RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2023
DOI: 10.32091/RIID0108
Articolo sottoposto a peer review

Il *Cyber Resilience Act*: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali

Pier Giorgio Chiara

Il 15 settembre 2022 la Commissione europea ha presentato la proposta di "Regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020" (*Cyber Resilience Act*, CRA). Questo articolo analizza in particolare il carattere "orizzontale" della proposta di regolamento CRA evidenziandone i principali pilastri. In particolare, il contributo prende in considerazione la nuova serie di obblighi imposti agli operatori economici, le procedure di valutazione della conformità e il quadro di sorveglianza del mercato, nonché l'interazione con altre iniziative legislative rilevanti. A fronte dell'approccio normativo settoriale adottato finora dalla Commissione in materia di requisiti di cybersicurezza per i prodotti, si ritiene che tale intervento orizzontale sia necessario non solo per creare le condizioni per lo sviluppo di prodotti connessi sicuri, ma anche – sul formante legislativo – per garantire un maggior grado di certezza del diritto, evitando quindi una moltiplicazione di obblighi per gli operatori e una frammentazione del mercato.

Legge sulla cyberresilienza – Diritto dell'UE – Diritto della cybersicurezza

1. Introduzione

I cyberattacchi e le minacce alle componenti hardware e software dei prodotti sono aumentati costantemente negli ultimi anni, non solo dal punto di vista quantitativo, ma anche in termini di impatto e sofisticazione[1]. La mancanza di un'adeguata sicurezza informatica nei prodotti con elementi digitali nell'Unione è dovuta a fallimenti di mercato e lacune normative. Ciò rappresenta un rischio non solo per il corretto funzionamento del mercato interno, ma anche per i diritti fondamentali e la sicurezza degli individui. Nel contesto odierno di crescente digitalizzazione permeante ogni settore delle nostre società, attori malintenzionati possono infatti compromettere prodotti digitali all'apparenza meno critici per interrompere le reti e i sistemi informativi ad essi collegati. Inoltre, i prodotti connessi che costituiscono la cosiddetta "Internet delle

P.G. Chiara è assegnista di ricerca in "Informatica giuridica" presso l'Università di Bologna.
Questo articolo è la traduzione in italiano di un articolo dello stesso autore già pubblicato in lingua inglese presso la "International Cybersecurity Law Review" dopo essere stato sottoposto a revisione (*double blind review*).

cose" (*Internet of Things*, IoT) interagiscono senza soluzione di continuità con la dimensione "fisica" in cui operano, attraverso sistemi interconnessi di sensori e attuatori. Pertanto, la sicurezza di questi prodotti è direttamente collegata alla sicurezza intesa come *safety*[2], ovvero la dimensione volta a proteggere l'integrità della vita dalla minaccia di un pericolo imminente[3].

Da un punto di vista economico, il fallimento del mercato nel fornire standard ottimali di cybersicurezza è dovuto a due problemi principali, ovvero le asimmetrie informative e le esternalità negative. In primo luogo, i consumatori non sono generalmente in grado di valutare il livello complessivo di sicurezza dei prodotti digitali e potrebbero non essere disposti a pagare per opzioni più sicure[4]; in secondo luogo, diversi modelli che analizzano il livello ottimale di investimento nella cybersicurezza hanno concluso che il mercato della cybersicurezza è caratterizzato da un livello di investimento sub-ottimale[5].

Da un punto di vista giuridico, il quadro normativo dell'Unione appare frammentato in relazione ai requisiti di cybersicurezza per i prodotti con elementi digitali, in quanto le varie iniziative adottate finora a livello comunitario (e nazionale) affrontano solo in parte i problemi identificati. In particolare, la legislazione settoriale sulla sicurezza dei prodotti è stata modificata per includere requisiti essenziali di cybersicurezza: Regolamento (UE) 2017/745[6], Regolamento delegato (UE) 2022/30 della Commissione, proposta di regolamento sulle macchine e proposta di regolamento sulla sicurezza generale dei prodotti. Tale approccio "verticale' rischia di accrescere l'incertezza giuridica e la frammentazione del mercato per quanto riguarda i requisiti di cybersicurezza relativi ai prodotti.

