Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 – Anticipazione fascicolo
V ed. Incontro fra i giovani studiosi di diritto UE

L'Unione europea come *standard-setter* in materia di cybersicurezza nel contesto della sua autonomia strategica aperta

Virginia Remondino*

SOMMARIO: 1. Introduzione. – 2. Gli *standard* (europei) come pilastro dell'autonomia strategica aperta dell'Unione. – 3. Tra resilienza del mercato interno e tutela dei valori europei: quale approccio nella definizione di *standard* di cybersicurezza dei prodotti? – 4. La concretizzazione del paradigma: il regolamento 2024/2847 sulla cyberresilienza. – 5. Le implicazioni costituzionali della concretizzazione del paradigma: l'autonomia strategica aperta al vaglio del diritto internazionale. – 6. Considerazioni conclusive.

1. *Introduzione*

Negli ultimi anni, l'autonomia strategica (aperta) si è imposta come un concetto «en vogue»[1], o una «buzzword»[2], nel panorama politico e

* Assegnista di ricerca in Diritto dell'Unione europea, *Alma Mater Studiorum* - Università di Bologna. Ricerca finanziata dal programma PNRR - Missione 4 istruzione e ricerca - componente 2 dalla ricerca all'impresa, Investimento 1.3, PE0000014 - "SEcurity and RIghts in the CyberSpace", finanziato dalla Commissione europea nell'ambito del NextGeneration EU Programme.

[1] F. HOFFMEISTER, *Strategic Autonomy in the European Union's External Relations Law*, in *CMLR*, 2023, p. 667 ss., spec. p. 667.

[2] E. KASSOTI, R. A. WESSEL, *Strategic Autonomy: The Legal Contours of a Security Policy Construct*, in *European Foreign Affairs Review*, 2023, p. 305 ss., spec. p. 305.

normativo dell'Unione europea (Unione o "UE"), un concetto capace di guidare e plasmare l'azione dell'UE tanto nella sua dimensione interna, quanto in quella esterna[3]. Sebbene non esista, ad oggi, una definizione univoca di autonomia strategica, tale nozione è stata concettualizzata, in termini comprensivi, come «the political, institutional and material ability of the EU and its member states to manage their interdependence with third parties, with the aim of ensuring the well-being of their citizens and implementing self-determined policy decisions»[4]. In altre parole, l'autonomia strategica mirerebbe a proteggere e promuovere gli interessi comuni dei cittadini europei, tutelando al contempo i principi e i valori su cui l'Unione si fonda[5]. Allo stesso tempo, caratterizzandosi come "aperta", l'autonomia strategica non esclude la cooperazione dell'Unione con i paesi terzi e le organizzazioni internazionali. Ciò, nelle parole della Commissione, «[s]ignifica che l'UE continua a cogliere i benefici delle

[3] European External Action Service (EEAS), *Shared Vision, Common Action: a Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, 2016, www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf, p. 9. In generale sul tema, si veda R. GARCÍA PÉREZ, *Strategic Autonomy of the European Union: a Perspective*, in E. CONDE, Z. V. YANEVA, M. SCOPELLITI (eds.), *The Routledge Handbook of European Security Law and Policy*, London, 2019, p. 81 ss.; N. TOCCI, *European Strategic Autonomy. What It Is, Why We Need It, How to Achieve It*, in *Istituto Affari Internazionali*, 2021; F. HOFFMEISTER, *op. cit.*; C. RAPOPORT, *Setting Norms and Promoting a Rules-based International Legal Order: Enhancing Strategic Autonomy Through the Autonomy of the EU Order*, in *EP*, 2023, p. 447 ss.; C. BEAUCILLON, *Strategic Autonomy: a New Identity for the EU as a Global Actor*, *ivi*, 2023, p. 417 ss.

[4] N. HELWIG, *EU Strategic Autonomy: a Reality Check for Europe's Global Agenda*, in *FIIA Working Paper*, n. 119, 2020, www.fiia.fi/wp-content/uploads/2020/10/wp119_strategic_autonomy-2.pdf, p. 4. Analogamente vedasi anche Damen, il quale definisce l'autonomia strategica come «the capacity of the EU to act autonomously – that is, without being dependent on other countries – in strategically important policy areas. These can range from defence policy to the economy, and the capacity to uphold democractic values». Cfr. M. DAMEN, *EU Strategic Autonomy 2013-2023: from Concept to Capacity*, in *EPRS Briefing PE 733.58*, 2022, p. 1. Per ulteriori definizioni e concettualizzazioni del termine, si rimanda a P. MORILLAS, *An Architecture Fit for Strategic Autonomy: Institutional and Operational Steps towards a More Autonomous EU External Action*, in *FEPS Policy Brief*, November 2021; F. HOFFMEISTER, *op. cit.*, p. 673.

[5] EEAS, *Shared Vision,* cit., p. 4.

opportunità internazionali, difendendo al contempo con risolutezza i propri interessi»[6].

Emerso originariamente nell'ambito della politica estera e di sicurezza comune (PESC) dell'Unione[7], il concetto di autonomia strategica aperta è stato successivamente esteso – e adattato – ad altre politiche dell'UE, tra cui la politica commerciale comune (PCC)[8], la politica industriale[9] ed il mercato interno[10]. A fronte di questa evoluzione dell'ambito d'applicazione della nozione in esame, un documento redatto per conto della Commissione europea nel 2021[11] ha individuato – sulla base di *trend* geopolitici ed economici che potrebbero influenzare la capacità dell'Unione di agire negli anni a venire – alcune aree prioritarie in cui l'autonomia strategica aperta andrà, presumibilmente, a rivestire un ruolo chiave. Tra queste, figura la definizione e la promozione di *standard* capaci di promuovere, oltre i confini dell'UE, tanto gli interessi strategici quanto i valori di cui

---

[6] Commissione europea, *Riesame della politica commerciale - Una politica commerciale aperta, sostenibile e assertiva*, COM (2021) 66final, 18 febbraio 2021, p. 4.

[7] F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *European Foreign Affairs Review*, 2023, p. 323 ss., spec. p. 328.

[8] Per una panoramica sul ruolo giocato dal concetto di autonomia strategica aperta nel contesto della politica commerciale comune dell'Unione, si rimanda a G. KÜBEK, I. MANCINI, *EU Trade Policy between Constitutional Openness and Strategic Autonomy*, in *ECLR*, 2023, p. 518 ss.; W. WEIß, C. FURCULITA, *Open Strategic Autonomy in EU Trade Policy: Assessing the Turn to Stronger Enforcement and More Robust Interest Representation*, Cambridge, 2024.

[9] Commissione europea, *Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa*, COM (2021) 350final, 5 maggio 2021, p. 3. È interessante rilevare che, in materia di politica industriale, la precedente comunicazione della Commissione dal titolo «Una nuova strategia industriale per l'Europa» conteneva una definizione *ad hoc* del concetto di autonomia strategica, consistente «nel ridurre la dipendenza dalle fonti esterne per ciò di cui abbiamo più bisogno: materiali e tecnologie critici, prodotti alimentari, infrastrutture, sicurezza e altri settori strategici». Cfr. Commissione europea, *Una nuova strategia industriale per l'Europa*, COM (2020) 102final, 10 marzo 2020, pp. 14-15.

[10] V. C. ALCIDI ET AL., *What ways and means for a real strategic autonomy of the EU in the economic field?*, *CEPS Report for the European Economic and Social Committee*, 2023, spec. p. 8.

[11] C. CAGNIN ET AL., *Shaping and Securing the EU's Open Strategic Autonomy by 2040 and Beyond*, Luxembourg, 2021.

all'art. 2 TUE, rappresentando questi ultimi «l'identità stessa»[12], o «l'impronta identitaria»[13], dell'Unione europea.

Standard[14] che, recentemente, hanno assunto un ruolo di primo piano in ambito digitale, anche con riguardo alla cybersicurezza dei

[12] Come notoriamente enunciato nelle famose "sentenze gemelle" del febbraio 2022, nella sentenza del giugno 2023 riguardante la riforma del sistema giudiziario polacco nonché, di recente, nella sentenza sulla "vendita" della cittadinanza dell'Unione. Si veda Corte giust. 16 febbraio 2022, C-156/21, *Ungheria/Parlamento e Consiglio*, punto 127; 16 febbraio 2022, C-157/21, *Polonia/Parlamento e Consiglio*, punto 145; 5 giugno 2023, C-204/21, *Commissione/Polonia*, punto 67; 29 aprile 2025, C-181/23, *Commissione/Malta*, spec. punto 93. Per riflessioni riguardanti le menzionate "sentenze gemelle", si veda *ex multis* E. PERILLO, *Il rispetto dello "Stato di diritto europeo" alla luce delle sentenze Ungheria e Polonia sulla clausola di condizionalità finanziaria. Quali prospettive?*, in questa *Rivista*, n. 1, 2022, p. 407 ss.; A. FESTA, *Le sentenze «gemelle» del 16 febbraio 2022: oltre la questione di legittimità, un «manifesto» sui fondamenti del diritto europeo*, in *Papers di diritto europeo*, 2022, p. 81 ss.; G. CONTALDI, *Le sentenze della Corte di giustizia sui ricorsi di Polonia e Ungheria e l'emersione del concetto di identità europea*, in *EJ*, 30 dicembre 2022, p. 87 ss.; V. BORGER, *Constitutional identity, the rule of law, and the power of the purse: The ECJ approves the conditionality mechanism to protect the Union budget: Hungary and Poland v. Parliament and Council*, in *CMLR*, 2022, p. 1771 ss. Per riflessioni riguardanti la sentenza *Commissione c. Polonia*, sopra citata, cfr. E. SAVOLDELLI, *La "muzzle law" polacca al vaglio della Corte di giustizia: una prima lettura della sentenza resa nella causa C-204/21, Commissione c. Polonia (vita privata dei giudici)*, in *EJ*, 10 luglio 2023; M. LANOTTE, *Warsaw does not fulfil, and Luxembourg cuts the sanction in half. It doesn't add up!*, in questa *Rivista*, 2023; S. PITTO, *Judicial Independence Under Siege in Poland. The Last Landmark Ruling by the ECJ: repetita iuvant?*, in *DPCE*, 2023, p. 3015 ss. In relazione alla citata sentenza *Commissione/Malta*, cfr. M. CHAMON, *Commission v Malta (C-181/23) and the Trilemma of EU Citizenship*, in *ELR*, 2025, p. 475 ss.; C. DELLI CARRI, *La "mercificazione" della cittadinanza è contraria al diritto dell'Unione europea. Note a margine della sentenza C-181/23 della Corte di giustizia*, in *Unione europea e Diritti*, n. 2, 2025, p. 1 ss.; D. V. KOCHENOV, G. IÑIGUEZ, *EU Citizenship's New Essentialism*, in *ELR*, 2025, p. 455 ss.; S. POLI, *Revoca e attribuzione della cittadinanza: quali condizionamenti impongono le disposizioni dei Trattati sulla cittadinanza europea e quelle sulla Politica Estera e di Sicurezza Comune?*, in questa *Rivista*, 2025, p. 1 ss.; U. VILLANI, *La Corte di giustizia dinanzi alla "cittadinanza (di Malta) in vendita"*, in *RCE*, n. 2, 2025, p. 1 ss.

[13] L. S. ROSSI, *Il valore giuridico dei valori. L'Articolo 2 TUE: relazioni con altre disposizioni del diritto primario dell'UE e rimedi giurisdizionali*, in *federalismi.it*, n. 19, 2020, p. iv. ss.

[14] Ai fini del presente lavoro il termine "*standard*" è utilizzato in senso ampio, andando a ricomprendere non soltanto le "norme" come definite all'art. 2, punto 1, del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, ma anche i requisiti tecnici previsti da determinati atti di diritto derivato dell'Unione.

prodotti *hardware* e *software* presenti sul mercato interno[15]. Questo, in particolare, a seguito dell'adozione nell'ottobre del 2024 del regolamento 2024/2847 sulla cyberresilienza (*Cyber Resilience Act* o "CRA")[16], che stabilisce precisi requisiti orizzontali in materia di cybersicurezza dei prodotti con elementi digitali messi a disposizione sul mercato interno.

