Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di

Raffaella Brighi e Giovanna Adinolfi

Giappichelli

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche


IUSTITIAM COLIMUS

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di
Raffaella Brighi e Giovanna Adinolfi

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111

http://www.giappichelli.it

ISBN/EAN 979-12-211-1735-6
ISBN/EAN 979-12-211-6531-9 (ebook)

Il volume è esito del progetto di ricerca "Ecocyber - Risk management for future cyber-physical ecosystems" nell'ambito dello Spoke 8 del Paternariato esteso SERICS- SEcurity and RIghts in the CyberSpace.
Finanziato dall'Unione Europea – NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 – Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca – D. D. 341 del 15/03/2022, PE7 SERICS – SEcurity and RIghts in the CyberSpace , Codice proposta: PE00000014, CUP: J33C22002810001,finanziato con Decreto n. 1556 del 11/10/2022.
I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, né può l'Unione Europea essere ritenuta responsabile per esse.

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: LegoDigit s.r.l. - Lavis (TN)

Indice

pag.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi

pag.

Capitolo 4

La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*

Giulia Gabrielli

Capitolo 5

Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente

Riccardo Allegri, Giorgio Scichilone

Capitolo 6

Politiche di cybersicurezza e implicazioni strategiche: una lettura politologica

Luigi Martino, Giampiero Giacomello, Oltion Preka

pag.

Parte II

Cybersicurezza e protezione degli eco-sistemi cyberfisici: una visione strumentale

Capitolo 7

Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il *Cyber Resilience Act*

Pier Giorgio Chiara

Capitolo 8

Il *Cyber Resilience Act* nella prospettiva degli accordi commerciali dell'Unione europea

Giovanna Adinolfi, Rachele Magnaghi

pag.

Capitolo 9

Profili informatico-giuridici della cybersicurezza nel procurement sanitario

Marco Mancarella

Capitolo 10

Cybersicurezza e *cyber deception*: sfide e prospettive processualpenalistiche

Mariagisa Landolfi

pag.

Parte III

Cybersicurezza e tutela dei diritti fondamentali: una prospettiva critica

Capitolo 11

Polizia, *big data* e società digitale: sicurezza dei dati, sicurezza dai dati

Giulia Fabini

Capitolo 12

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

Virginia Remondino

pag.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese, Giulia Lasagni

Parte IV

Consapevolezza, educazione e politiche

Capitolo 14

Cybersicurezza e fattore umano: un approccio educativo inclusivo

Antonella Carbonaro, Enrico Gnagnarella

pag.

Capitolo 15

Per un uso consapevole e sicuro delle tecnologie: strategie educative e strumenti di intervento

Valeria Barone, Thomas Casadei

pag.

Capitolo 8

Il *Cyber Resilience Act* nella prospettiva degli accordi commerciali dell'Unione europea

Giovanna Adinolfi [*], Rachele Magnaghi [**]

Abstract: Il presente capitolo intende esaminare il *Cyber Resilience Act* dell'Unione europea nella prospettiva del diritto del commercio internazionale. Il punto di partenza dell'analisi risiede nel fatto che i requisiti, tanto sostanziali quanto procedurali, introdotti dai legislatori europei allo scopo di ridurre il rischio di attacchi informatici attraverso prodotti con elementi digitali, trovano applicazione anche in relazione all'immissione sul mercato dell'Unione europea di beni originari da Paesi terzi. Alla luce di ciò, appare opportuno procedere a una verifica della compatibilità del CRA con il quadro normativo multilaterale di riferimento (in particolare, l'Accordo sugli ostacoli tecnici agli scambi che fa capo all'Organizzazione mondiale del commercio), posto che la misura appare suscettibile di avere un impatto sugli scambi internazionali. Particolare attenzione è data agli obblighi di non discriminazione e necessità della misura previsti dall'Accordo TBT.

Keywords: Cyber Resilience Act – Importazioni – Accordo TBT – Non discriminazione – Necessità – Standard internazionali

---

[*] Professoressa ordinaria di diritto internazionale presso il Dipartimento di studi internazionali, giuridici e storico-politici, Università degli Studi di Milano, giovanna.adinolfi@unimi.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. Sebbene il lavoro sia frutto di una riflessione congiunta delle autrici, sono da attribuire a Giovanna Adinolfi i paragrafi 1, 2 e 4 e a Rachele Magnaghi i paragrafi 3, 3.1, 3.2, 3.3 e 3.4.

[**] Assegnista di ricerca presso il Dipartimento di studi internazionali, giuridici e storico-politici, Università degli Studi di Milano, rachele.magnaghi@unimi.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Il *Cyber Resilience Act* (CRA) adottato il 23 ottobre 2024 [1] si inserisce nella disciplina dell'Unione europea in materia di cybersicurezza [2]. Le sue finalità possono essere ricondotte a due specifiche esigenze. Sulla base dell'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE), i legislatori europei sono intervenuti allo scopo di superare i limiti e le lacune del quadro normativo in tema di caratteristiche tecniche dei prodotti con elementi digitali (PED) che discendeva dal combinato disposto delle legislazioni nazionali e degli atti dell'Unione europea pertinenti. Seguendo la tradizionale prospettiva del "ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato" (art. 114, par. 1 TFUE), il Regolamento dispone un'armonizzazione minima ed orizzontale definendo i requisiti essenziali che i PED devono soddisfare per essere immessi sul mercato dell'Unione. Parallelamente, il CRA non trascura il fatto che i prodotti con elementi digitali possono costituire punti di accesso ad attacchi informatici, suscettibili di avere un profondo impatto negativo sulla vita politica, economica e sociale degli Stati. Si tratta infatti sia di beni di uso comune sia di componenti essenziali per il funzionamento di organizzazioni pubbliche e private. Il CRA li definisce quindi in termini molto ampi e generali, senza far riferimento a specifiche tipologie [3], e mira a ridurre la loro vulnerabilità agli attacchi informatici migliorando le garanzie di cybersicurezza collegate al loro uso.

Questa duplice finalità (realizzazione del mercato interno nel settore rilevante e aumento dei livelli di cybersicurezza) è perseguita introducendo una disciplina sostanziale che si applica ai PED indipendentemente dalla loro origine: realizzati presso stabilimenti localizzati nel territorio dell'Unione o importati da Stati terzi, i PED possono essere commercializzati nel mercato interno solo se soddisfano i requisiti essenziali stabiliti dal CRA [4]. Da questo approccio

---

[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo ai 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), GU L 2024/2847, 20.11.2024. Per una disamina, si veda, in questo volume, P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il Cyber Resilience Act*.

[2] Per una analisi delle finalità e dei contenuti normativi della strategia dell'Unione europea in materia di cybersicurezza, v. H. CARRAPICO-B. FARRAND, *Cybersecurity trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics*, in *Journal of Common Market Studies*, 2024, p. 147 e, in questo volume, F. CASOLARI, F. FERRI, S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*.

[3] Art. 3, parr. 1 e 2, CRA.

[4] *Ivi*, art. 4.

normativo deriva la previsione di obblighi rivolti sia a fabbricanti dell'Unione europea sia agli operatori economici coinvolti nell'immissione nel mercato interno di PED originari da paesi terzi. Quest'ultima prospettiva guida l'analisi che segue, intesa a individuare se e in quale misura il Regolamento introduca una barriera all'importazione dei beni considerati, tenendo in particolare conto degli obblighi che l'Unione ha assunto per effetto della partecipazione ad una fitta rete di trattati di liberalizzazione commerciale, *in primis* gli accordi che fanno capo all'Organizzazione mondiale del commercio (OMC).

L'esigenza di questa analisi sorge sulla base di una considerazione più generale, ovvero che le normative nazionali che fissano le caratteristiche dei beni che possono essere commercializzati nel territorio degli Stati (qui di seguito, normative tecniche) sono oggi considerate tra le principali barriere all'interscambio commerciale. Nell'ambito della loro *jurisdiction to prescribe*, gli Stati hanno da sempre mostrato una più o meno elevata propensione, nel perseguimento di finalità legittime quali la tutela dei consumatori, dell'ambiente, della sicurezza nazionale o dell'ordine pubblico, a definire i requisiti (tra cui dimensioni, composizione, etichettatura, imballaggi, processi produttivi) cui i beni devono rispondere per poter essere impiegati ed oggetto di operazioni di compravendita sul mercato nazionale. Il rilievo di queste normative è però aumentato nei decenni più recenti, in conseguenza di una serie di fattori: la ricerca scientifica e tecnologica, che ha messo in evidenza come l'utilizzo di determinati beni possa avere un impatto negativo sull'ambiente o sulla vita e la salute delle persone; le istanze provenienti dalla società civile, che sostengono la necessità che gli individui facciano scelte di consumo consapevoli; le crescenti sfide alla sicurezza nazionale, che oggi hanno non solo natura militare ma sono anche collegate al funzionamento ordinato di talune infrastrutture (quali i sistemi di trasporto, delle telecomunicazioni, energetici, sanitari ed elettorali). È proprio in questa ottica che si inserisce il *Cyber Resilience Act*, soprattutto nella sua dimensione valoriale, ove i legislatori europei hanno posto l'attenzione anche sulla difesa di taluni principi e valori fondamentali dell'Unione [5].