In questo contesto, la Presidente della Commissione europea Von der Leyen ha annunciato nel discorso sullo stato dell'Unione del 2021 un nuovo "Cyber Resilience Act" (CRA), al fine di garantire un quadro coerente di cybersicurezza con precisi obblighi per i fabbricanti di prodotti con elementi digitali, come già auspicato dalla Strategia di cybersecurity 2020 dell'UE per il Decennio digitale[7], dalle conclusioni del Consiglio del 2 dicembre 2020[8] e dalla Risoluzione del Parlamento europeo del 10 giugno 2021[9]. Pertanto, il 15 settembre 2022 la Commissione ha presentato la c.d. proposta di regolamento sulla cyberresilienza (CRA)[10]. L'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE) è stato individuato come base giuridica dell'atto (coerentemente con la scelta fatta per le direttive NIS e NIS2, e il *Cybersecurity Act*), in quanto prevede l'adozione di misure volte a garantire l'istituzione e il funzionamento del mercato interno.

Questo articolo si propone di fornire una panoramica generale della proposta CRA. In particolare, il paragrafo 2 chiarisce l'ambito di applicazione orizzontale del regolamento proposto; il paragrafo 3 affronta i diversi obblighi posti agli operatori economici; il paragrafo 4 illustra le diverse procedure di valutazione della conformità, mentre il paragrafo 5 analizza il quadro di sorveglianza del mercato e di applicazione delle norme. Infine, il paragrafo 6 evidenzia l'interazione tra la proposta CRA e la legislazione comunitaria esistente o *in fieri* in materia di cybersicurezza per i prodotti, tra cui la proposta di regolamento sull'intelligenza artificiale (AIA), la proposta di regolamento sulla sicurezza generale dei prodotti (GPSR), la proposta di regolamento macchine (MR), l'atto delegato che integra la direttiva sulle apparecchiature radio, la direttiva NIS2 e il *Cybersecurity Act*. Il paragrafo 7 conclude l'elaborato con alcune osservazioni sull'importanza, *rectius*: la necessità, di questa iniziativa legislativa orizzontale.

2. L'ambito di applicazione "orizzontale" del *Cyber Resilience Act*

La proposta di regolamento si applica «ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete»[11]. La proposta di regolamento fornisce una definizione ampia di "prodotti con elementi digitali", ossia «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente»[12].

Inizialmente, nelle consultazioni pubbliche preliminari alla valutazione d'impatto, la Commissione faceva riferimento a "prodotti digitali e servizi ausiliari", senza specificare però cosa si intendesse in dettaglio per "servizio ausiliario". A tal proposito, emerse un primo dibattito tra i diversi portatori di interesse. Da un lato, Digitaleurope, la principale associazione di categoria che rappresenta le industrie coinvolte nella trasformazione digitale nell'UE, ha sostenuto che l'ambito di applicazione del CRA non dovrebbe comprendere il software generico né i "servizi accessori", dal momento che operano entrambi indipendentemente da uno specifico prodotto tangibile e non sono adatti allo stesso trattamento legislativo[13]. D'altra parte, altre associazioni industriali e di tutela dei consumatori come Eurosmart, BEUC (*Bureau Européen des Unions de Consommateurs*) e ANEC (Associazione Europea per il Coordinamento della Rappresentanza dei Consumatori nella Standardizzazione) ritengono che l'ambito di applicazione del CRA debba essere tanto ampio da coprire non solo il software "non incorporato"[14] ma anche i servizi digitali del cloud[15], anche se, in quest'ultimo caso,

potrebbero verificarsi sovrapposizioni con il perimetro normativo della direttiva (UE) 2022/2555 (c.d. NIS2) (cfr. *infra* paragrafo 6).