Su questo sfondo – posta una riflessione preliminare circa il rapporto tra autonomia strategica aperta e promozione internazionale degli *standard* europei (par. 2) – il presente contributo ricostruisce anzitutto il paradigma a cui l'Unione sostiene di ispirarsi nella definizione degli *standard* di cybersicurezza a livello sovranazionale, così come descritto nei documenti di *policy* (par. 3). Si valuterà poi in quale misura il regolamento sulla cyberresilienza rispecchi, in concreto, tale paradigma (par. 4). In questo modo, si rifletterà sulle implicazioni costituzionali generate dalla promozione del paradigma mediante il regolamento in oggetto, con specifico riguardo all'azione esterna dell'Unione. Infatti, in quanto strumento che concretizza l'autonomia strategica aperta, il CRA si applica anche ai prodotti connessi fabbricati oltre i confini dell'UE. Pertanto, il *focus* dell'indagine è dedicato agli obiettivi che l'Unione si prefigge di realizzare nelle sue relazioni internazionali, nonché alla portata degli eventuali limiti posti al conseguimento degli stessi (par. 5). Da ultimo, verranno presentate alcune considerazioni conclusive (par. 6).

2. *Gli* standard *(europei) quale pilastro dell'autonomia strategica aperta dell'Unione*

Il legame intercorrente tra autonomia strategica aperta e definizione e proiezione internazionale degli *standard* europei emerge chiaramente

[15] A. VOLPATO, M. ELIANTONIO, S. RÖTTGER-WIRTZ, *Global Standards and EU Law: Introduction*, in A. VOLPATO, M. ELIANTONIO, S. RÖTTGER-WIRTZ (eds.), *Global Standards and EU Law Challenges for the EU Principles of Good Governance*, Cheltenham, 2025, p. 1 ss., spec. pp. 9-10.

[16] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).

dalla comunicazione della Commissione del 2022 sulla strategia dell'UE in materia di normazione[17], in cui viene evidenziato che gli *standard* «non sono una finalità a sé stante [bensì] parte integrante di obiettivi strategici volti a promuovere […] l'autonomia strategica aperta»[18]. In questo senso, la comunicazione riconosce che, se «[t]radizionalmente l'Unione europea […] ha ottenuto buoni risultati nel tradurre le norme internazionali in norme europee»[19], attualmente l'obiettivo che si pone l'UE è quello di «plasmare [le] norme internazionali»[20], rafforzando così il proprio ruolo di «*rule generator*»[21] a livello multilaterale[22]. Questa necessità, secondo la Commissione, è motivata dal fatto che l'Unione deve confrontarsi con una «concorrenza agguerrita»[23] a livello globale, in cui diversi Paesi terzi (tra cui gli Stati Uniti e la Cina)[24], agendo attivamente nel campo della normazione, cercano di garantire alle proprie imprese un vantaggio competitivo – il c.d. «vantaggio del pioniere»[25] – su scala mondiale[26].

In questo contesto, particolare importanza è attribuita agli *standard* riguardanti le tecnologie nuove ed emergenti, nonché i relativi prodotti e servizi, tra cui sono ricompresi i sistemi di intelligenza artificiale, le *blockchains*, le tecnologie quantistiche, l'internet delle cose (*Internet of Things*, o "*IoT*") e le valute digitali[27]. Infatti, nelle sue conclusioni sulla

[17] Commissione europea, *Una strategia dell'UE in materia di normazione - Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM (2022) 31final, 2 febbraio 2022.
[18] *Ivi*, p. 11.
[19] *Ivi*, p. 6.
[20] *Ibidem*, enfasi aggiunta. Ciò, in particolare, facendo leva sul proprio potere di mercato. Si veda sul punto COM (2020) 102final, cit., p. 3. In tal modo, prendendo in prestito un'espressione utilizzata da Damro, l'Unione agirebbe sulla scena internazionale come "market power", sfruttando il proprio potere di mercato per "esportare" le norme del proprio ordinamento giuridico. Cfr. C. DAMRO, *Market Power Europe*, in *JEEP*, 2012, p. 682 ss.
[21] Così F. CASOLARI, *Per una vera Unione di diritto: cinque priorità per l'ordinamento giuridico dell'Unione europea*, in *federalismi.it*, 2025, p. iv ss.
[22] Sul tema, si veda M. CREMONA, *The Union as a Global Actor: Rules, Models and Identity*, in *CMLR*, 2004, p. 553 ss.
[23] COM (2022) 31final, cit., p. 6.
[24] Sul punto, si veda C. CAGNIN ET AL., *op. cit.*, p. 15.
[25] COM (2021) 750final, cit., p. 14.
[26] C. CAGNIN ET AL., *op. cit.*, p. 4.
[27] V. Commissione europea, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192final, 6 maggio 2015, pp. 16-17; Commissione europea, *Plasmare il futuro digitale dell'Europa*, COM (2020) 67final, 19 febbraio 2020, p. 14.

diplomazia digitale[28], il Consiglio ricomprende tra gli obiettivi di azione prioritaria dell'UE quello di «influenzare la definizione di norme tecnologiche internazionali»[29], al fine di «rafforzare il ruolo globale dell'UE nelle questioni digitali»[30]. Obiettivo, quest'ultimo, ripreso dalla strategia europea per la sicurezza economica del 2023[31], nonché dalla più recente strategia digitale internazionale per l'Unione europea[32].

Da questa prospettiva, dunque, la necessità per l'Unione di definire e promuovere i propri *standard* – quale espressione dell'autonomia strategica aperta – si intreccia con un'ulteriore e collegata esigenza: quella di consolidare la "sovranità digitale (o tecnologia) europea"[33] a livello internazionale[34]. Tale controversa nozione[35], riferendosi «to

[28] Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla diplomazia digitale dell'UE*, Doc. 11406/22, 18 luglio 2022.
[29] *Ivi*, punto 6.
[30] *Ibidem*.
[31] Commissione europea e Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (AR-PESC), *Strategia europea per la sicurezza economica*, JOIN (2023) 20final, 20 giugno 2023, p. 9. Si veda anche Commissione europea, *Impulso alla sicurezza economica dell'Europa: introduzione a cinque nuove iniziative*, COM (2024) 22final, 24 gennaio 2024, p. 8.
[32] Commissione e AR-PESC, *Una strategia digitale internazionale per l'Unione europea*, JOIN (2025) 150final, 5 giugno 2025.
[33] Il concetto di "sovranità digitale (o tecnologica) europea" è stato menzionato, per la prima volta, dalla Presidente della Commissione europea Ursula von der Leyen durante il discorso sullo stato dell'Unione del 2020, figurando successivamente nella nota "bussola per il digitale 2030". Cfr. Commissione, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM (2021) 118final, 9 marzo 2021, p. 1. Per commenti sulla concettualizzazione di questa nozione, v. L. FLORIDI, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 2020, p. 369 ss.; S. POLI, E. FAHEY, *The strengthening of the European Technological Sovereignty and its legal bases in the Treaties*, in *EJ*, 2022, p. 147 ss.; G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 2022, p. 809 ss.; L. MOLA, *Fostering 'European Technological Sovereignty' Through the CSDP: Conceptual and Legal Challenges. First Reflections Around the 2022 Strategic Compass*, in *EP*, 2023, p. 459 ss.; S. YAKOULEVA, *On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows*, in *LIEI*, 2023, p. 339 ss.
[34] C. MICHEL, *Digital sovereignty is central to European strategic autonomy*, *Speech at "Masters of digital 2021" online event*, 3 February 2021.
[35] Criticamente sul punto vedasi S. POLI, *Reinforcing Europe's Technological Sovereignty Through Trade Measures: The EU and Member States' Shared Sovereignty*, in *EP*, 2023, p. 429 ss.

Europe's ability to act independently in the digital world»[36], si specifica infatti (oltre che nell'essere economicamente indipendenti da Stati terzi per quanto attiene alla produzione e all'utilizzo di infrastrutture e tecnologie digitali[37]) nella c.d. «normative digital sovereignity»[38], che riguarda specificamente la capacità dell'Unione di determinare il quadro normativo, tanto europeo quanto internazionale, nel rispetto del quale devono operare le tecnologie digitali.

Su questo sfondo, un ruolo centrale è stato recentemente assunto dalla cybersicurezza[39] e, più in particolare, dalla definizione di *standard* volti a rendere i prodotti con elementi digitali presenti sul mercato interno (cyber)sicuri. All'interno di un quadro normativo in crescente evoluzione – che ha visto l'adozione del regolamento 2025/38 sulla cybersolidarietà[40] e della direttiva 2022/2555 sulla sicurezza delle reti

---

[36] Così T. MADIEGA, *Digital sovereignty for Europe*, in *EPRS Ideas Paper, PE 651.992*, 2020, p. 1. In dottrina, Smuha definisce la "sovranità digitale europea" come: «the European Union's ability to decide autonomously on its relationship with digital technology, both economically and normatively». Cfr. N. A. SMUHA, *Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective*, in G. BARRETT, P. MÜLLER-GRAFF, J. RAGEADE, V. VADÁSZ (eds.), *European Sovereignity: the Legal Dimension*, Cham, 2024, p. 127 ss., spec. 135.

[37] Si veda sul punto N. A. SMUHA, *op. cit.*, pp. 132-134, che utilizza in proposito il termine "economic digital sovereignity". Questa specificazione del concetto di "sovranità tecnologica (o digitale) europea" traspare chiaramente dal piano d'azione, presentato dalla Commissione, sulle sinergie tra l'industria civile, della difesa e dello spazio. Cfr. Commissione, *Piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio*, COM (2021) 70final, 22 febbraio 2021.

[38] Pur non facendo espresso riferimento alle nozioni di "economic digital sovereignity" e di "normative digital sovereignity", Poli e Fahey sembrano considerare la prima come necessario prerequisito della seconda. Le Autrici affermano infatti che «[s]hould the EU achieve a position of world leader in this area [*i.e.* that of digital technologies], it would also become capable of setting global standards». Cfr. S. POLI, E. FAHEY, *op. cit.*, p. 153.

[39] Ad oggi non vi è una definizione, internazionalmente accettata, del termine "cybersicurezza". Tuttavia, nell'ambito del diritto UE, esso viene concettualizzato come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche». V. art. 2, punto 1, regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[40] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di

e dei sistemi informativi[41], la revisione del regolamento 2019/881 sulla cybersicurezza[42], nonché la raccomandazione del Consiglio del 6 giugno 2025 relativa a un programma dell'UE per la gestione delle crisi informatiche[43] – questa necessità ha trovato, come anticipato, concretizzazione nel *Cyber Resilience Act*.

Il CRA ha così contribuito ad attuare una delle nove priorità strategiche enunciate dal programma di lavoro annuale dell'Unione per la normazione europea per il 2023[44], in cui si poneva come obiettivo della normazione proprio quello di «creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri»[45].

Oltre alla definizione (interna) di *standard* in materia di cybersicurezza, il CRA svolge anche un importante ruolo di promozione esterna di tali *standard* considerato che, come si esaminerà[46], esso si applica ai prodotti con elementi digitali messi a disposizione sul mercato interno indipendentemente dal loro luogo di produzione, contribuendo al ruolo dell'UE come attore digitale globale[47]. Un approccio che, così, sembra concretizzare quanto definito dalla strategia dell'UE in materia di cybersicurezza per il decennio

preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà).

[41] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 202, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[42] Regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti.

[43] Raccomandazione del Consiglio, del 6 giugno 2025, relativa a un programma dell'UE per la gestione delle crisi informatiche C/2025/3445.

[44] Commissione europea, *Programma di lavoro annuale dell'Unione per la normazione europea per il 2023*, adottato dalla Commissione *ex* art. 8 del regolamento (UE) n. 1025/2012.