Al contempo, a fronte della riduzione ed eliminazione delle tradizionali barriere doganali al commercio che si è registrata a partire dal secondo dopoguerra, è emerso come le normative tecniche adottate dagli Stati possono comportare (talvolta intenzionalmente) una restrizione del commercio internazionale dei beni interessati. In generale, l'esistenza di regolamentazioni nazionali riguardo alle caratteristiche tecniche di un medesimo bene che si differenziano nei loro contenuti impedisce ai fabbricanti localizzati in uno Stato (salvo sostenere costi di produzione più elevati) di servire anche i mercati esteri. In questa prospettiva, si intende quindi analizzare se il CRA possa determinare la chiusura del mercato

[5] A tale riguardo, v. D. DIVERIO, *Le misure di armonizzazione dell'Unione europea in materia di cibersicurezza: profili istituzionali e basi giuridiche*, in *Eurojus*, 2024, p. 17 ss.

dell'Unione di prodotti con elementi digitali di origine straniera.

A questo scopo, l'analisi che segue evidenzia in primo luogo la disciplina prevista dal CRA in materia di importazione di prodotti con elementi digitali originari da Paesi terzi. Successivamente, l'attenzione sarà rivolta a verificare la compatibilità di questa normativa con gli obblighi internazionali assunti dall'Unione europea nel quadro degli accordi multilaterali facenti capo all'Organizzazione mondiale del commercio, con particolare riguardo all'Accordo sugli ostacoli tecnici agli scambi (*Agreement on Technical Barriers to Trade*, di seguito Accordo TBT). Questo, infatti, salvaguarda il potere dei 166 Membri dell'OMC di perseguire sul piano interno interessi legittimi definendo le caratteristiche tecniche dei beni commercializzati nei rispettivi mercati. Al contempo, allo scopo di impedire che le normative tecniche siano adottate con finalità (anche) protezionistiche, l'Accordo TBT pone alcune condizioni, *in primis* quelle di non discriminazione e necessità, e sollecita gli Stati ad agire in modo concertato, superando così le possibili incoerenze tra le rispettive discipline nazionali. Secondo queste diverse prospettive sarà quindi esaminato il CRA. Alcune considerazioni finali chiuderanno il lavoro.

2. L'impatto del Regolamento sulle importazioni nell'Unione europea di PED provenienti da paesi terzi

Come già anticipato, in base al CRA anche i prodotti con elementi digitali originari da Paesi terzi possono essere messi a disposizione sul mercato dell'Unione solo se soddisfano i requisiti essenziali di cybersicurezza di cui alla parte I dell'Allegato I al Regolamento e se i produttori hanno messo in atto processi conformi alla successiva parte II [6]. L'applicazione di tale comando coinvolge tre diverse categorie di soggetti, ovvero i fabbricanti esteri, gli importatori e i rappresentanti autorizzati, cui eventualmente i fabbricanti abbiano conferito mandato ad agire per loro conto [7]. Dal momento che il fabbricante estero sfugge all'ambito di applicazione territoriale del diritto dell'Unione europea, la conformità dei PED importati ai requisiti di processo e di prodotto definiti dai legislatori europei è realizzata per effetto di prescrizioni rivolte agli importatori e ai rappresentanti autorizzati, le cui attività ricadono a tutti gli effetti nella sfera di operatività del CRA [8].

[6] Art. 6 e art. 19, par. 1, CRA.

[7] V. artt. 13-15, 18 e 19, CRA.

[8] V. la definizione di rappresentante autorizzato e importatore offerta all'art. 3, rispettivamente commi 15 e 16.

In particolare, secondo l'art. 19, par. 2 CRA agli importatori si impone di accertare che il fabbricante estero dei PED che intendono immettere nel mercato dell'Unione abbia (i) redatto una *dichiarazione di conformità* di cui all'art. 28 CRA che attesti il rispetto dei requisiti essenziali di cybersicurezza previsti dal Regolamento, (ii) eseguito o fatto eseguire una *procedura di valutazione di conformità* secondo le modalità previste dal CRA e, infine, (iii) apposto la *marcatura CE* conformemente all'art. 30. Con l'intento di facilitare l'ingresso di PED esteri, i produttori stranieri possono nominare un proprio rappresentante autorizzato nel territorio dell'Unione col mandato, tra l'altro, di eseguire le attività sottoposte all'accertamento da parte degli importatori [9].

Anche per i PED importati è pienamente efficace la tecnica di armonizzazione c.d. di normalizzazione (oltre che minima e orizzontale, come sopra indicato) [10], in base alla quale il CRA si limita a prescrivere requisiti "essenziali" di cybersicurezza e rimanda la definizione di requisiti "specifici" all'adozione di "norme comuni", ovvero a) *norme armonizzate* approvate da organismi europei di armonizzazione in base al Regolamento 1025/2012 [11], b) *specifiche comuni* approvate dalla Commissione europea secondo quanto previsto all'art. 27, parr. 2.5 CRA o, infine, c) *sistemi europei di certificazione della cybersicurezza* adottati dalla Commissione europea su proposta dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), secondo le procedure di cui agli artt. 29 e 38 del *Cybersecurity Act* (CSA) [12].

---

[9] V. il combinato disposto di art. 13, par. 12, commi 2 e 3 e art. 18, par. 2.

[10] In generale, v. T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno*, Cacucci editore, Bari, 2018.

[11] Art. 27, par. 1 e par. 6, CRA. V. Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio, GU L 316, 14.11.2012, p. 12 ss. Sulle richieste avanzate dalla Commissione europea agli organismi europei di normazione per l'adozione di norme armonizzate relative ai requisiti specifici di cybersicurezza dei PED, v. i riferimenti alla nota 60 del contributo di P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti,* cit. in questo volume.

[12] Art. 27, par. 8, CRA. V. 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»), GUUE L 151, 7.6.2019, p. 15 ss. Un sistema europeo è stato adottato con il Regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024 recante modalità di applicazione del regolamento (UE) 2019/771 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cybersicurezza basata sui criteri

In base alla menzionata tecnica di "normalizzazione", le norme comuni così individuate sono prive di efficacia giuridica vincolante [13]. Non è infatti escluso che la conformità ai requisiti essenziali di cui al CRA di un prodotto con elementi digitali possa essere garantita dal possesso di caratteristiche specifiche diverse da quelle indicate nelle norme comuni, sotto piena responsabilità, per i PED originari da paesi terzi, degli importatori e, eventualmente, dei rappresentanti dei produttori stranieri. L'incentivo a conformarvisi risiede tuttavia nella presunzione di conformità ai requisiti "essenziali" obbligatori, che opera laddove la dichiarazione di conformità di cui all'art. 28 CRA richiami una delle tre categorie di norme comuni.

La tecnica della normalizzazione è abbandonata per i prodotti con elementi digitali "critici" (qui di seguito, PED critici) elencati nell'Allegato IV al Regolamento [14]. In virtù delle loro funzioni specifiche, dell'importanza che rivestono per l'attività degli operatori economici in settori da cui può dipendere il funzionamento di infrastrutture o catene di approvvigionamento critiche o, infine, degli effetti particolarmente gravi di eventuali attacchi informatici nei loro confronti, è infatti riconosciuto alla Commissione il potere di stabilire che i PED critici possano essere messi in circolazione nel mercato dell'Unione europea solo se soddisfano i requisiti di cui a un sistema europeo di certificazione della cybersicurezza approvato in base al *Cybersecurity Act* [15]. Per l'accesso al mercato dell'Unione, l'importatore deve quindi accertare (e l'eventuale rappresentante autorizzato assume la responsabilità di dichiarare) che i PED critici importati sono conformi al pertinente sistema europeo.

La disciplina contenuta nel CRA si applica ai PED importati anche con riferimento a quanto previsto per le procedure di valutazione di conformità, ovvero

---

comuni (EUCC), GU L 2024/482, 7.2.2024: in dottrina, v. R. RAMPÁŠEK-M. MESARČIK-J. ANDRAŠKO, *Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification?*, in *Computer Law & Security Review*, 2025.

[13] Questa circostanza non esclude che le norme comuni approvate da organismi europei di armonizzazione siano comunque parte del diritto dell'Unione europea, giacché costituiscono «misur[e] di attuazione necessaria e strettamente regolamentata dei requisiti essenziali definiti [da un atto di diritto derivato UE], realizzata su iniziativa e sotto la direzione nonché il controllo della Commissione»: sentenza del 27 ottobre 2016, James Elliott Construction Limited c. Irish Asphalt Limited, C-613/14, EU:C:2016:821, punto 43. Per un commento, con riferimento al CRA, v. M.R. 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. 14.

[14] Art. 8, CRA.

[15] *Ibidem*. A tale riguardo, si segnala che l'alinea 46 del preambolo al CRA afferma che taluni PED critici rientrano nell'ambito di applicazione dell'EUCC (v. *supra* n. 12) e che, pertanto, potrebbe essere opportuno subordinarne l'introduzione e la circolazione nel mercato interno al rispetto dei requisiti specifici ivi previsti.

riguardo ai processi che devono essere messi in atto per verificare che i beni in questione rispettino i requisiti essenziali di cui all'Allegato I del CRA. In tal caso, è previsto che gli importatori debbano accertare che prodotti con elementi digitali originari da paesi terzi siano stati sottoposti a una delle procedure di valutazione della conformità individuate dal Regolamento, differenziate in base al diverso rischio di cybersicurezza collegato alle loro funzionalità. L'art. 32 distingue le procedure di controllo interno condotte dal produttore estero o da un suo rappresentante autorizzato (Allegato VIII, modulo A e modulo H); le procedure realizzate da organismi autorizzati stabiliti nel territorio dell'Unione europea in ossequio alle prescrizioni dello stesso CRA (Allegato VIII, modulo B, unitamente a una procedura di controllo interno condotta secondo il successivo modulo C); infine, le procedure realizzate in base a un sistema europeo di certificazione della cybersicurezza, ove disponibile e applicabile. Vincoli stringenti sono previsti per i c.d. PED "importanti" definiti dall'art. 7 e Allegato III CRA, per i quali, in base al diverso grado di rischio, la procedura di controllo interno è esclusa *in toto* o in parte [16]. Una disciplina ancora più restrittiva è prevista per i PED critici di cui all'Allegato IV CRA [17].

