo dell'Unione europea verso la sovranità tecnologica e digitale. Si sostiene che la proposta rifletta uno spostamento dal tradizionale ruolo dell'UE di coordinamento e integrazione del mercato verso una forma di intervento più simile a quella statale in ambiti sensibili quali la sicurezza e la politica industriale. Tale trasformazione solleva preoccupazioni riguardo all'equilibrio delle competenze tra l'Unione e gli Stati membri, nonché questioni di legittimità democratica.
L'analisi evidenzia che il CSA2, fondato sulla base giuridica del mercato interno (articolo 114 TFUE), introduce misure – come schemi obbligatori di certificazione della cybersicurezza e restrizioni sulle catene di approvvigionamento – che perseguono obiettivi che vanno oltre l'armonizzazione del mercato, includendo considerazioni geopolitiche e di sicurezza. Tale espansione rischia di violare il principio di attribuzione, come interpretato dalla Corte di giustizia, e può inoltre entrare in conflitto con i principi di proporzionalità e sussidiarietà, considerata la disponibilità di alternative meno restrittive e più decentrate.
Il testo approfondisce inoltre possibili incompatibilità con i diritti fondamentali dell'UE, in particolare la libertà d'impresa, il diritto di proprietà e il principio di non discriminazione, come tutelati dalla Carta dei diritti fondamentali. Preoccupazioni simili emergono anche rispetto alla Convenzione europea dei diritti dell'uomo, soprattutto riguardo a restrizioni indirette sulle attività economiche e sull'accesso al mercato che potrebbero costituire interferenze sproporzionate con i diritti di proprietà.
Dal punto di vista del diritto costituzionale italiano, il regolamento proposto potrebbe entrare in contrasto con principi fondamentali quali l'uguaglianza (art. 3 Cost.), la libertà di iniziativa economica (art. 41 Cost.) e il requisito di legalità, ragionevolezza e proporzionalità dell'azione amministrativa. Lo studio considera anche il ruolo della giurisprudenza della Corte costituzionale italiana, che potrebbe limitare l'applicazione interna del diritto dell'UE quando siano in gioco principi costituzionali fondamentali.
Infine, il documento avverte dell'esistenza di un significativo rischio di contenzioso sia a livello europeo sia nazionale, comprese azioni di annullamento e rinvii pregiudiziali alla Corte di giustizia, oltre ai meccanismi di controllo di costituzionalità. Si conclude che il rafforzamento della sovranità tecnologica europea non dovrebbe basarsi su un'eccessiva centralizzazione, bensì su un autentico modello di governance multilivello che bilanci l'intervento dell'UE con l'autonomia degli Stati membri e rispetti i diritti fondamentali e le

[58] Un ulteriore strumento rilevante è rappresentato dalla disciplina del *golden power*, progressivamente estesa anche al settore delle tecnologie digitali e delle reti di comunicazione elettronica (in particolare 5G). Tale meccanismo consente al Governo italiano di esercitare poteri speciali su operazioni societarie e contratti riguardanti asset strategici, inclusi quelli relativi alla sicurezza delle reti e delle infrastrutture ICT, al fine di prevenire rischi per la sicurezza nazionale. In questo senso, esso costituisce un punto di intersezione tra tutela della sicurezza statale e regolazione del mercato interno, riflettendo a livello nazionale le medesime tensioni che emergono a livello europeo (v. anche M. Clarich, *La disciplina del golden power in Italia e l'estensione dei poteri speciali alle reti 5G*, in G. Napolitano (a cura di), *Foreign Direct Investment screening. Il controllo sugli investimenti esteri diretti*, Bologna, 2019, 118).

garanzie costituzionali.

Abstract. This paper examines the legal limits of the proposed EU Cybersecurity Regulation COM(2026) 11 (CSA2), situating it within the broader evolution of the European Union toward technological and digital sovereignty. It argues that the proposal reflects a shift from the EU's traditional role of coordination and market integration toward a more state-like intervention in sensitive domains such as security and industrial policy. This transformation raises concerns regarding the balance of competences between the Union and Member States, as well as issues of democratic legitimacy.
The analysis highlights that CSA2, grounded in the internal market legal basis (Article 114 TFEU), introduces measures – such as mandatory cybersecurity certification schemes and restrictions on supply chains – that pursue objectives extending beyond market harmonization, including geopolitical and security considerations. This expansion risks violating the principle of conferral, as interpreted by the Court of Justice, and may also conflict with the principles of proportionality and subsidiarity, given the availability of less restrictive and more decentralized alternatives.
The paper further explores potential incompatibilities with EU fundamental rights, particularly the freedom to conduct a business, the right to property, and the principle of non-discrimination, as protected by the Charter of Fundamental Rights. Similar concerns arise under the European Convention on Human Rights, especially regarding indirect restrictions on economic activities and market access that may amount to disproportionate interferences with property rights.
From the perspective of Italian constitutional law, the proposed regulation may clash with core principles such as equality (art. 3), freedom of economic initiative (art. 41), and the requirement of legality, reasonableness, and proportionality in administrative action. The study also considers the role of Italian Constitutional Court case-law, which may constrain the domestic application of EU law where fundamental constitutional principles are at stake.
Finally, the paper warns of a significant risk of litigation at both EU and national levels, including actions for annulment and preliminary references to the Court of Justice, as well as constitutional review mechanisms. It concludes that strengthening European technological sovereignty should not rely on excessive centralization but rather on a genuinely multi-level governance approach that balances EU intervention with Member State autonomy and respects fundamental rights and constitutional guarantees.

Parole chiave. Cybersicurezza – Proporzionalità – *Governance* multilivello – Mercato interno.

Key words. Cybersecurity – Proportionality – Multi-level governance – Internal market.

Issn 2421-0528