[45] *Ivi*, priorità strategica n. 4 (cybersicurezza e requisiti di accessibilità), azione n. 5 (requisiti di cybersicurezza per i prodotti con elementi digitali). È interessante rilevare che già nel 2016, con la comunicazione dal titolo «Digitalizzazione dell'industria europea», la Commissione aveva identificato la cybersicurezza come un'area prioritaria per l'attività di normazione europea: Commissione europea, *Digitalizzazione dell'industria europea - Cogliere appieno i vantaggi di un mercato unico digitale*, COM (2016) 180final, 19 aprile 2016, p. 13.

[46] V. *infra*, par. 4.

[47] Il riferimento è a E. FAHEY, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022.

digitale del 2020[48], in cui la Commissione e l'Alto rappresentante ponevano espressamente l'accento sulla necessità per l'Unione di guidare, oltre i confini dell'UE, la definizione di *standard* relativi alla *cybersecurity*[49], innovando sotto questo profilo rispetto alla strategia sulla cybersicurezza del 2013[50].

3. *Tra resilienza del mercato interno e tutela dei valori europei: quale approccio nella definizione di* standard *di cybersicurezza dei prodotti?*

Nelle proprie conclusioni sulla cybersicurezza dei dispositivi connessi[51], del 2 dicembre 2020, il Consiglio sottolineava che:

> «l'Unione europea e i suoi Stati membri garantiscano la loro sovranità digitale e la loro autonomia strategica […]. Ciò include il rafforzamento della capacità di compiere scelte tecnologiche autonome e, in quanto uno dei principali pilastri, […] prodotti […] resilienti e sicuri […]. [Al contempo] i valori fondamentali dell'Unione europea preservano in particolare la vita privata, la sicurezza, l'uguaglianza, la dignità umana, lo Stato di diritto e l'internet aperta come prerequisiti per realizzare una società, un'economia e un'industria antropocentriche e orientate al settore digitale»[52].

Si mette dunque in luce la doppia natura che caratterizza l'approccio dell'Unione alla cybersicurezza dei prodotti connessi, un approccio che

[48] Commissione e AR-PESC, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN (2020) 18final, 16 dicembre 2020. Per una panoramica circa i principali ambiti d'azione della Strategia, si veda M. ROBLES-CARRILLO, *The European Union Strategy for Cybersecurity*, in D. MOURA VICENTE, S. DE VASCONCELOS CASIMIRO, C. CHEN (eds.), *The Legal Challenges of the Fourth Industrial Revolution: the European Union's Digital Strategy*, Cham, 2023, p. 173 ss.
[49] JOIN (2020) 18final, cit., p. 28.
[50] *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN (2013) 1final, 7 febbraio 2013. Silente circa la promozione internazionale di *standard* di cybersicurezza è anche la successiva strategia dell'Unione in materia di cybersicurezza: *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN (2017) 450final, 13 settembre 2017.
[51] Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, 2020/C 427/04, 2 dicembre 2020.
[52] *Ivi*, punto 1.

tende, simultaneamente, verso la resilienza del mercato interno[53] e la tutela dei valori europei.

Da un lato, infatti, la cybersicurezza è considerata una precondizione necessaria per assicurare la corretta operatività dei prodotti connessi, affrontandone le vulnerabilità tecniche diffuse e, di conseguenza, rafforzando la (cyber)resilienza[54] del mercato interno da eventuali attacchi informatici. In questo senso, le menzionate conclusioni del Consiglio riconoscono che, oltre alle tecnologie quali l'intelligenza artificiale, il *cloud computing* e le *blockchains*, «qualsiasi altra nuova applicazione e opportunità per una crescita economica sostenibile e un livello più elevato di digitalizzazione della nostra società [può] essere realizzat[a] *solo mediante dispositivi connessi sicuri sotto il profilo informatico*»[55]. Questo poiché i prodotti *hardware* e *software* sono sempre più soggetti ad attacchi informatici[56], i quali

[53] Così già Y. MIADZVETSKAYA, R. A. WESSEL, *The Externalisation of the EU's Cybersecurity Regime: the Cyber Diplomacy Toolbox*, in *EP*, 2022, p. 413 ss., p. 418.

[54] Sebbene il termine "resilienza" sia ricorrente nella strategia del 2020 sulla cybersicurezza, esso non viene definito esplicitamente. La relazione di previsione strategica del 2020, invece, lo concettualizza come: «la capacità non solo di resistere alle sfide e farvi fronte, ma anche di attraversare le transizioni in modo sostenibile, giusto e democratico». Commissione europea, *Relazione 2020 in materia di previsione. Previsione strategica: tracciare la rotta verso un'Europa più resiliente*, COM (2020) 493final, 9 settembre 2020, p. 2. Per approfondimenti sul termine e sulle sue implicazioni, si veda A. R. MANCA, P. BENCZUR, E. GIOVANNINI, *Building a Scientific Narrative Towards a More Resilient EU Society – Part 1: a Conceptual Framework*, JRC Report No. RC106265, Luxemburg, 2017. Da questa prospettiva, Kamara descrive dunque la "cyberresilienza" come «the preparedness of organisations against and ability to recover after cyber-attacks»: I. KAMARA, *European Cybersecurity Standardisation: a Tale of Two Solitudes in View of Europe's Cyber Resilience*, in *Innovation: The European Journal of Social Science Research*, 2024, p. 1441 ss. Per riflessioni sul legame intercorrente tra resilienza e cybersicurezza: I. LINKOV, A. KOTT, *Fundamental Concepts of Cyber Resilience: Introduction and Overview*, in I. LINKOV, A. KOTT (eds.), *Cyber Resilience of Systems and Networks*, Cham, 2019, p. 1 ss.; R. A. WESSEL, *op. cit.*, p. 283 ss.; E. LONGO, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Torino, 2024, p. 203 ss., spec. p. 208.

[55] Consiglio, *Conclusioni sulla cibersicurezza dei dispositivi connessi*, cit., punto 2, enfasi aggiunta.

[56] Tale criticità viene chiaramente evidenziata in Commission, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products

presentano – data la natura senza frontiere del cyberspazio[57] – una spiccata dimensione transfrontaliera[58].

In aggiunta, alti livelli di cybersicurezza dei prodotti connessi sono ritenuti indispensabili per promuovere la capacità di innovazione e la competitività dei produttori europei di tali tecnologie[59], accrescendo al contempo la fiducia dei consumatori nell'utilizzo dei prodotti connessi[60].

Questo approccio è stato poi ribadito dalla menzionata strategia dell'UE in materia di cybersicurezza per il decennio digitale. All'interno di una specifica sezione dal titolo «resilienza, sovranità tecnologica e leadership», veniva infatti affermato che, con l'aumento dei dispositivi connessi presenti sul mercato interno e, in particolare, con la diffusione crescente dell'*Internet of Things*, si rendeva necessario rafforzare gli *standard* di cybersicurezza dei prodotti connessi, al fine di «garantire la resilienza complessiva»[61]. Analogamente, sebbene in termini più generici, la successiva strategia dell'UE in materia di normazione ha posto l'accento sul valore delle norme europee quali strumenti capaci di assicurare proprio la resilienza del mercato interno[62].

L'enfasi posta dalle istituzioni UE sulla definizione di *standard* dei prodotti connessi quale condizione necessaria per tutelare e rafforzare

---

with digital elements and amending Regulation (EU) 2019/1020, SWD (2022) 282final, Part 1/3, 15 September 2022, p. 2.

[57] L'agenzia dell'Unione europea per la cybersicurezza (ENISA) definisce tale termine come: «the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace». ENISA, *Definition of Cybersecurity. Gaps and Overlaps in Standardisation*, 2015, p. 7.

[58] Relazione che accompagna la proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, del 15 settembre 2022, p. 1.

[59] Consiglio, *Conclusioni sulla cibersicurezza dei dispositivi connessi*, cit., punto 3.

[60] Id., *Council Conclusions on the Future of Cybersecurity: Implement and Protect Together*, doc. 10133/24, 21 May 2024, punto 1. Sul punto, C. SCHMITTNER ET AL., *Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act*, in M. YILMAZ ET AL. (eds.), *Systems, Software and Services Process Improvement*, Cham, 2024, p. 390 ss., spec. p. 391.

[61] JOIN (2020) 18final, cit., p. 10.

[62] COM (2022) 31final, cit., p. 1.

la resilienza del mercato interno non deve però sorprendere. Infatti, questa necessità si colloca in un contesto più ampio, che ha visto nell'affermazione di un «mercato unico per la cibersicurezza»[63] un requisito necessario per garantire il corretto funzionamento delle reti, dei servizi essenziali e delle infrastrutture critiche situate nel territorio dell'UE, nonché la sicurezza economica dell'Unione[64].

Dall'altro lato, l'approccio dell'Unione alla definizione di *standard* di cybersicurezza dei prodotti connessi tende alla salvaguardia e alla promozione internazionale dei valori posti alla base dell'ordinamento giuridico dell'UE. Un approccio, questo, che traspariva già dalla strategia in materia di cybersicurezza del 2013. Infatti, pur non riferendosi espressamente alla *promozione* internazionale di *standard* relativi alla cybersicurezza, essa sottolineava che l'azione dell'Unione relativa alla sicurezza nel cyberspazio doveva essere fondata sui diritti e sulle libertà fondamentali sancite dalla Carta dei diritti fondamentali dell'Unione europea, nonché sui valori europei[65]. La successiva comunicazione congiunta della Commissione e dell'Alto rappresentante dal titolo «[r]esilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE»[66] ribadiva tale visione.

Un focus (più) specifico sull'approccio valoriale che caratterizza l'azione dell'Unione in materia di *cybersecurity* emerge chiaramente dalla sezione della strategia dell'UE in materia di cybersicurezza dal titolo «promuovere un ciberspazio globale e aperto», ove la Commissione e l'Alto Rappresentante mettono in luce il contributo che l'Unione, «in quanto forte blocco economico e commerciale fondato sui valori democratici fondamentali»[67], può offrire alla definizione e promozione di *standard* internazionali in linea con i suoi valori e diritti

[63] JOIN (2020) 18final, cit., p. 6.
[64] Si veda sul punto Commissione europea e Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza, *Strengthening EU Economic Security*, JOIN (2025) 977final, 3 dicembre 2025.
[65] Viceversa, evidenzia la Comunicazione, non sarebbe possibile garantire la tutela di tali diritti e valori senza disporre di reti e sistemi informatici sicuri. V. JOIN (2013) 1final, cit., p. 4. Per un commento relativo alla tutela dei valori nel contesto della Strategia dell'Unione del 2013 in materia di cybersicurezza, si veda R. A. WESSEL, *op. cit.*, p. 286.
[66] JOIN (2017) 450final, cit., spec. p. 20.
[67] *Ivi*, p. 22.

fondamentali[68]. Ciò coerentemente con l'obiettivo cardine di tale strategia, cioè quello di garantire un «ciberspazio aperto e globale, nonché lo Stato di diritto, i diritti fondamentali, la libertà e la democrazia, ossia i valori chiave dell'UE»[69].

Questo "approccio valoriale" alla definizione degli *standard* in materia di cybersicurezza porta alla formulazione di due considerazioni. In primo luogo, un simile approccio è coerente con quello che emerge dalla strategia dell'UE in materia di normazione, ove la Commissione pone in evidenza come la definizione degli *standard* europei non deve rappresentare una «finalità a sé stante»[70], ma deve contribuire a preservare e rafforzare i valori su cui l'Unione si fonda[71].

In secondo luogo, e da una prospettiva di più ampio respiro, "l'approccio valoriale" nella definizione degli *standard* relativi alla cybersicurezza dei prodotti si pone in linea di continuità con il paradigma etico-valoriale e antropocentrico che sta caratterizzando l'azione dell'Unione in ambito digitale, sulla scorta del processo di «costituzionalizzazione»[72] della transizione tecnologica europea. Senza pretesa di esaustività, si ricordi che nella comunicazione del 2020 dal titolo «Plasmare il futuro digitale dell'Europa», la Commissione esprimeva la propria intenzione di far sì che «le soluzioni digitali di cui

[68] Si legge nella Strategia che: «[l]a formulazione di norme internazionali nei settori delle tecnologie emergenti e nell'architettura di base di Internet *in linea con i valori dell'UE* è essenziale per garantire che Internet rimanga globale e aperta, che le tecnologie siano antropocentriche, attente alla riservatezza, e che il loro uso sia legale, sicuro ed etico» (enfasi aggiunta).