Un terzo fattore sottoposto all'accertamento dell'importatore riguarda la marcatura CE quale segno distintivo. Apposta sui PED importati dal produttore straniero o da un suo rappresentante autorizzato, la marcatura deve essere conforme ai requisiti previsti dalla normativa rilevante dell'Unione [18], oltre che dall'art. 30 CRA, pena la mancata immissione nel mercato interno.

La disciplina brevemente descritta risponde all'obiettivo principale di garantire la cybersicurezza dei PED impiegati nel territorio dell'Unione europea. In sintesi, anche se importati, questi devono soddisfare i requisiti essenziali di processo e di prodotto previsti da CRA; una presunzione di conformità opera laddove i PED rispondano alle caratteristiche tecniche previste dalle eventuali specifiche comuni elaborate dalla Commissione europea o da organismi europei di armonizzazione; per i PED critici, la Commissione europea può prescrivere la loro immissione sul mercato sia subordinata al rispetto di un sistema europeo di certificazione della cybersicurezza. Inoltre, devono essere state eseguite le procedure di valutazione di conformità ai requisiti essenziali previste dal CRA, differenziate al grado di rischio relativo di ciascun PED. Infine, sul PED deve essere apposta la marcatura CE.

---

[16] Art. 32, parr. 2 e 3, CRA.

[17] *Ivi*, art. 32, par. 4.

[18] V. Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93, in GU L 218, 13.8.2008, p. 30 ss.

I PED originari da paesi terzi che non rispondono a una o più di queste caratteristiche, pur soddisfacendo gli eventuali requisiti di cybersicurezza previsti dall'ordinamento dello Stato di origine, per quanto sofisticati e adeguati a prevenire o limitare gli effetti negativi di attacchi informatici, non possono essere importati nel territorio dell'Unione. Da questo elemento discendono i potenziali effetti restrittivi sugli scambi internazionali del CRA [19].

3. La compatibilità del *Cyber Resilience Act* con l'Accordo TBT

Alla luce delle considerazioni sin qui svolte appare necessario approfondire la compatibilità del CRA con l'Accordo TBT.

Le norme dell'OMC applicabili agli ostacoli tecnici agli scambi vanno oltre le disposizioni generali relative alle barriere non tariffarie, così come stabilite nell'Accordo generale sulle tariffe doganali e sul commercio del 1994 (*General Agreement on Tariffs and Trade* – GATT 1994) e promuovono l'armonizzazione regolamentare. Invero, le disposizioni principali dell'Accordo TBT incoraggiano i Membri dell'OMC ad armonizzare le proprie misure nazionali con gli standard elaborati dagli organismi internazionali di normazione competenti.

L'Accordo riveste un ruolo centrale poiché intende garantire che le misure tecniche, pur perseguendo obiettivi legittimi di interesse pubblico, tra cui la tutela della sicurezza nazionale, non si traducano in restrizioni arbitrarie, ingiustificate o sproporzionate agli scambi internazionali.

Il CRA, introducendo requisiti essenziali per l'immissione sul mercato europeo dei PED, mette in evidenza la tensione tra la tutela di interessi pubblici legittimi – tra i quali la sicurezza nazionale riveste un ruolo preminente nel contesto della cybersicurezza [20] – e l'osservanza dei vincoli derivanti dalla disciplina commerciale multilaterale. Sotto quest'ultimo profilo, assumono particolare rilievo il principio di non discriminazione, l'obbligo di proporzionalità delle misure rispetto agli obiettivi perseguiti e la necessità di evitare che le misure adottate si traducano in barriere al commercio più gravose del necessario. In questa prospettiva, emerge con chiarezza, come già osservato in altri

[19] In generale, sul tema v. A.H. LIM, *Trade Rules for Industry 4.0. Why the Technical Barriers to Trade Agreement Matters Even More*, in S. PENG-C-F LIN-T. STREINZ (a cura di), *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration*, Cambridge University Press, Cambridge, 2021, p. 97.

[20] N. MISHRA, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, in *Journal of World Trade*, 2020, vol. 54, n. 4, pp. 567-590.

settori [21], la necessità di operare un bilanciamento equilibrato tra interessi economici e interessi di natura non economica.

Sebbene in dottrina il CRA abbia suscitato ampie riflessioni, soprattutto in merito alla sua opportunità e alla tutela dei diritti fondamentali [22], l'aspetto della compatibilità con il diritto del commercio internazionale sembra essere rimasto in gran parte trascurato. Tale questione merita invece attenzione, considerato che il CRA costituisce anche una misura di natura commerciale e, di conseguenza, rientra nel campo di applicazione della normativa dell'OMC.

Nonostante la letteratura abbia approfondito le interazioni tra la normativa in materia di cybersicurezza e gli accordi dell'OMC [23], esaminandone differenti prospettive, tra cui quella della neutralità tecnologica [24], ad oggi, non si riscontra un'analisi specifica riguardo al CRA.

Lo scopo della presente indagine è dunque duplice: offrire un inquadramento generale della questione e, al contempo, contribuire a colmare in parte la lacuna riscontrabile nella letteratura sul punto.

A livello metodologico, l'analisi sarà condotta principalmente alla luce della giurisprudenza dell'Organo di risoluzione delle controversie (*Dispute Settlement Body* – DSB) dell'OMC.

Benché allo stato attuale non sembri verosimile l'apertura di una controversia specificamente incentrata sul Regolamento – per ragioni di opportunità politica e sistemica – risulta comunque opportuno procedere a una verifica della sua compatibilità con il quadro normativo multilaterale di riferimento, posto che

---

[21] Cfr. J. CHAISSE-C. RODRÍGUEZ-CHIFFELLE, *WTO's legacy, roadblocks, and future in global economic regulation: an introduction*, in J. CHAISSE-C. RODRÍGUEZ-CHIFFELLE (ed.), *The Elgar Companion to the World Trade Organization*, Edward Elgar Publishing, 2023, p. 7. In materia di cambiamenti climatici, ad esempio, emerge l'anacronismo di talune disposizioni dell'OMC rispetto alla necessità di affrontare problematiche contemporanee, per le quali, al fine di contrastare efficacemente il fenomeno, può rendersi necessaria l'adozione di misure talvolta restrittive per il commercio internazionale. V. *ex multis*, S. AHMAD, *Examining the Inadequacy of the GATT's Rules-Exceptions Paradigm in the Fight Against Climate Change: The Case for a WTO Climate Waiver*, in *Penn Carey Law: Legal Scholarship Repository*, 2024.

[22] P.G. CHIARA, *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction*, in *International Cybersecurity Law Review*, 2022, vol. 2, n. 3, pp. 255-272; 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, pp. 1-16; P. ECKHARDT-A. KOTOVSKAIA, *The EU's Cybersecurity Framework: The Interplay between the Cyber Resilience Act and the NIS 2 Directive,* in *International Cybersecurity Law Review*, 2023, vol. 4, n. 2, pp. 147-164.

[23] J.P. MELTZER, *Cybersecurity, Digital Trade, and Data Flows*, Working Paper n. 132 del Global Economy and Development Brookings Institution, 2020.

[24] G. GAGLIANI, *Cybersecurity, Technological Neutrality, and International Trade Law*, in *Journal of International Economic Law*, 2020, vol. 23, n. 3, pp. 723-745.

la misura pare suscettibile di avere un impatto significativo sugli scambi commerciali.

3.1. Considerazioni preliminari sulla qualificazione del CRA ai sensi del TBT

Il primo profilo giuridico che emerge in relazione al Regolamento concerne la sua qualificazione ai sensi dell'Accordo TBT. La fase di qualificazione costituisce, infatti, un presupposto indefettibile per l'avvio di un'analisi giuridica. L'Accordo disciplina una «categoria limitata di misure» [25], distinguendo, a tal fine, tra regolamenti tecnici, standard e procedure di valutazione della conformità [26], e stabilendo prescrizioni differenziate in funzione della classificazione della misura.

Considerata la complessità e la portata del CRA, tale fase risulta particolarmente articolata. Innanzitutto, occorre fare riferimento all'Allegato 1.1 dell'Accordo TBT, che definisce il regolamento tecnico come «un documento [27] che stabilisce le caratteristiche di un prodotto o i relativi processi e metodi di produzione, comprese le disposizioni amministrative applicabili, al quale la conformità è obbligatoria. Esso può altresì comprendere, o trattare esclusivamente, terminologia, simboli, requisiti di imballaggio, marcatura o etichettatura così come si applicano a un prodotto, a un processo o a un metodo di produzione».