L'ambito di applicazione della proposta della Commissione è quindi ancora più ampio di quello originariamente previsto nella *call for evidence*. Infatti, la definizione di "prodotti con elementi digitali" sopramenzionata si estende anche al software quale prodotto separato dall'hardware (*standalone*), come testimonia l'uso disgiuntivo della congiunzione "o". Ciò è confermato dalla lettura del considerando 46 della proposta CRA, che prevede esplicitamente prodotti con elementi digitali sotto forma di software. Senza soffermarsi sulle conseguenze giuridiche scaturenti dal considerare il software come un prodotto – a cui è dedicata ampia letteratura[16] – in quanto ciò esulerebbe dallo scopo del presente articolo, si cercherà di capire in che misura il CRA copra il software come prodotto.

La relazione di accompagnamento alla proposta parte dalla considerazione che l'attuale quadro giuridico dell'UE non affronti la cybersicurezza del software non incorporato[17]. A tal fine, l'opzione strategica scelta dalla Commissione per rispondere a tale problema è stata quella di coprire l'intera catena di approvvigionamento digitale, attraverso la definizione di specifici requisiti orizzontali di cybersicurezza per tutti i prodotti con elementi digitali immessi o resi disponibili sul mercato interno. «Anche il software non incorporato, spesso esposto a vulnerabilità, rientrerebbe in tale intervento normativo, garantendo così un approccio coerente nei confronti di tutti i prodotti con elementi digitali, con una chiara ripartizione delle responsabilità dei vari operatori economici»[18].

Tuttavia, il considerando 9 della proposta specifica che il CRA non disciplinerà il servizio a livello di software (*Software-as-a-Service*, SaaS), «ad eccezione delle soluzioni di elaborazione dati da remoto relative a un prodotto con elementi digitali, intese come una qualsiasi elaborazione dati a distanza per la quale il software è progettato e sviluppato dal fabbricante del prodotto in questione o sotto la sua responsabilità e la cui assenza impedirebbe a tale prodotto con elementi digitali di svolgere una delle sue funzioni». In tal senso, sembra che la prospettiva "accessoria" della *call for evidence* originale della Commissione sia in qualche modo rimasta, in quanto il software come servizio (SaaS) – escluso in via di principio – possa comunque rientrare nell'ambito di applicazione del CRA secondo un criterio di strumentalità, e cioè se progettato e sviluppato per un prodotto con elementi digitali. In ultimo, è importante evidenziare che il software libero e open-source è escluso dal campo di applicazione della proposta, affinché innovazione e ricerca non siano ostacolate[19].

Per quanto riguarda le altre esclusioni, la proposta chiarisce che il CRA non si applicherebbe ai prodotti con elementi digitali che rientrano già nell'ambito di applicazione del Regolamento (UE) 2017/745 (Regolamento sui dispositivi medici), del Regolamento (UE) 2017/746 (Regolamento sui dispositivi medico-diagnostici in vitro) e del Regolamento (UE) 2019/2144 (Regolamento generale sull'omologazione degli autoveicoli), né si applicherebbe ai prodotti con elementi digitali che sono stati certificati in conformità al Regolamento (UE) 2018/1139 (recante norme comuni nel settore dell'aviazione civile). Sono inoltre esclusi dall'ambito di applicazione del CRA i prodotti con elementi digitali sviluppati esclusivamente per la sicurezza nazionale, per scopi militari o specificamente progettati per il trattamento di informazioni classificate[20].

La proposta segue un approccio basato sul rischio[21]. In relazione al livello di rischio di cybersicurezza legato alla categoria di prodotto, determinato dalla Commissione tenendo conto di diversi criteri quali la funzionalità legata alla cybersecurity, l'uso previsto in ambienti sensibili o per lo svolgimento di funzioni critiche e l'entità di un impatto negativo[22], specifici prodotti con elementi digitali possono essere classificati come "critici" o "altamente critici" se la loro funzionalità principale rientra in tali categorie. La prima categoria – di cui all'Allegato III della proposta CRA – è ulteriormente suddivisa in classe I e classe II, con la classe II che rappresenta un rischio maggiore per la cybersicurezza. La categoria di prodotti altamente critici, invece, può essere creata in futuro dalla Commissione attraverso l'adozione di atti delegati[23].