[69] *Ivi*, p. 2.

[70] COM (2022) 31final, cit., p. 11.

[71] *Ivi*, p. 4. Analogamente, si veda la relazione di previsione strategica del 2020, in cui la Commissione sottolinea la necessità per l'Unione di definire gli *standard* internazionali affinché rispecchino i valori dell'UE: COM (2020) 493final, cit., p. 16.

[72] Per riflessioni sul tema, v. *inter alia* C. PADOVANI, M. SANTANIELLO, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-system*, in *International Communication Gazette*, 2018, p. 295 ss.; E. CELESTE, *Digital Constitutionalism: a New Systematic Theorisation*, in *International Review of Law, Computers & Technology*, 2019, p. 76 ss.; G. DE GREGORIO, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 2021, p. 41 ss.; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: a Road Towards Digital Constitutionalism?*, Oxford, 2021; G. DE GREGORIO, R. RADU, *Digital Constitutionalism in the New Era of Internet Governance*, in *International Journal of Law and Information Technology*, 2022, p. 68 ss.; F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *DUE*, 2022, p. 277 ss.

si avvale la società europea affondino le radici nei nostri *valori comuni*»[73]. Successivamente, l'esigenza di ancorare il processo di transizione digitale ai valori e ai diritti fondamentali europei è stata consacrata sia nella decisione 2022/2481 che istituisce il programma strategico per il decennio digitale 2030[74], sia nella nota Dichiarazione europea sui diritti e i principi digitali per il decennio digitale[75], adottata sotto forma di una dichiarazione comune del Parlamento europeo, del Consiglio e della Commissione. Pur non costituendo uno strumento giuridico vincolante, essa rappresenta un importante tassello volto a promuovere il modello europeo per la trasformazione digitale, un modello che, preme ribadirlo, è basato sui valori e sui diritti fondamentali europei, che devono essere rispettati tanto nello spazio fisico quanto in quello virtuale[76].

Su queste basi, il successivo paragrafo intende chiarire in quale misura il *Cyber Resilience Act* concretizzi il descritto paradigma, in particolare mediante la previsione di *standard* relativi alla cybersicurezza dei prodotti con elementi digitali.

[73] COM (2020) 67final, cit., p. 1, enfasi aggiunta.
[74] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030, in particolare art. 3, par. 1, lett. *a*).
[75] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, 2023/C 23/01, 23 gennaio 2023. Per commenti, anche precedenti all'adozione della Dichiarazione, v. L. CIANCI, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?*, in *DPCE*, 2022, p. 381 ss.; E. CELESTE, *Towards a European Declaration on Digital Rights and Principles: Guidelines for the Digital Decade*, in *Dcubrexitinstitute.eu*, 7 February 2022; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Osservatorio DUE*, 17 marzo 2022; C. COCITO, P. DE HERT, *The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights)*, in *Computer Law & Security Review*, vol. 50, 2023, p. 1 ss.; E. CELESTE, *Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights*, in A. ENGEL, X. GROUSSOT, G. T. PETURSSON (eds.), *New Directions in Digitalisation. Perspectives from EU Competition Law and the Charter of Fundamental Rights*, Cham, 2025, p. 255 ss.
[76] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, cit., punto 1.

4. *La concretizzazione del paradigma: il regolamento 2024/2847 sulla cyberresilienza*

Annunciato dalla presidente della Commissione europea Ursula von der Leyen nel suo discorso sullo stato dell'Unione del 2021[77], il regolamento 2024/2847 sulla cyberresilienza è stato adottato dal Parlamento europeo e dal Consiglio nel mese di ottobre 2024, entrando ufficialmente in vigore il 10 dicembre dello stesso anno[78]. Adottato *ex* art. 114 TFUE[79], il CRA mira a diminuire le vulnerabilità dei prodotti con elementi digitali presenti sul mercato europeo[80], aumentando al contempo la responsabilità dei fabbricanti di tali prodotti durante il loro intero ciclo di vita[81].

Obiettivo cardine del regolamento è dunque quello di garantire uniformità nei requisiti di cybersicurezza propri dei «prodotti con elementi digitali»[82] presenti sul mercato, riducendo la frammentazione

[77] Commission, Discorso sullo stato dell'Unione 2021 della Presidente Ursula von der Leyen, 15 settembre 2021, SPEECH/21/4701.

[78] Ai sensi dell'art. 71, par. 2, reg. 2024/2847, cit., quest'ultimo si applicherà a partire dall'11 dicembre 2027. Tuttavia, l'art. 14 dello stesso (relativo agli obblighi di segnalazione posti in capo ai fabbricanti dei prodotti con elementi digitali) troverà applicazione a decorrere dall'11 settembre 2026, mentre il capo IV dall'11 giugno 2026.

[79] La Corte di giustizia ha confermato la legittimità dell'art. 114 TFUE quale base giuridica per gli atti di diritto derivato dell'Unione che presentano profili inerenti alla cybersicurezza nella sentenza Corte giust. 2 maggio 2006, C-217/04, *Regno Unito/ Parlamento e Consiglio*. Per una riflessione sull'uso di tale base giuridica nel contesto degli atti dell'Unione in materia di cybersicurezza, si rimanda a Y. MIADZVETSKAYA, R. A. WESSEL, *op. cit.*, pp. 418-421.

[80] Ai sensi dell'art. 2, par. 1, reg. 2024/2847, cit., esso si applica: «ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.» Per approfondimenti relativi all'ambito d'applicazione del regolamento, antecedenti alla sua adozione, si veda P. G. CHIARA, *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in *Rivista italiana di informatica e diritto*, vol. 5, n. 1, 2023, p. 143 ss., spec. pp. 144-145; M. BURRI, Z. ZIHLMANN, *The Cyber Resilience Act - an Appraisal and Contextualization*, in *EuZ*, n. 2, 2023, pp. B16-B20; M. RAIZ SHAFFIQUE, *Cyber Resilience Act 2022: a Silver Bullet for Cybersecurity of IoT Devices or a Shot in the Dark?*, in *Computer Law & Security Review*, 2024, p. 1 ss., spec. p. 7.

[81] Considerando n. 2, reg. 2024/2847, cit.

[82] Il *Cyber Resilience Act* abbraccia una definizione ampia del termine che, *ex* art. 3, punto 1, ricomprende «qualsiasi prodotto software o hardware e le relative soluzioni

normativa scaturente dalle diverse iniziative intraprese sia a livello UE, sia a livello nazionale[83].

Ciò posto, il CRA non si caratterizza unicamente come un atto volto ad incidere nella sfera del mercato interno dell'Unione. Infatti, applicandosi ai prodotti con elementi digitali messi a disposizione sul mercato europeo, indipendentemente dal loro luogo di produzione, il *Cyber Resilience Act* incide altresì sui produttori dei suddetti beni situati in Stati terzi, sulla scorta del c.d. "effetto Bruxelles"[84]. Questo non rappresenta certamente una peculiarità del regolamento in esame, caratterizzando anche altri atti normativi adottati dall'UE in ambito digitale, tra cui il regolamento generale sulla protezione dei dati personali ("GDPR")[85] e, più di recente, il regolamento 2022/2065 sui

---

di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente».

[83] Queste iniziative ricomprendono, ad esempio, la normativa dell'UE in materia di responsabilità per danno da prodotti difettosi (di cui alla direttiva 85/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi), nonché diverse iniziative intraprese a livello nazionale. V. relazione che accompagna la proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il reg. (UE) 2019/1020, cit., p. 4.

[84] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020. Sugli effetti extraterritoriali degli atti di diritto UE, vedasi altresì M. CREMONA, J. SCOTT (eds.), *EU Law Beyond EU Borders: the Extraterritorial Reach of EU Law*, Oxford, 2019; F. CASOLARI, M. GATTI (eds.), *The Application of EU Law Beyond Its Borders*, in *CLEER Papers*, n. 3, 2022. Con specifico riguardo alla proposta di *Cyber Resilience Act*, si veda M. BURRI, Z. ZIHLMANN, *op. cit.*, secondo cui, facendo leva sull'"effetto Bruxelles", il CRA potrebbe essere considerato «the "GDPR for IoT"».

[85] Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Sull'applicazione extraterritoriale del GDPR, vedasi *inter alia* S. SALUZZO, *The Principle of Territoriality in EU Data Protection Law*, in T. NATOLI, A. RICCARDI (eds.), *Borders, Legal Spaces and Territories in Contemporary International Law. Within and Beyond*, Cham, 2019, p. 121 ss.; C. RYNGAERT, M. TAYLOR, *The GDPR as Global Data Protection Regulation?*, in *AJIL Unbound*, 2020, p. 5 ss.; S. GUNST, F. DE VILLE, *The Brussels Effect: How the GDPR Conquered Silicon Valley*, in *European Foreign Affairs Review*, 2021, p. 437 ss.; C. PERARO, *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione europea verso Paesi terzi*, in *OIDU*, 2021, p. 666 ss.; O. J. GSTREIN, A. ZWITTER, *Extraterritorial Application of the GDPR: Promoting European Values or Power?*, in *Internet Policy Review*, 2021, p.

servizi digitali[86], il regolamento 2022/1925 sui mercati digitali[87], nonché il regolamento 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale o "*AI Act*")[88].

Ne consegue che il CRA assume una spiccata rilevanza per quanto attiene alla definizione e alla promozione di *standard* in materia di cybersicurezza dei prodotti a livello internazionale, considerato che i summenzionati fabbricanti – situati oltre i confini dell'Unione – dovranno soddisfare i requisiti ivi determinati per poter commercializzare i loro prodotti nel mercato interno, rafforzando di conseguenza la posizione dell'Unione quale *standard-setter* a livello globale[89].

---

1 ss.; C. KUNER, *Protecting EU Data Outside EU Borders under the GDPR*, in *CMLR*, 2023, p. 77 ss.

[86] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali). Ai sensi dell'art. 2, par. 1, esso si applica «ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, *indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari*», enfasi aggiunta. Per riflessioni in dottrina, v. K. SCHLEDT, S. WEGMANN, *Digital Empire? Extraterritorial Application of the Digital Services Act and Specific challenges for non-EU companies: Taking Chinese Companies as Example*, in *Computer Law Review International*, 2024, p. 138 ss.

[87] Art. 1, par. 2, regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali). Per un commento sull'ambito di applicazione territoriale del regolamento, cfr. H. DREWES, A. KIRK, *Extraterritorial Effects of the Digital Markets Act: The 'elusive long arm' of European Digital Regulation*, in *World Competition*, 2024, p. 473 ss.

[88] Art. 2, par. 1, lett. *a*) e *c*), regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Per alcune riflessioni in senso critico, cfr. E. CIRONE, *L'AI Act e l'obiettivo (mancato) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in questa *Rivista*, fasc. spec. n. 2, 2024, p. 51 ss.; M. ALMADA, A. RADU, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *GLJ*, 2024, p. 646 ss.

[89] In questo senso anche M. BURRI, Z. ZIHLMANN, *op. cit.*, p. B25; P. CAR, S. DE LUCA, *EU Cyber Resilience Act*, in *EPRS Briefing No. PE 739.259*, 2024, p. 4.

Alla luce di quanto esposto, appare quindi cruciale individuare quali siano i requisiti che i prodotti con elementi digitali devono rispettare[90] e, più specificamente, se e in quale misura essi traducono il paradigma precedentemente illustrato.

Per semplicità, è possibile suddividere in tre categorie le condizioni che consentono ai prodotti con elementi digitali di essere immessi sul mercato interno[91]. In primo luogo, si stabilisce che essi devono essere correttamente installati, utilizzati in modo conforme alla loro finalità prevista (o ragionevolmente prevedibile), oggetto di una manutenzione adeguata e, qualora applicabile, presentare i necessari aggiornamenti di sicurezza[92]. In secondo luogo, tali prodotti devono rispettare i «requisiti essenziali di cibersicurezza» di cui all'Allegato I, parte I, del regolamento[93]. Tali requisiti riguardano sia le specifiche tecniche dei prodotti volte a rafforzarne la sicurezza complessiva – tra cui rientrano l'assenza di vulnerabilità sfruttabili note[94], la previsione di aggiornamenti di sicurezza volti ad affrontare le vulnerabilità[95] e la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo[96] – sia alcune proprietà che presentano una più spiccata dimensione valoriale.