Stante la definizione sopra riportata, l'Organo di Appello (OdA) [28] ha elaborato un test tripartito volto a determinare se una misura possa qualificarsi come regolamento tecnico [29]. In primo luogo, il prodotto oggetto della misura deve

---

[25] *European Communities – Measures Affecting Asbestos and Products Containing Asbestos*, Organo d'Appello, 5 aprile 2001, WT/DS135/AB/R, (EC – Asbestos), par. 80.

[26] Si noti che tali tre misure sono descritte nell'Allegato 1 dell'Accordo TBT.

[27] Il termine «documento» ricomprende una vasta gamma di strumenti e si applica a diverse tipologie di misure ed è definibile come «qualcosa di scritto, inciso, ecc., che fornisce prova o informazione su qualsiasi argomento» e che possiede un contenuto normativo.

[28] Per maggiori informazioni v. P. VAN DEN BOSSCHE-W. ZDOUC (eds), *The Law and Policy of the World Trade Organization: Text, Cases, and Materials*, V ed., Cambridge University Press, Cambridge, 2022, pp. 233-244; P. VAN DEN BOSSCHE, *The Demise of the WTO Appellate Body: Lessons for Governance of International Adjudication?*, WTI Working Paper, n. 02/2021, 2021.

[29] *European Communities – Trade Description of Sardine*, Organo d'Appello, 23 ottobre 2002, WT/DS231/AB/R, (EC – Sardines), par. 176; *EC – Asbestos*, *op. cit.*, parr. 66-70; *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, Panel, 24 aprile 2012, WT/DS406/R, (US – Clove Cigarettes, Panel), parr. 7.24-7.25. Si noti che tali requisiti debbono essere soddisfatti cumulativamente, v. *European Communities – Measures Prohibiting the*

essere identificato o quantomeno identificabile. In secondo luogo, il documento applicabile al prodotto così individuato deve prescrivere caratteristiche proprie del prodotto, oppure processi e metodi di produzione ad esso riferiti. Infine, il rispetto di tali caratteristiche deve essere obbligatorio.

Riguardo alla "identificabilità" del prodotto, lo stesso non deve essere esplicitamente menzionato nel documento [30]. Invero, la nozione stessa di «caratteristica del prodotto» può fungere da criterio identificativo [31]. Quest'ultima è stata interpretata come comprensiva di «qualsiasi elemento oggettivamente definibile, qualità, attributo o altro segno distintivo di un prodotto» [32].

Il secondo requisito del test, ossia la definizione delle caratteristiche del prodotto, comporta che il documento in esame contenga disposizioni che ne determinino le proprietà specifiche. Le caratteristiche del prodotto comprendono sia elementi e qualità intrinseche del bene, sia aspetti ad esse connessi, quali i mezzi di identificazione, le modalità di presentazione e l'aspetto esteriore del prodotto [33]. L'importanza di queste caratteristiche correlate è chiarita dalla seconda frase dell'Allegato 1.1, secondo cui i regolamenti tecnici possono «comprendere o trattare esclusivamente terminologia, simboli, imballaggio, marcatura o requisiti di etichettatura» [34]. Sulla base di tale disposizione, requisiti relativi all'etichettatura o all'imballaggio sono stati ritenuti costituire regolamenti tecnici in diversi contenziosi [35].

Infine, affinché una misura possa essere qualificata come regolamento tecnico, essa deve disciplinare le caratteristiche del prodotto in «modo vincolante o cogente» [36]. In altri termini, la conformità ai requisiti deve risultare obbligatoria. A tale scopo, la presenza di sanzioni pecuniarie o penali poste a presidio del rispetto delle caratteristiche sancite dalla misura costituisce, di norma, un chiaro indicatore del carattere obbligatorio della stessa [37].

Importation and Marketing of Seal Products, Organo d'Appello, 18 giugno 2014, WT/DS400/AB/RWT/DS401/AB/R, (EC – Seal Products), parr. 5.28-5.29.

[30] *EC – Sardines*, *op. cit.*, parr. 176, 182, 183.

[31] *EC – Asbestos*, *op. cit.*, par. 70.

[32] Idem, par. 67.

[33] Idem.

[34] *EC – Seal Products*, *op. cit.*, par. 5.14. L'OdA ha precisato che gli elementi indicati in tale seconda frase «si aggiungono a, e possono essere distinti da» quelli contemplati nella prima frase dell'Allegato 1.1.

[35] Per maggiori dettagli cfr. E. SHEARGOLD, *Article 1 and Annex 1 TBT: General Provisions and Terms and Their Definitions*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022.

[36] *US – Tuna II (Mexico)*, *op. cit.*, par. 185.

[37] V. *EC – Asbestos*, *op. cit*., par. 72.

Alla luce di queste premesse, come già anticipato, il CRA prevede che i PED possano essere immessi sul mercato «soltanto se» (i) soddisfano i requisiti essenziali di cybersicurezza di cui alla parte I dell'Allegato I; e (ii) i processi predisposti dai fabbricanti per la loro produzione rispettano i requisiti stabiliti nella parte II del medesimo Allegato [38]. Inoltre, il Regolamento impone per i PED importanti (Allegato III) e i PED critici (Allegato IV) ulteriori requisiti per garantire la loro sicurezza informatica, alla luce dei maggiori rischi di vulnerabilità [39].

Il CRA stabilisce dunque le caratteristiche dei PED che gli operatori economici *devono* rispettare affinché i PED possano essere immessi sul mercato.

Ai fini dell'attestazione della conformità a tali requisiti, il Regolamento prevede l'apposizione della marcatura CE [40] accompagnata dalla dichiarazione di conformità [41], con eventuale possibilità o necessità di avvalersi di norme e sistemi europei di riferimento e quindi fruire di una presunzione di conformità [42]. Invero, per i PED critici, il ricorso al sistema europeo di certificazione della cybersicurezza – in alcune circostanze – diviene necessario ai fini dell'attestazione della conformità dei prodotti e, conseguentemente, della loro immissione sul mercato [43].

Il Regolamento prevede altresì procedure di valutazione della conformità differenziate in funzione del rischio relativo al prodotto [44] e definisce un quadro chiaro e vincolante per garantire la sicurezza dei prodotti digitali e la conformità ai requisiti essenziali, contribuendo alla protezione degli utenti e alla libera circolazione dei PED nel mercato interno dell'Unione europea.

Infine, il CRA prevede, *inter alia*, sanzioni amministrative in caso venga rilevata la non conformità ai requisiti essenziali prescritti [45].

Considerate tali principali caratteristiche del CRA e la definizione contenuta nell'Allegato 1.1 del TBT, si può dunque concludere che esso costituisce un regolamento tecnico ai sensi dell'Accordo.

Ciò comporta l'applicabilità dei principi enucleati nell'art. 2 TBT, i cui profili più rilevanti saranno esaminati nel dettaglio nelle sezioni successive.

---

[38] Art. 6, CRA.

[39] *Ivi*, artt. 7-8.

[40] *Ivi*, art. 30, v. *supra*.

[41] *Ivi*, art. 28, v. *supra*.

[42] *Ivi*, art. 27, v. *supra*.

[43] *Ivi*, art. 8, par. 1. Ai sensi dell'art. 32, par. 4 b), laddove le condizioni di cui all'art. 8 non sono soddisfatte agli operatori è garantita la possibilità di ricorrere alle procedure di conformità previste per i PED importanti di classe II.

[44] *Ivi*, art. 32.

[45] *Ivi*, art. 64.

Più nello specifico, essi includono il principio della nazione più favorita e del trattamento nazionale (art. 2.1), la prevenzione di ostacoli non necessari al commercio internazionale (art. 2.2), l'armonizzazione e il ricorso a standard internazionali (art. 2.4) e il riconoscimento dell'equivalenza (art. 2.7).

Per ragioni di completezza, va osservato che la complessità del CRA comporta l'emergere di ulteriori profili – seppur di minor rilevanza – ai sensi dell'Accordo TBT, che tuttavia, per motivi di sintesi e opportunità, non saranno approfonditi in questa sede.

L'Allegato 1.3 del TBT, definisce «procedura di valutazione della conformità» una «procedura utilizzata, direttamente o indirettamente, per determinare che i requisiti pertinenti nei regolamenti tecnici o nelle norme siano soddisfatti». Ai sensi della nota esplicativa all'Allegato 1.3, le procedure di valutazione della conformità «includono, tra l'altro, procedure di campionamento, prova e ispezione; valutazione, verifica e assicurazione della conformità; […]» [46].

Alla luce di tale definizione, appare evidente che le procedure di cui all'Allegato VIII del CRA rientrino nella categoria delle procedure di valutazione della conformità e, pertanto, soggiacciano all'applicazione degli artt. 5-9 dell'Accordo TBT. Invero, come ben sottolineato dalla giurisprudenza del DSB, un singolo provvedimento può contenere sia un regolamento tecnico sia le relative procedure di valutazione della conformità [47], situazione che appare applicabile anche al CRA.

Va tuttavia osservato che se sotto il profilo del regolamento tecnico, il CRA introduce requisiti essenziali e distinzioni in termini di obblighi basati sul livello di rischio presentato dalle categorie di PED [48], sul piano delle procedure di conformità esso si limita a richiamare i moduli già stabiliti e previsti dalla Decisione 768/2008/CE, senza introdurre modifiche di carattere sostanziale alle stesse.