La differenza tra prodotti con elementi digitali "non critici", "critici" e "altamente critici" risiede essenzialmente nella diversa procedura di valutazione della conformità – istituto tipico della normativa sulla sicurezza dei prodotti – a cui devono essere sottoposti. Mentre i prodotti "critici" sono soggetti alle specifiche procedure di valutazione della conformità di cui all'art. 24, paragrafi 2 e 3, della proposta CRA[24] (si veda *infra* paragrafo 4), i fabbricanti di prodotti "altamente critici" sono tenuti a ottenere un certificato europeo di cybersicurezza nell'ambito di un sistema europeo di certificazione della cybersicurezza a norma del regolamento (UE) 2019/881 (*Cybersecurity Act*, CSA) per dimostrare la conformità ai requisiti essenziali di cui all'allegato I, o a parti di esso[25].

3. Obblighi degli operatori economici

Un altro aspetto connesso al carattere orizzontale della proposta è l'ampio raggio degli obblighi posti

dal CRA in termini di operatori economici interessati. Un'ampia gamma di soggetti dovrà conformarsi al nuovo insieme di norme, dai fabbricanti fino ai distributori e agli importatori, in relazione alle loro responsabilità nella catena di approvvigionamento. A questo proposito, va sottolineato il nuovo approccio della legislazione europea in materia di cybersicurezza, che stabilisce norme per regolare le relazioni tra le parti lungo l'intera catena di approvigionamento dei prodotti con elementi digitali. Se fino ad ora, infatti, i rapporti tra gli operatori di mercato nella catena di fornitura in materia di cybersicurezza dei prodotti sono stati principalmente regolati da contratti secondo migliori pratiche o linee guida condivise, con il CRA i fabbricanti dovranno svolgere per legge una "due diligence" quando integrano componenti provenienti da terze parti nei prodotti con elementi digitali che immetteranno sul mercato[26].

Tre principali condizioni generali regolano l'immissione sul mercato di prodotti con elementi digitali: (i) sono correttamente installati, manutenuti, utilizzati per la finalità prevista e, se del caso, aggiornati[27]; (ii) sono stati progettati, sviluppati e prodotti in conformità ai requisiti essenziali di cui alla sezione 1 dell'allegato I[28]; e (iii) i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di cui alla sezione 2 dell'allegato I[29].

In base ai requisiti essenziali relativi alle proprietà dei prodotti di cui alla sezione 1 dell'allegato I, i prodotti con elementi digitali (i) devono essere progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cybersicurezza in base ai rischi; e (ii) devono essere consegnati senza vulnerabilità sfruttabili note. Inoltre, l'allegato I, sezione 1, elenca altri undici requisiti tecnici che i prodotti devono possedere, tra cui: configurazione sicura per impostazione predefinita; protezione da accessi non autorizzati mediante meccanismi di controllo appropriati; protezione della riservatezza dei dati personali o di altro tipo trattati mediante una crittografia all'avanguardia, ecc.

Invece, la sezione 2 dell'allegato I stabilisce requisiti essenziali in termini di processi messi in atto dai fabbricanti per la gestione delle vulnerabilità. Tali requisiti comprendono: l'identificazione e la documentazione delle vulnerabilità e dei componenti contenuti nel prodotto, anche attraverso la stesura di una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che comprenda almeno le dipendenze di primo livello del prodotto; la correzione delle vulnerabilità senza ritardo, anche attraverso la fornitura di aggiornamenti di sicurezza; l'applicazione di test e riesami efficaci e periodici della sicurezza del prodotto; la divulgazione al pubblico di informazioni sulle vulnerabilità risolte, una volta che sia stato reso disponibile un aggiornamento di sicurezza, ecc.

In linea con l'approccio basato sul rischio della proposta, i fabbricanti devono effettuare una valutazione dei rischi di cybersicurezza associati a un prodotto, i risultati della quale devono essere presi in considerazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, al fine di soddisfare pienamente l'obbligo di immettere un prodotto sul mercato in conformità ai requisiti essenziali di cui alla sezione 1, allegato I[30]. La valutazione dei rischi deve essere inclusa nella documentazione tecnica *ex* art. 23 e di cui all'allegato V[31].