---

[90] Ai sensi dell'art. 13 del *Cyber Resilience Act* viene posto in capo ai fabbricanti dei prodotti con elementi digitali l'obbligo di assicurarsi che, al momento della loro immissione sul mercato interno, detti prodotti siano stati progettati, sviluppati e fabbricati conformemente ai requisiti di cui all'Allegato I, parte I. I fabbricanti devono inoltre garantire, per l'intera durata del periodo di assistenza, che le vulnerabilità di tali prodotti - compresi i loro componenti - siano gestite in modo efficace e in conformità ai requisiti previsti dall'Allegato I, parte II. In aggiunta, il CRA prevede alcuni obblighi, principalmente di *due diligence*, per altri operatori economici, tra cui i rappresentanti autorizzati, gli importatori e i distributori.

[91] Saranno successivamente le organizzazioni europee di normazione, di natura privata, a specificare tali requisiti in norme armonizzate, sulla base di una richiesta della Commissione. Nello specifico, il 3 febbraio 2025 la Commissione europea ha adottato una decisione di esecuzione riguardante una richiesta di normazione, sottoposta a CEN, CENELEC e ETSI, relativa ai requisiti essenziali di cybersicurezza propri del *Cyber Resilience Act*. V. Commission, *Implementing decision on a standardisation request as regards products with digital elements in support of Regulation (EU) 2024/2847*, C (2025) 618final, 3 February 2025.

[92] Art. 6, lett. *a*), reg. 2024/2847, cit.

[93] *Ibidem*.

[94] *Ivi*, allegato I, parte I, lett. *a*).

[95] *Ivi*, lett. *c*).

[96] *Ivi*, lett. *d*).

In particolare, viene specificato che i prodotti con elementi digitali devono esser in grado di proteggere la riservatezza dei dati personali trasmessi o altrimenti trattati, nonché tutelarne l'integrità da eventuali manipolazioni non autorizzate da parte dell'utilizzatore[97]. In aggiunta, nel rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. *c*), del GDPR, i prodotti con elementi digitali potranno trattare esclusivamente i dati che siano «pertinenti e limitati a quanto necessario in relazione alla finalità prevista del prodotto»[98]. La previsione di requisiti relativi alla tutela dei dati personali, in quanto diritto fondamentale garantito dall'art. 8 della Carta, rispecchierebbe – seppur limitatamente – quanto previsto dalla relazione che accompagna la proposta di regolamento, ove si enfatizzava come quest'ultimo potesse essere in grado di «migliorare in una certa misura la tutela dei diritti e delle libertà fondamentali (…) o la dignità e l'integrità della persona»[99].

In terzo luogo, il CRA specifica che i «processi» messi in atto dal fabbricante di prodotti con elementi digitali devono rispettare gli otto requisiti di gestione delle vulnerabilità elencati nell'Allegato I, parte II, del regolamento. Questi presentano un carattere eminentemente tecnico riguardando, ad esempio, i meccanismi per distribuire in modo sicuro gli aggiornamenti dei prodotti con elementi digitali[100], nonché la messa in atto di una specifica «politica di divulgazione coordinata delle vulnerabilità»[101].

Ne consegue che i requisiti di cui al *Cyber Resilience Act* sembrerebbero dar forma, principalmente, alla prima delle due dimensioni che contraddistinguono l'approccio dell'Unione alla determinazione e promozione degli *standard* di cybersicurezza dei

[97] *Ivi*, lett. *e*) e *f*).
[98] *Ivi*, lett. *g*).
[99] Relazione che accompagna la proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, cit., p. 9. Da questa prospettiva, la menzionata relazione sembra rispondere a quanto previsto dalla relazione del 2021 sull'applicazione della Carta, in cui la Commissione si impegnava a valutare gli effetti sui diritti fondamentali derivanti dalla proposta del CRA. Si veda Commissione, *Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*, COM (2021) 819final, 10 dicembre 2021, p. 38.
[100] Allegato I, parte II, punto 7, reg. 2024/2847, cit.
[101] *Ivi*, allegato I, parte II, punto 5.

prodotti connessi. Quella, cioè, volta a rafforzare la resilienza del mercato. Ciò pare in linea con l'impianto sistemico del CRA in cui – nonostante quanto auspicato dalla relazione che accompagna la proposta di regolamento – non troviamo alcun espresso riferimento ai valori dell'Unione, e soltanto limitati rimandi alla tutela dei diritti fondamentali[102]. Ad un primo esame, questo intento del legislatore si evince già dalla scelta della base giuridica del regolamento. Ossia, il solo articolo 114 TFUE[103], non accompagnato da altre basi giuridiche volte a tutelare i diritti fondamentali degli individui (tra cui l'articolo 16 TFUE), come è invece avvenuto nel noto caso dell'*AI Act*[104].

Ad una più attenta analisi, quanto esposto sembra altresì trovare conferma nella specifica declinazione dell'approccio basato sul rischio abbracciata dal CRA[105]. Esso, infatti, suddivide i prodotti con elementi

[102] Oltre alla previsione dei menzionati requisiti inerenti alla tutela dei dati personali, di cui all'allegato I, parte I, reg. 2024/2847, cit., i diritti fondamentali sono espressamente richiamati all'art. 57, par. 1, lett. *b*), del regolamento in esame. In particolare, vi si prevede che un'autorità di vigilanza del mercato di uno Stato membro possa chiedere a un determinato operatore economico di adottare misure appropriate nel caso in cui, sebbene conforme al regolamento, un prodotto con elementi digitali e i processi messi in atto dal fabbricante presentino un rischio significativo per «la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali». Per riflessioni in dottrina, si rimanda a P. G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, in *European Journal of Risk Regulation*, 2025, p. 1 ss., spec. p. 11; V. REMONDINO, *Il Cyber Resilience Act come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli*, in R. BRIGHI, G. ADINOLFI (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche*, Torino, 2025, p. 271 ss.

[103] La scelta dell'art. 114 TFUE quale base giuridica del *Cyber Resilience Act* viene esplicitata in Commissione, *Impact Assessment*, SWD (2022) 282final, cit., p. 18.

[104] Per alcune riflessioni sulla scelta della (doppia) base giuridica dell'*AI Act*, anche precedenti alla sua adozione, vedasi *inter alia* A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, p. 38 ss.; C. SCHEPISI, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in questa *Rivista*, 2022, p. 330 ss.; M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in questa *Rivista*, fasc. spec. n. 2, 2024, p. 1 ss., spec. pp. 12-13.

[105] Come noto tale approccio, nato nell'ambito della regolamentazione inerente alla sicurezza dei prodotti, ha, negli ultimi anni, caratterizzato numerosi atti adottati dall'UE in ambito digitale, tra cui il menzionato *AI Act*. Per un'esaustiva disamina

digitali in tre distinte categorie (prodotti di *default*, prodotti con elementi digitali importanti[106] e prodotti con elementi digitali critici[107]), alle quali corrispondono differenti procedure di valutazione dei requisiti di cybersicurezza precedentemente illustrati. In particolare, un prodotto con elementi digitali è considerato «importante» se la sua «funzionalità principale»[108] rientra in una delle categorie di cui all'allegato III del regolamento[109]. Si tratta, nello specifico, di prodotti le cui vulnerabilità possono comportare un impatto negativo grave, a causa della loro «funzionalità legata alla cibersicurezza»[110] o della specifica funzione da essi svolta, che può comportare il rischio di danneggiare altri prodotti con elementi digitali, nonché di arrecare danni alla salute, alla sicurezza o all'incolumità degli utilizzatori di tali prodotti mediante manipolazione diretta[111].

I medesimi criteri vengono applicati per definire i prodotti con elementi digitali critici[112], ai quali tuttavia il CRA aggiunge due ulteriori requisiti: l'esistenza di una «dipendenza critica»[113] da tale categoria di prodotti da parte dei soggetti di cui all'art. 3 della direttiva 2022/2555[114]; nonché la possibilità che gli incidenti e le vulnerabilità di tali prodotti possano causare «gravi perturbazioni delle catene di approvvigionamento critiche in tutto il mercato interno»[115].

---

circa l'evoluzione e le caratteristiche dell'approccio basato sul rischio nell'ambito del diritto UE, vedasi G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, 2022, p. 473 ss.

[106] Reg. 2024/2847, cit., art. 7.

[107] *Ivi*, art. 8.

[108] *Ivi*, art. 7, par. 1.

[109] Tali prodotti si suddividono, a loro volta, in prodotti di "classe I" (tra cui sono ricompresi, ad esempio, i *browser* autonomi e incorporati, i sistemi di gestione delle *password* e i sistemi di gestione della rete) e in prodotti di "classe II" (ad esempio, microprocessori a prova di manomissione).

[110] Considerando n. 43, reg. 2024/2847, cit.

[111] *Ivi*, art. 7, par. 2, lett. *a*) e lett. *b*).

[112] *Ivi*, art. 8, par. 2. Si tratta, nello specifico, di prodotti con elementi digitali la cui funzionalità principale è elencata nell'allegato IV del regolamento in esame.

[113] *Ivi*, art. 8, par. 2, lett. *a*).

[114] Figurano in tale categoria, ad esempio, i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, che si considerano medie imprese ai sensi dell'art. 2 dell'allegato alla raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese.

[115] Art. 8, par. 2, lett. *b*), reg. 2024/2847, cit.

Il regolamento in esame pare dunque plasmare il rischio associato ai prodotti con elementi digitali principalmente (se non unicamente) sui potenziali impatti negativi in termini di resilienza complessiva del mercato interno. Da questa prospettiva, il CRA si distingue perciò nettamente da altri atti adottati dall'Unione in ambito digitale, tra cui il menzionato regolamento sull'intelligenza artificiale, ove l'approccio basato sul rischio trova, almeno in via teorica, la sua *raison d'être* nella tutela dei valori europei e dei diritti fondamentali sanciti dalla Carta[116].

5. *Le implicazioni costituzionali della concretizzazione del paradigma: l'autonomia strategica aperta al vaglio del diritto internazionale*

Alla luce delle esaminate caratteristiche che contraddistinguono la definizione degli *standard* di cybersicurezza dei prodotti con elementi digitali, ci si può domandare quali siano le implicazioni generate dalla promozione di tale paradigma nell'ambito dell'azione esterna dell'Unione.

In prima battuta, si rileva che la promozione internazionale di *standard* europei in materia di cybersicurezza dei prodotti con elementi digitali, così come concretizzati dal *Cyber Resilience Act*, rispecchia uno degli obiettivi cardine che guida l'azione dell'UE sulla scena internazionale[117]. Segnatamente, quello di salvaguardare non soltanto i

[116] V. G. DE GREGORIO, P. DUNN, *op. cit.*, p. 477.

[117] Preme ricordare che, *ex* art. 21, par. 3, TUE, gli obiettivi di cui al par. 2 del medesimo articolo trovano applicazione non soltanto «[n]ell'elaborazione e attuazione dell'azione esterna nei vari settori compresi nel presenti titolo e nella parte quinta del trattato sul funzionamento dell'Unione europea», ma anche con riferimento agli "aspetti esterni" delle altre politiche dell'Unione, tra cui il mercato interno. Sugli obiettivi dell'azione esterna dell'UE, vedasi *ex multis* I. BOSSE-PLATIÈRE, *L'article 3 du traité UE: recherche sur une exigence de cohérence de l'action extérieure de l'Union européenne*, Bruxelles, 2009; M. E. BARTOLONI, E. CANNIZZARO, *Art. 21 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 222 ss.; J. LARIK, *Foreign Policy Objectives in European Constitutional Law*, Oxford, 2016; E. KASSOTI, R. A. WESSEL, *The Normative Effect of Article 3(5) TEU: Observance and Development of International Law by the European Union*, in P. GARCÍA ANDRADE (dir.), *Interacciones entre el Derecho de la Unión Europea y el Derecho Internacional Público*, Madrid, 2023, p. 19 ss.; E. CANNIZZARO, *The Value of International Values*, in W. T. DOUMA ET AL. (eds.), *The Evolving Nature of EU External Relations Law*, The Hague, 2021, p. 3 ss.; M. CREMONA, *Human Rights as*

valori dell'Unione[118] – che, nel caso del CRA, troverebbero un'embrionale concretizzazione nel diritto fondamentale alla tutela dei dati personali – ma anche i suoi interessi fondamentali[119], *ex* art. 21, par. l, lett. *a*), TUE[120].