Pertanto, il carattere innovativo e al contempo potenzialmente problematico del CRA, che richiede una valutazione attenta alla luce dell'Accordo TBT, si rinviene nel suo inquadramento quale regolamento tecnico, piuttosto che nelle procedure di valutazione della conformità da esso previste. Precisamente, acquisiscono particolare rilevanza i requisiti essenziali prescritti dal CRA all'Allegato I per tutti i PED. Invero, essi appaiono *prima facie* suscettibili di creare discriminazione e di configurarsi come un ostacolo tecnico agli scambi internazionali [49].

---

[46] *Russia – Measures Affecting the Importation of Railway Equipment and Parts Thereof*, Organo d'Appello, 5 marzo 2020, WT/DS499/AB/R, par. 5.210.

[47] *European Communities – Protection of Trademarks and Geographical Indications for Agricultural Products and Foodstuffs*, Panel, 20 aprile 2005, WT/DS290/R, par. 7.512.

[48] Cfr. P.G. CHIARA, *The Cyber Resilience Act*, *op. cit*.

[49] Art. 42, par. 4, CRA.

Ulteriore profilo di interesse, ai sensi del diritto OMC, risulta essere il richiamo "vincolante" al sistema EUCC previsto per i PED critici individuati con atto delegato dalla Commissione. Sebbene il richiamo al EUCC – considerato isolatamente – possa rientrare nella definizione di "standard" di cui all'Allegato 1.2 TBT [50], nell'ambito dei PED critici la loro potenziale trasformazione in prescrizioni vincolanti ne muterebbe la qualificazione in regolamento tecnico, con la conseguente applicabilità della normativa pertinente.

3.2. Conformità del CRA all'art. 2.1 del TBT

Essendo un regolamento tecnico, nell'analisi del CRA assume particolare rilievo, in primo luogo, il principio di non discriminazione sancito dall'art. 2.1 dell'Accordo TBT.

La norma, come interpretata dalla giurisprudenza dell'OMC, delinea un "test a tre livelli" che richiede di verificare se (i) la misura costituisce un regolamento tecnico; (ii) i prodotti importati e quelli nazionali siano considerati prodotti «simili»; e (iii) ai prodotti importati sia garantito un trattamento non meno favorevole rispetto ai prodotti nazionali simili [51]. In tale contesto, assume preminente rilievo il concetto di «trattamento non meno favorevole», che deve essere interpretato alla luce del contesto normativo, nonché dell'oggetto e della finalità proprie dell'Accordo TBT [52]. Quest'ultimo mira a perseguire un equilibrio tra l'obiettivo della liberalizzazione degli scambi e il diritto dei Membri dell'OMC di adottare regolamentazioni volte alla tutela di obbiettivi legittimi [53].

Come costantemente affermato dal DSB dell'OMC [54], l'interpretazione dell'art. 2.1 TBT deve essere effettuata tenendo conto del contesto sistematico offerto dallo stesso Accordo, in particolare dell'art. 2.2 e del preambolo che, nel

---

[50] Si noti che tale definizione riproduce quella di regolamento tecnico con la sola differenza della natura meramente volontaria.

[51] *US – Tuna II (Mexico)*, *op. cit.*, par. 202.

[52] *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, Organo d'Appello, 24 aprile 2012, WT/DS406/AB/R, (US – Clove Cigarettes), par. 169; *United States – Certain Country of Origin Labelling (COOL) Requirements*, Organo d'Appello, 23 luglio 2012, WT/DS384/AB/R WT/DS386/AB/R, (US – COOL), par. 271.

[53] *US – Clove Cigarettes*, *op. cit.*, parr. 174, 94-95.

[54] *Ivi*, parr. 182, 215; *US – COOL*, *op. cit.*, par. 271. È opportuno osservare che, nel caso EU – *Palm Oil (Malaysia)*, il Panel ha indicato che la natura e il contenuto della valutazione ai sensi dell'art. 2.1 riguardante il trattamento meno favorevole si applicano *mutatis mutandis* alla valutazione e al bilanciamento condotti ai sensi dello *chapeau* dell'art. XX GATT. *European Union and Certain Member States – Certain Measures Concerning Palm Oil and Oil Palm Crop-Based Biofuels (Malaysia)*, Panel, 26 aprile 2024, WT/DS600/R, (EU – Palm Oil (Malaysia), Panel), parr. 7.498, 7.499, 7.1097.

suo sesto considerando, ricalca lo *chapeau* dell'art. XX GATT 1994. Esso, invero, chiarisce che nessun Paese può essere privato della possibilità di adottare misure necessarie alla tutela di un obiettivo legittimo, «ai livelli che ritiene appropriati», purché tali misure non siano applicate in modo da costituire una discriminazione arbitraria o ingiustificabile tra Paesi in cui prevalgono condizioni analoghe, né rappresentino una restrizione dissimulata al commercio internazionale, e siano in ogni caso conformi alle restanti disposizioni dell'Accordo.

Alla luce di tale inquadramento, emerge che l'art. 2.2 integra e specifica la portata dell'art. 2.1, suggerendo che non ogni ostacolo al commercio internazionale risulta vietato, bensì soltanto quelli «non necessari», ossia sproporzionati rispetto agli obiettivi perseguiti o applicati in modo discriminatorio.

L'analisi del «trattamento meno favorevole» ai sensi dell'art. 2.1 non può pertanto prescindere da una valutazione congiunta della giustificazione e proporzionalità della misura, secondo un approccio coerente con la funzione di bilanciamento tra esigenze di liberalizzazione degli scambi e tutela di interessi pubblici legittimi che permea l'Accordo TBT. Il rinvio interpretativo al contenuto del preambolo e all'art. 2.2 del TBT consente al "*even-handedness analysis*", ossia al bilanciamento di interessi che nel sistema del GATT 1994 è rinvenibile nello *chapeau* dell'art. XX, di trovare "applicazione indiretta" anche nel TBT [55]. Invero, l'Accordo TBT, a differenza del GATT 1994, non contempla una clausola generale di eccezione che consenta di giustificare una misura incompatibile con l'obbligo di non discriminazione, sulla base della tutela di obiettivi regolatori legittimi.

Ne deriva che la verifica dell'esistenza di un «trattamento meno favorevole» si articola in due momenti distinti [56]. In primo luogo, occorre accertare se la misura comporti un impatto negativo sui prodotti importati rispetto a quelli nazionali, incidendo sulle condizioni di concorrenza e sull'accesso al mercato; in secondo luogo, è necessario stabilire se tale impatto negativo non sia riconducibile a una «distinzione regolatoria legittima», vale a dire a una misura proporzionata e funzionale al perseguimento di un obiettivo legittimo [57].

Come già anticipato, i PED provenienti da Paesi terzi che non rispettino una o più delle caratteristiche richieste non possono essere immessi nel mercato del-

[55] Per maggiori informazioni riguardo all'interazione tra art. XX GATT e 2.1 TBT cfr. L. TAMIOTTI-D. RAMOS, *Article 2 TBT: Preparation, Adoption and Application of Technical Regulations by Central Government Bodies*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022. Si noti tuttavia che pur riconoscendo analogie tra l'art. XX GATT e 2.1 TBT, l'OdA ha messo in guardia contro una trasposizione diretta di tale analisi, sottolineando che si tratta di due disposizioni distinte, ciascuna con una specifica operatività giuridica, cfr. *inter alia*, *EC – Seal Products*, *op. cit.*, par. 5.313.

[56] *US – Clove Cigarettes*, *op. cit.*, par. 169.

[57] *Ivi*, parr. 182, 215; *US – COOL*, *op. cit.*, par. 271.

l'Unione, anche qualora risultino conformi a regimi di cybersicurezza nazionali sofisticati e idonei a prevenire o mitigare gli effetti di attacchi informatici. In tale prospettiva, il CRA, imponendo l'osservanza dei requisiti essenziali di cui all'Allegato I, rischia di determinare l'esclusione di prodotti extra-Ue, sebbene conformi a standard di sicurezza differenti ma potenzialmente equivalenti, con possibili effetti negativi sulla concorrenza dei prodotti importati rispetto a quelli interni. Ne deriva la necessità di esaminare il Regolamento alla luce del principio di non discriminazione, interpretato secondo la nozione di trattamento nazionale.

In considerazione dei passaggi sopra delineati e dei criteri elaborati dal DSB [58], i PED europei ed extra-Ue possono essere considerati agevolmente «prodotti simili», e dunque l'attenzione deve concentrarsi sull'analisi dell'eventuale esistenza di un trattamento meno favorevole a loro carico.

Occorre verificare *in primis* se la misura in esame influisca *de jure* o *de facto* [59] sulle pari opportunità competitive tra i prodotti importati e i prodotti interni simili [60]. Tale valutazione deve essere condotta attraverso l'analisi del design, della struttura e del funzionamento previsto della misura in questione [61].

Sebbene il CRA trovi applicazione in modo uniforme a tutti i PED, indipendentemente dalla loro provenienza, l'obbligo di conformarsi ai requisiti essenziali determinati dall'Unione europea, senza la possibilità di dimostrare l'equivalenza – in termini di efficacia – dei requisiti di cybersicurezza previsti dall'ordinamento del Paese d'origine, può determinare oneri aggiuntivi per gli operatori economici extra-Ue che intendano accedere al mercato europeo.