I fabbricanti hanno anche diversi obblighi di documentazione per quanto riguarda la gestione delle vulnerabilità e delle informazioni fornite da terze parti[32]. In particolare, l'art. 23 specifica il contenuto della documentazione tecnica che il fabbricante deve redigere prima dell'immissione del prodotto sul mercato e che deve essere tenuta a disposizione delle autorità di vigilanza del mercato per dieci anni dopo l'immissione del prodotto sul mercato[33]. Pertanto, in relazione alla cooperazione con le autorità di vigilanza, i fabbricanti dovranno anche: (i) fornire a tale autorità tutte le informazioni necessarie per dimostrare la conformità ai requisiti essenziali dell'allegato I e cooperare in merito a qualsiasi misura adottata per eliminare i rischi di cybersicurezza posti dal prodotto[34]; e (ii) informare l'autorità in merito alla cessazione delle proprie attività con la conseguenza di non essere in grado di rispettare gli obblighi del Regolamento[35].

Inoltre, i fabbricanti devono garantire che i prodotti con elementi digitali siano accompagnati dalle informazioni e dalle istruzioni di cui all'allegato II, in forma elettronica o fisica, in un linguaggio chiaro, comprensibile e leggibile da parte degli utilizzatori[36], e forniscono la dichiarazione di conformità UE[37].

L'articolo 11, che stabilisce gli obblighi di segnalazione dei fabbricanti, adotta un approccio "centralizzato". Il fabbricante notifica all'ENISA (Agenzia dell'Unione europea per la sicurezza informatica), senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne viene a conoscenza, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto, compresi i dettagli e le eventuali misure di attenuazione adottate. L'ENISA, a meno di giustificati motivi legati al rischio di cybersicurezza[38], inoltra la notifica al *Computer Security Incident Response Team* (CSIRT) designato ai fini della divulgazione coordinata delle vulnerabilità nell'ambito del perimetro normativo della direttiva NIS2. Inoltre, qualora si verificasse un incidente al prodotto con elementi digi-

tali, i fabbricanti – oltre all'ENISA, che trasmette poi la notifica ai punti di contatto unici designati a norma della NIS2 – hanno un ulteriore obbligo di notifica verso: (i) gli utenti del prodotto che, se del caso, devono essere informati sulle misure correttive da adottare per mitigare l'impatto dell'incidente[39]; (ii) la persona o il soggetto che si occupa della manutenzione del componente integrato nel prodotto interessato da una vulnerabilità identificata dal fabbricante[40]. Questo impianto procedurale è un altro esempio di come il CRA tenga conto della cybersicurezza lungo tutta la catena di approvvigionamento.

Infine, gli articoli 12, 13 e 14 impongono obblighi agli operatori economici diversi dal fabbricante, ossia, rispettivamente, ai rappresentanti autorizzati, agli importatori e ai distributori. È importante notare che se l'importatore o il distributore (i) immette un prodotto sul mercato con il proprio nome o marchio o (ii) effettua una modifica sostanziale del prodotto, allora tale soggetto sarà considerato un fabbricante ai sensi del CRA e sarà pertanto soggetto agli obblighi di cui all'articolo 10 e all'articolo 11, paragrafi 1, 2, 4 e 7[41]. Lo stesso vale per qualsiasi persona fisica o giuridica che effettui una modifica sostanziale[42].

Assume quindi rilevanza centrale cosa si intenda per "modifica sostanziale" ai sensi del CRA. Secondo l'art. 3, punto (31) del CRA, "modifica sostanziale" è definita come «una modifica del prodotto con elementi digitali a seguito della sua immissione sul mercato che incide sulla conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, sezione 1, o comporta una modifica dell'uso previsto per il quale il prodotto con elementi digitali è stato valutato».

4. Conformità con i requisiti essenziali

La proposta CRA segue l'architettura e i principi della legislazione armonizzata del "nuovo quadro normativo" (*new legislative framework*, NLF). L'NLF, in linea con il cosiddetto "nuovo approccio" degli anni Ottanta, si basa sulla definizione di requisiti essenziali di alto livello in termini di sicurezza che i prodotti devono soddisfare per essere immessi nel mercato interno; tali requisiti sono poi dettagliati da norme tecniche armonizzate (standard) redatte dagli organismi europei di normazione (ossia ETSI, CEN, CENELEC) sulla base di una richiesta di normazione da parte della Commissione[43].