Come evidenziato in dottrina, tale obiettivo andrebbe a conferire una dimensione eminentemente «costituzionale» al concetto (politico) di autonomia strategica che, nelle parole di Rapoport, è legato alla capacità dell'Unione «to play an active role on the international scene by *equipping itself with the tools it needs* to manage interdependecies *in accordance with its interests and values*»[121].

Questa lettura del concetto di autonomia strategica – che vede in quest'ultima una "leva", nelle mani del legislatore sovranazionale, per poter adottare (unilateralmente) strumenti giuridici volti a promuovere i valori e gli interessi dell'UE sulla scena internazionale – presenta perciò un forte legame con l'autonomia regolatoria riconosciuta in capo all'Unione stessa, in quanto ordinamento giuridico «di nuovo genere»[122] ed autonomo rispetto a quello internazionale. Ne consegue che l'Unione, agendo conformemente al proprio quadro costituzionale, è libera di determinare il livello di protezione di specifici interessi pubblici[123], tra cui può essere ricompresa la cybersicurezza *lato sensu* intesa[124].

---

a Value of EU Trade Policy, in M. BALBONI, C. DANISI (eds.), *Human Rights as a Horizontal Issue in EU External Policy*, Naples, 2021, p. 161 ss.

[118] Per riflessioni sulla proiezione dei valori dell'Unione europea sulla scena internazionale, cfr. E. SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2016.

[119] Nel caso del *Cyber Resilience Act*, tali interessi riguarderebbero la volontà delle istituzioni politiche dell'UE di promuovere la resilienza del mercato interno attraverso specifici *standard* riguardanti la cybersicurezza dei prodotti con elementi digitali.

[120] Si veda sul punto Hoffmeister, secondo cui il concetto di autonomia strategica sarebbe intrinsecamente connesso a quanto disposto dall'art. 21, par. 2, lett. *a*), TUE. V. F. HOFFMEISTER, *op. cit.*, p. 672.

[121] C. RAPOPORT, *Setting Norms*, cit., p. 448, enfasi aggiunta.

[122] Come riconosciuto nella celebre sentenza Corte giust. 5 febbraio 1963, 26/62, *Van Gend en Loos*.

[123] Corte giust. parere 30 aprile 2019, 1/17, punto 150. Sul punto, v. C. RAPOPORT, *Balancing on a Tightrope: Opinion 1/17 and the ECJ's Narrow and Tortuous Path for Compatibility of the EU's investment Court System (ICS)*, in *CMLR*, 2020, p. 1725 ss., spec. pp. 1751-1755.

[124] A questo proposito, è interessante rilevare che diversi accordi di libero scambio recentemente negoziati e/o conclusi dall'Unione con Paesi terzi ricomprendono la

Detto ciò, è però necessario chiedersi se, ed eventualmente in quale misura, il perseguimento dei menzionati obiettivi dell'Unione tramite atti unilaterali capaci di produrre effetti *de facto* a livello internazionale (quale il *Cyber Resilience Act*) trovi, all'interno del quadro costituzionale dell'Unione, dei limiti.

A questo proposito, viene in rilievo il necessario rispetto del diritto internazionale[125] (di natura sia pattizia[126] che consuetudinaria[127]) vincolante per le istituzioni dell'Unione, in quanto fonte sovraordinata al diritto derivato[128]. Come evidenziato in dottrina[129], un *corpus* di regole che acquisisce indubbiamente importanza – data la natura del CRA quale atto volto a definire gli *standard* dei prodotti con elementi digitali immessi sul mercato interno – è rappresentato dal diritto dell'Organizzazione mondiale del commercio (OMC)[130]. Invero, dubbi

cybersicurezza all'interno degli obiettivi politici legittimi che possono essere perseguiti dalle Parti in virtù del loro rispettivo "*right to regulate*". Si veda, in via esemplificativa, l'accordo tra l'Unione europea e il Giappone per un partenariato economico, art. 18.1, par. 2, lett. *h*).

[125] *Ex* art. 3, par. 5, e art. 21, par. 1, TUE.

[126] Come noto, ai sensi dell'art. 216, par. 2, TFUE, gli accordi internazionali conclusi dall'Unione vincolano sia le istituzioni UE sia gli Stati membri.

[127] Corte giust. 16 giugno 1998, C-162/96, *Racke*, punto 45; 21 dicembre 2011, C-366/10, *Air Transport Association of America*, punto 101. Si veda sul tema A. GIANELLI, *Customary International Law in the European Union*, in E. CANNIZZARO, P. PALCHETTI, R. A. WESSEL (eds.), *International Law as Law of the European Union*, Leiden, 2011, p. 93 ss.

[128] Corte giust. 10 settembre 1996, C-61/94, *Commissione/Germania*, punto 52; 3 giugno 2008, C-308/06, *Intertanko*, punto 42.

[129] Sul legame tra *standard* in materia di cybersicurezza e le norme dell'Organizzazione mondiale del commercio, si rimanda a S. PENG, *Cybersecurity Threats and the WTO National Security Exceptions*, in *Journal of international Economic Law*, 2015, p. 449 ss.; A. ODDENINO, *Digital Standardization, Cybersecurity issues and International Trade Law*, in *Questions of International Law*, 2018, p. 31 ss.; J. P. MELTZER, *Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules*, in *Global Economy & Development working paper*, n. 132, 2020; N. MISHRA, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, in *Journal of World Trade*, 2020, p. 567 ss.; G. GAGLIANI, *Cybersecurity, Technological Neutrality, and International Trade Law*, in *Journal of International Economic Law*, 2020, p. 723 ss.; S. PENG, *Cybersecurity and Trade Governance*, in J. CHAISSE, C. RODRÍGUEZ-CHIFFELLE (eds.), *The Elgar Companion to the World Trade Organization*, Cheltenham, 2023, p. 35 ss.

[130] L'Unione è parte dell'accordo che istituisce l'OMC insieme ai suoi Stati membri. V. decisione del Consiglio, del 22 dicembre 1994, relativa alla conclusione a nome

circa la possibile incompatibilità del regolamento con il diritto OMC erano già stati mossi, in fase di proposta, da alcuni paesi terzi in seno al comitato OMC sugli ostacoli tecnici agli scambi[131], costituito nel quadro dell'omonimo accordo internazionale[132].

Sebbene un'analisi puntuale della compatibilità del *Cyber Resilience Act* con le norme del diritto OMC vada oltre lo scopo della presente indagine[133], è interessante rilevare che la necessità di plasmare il contenuto del regolamento in linea con gli obblighi propri del diritto OMC sembra trasparire già dal preambolo del CRA, in cui si sottolinea che «[n]ei suoi rapporti con i paesi terzi l'Unione si sforza di promuovere il commercio internazionale di prodotti soggetti a regolamentazione»[134]. Nelle intenzioni del legislatore, questo sarebbe possibile attraverso la conclusione, *ex* art. 218 TFUE, di accordi sul reciproco riconoscimento[135], mediante i quali le parti accettano i rispettivi risultati delle valutazioni di conformità al fine di «promuovere e facilitare il commercio internazionale»[136]. Intenzione, questa,

della Comunità europea, per le materie di sua competenza, degli accordi dei negoziati multilaterali dell'Uruguay Round.

[131] Ad esempio, nell'ambito dell'incontro del Comitato tenutosi nel novembre del 2023, la Cina aveva evidenziato che, in assenza di una definizione dell'espressione "fattori di rischio non tecnici" di cui ai capi secondo e quinto della Proposta di CRA – definizione che si sarebbe dovuta basare su criteri trasparenti, non discriminatori e proporzionati – il testo del regolamento avrebbe potuto violare i principi della nazione più favorita e del trattamento nazionale. V. WTO, Committee on Technical Barriers to Trade – Minutes of the Meeting 8-10 November 2023, G/TBT/M/91, 1.2.2024, www.docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/TBT/M91.pdf&Open=True, par. 2.118. Tale preoccupazione è stata altresì avanzata in occasione dell'incontro del Comitato del marzo 2024, in cui la Cina ha sottolineato che «[i]t is recommended to clarify the scope of "non-technical risk factors", and relevant factors should be based on validated, transparent, non-discriminatory, and proportionate criteria». Cfr. WTO, Committee on Technical Barriers to Trade – Minutes of the Meeting 13-15 March 2024, G/TBT/M/92, 24 May 2024, www.docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/TBT/M92.pdf&Open=True, par. 2.66.

[132] Accordo sugli ostacoli tecnici agli scambi del 1994.

[133] Per un'indagine sulla compatibilità del CRA con l'Accordo sugli ostacoli tecnici agli scambi, si rimanda a G. ADINOLFI, R. MAGNAGHI, *Il Cyber Resilience Act nella prospettiva degli accordi commerciali dell'Unione europea*, in R. BRIGHI, G. ADINOLFI (a cura di), *op. cit.*, p. 175.

[134] Considerando n. 123, reg. 2024/2847, cit.

[135] Il rinvio è dunque al principio del mutuo riconoscimento degli *standard*, di cui al menzionato accordo sugli ostacoli tecnici agli scambi.

[136] Art. 34, reg. 2024/2847, cit.

reiterata dalla Commissione europea e dall'Alto rappresentante nella strategia digitale internazionale per l'Unione europea del giugno 2025[137].

È bene però evidenziare che, anche qualora l'Unione concludesse tale tipologia di accordi con Stati terzi, ciò non inciderebbe sulla (eventuale) incompatibilità del CRA con le norme dell'Organizzazione. Nella sfera del diritto internazionale, la possibilità di invocare l'incompatibilità del *Cyber Resilience Act* con le disposizioni del diritto OMC potrebbe portare all'instaurazione di una controversia dinnanzi al meccanismo di soluzione delle controversie dell'Organizzazione mondiale del commercio[138]. In tale sede, dall'accertamento dell'incompatibilità del CRA con le norme OMC deriverebbe la responsabilità internazionale dell'Unione che, qualora non

[137] JOIN (2025) 140final, cit., p. 10.