Tali operatori sono infatti tenuti a sostenere costi supplementari sia di natura

---

[58] Secondo l'interpretazione degli organi di risoluzione delle controversie dell'OMC, la "similitarità" dei prodotti deve essere valutata, tra l'altro, sulla base di quattro criteri generali, e cioè: (i) le proprietà, la natura e la qualità dei prodotti; (ii) gli usi finali dei prodotti; (iii) i gusti e le abitudini dei consumatori – più compiutamente indicati come percezioni e comportamenti dei consumatori – rispetto ai prodotti; e (iv) la classificazione tariffaria dei prodotti, cfr. *inter alia*, *United States – Certain Measures Affecting Imports of Poultry from China*, Panel, 25 ottobre 2010, WT/DS392/R, parr. 7.424-7.427, 7.429; *Indonesia – Certain Measures Affecting the Automobile Industry*, Panel, 23 luglio 1998, WT/DS54/R; WT/DS55/R; WT/DS59/R; WT/DS64/R, par. 14.109; *Philippines – Taxes on Distilled Spirits*, Organo d'Appello, 20 gennaio 2012, WT/DS396/AB/R; WT/DS403/AB/R, parr. 7.31-7.37, 7.124-7.127. DS396/AB/R; WT/DS403/AB/R, parr. 7.31-7.37, 7.124-7.127.

[59] *US – COOL*, *op. cit.*, par. 286.

[60] *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products (Article 21.5 Mexico)*, Organo d'Appello, 11 gennaio 2019, WT/DS381/AB/RW, (*US – Tuna II (Mexico) (Article 21.5 Mexico)*), par. 7.29.

[61] *United States – Certain Country of Origin Labelling (COOL) Requirements (Article 21.5 – Canada and Mexico)*, Organo d'Appello, 29 maggio 2015, WT/DS384/AB/RW; WT/DS386/AB/RW, (US – COOL (Article 21.5 – Canada and Mexico)), par. 5.15.

amministrativa sia di ulteriore certificazione, al fine di ottenere l'immissione dei prodotti di provenienza extra-Ue sul mercato dell'Unione. In questo contesto, il requisito in esame ben può determinare una distinzione regolatoria tra prodotti nazionali e prodotti importati simili, con possibili implicazioni in termini di impatto negativo sulle condizioni di concorrenza ai sensi dell'art. 2.1 del TBT.

Tuttavia, la mera esistenza di una distinzione regolatoria non implica l'esistenza di un «trattamento meno favorevole» né, dunque, una violazione dell'art. 2.1 TBT. È necessario infatti verificare se l'impatto negativo sui prodotti importati possa essere ricondotto a una «distinzione regolatoria legittima» [62]. Tale passaggio si configura quale momento di bilanciamento volto ad accertare, in conformità alla logica sottesa allo *chapeau* dell'art. XX GATT 1994, se la differenza di trattamento derivante dal regolamento tecnico possa ritenersi proporzionata e giustificata in relazione all'obiettivo legittimo perseguito, ovvero se essa si traduca in una forma di discriminazione arbitraria o ingiustificabile, non spiegabile alla luce di tale finalità.

L'analisi richiede quindi una valutazione accurata del progetto, della struttura, dell'architettura, del funzionamento e dell'applicazione del regolamento tecnico in esame, al fine di stabilire se la misura sia effettivamente equa o se, al contrario, discrimini i prodotti importati [63]. A tal proposito, risulta essenziale concentrarsi sulla natura della distinzione regolatoria. *In primis*, va individuato l'«obiettivo legittimo» sottostante alla misura, a cui segue l'esame del design e delle condizioni della sua applicazione.

Nel caso di specie, l'obiettivo perseguito dal Regolamento riguarda principalmente la protezione della cybersicurezza [64], finalità che può essere agevolmente assimilata alla tutela della sicurezza nazionale [65]. La legittimità di tale obiettivo è rafforzata dal fatto che la sicurezza nazionale [66] viene esplicitamente menzionata come finalità *legittima* nella lista contenuta all'art. 2.2 e nel settimo paragrafo del preambolo del TBT.

Per quanto riguarda la "proporzionalità" della misura, l'OdA ha sottolineato la necessità di valutare se l'impatto negativo dovuto alle distinzioni regolatorie

---

[62] *US – Clove Cigarettes*, *op. cit*., par. 182, 215; *US – COOL, op. cit*., par. 271.

[63] *EU – Palm Oil (Malaysia), Panel, op. cit*., par. 7.498; *US – COOL, op. cit*., par. 271; *US – Clove Cigarettes, op. cit*., par. 182; *US – Tuna II (Mexico)*, *op. cit*., par. 225.

[64] Sebbene il concetto non sia menzionato esplicitamente nel Regolamento, esso può essere facilmente desunto dal contenuto e dai "considerando" ivi contenuti, v. *ex multis* Par. 1-2 Considerando CRA e COMMISSIONE EUROPEA, *Executive Summary of the Impact Assessment Report*, 2022.

[65] N. MISHRA, *op. cit*.

[66] G. GAGLIANI, *op. cit*.

sia «calibrato» in relazione al rischio che la misura mira a prevenire [67].

Alla luce delle analogie tra l'interpretazione dello *chapeau* dell'art. XX del GATT 1994 e dell'art. 2.1 del TBT, considerato anche il linguaggio del sesto considerando del preambolo del TBT, è possibile [68] ricorrere all'analisi giurisprudenziale sviluppata in relazione all'art. XX per orientare la valutazione dell'equità della misura [69]. Assumono dunque particolare rilievo il nesso tra l'eventuale discriminazione e l'obiettivo della misura [70] e la ragione posta alla base della differenza di trattamento [71]. Invero, una discriminazione può essere considerata arbitraria o ingiustificabile quando le motivazioni addotte a giustificazione della stessa risultano prive di una connessione razionale con l'obiettivo della misura, oppure sono in contrasto con tale obiettivo [72].

Nel caso di specie, le distinzioni regolatorie introdotte dal CRA appaiono concretamente correlate all'obiettivo finale perseguito, ossia la tutela della cybersicurezza e, più in generale, della sicurezza nazionale, obiettivo esplicitamente riconosciuto come legittimo dall'art. 2.2 TBT.

Alla luce di tali considerazioni, la discriminazione *de facto* a svantaggio dei PED importati introdotta dal CRA può quindi ritenersi legittima rispetto agli scopi perseguiti.

Inoltre, pur comportando un maggiore onere per gli operatori economici extra-Ue, la misura non pare potersi ritenere una discriminazione arbitraria o ingiustificabile, poiché gli adempimenti richiesti risultano funzionalmente connessi alla prevenzione dei rischi che il Regolamento intende mitigare.

Analoghe considerazioni possono essere estese alle distinzioni regolatorie derivanti dai diversi oneri di certificazione imposti in funzione delle

---

[67] Per maggiori dettagli, cfr. *US – Tuna II (Mexico)*, *op. cit*., par. 297; *US – COOL, op. cit.*, par. 340.

[68] Si noti tuttavia che sebbene l'esistenza di una discriminazione arbitraria o ingiustificabile costituisca un modo per dimostrare la mancanza di equità, non si tratta dell'unico criterio rilevante a tale fine. In altri termini, l'esame di un regolamento tecnico mediante l'applicazione della "connessione razionale" è considerato accettabile, ma non esaurisce necessariamente l'applicazione giuridica dell'art. 2.1 del TBT, cfr. L. TAMIOTTI-D. RAMOS, *op. cit.*; *US – Tuna II (Mexico) (Article 21.5 Mexico)*, *op. cit.*, parr. 7.90-7.92, 7.94-7.96.

[69] Per un approfondimento dell'analisi ai sensi dello *chapeau* dell'art. XX GATT, cfr. G. ADINOLFI, *Article XX GATT [Chapeau]*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022.

[70] Si noti che il nesso tra l'eventuale discriminazione e l'obiettivo della misura costituisce uno dei fattori principali, sebbene non l'unico, per accertare l'esistenza di una discriminazione arbitraria o ingiustificabile, cfr. *EC – Seal Products*, *op. cit.*, par. 5.321.

[71] *Brazil – Measures Affecting Imports of Retreaded Tyres*, Organo d'Appello, 17 dicembre 2007, WT/DS332/AB/R, (Brazil – Retreaded Tyres), parr. 226, 227, 246.

[72] *Brazil – Retreaded Tyres*, *op. cit.*, parr. 226, 227, 246.

diverse categorie di PED (di *default* [73] – né importanti né critici –, importanti e critici), nonché al regime meno gravoso in termini certificativi riconosciuto ai PED beneficiari della presunzione di conformità ai sensi dell'art. 27 CRA [74].

In conclusione, le differenze regolatorie introdotte dal CRA non sembrano configurare un «trattamento meno favorevole» ai sensi dell'Accordo TBT; di conseguenza, il Regolamento appare conforme all'art. 2.1 TBT.

3.3. Analisi ai sensi dell'art. 2.2 del TBT

Un ulteriore profilo meritevole di approfondimento concerne la necessità di verificare che il CRA non si traduca in un ostacolo non necessario al commercio internazionale, in linea con i principi di proporzionalità e ragionevolezza sanciti dall'art. 2.2 del TBT. Esso, infatti, prescrive che i Membri dell'OMC debbano garantire che la preparazione, l'adozione e l'applicazione dei regolamenti tecnici non avvengano «con l'intento o con l'effetto di creare ostacoli non necessari al commercio internazionale». Inoltre, devono assicurare che i propri regolamenti tecnici non siano «più restrittivi per il commercio del necessario per raggiungere un obiettivo legittimo, tenendo conto dei rischi derivanti dal mancato conseguimento di tale obiettivo».