[138] In generale sul tema, si rimanda a M. DISTEFANO, *Soluzione delle controversie nell'OMC e diritto internazionale*, Padova, 2001; G. SACERDOTI, *Il sistema di soluzione delle controversie dell'OMC a dieci anni dalla sua istituzione*, in E. SCISO (a cura di), *L'OMC 1995-2005: bilanci e prospettive*, Roma, 2006, p. 203 ss.; G. ADINOLFI, *La soluzione delle controversie*, in G. VENTURINI (a cura di), *L'Organizzazione mondiale del commercio*, Milano, 2015, p. 303 ss.
Occorre evidenziare che, a causa dell'attuale inoperatività dell'Organo d'appello dell'OMC, i Membri dell'Organizzazione potranno instaurare una controversia unicamente davanti ai *panel* costituiti ai sensi dell'Art. 6 dell'Intesa sulle norme e sulle procedure che disciplinano la risoluzione delle controversie del 1994, con la possibilità di appellare le decisioni dei suddetti *panel* mediante il meccanismo arbitrale di cui al *Multi-Party Interim Appeal Arbitration Arrangement* (*MPIA*) del 2020, di cui l'UE è parte. Per riflessioni sulla "crisi" dell'Organo d'appello dell'OMC, anche con riferimento al *MPIA*, cfr. E. BARONCINI, *Attacco ai magnifici sette: il blocco nella composizione dell'Organo d'appello dell'OMC*, in *Archivio giuridico Filippo Serafini*, n. 1, 2018, p. 35 ss.; G. VIDIGAL, *Living Without the Appellate Body: Multilateral, Bilateral and Plurilateral Solutions to the WTO Dispute Settlement Crisis*, in *The Journal of World Investment and Trade*, 2019, p. 862 ss.; E. PETERSMANN, *How Should WTO Members React to Their WTO Crises?*, in *World Trade Review*, 2019, p. 503 ss.; C. LO, J. NAKAGAWA, T. CHEN (eds.), *The Appellate Body of the WTO and Its Reform*, Singapore, 2020; E. BARONCINI, *La proposta europea di riforma dell'OMC*, in P. MANZINI, M. VELLANO (a cura di), *Unione europea 2020. I dodici mesi che hanno segnato l'integrazione europea*, Padova, 2021, p. 135 ss.; O. STARSHINOVA, *Is the MPIA a Solution to the WTO Appellate Body Crisis?*, in *Journal of World Trade*, 2021, p. 787 ss.; J. PAUWELYN, *The WTO's Multi-Party Interim Appeal Arbitration Arrangement (MPIA): What's New?*, in *World Trade Review*, 2023, p. 693 ss.; J. MIRANDA, M. SÁNCHEZ MIRANDA, *Chronicle of a Crisis Foretold: how the WTO Appellate Body Drove Itself into a Corner*, in *Journal of International Economic Law*, 2023, p. 435 ss.

ottemperasse alla decisione dell'organo che l'ha adottata, potrebbe subire ritorsioni giustificate dalla controparte[139].

All'interno dell'ordinamento giuridico dell'Unione, invece, competente a pronunciarsi sul punto sarà, eventualmente, la Corte di giustizia dell'Unione europea (Corte o "CGUE")[140]. Nondimeno, secondo costante giurisprudenza della Corte, le disposizioni proprie del diritto OMC non rappresentano norme c.d. "*self-executing*"[141], non

[139] Art. 22, Intesa sulle norme e sulle procedure che disciplinano la risoluzione delle controversie, cit. Sulla possibilità di adottare contromisure in sede OMC, si rimanda a A. KOTERA, *On the Legal Character of Retaliation in the World Trade Organization System*, in N. ANDO ET AL. (eds.), *Liber Amicorum Judge Shigeru Oda*, Leiden, 2001, p. 911 ss.; K. ANDERSON, *Peculiarities of Retaliation in WTO Dispute Settlement*, in *World Trade Review*, vol. 1, n. 2, 2002, p. 123 ss.; G. SACERDOTI, *The Nature of WTO Arbitrations on Retaliation*, in C. P. BROWN, J. PAUWELYN (eds.), *The Law, Economics and Politics of Retaliation in WTO Dispute Settlement*, Cambridge, 2010, p. 23 ss.

[140] Essendo spirato il termine di due mesi dalla pubblicazione dell'atto per poter presentare ricorso in annullamento, *ex* art. 263, par. 6, TFUE, la questione potrà essere sottoposta alla Corte unicamente tramite rinvio pregiudiziale di validità o sollevando un'eccezione di invalidità.

[141] Posto che l'accordo internazionale di cui trattasi non specifichi l'intenzione delle parti di conferire o meno efficacia diretta alle sue disposizioni, secondo costante giurisprudenza della Corte di giustizia, ciò si verificherebbe nel caso in cui: (i) l'Unione è vincolata dall'accordo internazionale in questione; (ii) «la natura e l'economia generale» dell'accordo internazionale non ostano all'esame della validità dell'atto di diritto derivato; e (iii) le disposizioni pattizie invocate appaiono «dal punto di vista del loro contenuto, incondizionate e sufficientemente precise». Cfr. *Air Transport Association of America*, sopra citata, punti 53-54. Dunque, come evidenziato da Lenaerts, il rango di fonti interposte conferito dai Trattati agli accordi internazionali conclusi dall'Unione non ha impedito alla Corte di limitarne l'invocabilità in giudizio. V. K. LENAERTS, *Direct Applicability and Direct Effect of International Law in the EU Legal Order*, in I. GOVAERE ET AL. (eds.), *The European Union in the World: Essays in Honour of Marc Maresceau*, Leiden, 2014, p. 45 ss., spec. pp. 56-57. Analogamente, si veda anche Tancredi, secondo cui all'interno dell'ordinamento giuridico dell'Unione «the superiority of international norms is not automatic, but finally decided by the EU Courts»: A. TANCREDI, *On the Absence of Direct Effect of the WTO Dispute Settlement Body's Decisions in the EU Legal Order*, in E. CANNIZZARO, P. PALCHETTI, R. A. WESSEL (eds), *op. cit.*, p. 249 ss., p. 264. Sull'invocabilità delle norme degli accordi internazionali conclusi dall'Unione, si veda ampiamente F. CASOLARI, *L'incorporazione del diritto internazionale nell'ordinamento dell'Unione europea*, Milano, 2008, p. 331 ss.; J. KLABBERS, *The Validity of EU Norms Conflicting with International Obligations*, in E. CANNIZZARO, P. PALCHETTI, R. A. WESSEL (eds), *op. cit.*, p. 111 ss.; F. MARTINES, *Direct Effect of International Agreements of the European Union*, in *EJIL*, 2014, p. 129 ss.; N. GHAZARYAN, *Who Are the 'Gatekeepers'?: in Continuation of the Debate on the Direct Applicability and the Direct Effect of EU International Agreements*, in *YEL*, 2018, p. 27 ss.

potendo dunque essere invocate in giudizio come norme-parametro alla luce delle quali vagliare la (in)compatibilità con esse degli atti di diritto derivato dell'UE[142]. Infatti, come evidenziato nella nota sentenza *Portogallo/Consiglio*[143], «tenuto conto della loro natura e della loro economia, gli accordi OMC non figurano in linea di principio tra le normative alla luce delle quali la Corte controlla la legittimità degli atti delle istituzioni comunitarie»[144]. Nello specifico, la CGUE giunge a tale conclusione sulla base di due considerazioni, tra loro strettamente interconnesse. Da un lato, la mancanza di reciprocità che caratterizza gli accordi dell'Organizzazione mondiale del commercio[145]; dall'altro, l'esigenza di garantire agli organi legislativi ed esecutivi dell'UE il necessario margine di manovra per adempiere agli obblighi di cui agli accordi OMC[146].

In questo modo, la Corte tutela l'autonomia[147] dell'ordinamento dell'Unione da possibili interferenze esterne. Specificamente,

[142] Tra le numerose pronunce della Corte, si veda in particolare Corte giust. 5 ottobre 1994, C-280/93, *Germania/Consiglio*, punti 105-109. Occorre tuttavia ricordare che le norme OMC possono, eccezionalmente, essere invocate come parametro al fine di sindacare la validità degli atti di diritto derivato dell'Unione. Il riferimento è alle note eccezioni c.d. «*Fediol e Nakajima*», che ricorrono nel caso in cui l'Unione abbia inteso dare esecuzione a un particolare obbligo assunto nell'ambito dell'OMC, oppure qualora un atto di diritto derivato faccia espresso rinvio a determinate disposizioni di diritto OMC. Cfr. Corte giust. 22 giugno 1989, 70/87, *Fediol/Commissione*, punti 19-22; 7 maggio 1991, C-69/89, *Nakajima/Consiglio*, punti 29-31. Per commenti in dottrina, si veda P. EECKHOUT, *Judicial Enforcement of WTO Law in the European Union – Some Further Reflections*, in *Journal of International Economic Law*, 2002, p. 91 ss.; F. SNYDER, *The Gatekeepers: the European Courts and WTO Law*, in *CMLR*, 2003, p. 313 ss.; P. J. KUIJPER, M. BRONCKERS, *WTO Law in the European Court of Justice*, in *CMLR*, 2005, p. 1313 ss.; P. MENGOZZI, *L'invocabilità in giudizio delle regole dell'Organizzazione mondiale del commercio e la giurisprudenza comunitaria*, in F. FRANCIONI, F. LENZERINI, M. MONTINI (a cura di), *Organizzazione mondiale del commercio e diritto della Comunità europea nella prospettiva della risoluzione delle controversie*, Milano, 2005, p. 155 ss.; C. DORDI, *The Absence of Direct Effect of WTO in the EC and in other Countries*, Torino, 2010.

[143] Corte giust. 23 novembre 1999, C-149/96.

[144] *Ivi*, punto 47. Ne consegue che, come evidenziato da Tancredi, gli atti di diritto derivato, anche se potenzialmente in contrasto con il diritto OMC, rimangono validi all'interno dell'ordinamento giuridico dell'Unione, risultando «immune from judicial review». Cfr. A. TANCREDI, *op. cit.*, p. 252.

[145] *Portogallo/Consiglio*, sopra citata, punti 44-45.

[146] *Ivi*, punto 46.

[147] La dottrina dedicata all'autonomia del diritto UE è ampia. Si veda *inter alia* S. VEZZANI, *L'autonomia dell'ordinamento giuridico dell'Unione Europea. Riflessioni*

privandosi del potere di dichiarare invalidi gli atti di diritto derivato alla luce delle norme OMC – posta la loro inidoneità a fungere da norme parametro – la CGUE riconosce come spetti unicamente agli organi legislativi ed esecutivi dell'Unione valutare se, ed eventualmente in quale misura, adempiere agli obblighi derivanti dagli accordi OMC. In ultima istanza, si difenderebbe il principio dell'equilibrio istituzionale[148] al fine di garantire non soltanto la corretta allocazione dei poteri tra le Istituzioni, ma anche l'effettiva capacità, del legislatore e dell'esecutivo, di bilanciare i differenti interessi in gioco, assicurando così il perseguimento di determinati interessi pubblici[149].

L'autonomia regolatoria presterebbe così il fianco ad una lettura che la avvicina ad una differente concezione, teorizzata da Lenaerts, del principio stesso di autonomia. Quella, cioè, di autonomia "funzionale"[150], che mira a tutelare – da un punto di vista sostanziale e non strettamente formale – le «caratteristiche essenziali dell'Unione e del diritto dell'Unione»[151], attinenti cioè «alla struttura costituzionale

all'indomani del parere 2/13 della Corte di giustizia, in *RDI*, 2016, p. 68 ss.; K. LENAERTS, *The Autonomy of European Union Law*, in *DUE*, 2018, p. 617 ss.; C. ECKES, *The Autonomy of the EU Legal Order*, in *Europe and the World: a Law Review*, 2020, p. 1 ss.; L. S. ROSSI, *Autonomie Constitutionnelle de l'Union Européenne, Droits Fondamentaux et Méthodes d'Intégrations des Valeurs "Externes"*, in A. ILIOPOULOU PENOT, L. XENOU (sous la direction de), *La Charte des droits fondamentaux, source de renouveau constitutionnel européen?*, Paris, 2020, p. 53 ss.; L. LIONELLO, *L'autonomia dell'ordinamento giuridico dell'Unione europea. Significato, portata e resistenze alla sua applicazione*, Torino, 2024; C. CONTARTESE, *The Principle of Autonomy in EU External Relations Law*, Padua, 2025.

[148] Conclusioni dell'Avv. gen. Ćapeta, del 17 novembre 2022, C-123/21 P, *Changmao Biochemical Engineering*, par. 41. In dottrina, vedasi A. TANCREDI, *op. cit.*, p. 260, secondo il quale «the whole problem of direct effect [of the WTO agreements] is, essentially, a matter of institutional balance between the judiciary and the EU political bodies».

[149] In questo senso A. ROSAS, *Case C-149/96, Portugal v. Council. Judgment of the Full Court of 23 November 1999, nyr.*, in *CMLR*, 2000, p. 797 ss., spec. p. 816; A. TANCREDI, *op. cit.*, p. 264.

[150] Si veda K. LENAERTS, *Le cadre constitutionnel de l'Union et l'autonomie fonctionnelle de son ordre juridique*, in J. MALENOVSKÝ, D. PETRLÍK (sous la direction de), *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux: liber amicorum Jirí Malenovský*, Bruxelles, 2020, p. 285 ss.

[151] Così Corte giust. 6 marzo 2018, C-284/16, *Achmea*, punto 33 e giurisprudenza ivi citata.

dell'Unione nonché alla natura stessa di tale diritto»[152], tra cui è ricompreso il principio dell'equilibrio istituzionale[153].

Da ciò deriva dunque che, se il concetto di autonomia strategica, perseguito mediante la definizione degli *standard* propri del CRA, può rappresentare una "spada" per la proiezione dei valori e degli interessi fondamentali dell'Unione nella sfera internazionale, il principio di autonomia funge da "scudo"[154], proteggendo l'ordinamento giuridico dell'UE da eventuali interferenze esterne, *in casu* le norme OMC.

Alla luce delle considerazioni che precedono, preme portare all'attenzione un ultimo punto. Se l'Unione, come esaminato, è indubbiamente chiamata a rispettare il diritto internazionale, al contempo essa è altresì tenuta a "sviluppare" quest'ultimo, *ex* art. 3, par. 5, TUE. Questo anche al fine di dar forma, concretamente, alla dimensione "aperta" della nozione di autonomia strategica. Da questa prospettiva, alcuni strumenti pattizi recentemente negoziati dall'Unione, nonché alcuni atti di *soft law*, sembrano testimoniare una crescente – seppur embrionale – tendenza volta a valorizzare la cooperazione tra le l'Unione e (alcuni) Stati terzi in materia di certificazioni e *standard* di cybersicurezza. Paradigmatici a questo riguardo sono i due accordi sul commercio digitale[155] negoziati dall'Unione con, rispettivamente, la Corea del Sud[156] e Singapore[157], i quali prevedono l'obbligo per le Parti di adoperarsi al fine di utilizzare, in materia di cybersicurezza, «risk-based approaches that rely on risk

[152] *Ibidem*.
[153] Parere 1/17, sopra citato, punti 109-110.
[154] V. K. LENARTS, J. A. GUTIERREZ-FONS, *Epilogue. High Hopes: Autonomy and the Identity of the EU*, in *EP*, 2023, p. 1495 ss., spec. p. 1499.
[155] Per un'analisi del contenuto di tali accordi, precedente alla conclusione dei negoziati, si rimanda a V. REMONDINO, *Gli accordi sul commercio digitale tra liberalizzazione degli scambi e protezione dei dati personali e della privacy: implicazioni per la politica commerciale comune dell'Unione europea*, in questa *Rivista*, 2024, p. 201 ss.
[156] Accordo sul commercio digitale UE-Corea, testo disponibile all'indirizzo www.circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/1bddb97a-c02e-41e6-95d1-6e41029c880f/details?download=true. I negoziati dell'accordo si sono conclusi in data 10 marzo 2025.
[157] Accordo sul commercio digitale UE-Singapore, testo disponibile all'indirizzo www.circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/66ccfa9f-e239-4893-8e12-64f8ff1d1221/details. L'accordo è stato firmato dalle Parti in data 7 maggio 2025.

management best practices and on standards developed in a consensus-based, transparent, and open manner»[158]. Da una prospettiva analoga, alcuni accordi di libero scambio recentemente conclusi dall'UE[159] includono, tra le aree di cooperazione bilaterale in materia di commercio digitale, la collaborazione sui profili di cybersicurezza "pertinenti per il commercio digitale"[160], tra cui possono essere ricompresi gli *standard* relativi ai prodotti connessi. Su questa scia si collocano anche alcuni "partenariati digitali"[161], strumenti di carattere non vincolante adottati dall'Unione con determinati Paesi terzi. Ad esempio, il partenariato digitale UE-Singapore evidenzia chiaramente l'intenzione delle Parti «towards cooperating in the area of cybersecurity certifications and technology-neutral, objective, open, transparent, and interoperable cybersecurity standards»[162].

Così, la ricerca di soluzioni comuni a problemi comuni, quali gli attacchi informatici, potrebbe rappresentare un'efficace sintesi di quanto precedentemente illustrato. Infatti, l'adozione di strumenti multilaterali o bilaterali potrebbe comunque prestarsi a proiettare esternamente l'approccio alla cybersicurezza dei prodotti con elementi digitali abbracciato dall'Unione, in linea con la nozione di autonomia strategica aperta, evitando però i rischi di incompatibilità con il diritto internazionale precedentemente illustrati.

6. *Considerazioni conclusive*

Negli ultimi anni, il concetto "pervasivo" di autonomia strategica aperta è stato in grado di guidare l'azione dell'Unione nelle sue

[158] Art. 21, par. 3, Accordo sul commercio digitale UE-Corea; art. 22, par. 3, accordo sul commercio digitale UE-Singapore.
[159] In via esemplificativa, si veda l'art. 12.14, par. 4, dell'accordo di libero scambio tra l'Unione europea e la Nuova Zelanda.
[160] *Ibidem*.
[161] Ad oggi, l'Unione europea ha siglato quattro partenariati digitali con Paesi terzi, ossia rispettivamente con il Canada, il Giappone, la Corea del Sud e Singapore. V. Commissione europea, *Partenariati digitali*, www.digital-strategy.ec.europa.eu/it/policies/partnerships.
[162] Partenariato digitale UE-Singapore, par. 27, www.digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership. Similmente, vedasi anche il partenariato digitale UE-Canada, par. 29, www.digital-strategy.ec.europa.eu/en/news/canada-european-union-digital-partnership.

relazioni con il resto del mondo. In particolare, un ruolo chiave è stato attribuito alla definizione di *standard* (europei) volti a promuovere, sulla scena internazionale, tanto gli interessi fondamentali dell'Unione, quanto i valori di cui all'art. 2 TUE. Come sottolineato, ciò ha assunto una spiccata rilevanza in relazione alla definizione degli *standard* riguardanti le tecnologie nuove ed emergenti, campo in cui l'UE mira a consolidare la propria "sovranità tecnologica (o digitale)" su scala globale.

In questo contesto, viene in rilievo la cybersicurezza – o, più specificamente – gli *standard* volti a rendere i prodotti connessi (cyber)sicuri. Come evidenziato dall'analisi dei documenti di *policy*, l'Unione ha recentemente delineato il proprio approccio in materia di cybersicurezza dei prodotti connessi cercando di mettere in luce due particolari esigenze. Da un lato, la necessità di garantire la resilienza del mercato interno, rappresentando la cybersicurezza una condizione necessaria per garantire la corretta operatività dei prodotti connessi. Dall'altro lato, la tutela e la promozione dei valori europei, ponendosi così in linea di continuità con il paradigma etico-valoriale e antropocentrico che guida la transizione tecnologica dell'UE, sulla scorta del processo di «costituzionalizzazione» di quest'ultima.

Prendendo le mosse da queste considerazioni, l'analisi si è soffermata sul *Cyber Resilience Act*, in quanto atto volto a definire specifici requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali messi a disposizione sul mercato interno, indipendentemente dal loro luogo di produzione. Si è così evidenziato che i requisiti previsti dal CRA sembrano concretizzare, principalmente, la prima delle due dimensioni che contraddistinguono l'approccio dell'Unione alla definizione degli *standard* in materia di cybersicurezza dei prodotti con elementi digitali. Ossia, quella che mira a rafforzare la resilienza del mercato interno.

Alla luce di queste caratteristiche, sono state esaminate le implicazioni costituzionali generate dalla promozione del suddetto paradigma nell'ambito dell'azione esterna dell'Unione. In primo luogo, è stato chiarito che la promozione a livello internazionale degli *standard* di cybersicurezza di cui al CRA rispecchia quanto disposto dall'art. 21, par. 2, lett. *a*), TUE, ai sensi del quale nelle sue relazioni

con il resto del mondo l'Unione è chiamata a salvaguardare non soltanto i suoi valori, ma anche i suoi interessi fondamentali. Così facendo, si conferisce al concetto, eminentemente politico, di autonomia strategica aperta una rilevanza costituzionale.

Ciò detto e in secondo luogo, occorre tenere a mente che il perseguimento degli obiettivi dell'azione esterna dell'UE incontra un limite, ossia il necessario rispetto del diritto internazionale vincolante per l'Unione, *in casu* le norme proprie del diritto OMC. Tuttavia, tale vincolo trova, a sua volta, un controlimite. Si è infatti illustrato che, secondo costante giurisprudenza della CGUE, le norme dell'Organizzazione mondiale del commercio non rappresentano disposizioni c.d. "*self-executing*", non potendo perciò essere invocate come norme-parametro alla luce delle quali sindacare l'eventuale incompatibilità con esse degli atti di diritto derivato dell'Unione. Privandosi del proprio potere di sindacato giurisdizionale, la Corte tutela così l'ordinamento dell'UE da possibili interferenze esterne, proteggendosi dietro allo "scudo" dell'autonomia.

Alla luce delle riflessioni che precedono, la promozione dell'autonomia strategica mediante l'adozione di atti unilaterali, da un lato, e la tutela dell'ordinamento giuridico dell'UE attraverso il principio di autonomia, dall'altro, potrebbero trovare un elemento di sintesi nello "sviluppo" del diritto internazionale, *ex* art. 3, par. 5, TUE. Ricordandosi che «nessuno è un'isola»[163], l'Unione potrebbe così proiettare sulla scena globale il proprio approccio in materia di cybersicurezza dei prodotti con elementi digitali, evitando al contempo possibili frizioni con il diritto internazionale.

[163] Così F. CASOLARI, *Per una vera Unione di diritto*, cit., p. xii.

ABSTRACT (ITA)

Espressione dell'autonomia strategica aperta dell'Unione, la definizione di *standard* volti a promuovere, sulla scena internazionale, i valori e gli interessi fondamentali dell'UE ha assunto, negli ultimi anni, una significativa importanza. In particolare, a seguito dell'adozione del regolamento 2024/2847 sulla cyberresilienza (*Cyber Resilience Act* o "CRA"), un ruolo chiave è stato attribuito alla formulazione di *standard* capaci di rendere i prodotti *hardware* e *software* presenti sul mercato interno (cyber)sicuri, indipendentemente dal loro luogo di produzione. Prendendo le mosse da questo contesto e premessa una riflessione sul rapporto tra autonomia strategica aperta e promozione internazionale degli *standard* europei, il presente contributo si pone un duplice obiettivo. Anzitutto, si intende ricostruire il paradigma a cui l'Unione intende ispirarsi nella definizione degli *standard* di cybersicurezza dei prodotti connessi, quale emerge dai documenti di *policy* delle istituzioni dell'UE, al fine di valutare in quale misura il *Cyber Resilience Act* dia effettiva concretizzazione a tale paradigma. In secondo luogo, si esaminano le implicazioni costituzionali generate dalla promozione del suddetto paradigma così come concretizzato dal CRA. Posto che quest'ultimo si applica anche ai prodotti con elementi digitali fabbricati oltre i confini dell'UE, l'indagine è dedicata agli obiettivi che l'Unione si prefigge di realizzare nelle sue relazioni esterne, nonché ai limiti posti al conseguimento degli stessi.

ABSTRACT (ENG)

Expression of the Union's open strategic autonomy, the definition of standards aiming to promote, on the international scene, the values and fundamental interests of the UE has gained, over the past few years, a significant importance. In particular, following the adoption of regulation 2024/2847 on cyber resilience (*Cyber Resilience Act* or "CRA"), a pivotal role has been attributed to the delineation of standards capable of making the hardware and software products available on the internal market (cyber)safe, independently from their

place of production. Against this backdrop and granted a preliminary reflection on the relationship between open strategic autonomy and the international advancement of European standards, the present contribution has a double objective. First, it aims to reconstruct the paradigm to which the Union intends to inspire its action in the definition of cybersecurity standards for connected products, as it emerges from the EU institutions' policy documents, with a view to evaluate to what extent the Cyber Resilience Act materializes the said paradigm. Secondly, the contribution examines the constitutional implications flowing from the promotion of the analyzed paradigm as concretized by the CRA. Given that this latter one also applies to the products with digital elements manufactured outside the EU's borders, the investigation is devoted to the objectives that the Union seeks to realize in its external relations, as well as to the limits set to their attainment.