In base all'interpretazione giurisprudenziale dell'OdA è richiesto di valutare se il regolamento tecnico sia più restrittivo per il commercio del necessario per conseguire un obiettivo legittimo, tenendo conto dei rischi derivanti dal mancato conseguimento di tale obiettivo. Questo passaggio richiede un esame articolato. Da un lato, occorre identificare l'obiettivo legittimo che il Membro dell'OMC intende perseguire e verificare la sua effettiva legittimità. Dall'altro, è necessario valutare la misura tecnica in relazione alla sua proporzionalità. In particolare, occorre accertare se le restrizioni imposte siano strettamente correlate al raggiungimento dell'obiettivo e se non eccedano quanto necessario per realizzarlo [75].

Tale approccio permette di distinguere tra regolamenti "giustificati", che

---

[73] PARLAMENTO EUROPEO, *EU Cyber-Resilience Act*, 2024.

[74] La presunzione di conformità opera da "ponte" tra la norma astratta (il requisito) e la realtà tecnica del prodotto (la sua progettazione e produzione). In pratica, l'adozione degli standard dell'Unione europea semplifica enormemente la dimostrazione della conformità, poiché non servirebbe sviluppare da zero prove tecniche, né giustificare altre soluzioni.

[75] *Australia – Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging*, Organo d'Appello, 29 giugno 2020, WT/DS435/AB/R; WT/DS441/AB/R, (Australia – Tobacco Plain Packaging (Honduras)), par. 6.3.

perseguono obiettivi legittimi in modo proporzionato, e misure che, pur formalmente legittime, generano effetti sproporzionati sugli scambi internazionali.

Come già emerso nell'analisi precedente, l'art. 2.2 TBT contiene un elenco non esaustivo di obiettivi legittimi, tra i quali ivi rientra, la tutela della sicurezza nazionale. Nel caso di specie, poiché la cybersicurezza può essere agevolmente ricondotta a tale categoria, il requisito può ritenersi soddisfatto.

Per quanto concerne il secondo step dell'esame, l'OdA ha chiarito che la valutazione della necessità di una misura richiede un'analisi relazionale, nota come "test di necessità", che comporta il bilanciamento di tre elementi strettamente interconnessi: (i) il grado in cui la regolamentazione tecnica limita gli scambi commerciali; (ii) il contributo effettivo della misura al conseguimento di un obiettivo legittimo; e (iii) i potenziali rischi derivanti dal mancato raggiungimento dell'obiettivo [76]. Qualora la misura sia preliminarmente considerata "necessaria", è possibile procedere a un'analisi comparativa [77], valutando se esistano soluzioni alternative meno restrittive o più efficaci nel perseguire lo stesso obiettivo, al fine di accertare la proporzionalità e la razionalità della regolazione adottata [78].

Nella definizione del c.d. "test della necessità", l'OdA ha precisato che il termine «necessario» non si limita a ciò che è «indispensabile». Tuttavia, una misura qualificata come necessaria si colloca significativamente più vicina al polo dell'indispensabile, piuttosto che all'estremo opposto rappresentato dal mero contributo al raggiungimento dell'obiettivo legittimo [79].

Per quanto concerne la determinazione del grado di restrittività commerciale, per "restrizione" è da intendersi qualsiasi misura che produca un effetto limitativo sugli scambi internazionali. In secondo luogo, secondo la giurisprudenza dell'OMC, occorre valutare in che misura – o se del tutto – il regolamento tecnico contribuisca effettivamente al conseguimento dell'obiettivo legittimo individuato. Tale valutazione deve considerare il design, la struttura, il funzionamento e l'applicazione concreta della misura, al fine di accertare l'effettivo impatto del regolamento sull'obiettivo [80].

L'OdA ha puntualizzato che l'adempimento ai sensi dell'art. 2.2 non

---

[76] *US – Tuna II (Mexico)*, *op. cit.*, par. 318; *US – COOL, op. cit.*, par. 374; *Australia – Tobacco Plain Packaging (Honduras)*, *op. cit.*, par. 6.3.

[77] Si noti che l'OdA ha chiarito la facoltatività di tale passaggio sulla base delle caratteristiche del caso di specie, cfr. *Australia – Tobacco Plain Packaging (Honduras)*, *op. cit.*, par. 6.4.

[78] *US – COOL (Article 21.5 – Canada and Mexico)*, *op. cit.*, par. 5.199. Per maggiori approfondimenti sull'analisi cfr. L. TAMIOTTI-D. RAMOS, *op. cit.*

[79] *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Organo d'Appello, 10 gennaio 2001, WT/DS161/AB/R; WT/DS169/AB/R, par. 161.

[80] *US – COOL*, *op. cit*., par. 373.

richiede il pieno raggiungimento dell'obiettivo, poiché, per definizione, un obiettivo legittimo può essere perseguito o conseguito in misura maggiore o minore. Invero, il sesto considerando del TBT stabilisce che ad un Membro dell'OMC non può essere impedito di adottare misure necessarie per conseguire i propri obiettivi legittimi «ai livelli che ritiene appropriati», mentre il settimo considerando conferma il diritto di adottare misure necessarie per la protezione degli interessi essenziali di sicurezza.

Riguardo ai rischi derivanti dal mancato conseguimento dell'obiettivo legittimo, l'art. 2.2 TBT indica un elenco non esaustivo di elementi pertinenti da considerare. Tra questi rientrano, in particolare, le informazioni scientifiche e tecniche disponibili, le tecnologie di trasformazione applicabili e gli usi finali previsti dei prodotti. Questi elementi consentono di valutare la proporzionalità della misura e la sua adeguatezza rispetto agli obiettivi perseguiti, bilanciando la protezione degli interessi legittimi con l'impatto sugli scambi internazionali [81].

Nel caso del CRA, i maggiori oneri gravanti sui PED extra-Ue, derivanti dall'imposizione dei requisiti essenziali europei, sono suscettibili di limitare gli scambi commerciali. Tuttavia, appare evidente che tali requisiti possano risultare altresì efficaci nel ridurre gli incidenti e gli attacchi informatici [82], garantendo così un incremento della cybersicurezza e, di conseguenza, della sicurezza nazionale [83].

Considerata la rilevanza e la sensibilità del tema della sicurezza nazionale, nonché la crescente minaccia rappresentata dagli attacchi e rischi cibernetici [84], pare dunque ragionevole considerare la misura proporzionata alla luce del bilanciamento previsto dall'art. 2.2 TBT.

Come anticipato, l'analisi relazionale può essere integrata da un'analisi comparativa, confrontando la misura oggetto della valutazione con eventuali misure alternative, ragionevolmente disponibili, meno restrittive per il commercio e in grado di apportare un contributo equivalente al raggiungimento dell'obiettivo legittimo. Poiché il CRA impone il rispetto di specifici requisiti, in parte fondati su standard internazionali [85], esso non sembra essere eccessivamente restrittivo se confrontato con altre misure, quali il divieto assoluto di

---

[81] L. TAMIOTTI-D. RAMOS, *op. cit*.

[82] COMMISSIONE EUROPEA, *op. cit*.

[83] Par. 1-2 Considerando, CRA.

[84] K. HUANG-S. MADNICK-N. CHOUCRI-F. ZHANG, *A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade*, in Global Policy, 2021, vol. 12, n. 5, p. 626.

[85] ENISA-JRC, *Cyber Resilience Act Requirements Standards Mapping – Joint Research Centre & ENISA Joint Analysis*, 2024.

importazione, le limitazioni al volume delle merci o dazi doganali elevati, nell'ottica del perseguimento dell'obiettivo di sicurezza.

In sintesi, alla luce delle interpretazioni giurisprudenziali dell'OdA e dell'analisi condotta, il CRA appare conforme ai requisiti dell'art. 2.2 dell'Accordo TBT.

3.4. Osservanza delle disposizioni degli artt. 2.4 e 2.7 del TBT

Uno degli obiettivi dell'Accordo TBT è la promozione dell'armonizzazione degli standard a livello internazionale. Pertanto, diviene necessario esaminare il CRA anche in tale contesto.

L'armonizzazione può essere definita come l'adozione, da parte di più Paesi, di standard e regolamentazioni comuni in una determinata materia, laddove in precedenza ciascuno di essi disponeva di un proprio insieme di requisiti [86]. Ai sensi dell'art. 2.4, i Membri dell'OMC devono «utilizzare gli standard internazionali come base per i propri regolamenti tecnici», salvo che tali standard risultino inefficaci o inadeguati al perseguimento degli obiettivi legittimi [87]. In tale contesto, assume particolare rilevanza il fatto che l'onere della prova circa l'assenza di fondamento su uno standard internazionale grava sulla parte che contesta la coerenza della misura [88].

Il termine «basato su» deve essere inteso in senso ampio. Esso significa che il regolamento tecnico deve essere «fondato su», «basato su», «costruito su» lo standard internazionale [89]. Tuttavia, ciò non significa che i Membri debbano necessariamente rispettare *in toto* lo standard internazionale pertinente. L'obbligo di utilizzare lo standard internazionale rilevante «come base» non è quindi un requisito rigido che impone di uniformare il regolamento tecnico a tale standard. Questa formulazione concede flessibilità ai Membri e riconosce che diversi approcci possono rispettare l'obbligo sancito dall'art. 2.4 TBT. Inoltre, lo stesso prevede che i Membri non sono obbligati a utilizzare standard internazionali come base per i propri regolamenti tecnici «quando tali standard internazionali o le parti pertinenti risultino inefficaci o inadeguati al perseguimento degli obiettivi legittimi prefissati».

L'OdA ha chiarito che tale disposizione implica la necessità di un esame

---

[86] J.P. TRACHTMAN, *Regulatory Jurisdiction and the WTO*, vol. 10, n. 3, in *Journal of International Economic Law*, 2007, pp. 631-651.

[87] E. SHEARGOLD, *op. cit*.

[88] *EC – Sardines*, *op. cit.*, par. 282.

[89] *European Communities – Measures Concerning Meat and Meat Products (Hormones)*, Organo d'Appello, 13 febbraio 1998, WT/DS26/AB/R; WT/DS48/AB/R, parr. 166, 242, 244.

approfondito e di una determinazione sulla legittimità degli obiettivi perseguiti dalla misura [90]. In tale contesto, gli obiettivi legittimi richiamati dall'art. 2.4 devono essere interpretati nel contesto dell'art. 2.2 del TBT.

La giurisprudenza dell'OMC ha inoltre chiarito il significato dei concetti di «inefficace» e «inadeguato» ai sensi dell'art. 2.4 del TBT. In particolare, un mezzo si considera inefficace quando non consegue l'obiettivo legittimo perseguito, mentre è definito inadeguato se non risulta particolarmente idoneo a garantirne il raggiungimento. In altri termini, la questione dell'efficacia riguarda i risultati concreti derivanti dall'impiego dei mezzi, mentre quella dell'adeguatezza attiene alla natura intrinseca degli strumenti adottati [91].

Nel caso del CRA, il rapporto congiunto di ENISA e Joint Research Centre del 2024, intitolato *Cyber Resilience Act Requirements Standards Mapping*, ha provveduto, da un lato, a creare una mappatura sistematica tra i requisiti essenziali del CRA (Allegato I) e gli standard tecnici esistenti; dall'altro, a condurre un'analisi delle lacune (*gap analysis*) per evidenziare in quali aree è necessario lo sviluppo di ulteriori standard armonizzati [92]. La mappatura ha mostrato che, sebbene esistano standard rilevanti come ETSI EN 303 645 (per la sicurezza dei dispositivi *Internet of Things*), EN ISO/IEC 27002:2022 (per i controlli di sicurezza), EN ISO/IEC 29147:2020 (per la *vulnerability disclosure*) ed EN ISO/IEC 30111: 2020 (per la gestione delle vulnerabilità nei prodotti *software*), nessuno di essi è in grado, preso singolarmente, di garantire il livello di protezione perseguito dal CRA e di coprire in modo esaustivo tutti i requisiti dell'Allegato I [93]. Tale indagine sottolinea quindi la necessità di armonizzare e sviluppare standard specifici che possano costituire in futuro strumenti riconosciuti per la presunzione di conformità, ai sensi del Regolamento. In tale contesto, ENISA ha altresì provveduto a mappare specificamente gli esistenti standard internazionali da utilizzare come base per il sistema EUCC [94]. Nel caso in cui la Commissione europea adotti un atto delegato, i sistemi europei di certificazione della cybersicurezza individuati assumerebbero carattere vincolante per i PED critici.

Gli studi hanno pertanto evidenziato come il CRA si fondi in parte sugli standard esistenti e come, al contempo, manchino standard in grado di garantire il livello di protezione perseguito dall'Unione.

---

[90] *EC – Sardines*, *op. cit.*, par. 286.

[91] *EC – Sardines*, *op. cit.*, par. 285.

[92] ENISA-JRC, *op. cit*.

[93] *Ivi*, pp. 6-42.

[94] ENISA-JRC, *op. cit*.; ENISA, *Cyber Resilience Act implementation via EUCC and its applicable technical elements*, 2025.

Nel contesto considerato, assume altresì rilevanza l'art. 2.7 del TBT, che impone ai Membri dell'OMC di considerare positivamente l'accettazione come equivalenti delle regolamentazioni tecniche adottate da altri Membri, anche qualora differiscano dalle proprie, a condizione che soddisfino adeguatamente gli obiettivi perseguiti dalla normativa nazionale. L'equivalenza rappresenta quindi uno strumento meno restrittivo degli scambi per raggiungere un obiettivo legittimo. Tuttavia, il linguaggio dell'art. 2.7 configura un obbligo di buona condotta e "*best efforts*" e non un vincolo rigido. Esso richiede invero solo di «prendere in considerazione positivamente» e non di «accettare» l'equivalenza, lasciando margine di valutazione soggettiva. Inoltre, la decisione di riconoscere come equivalenti le regolamentazioni tecniche di altri Membri si fonda su criteri soggettivi di soddisfazione [95].

Alla luce di quanto esposto, l'assenza di riconoscimento di requisiti esteri – pur potendo garantire un grado di protezione analogo – al fine di rafforzare la cybersicurezza nazionale e l'eventuale obbligatorietà dell'impiego dello schema EUCC in caso di atti delegati della Commissione, può considerarsi giustificata alla luce della sensibilità ed urgenza della materia (cybersicurezza – sicurezza nazionale) e dell'assenza di standard adeguati condivisi. Ne consegue che la mancata equivalenza con regolamentazioni tecniche adottate da altri Membri dell'OMC non deve essere considerata automaticamente come una violazione dell'art. 2.7 dell'Accordo TBT.

Per concludere, l'eventuale introduzione di ulteriori standard relativi ai requisiti essenziali di cybersicurezza, così come il mancato riconoscimento di standard esteri, non possono ritenersi in contrasto con gli artt. 2.4 e 2.7, in considerazione della particolare sensibilità del tema, dell'elevato livello di protezione che l'Unione europea intende perseguire e dell'assenza di standard internazionali idonei a garantire tale livello.

4. Conclusione

Il presente contributo si è confrontato con un profilo al quale la dottrina ha dedicato scarsa attenzione, guardando al possibile impatto del CRA sugli scambi internazionali per accertare se la disciplina così introdotta si ponga in contrasto con gli impegni assunti dall'Unione europea in base all'Accordo sugli ostacoli tecnici facente capo all'Organizzazione mondiale del commercio.

La *ratio* che è alla base di questo Accordo è quella di garantire agli Stati un margine di manovra entro il quale possono perseguire interessi generali anche

[95] L. TAMIOTTI-D. RAMOS, *op. cit*.

definendo le caratteristiche dei beni commercializzati sui rispettivi mercati nazionali, ma senza che ciò si traduca in un mutamento delle condizioni di competitività e in ostacoli non necessari agli scambi internazionali.

La disciplina sostanziale e procedurale posta dal CRA si applica ai prodotti con elementi digitali immessi sul mercato dell'Unione anche laddove essi siano originari da Paesi terzi. Ne derivano, pertanto, specifici obblighi in capo agli importatori e ai rappresentati autorizzati dei fabbricanti esteri, i quali sono tenuti a garantire che i PED prodotti in paesi extra-Ue soddisfino i requisiti essenziali di processo e di prodotto di cui all'Allegato I del Regolamento, siano stati sottoposti alle procedure di valutazione di conformità specificamente individuate rinviando alla normativa dell'Unione già in vigore e, infine, rechino la marcatura CE quale segno distintivo.

Dal confronto con l'Accordo TBT deriva che il CRA risponde pienamente agli obblighi di non discriminazione ivi previsti. Pur comportando un onere aggiuntivo per i fabbricanti esteri, tenuti a sostenere costi supplementari sia di natura amministrativa che di ulteriore certificazione per accedere al mercato dell'Unione, il CRA non applica nei loro confronti un «trattamento meno favorevole» rispetto a quello riservato ai produttori localizzati nel territorio dell'Unione. Pienamente legittimo è infatti, alla luce dell'art. 2.1 dell'Accordo TBT, perseguire un obiettivo di primaria importanza quale quello di garantire la cybersicurezza di beni di uso comune o posti alla base del funzionamento di infrastrutture necessarie all'ordinato svolgimento della vita politica, economica e sociale degli Stati.

Parimenti, non può affermarsi che il CRA si traduca in un ostacolo "non necessario" al commercio internazionale. Nonostante gli effetti restrittivi sulle importazioni, il rispetto dei requisiti essenziali prescritti, nonché l'eventualità che per i PED critici si imponga la conformità a un sistema europeo di certificazione adottato in base al CSA, appaiono strettamente funzionali a garantire la sicurezza dell'Unione europea, la sicurezza nazionale degli Stati membri e risultano proporzionati alla realizzazione di questo obiettivo.

Infine, da un'analisi della prassi che ha preceduto ed accompagnato l'entrata in vigore del CRA risulta evidente come i legislatori europei abbiano tenuto nella dovuta considerazione gli standard internazionali esistenti, integrando la loro disciplina in virtù dell'elevato livello di cybersicurezza perseguito.

Proprio queste circostanze contribuiscono a spiegare come allo stato attuale la legittimità del CRA non sia stata oggetto di particolari contestazioni in seno agli organi politici dell'OMC e non risulti verosimile l'apertura di una controversia innanzi agli organi contenziosi. In definitiva, il CRA dimostra come le regolamentazioni tecniche ben possano costituire degli utili strumenti di politica pubblica finalizzati al perseguimento di interessi generali e non sempre nascondano finalità protezionistiche.