Inoltre, il fabbricante, per dimostrare che i requisiti specifici connessi a un prodotto siano stati soddisfatti, deve attuare dei processi di c.d. valutazione della conformità. In tal senso, opera di norma negli atti legislativi dell'NLF una presunzione. I prodotti conformi alle norme armonizzate, o a parti di esse, i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea, si presumono conformi ai requisiti essenziali delle direttive e dei regolamenti dell'NLF. Lo stesso vale per il CRA[44]. Tale presunzione di conformità si estende anche ai prodotti e ai processi messi in atto dal fabbricante per i quali è stata rilasciata una dichiarazione di conformità o un certificato UE nell'ambito di un sistema europeo di certificazione della cybersicurezza adottato ai sensi del Regolamento (UE) 2019/881[45]. A questo proposito, la Commissione può adottare atti di esecuzione per specificare i sistemi che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali dell'allegato I e se un certificato di cybersicurezza elimina l'obbligo per un fabbricante di effettuare una valutazione di conformità da parte di terzi per i requisiti corrispondenti[46].

Qualora le norme armonizzate non dovessero esistere, fossero insufficienti o se ci fossero ritardi ingiustificati nella procedura di standardizzazione o se ancora la richiesta della Commissione non fosse stata accettata dagli organismi di standardizzazione, la Commissione può adottare, mediante atti di esecuzione, "specifiche comuni", le quali possono essere utilizzate per dimostrare la conformità ai requisiti essenziali dell'allegato I[47]. La presunzione di conformità di cui sopra opera anche con riferimento alle specifiche comuni[48].

La dichiarazione di conformità UE deve essere redatta dai fabbricanti nell'ambito degli obblighi di documentazione di cui all'art. 10, para. 7 ed attesta il rispetto dei requisiti essenziali applicabili di cui all'Allegato I[49]. L'Allegato IV illustra la struttura del modello di dichiarazione di conformità UE: in particolare, deve contenere gli elementi specificati nelle pertinenti procedure di valutazione della conformità, deve essere continuamente aggiornata e – se un prodotto con elementi digitali rientra nell'ambito di applicazione di più di un atto dell'Unione che richiede una dichiarazione di conformità UE – deve contenere l'identificazione degli atti comunitari interessati.

Il fabbricante esegue una valutazione della conformità del prodotto, prodromica all'immissione sul mercato, seguendo una delle procedure di cui all'allegato VI[50], tipiche dell'NLF, tra cui: (i) la procedura di controllo interno (basata sul modulo A della decisione 768/2008/CE); (ii) la procedura di esame UE del tipo (basato sul modulo B); (iii) conformità al tipo basata sul controllo interno della produzione (basata sul modulo C); (iv) conformità basata sulla garanzia della qualità totale (basata sul modulo H). I fabbricanti di prodotti critici delle classi I e II devono utilizzare per la conformità la procedura di esame

UE del tipo (basata sul modulo B) seguita dalla conformità al tipo basata sul controllo interno della produzione (basata sul modulo C) o dalla valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H)[51]. Per quanto riguarda in particolare i prodotti appartenenti alla classe I, tali procedure devono essere eseguite se il fabbricante non ha applicato o ha applicato solo in parte norme armonizzate, specifiche comuni o schemi europei di certificazione della cybersicurezza; oppure se tali norme armonizzate, specifiche comuni o schemi europei di certificazione della cybersicurezza non esistono[52].

Infine, prima di immettere il prodotto con elementi digitali sul mercato, il fabbricante appone la marcatura CE in modo visibile, leggibile e indelebile sul prodotto e segue i principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008[53].

Il capo IV della proposta definisce poi il quadro procedurale relativo alle interazioni con gli organismi nazionali di valutazione della conformità (organismi notificati). La proposta, in linea con l'NLF, lascia agli Stati membri la responsabilità di designare un'autorità incaricata di istituire ed eseguire le procedure necessarie per la valutazione e la notifica degli organismi di valutazione della conformità e il monitoraggio degli organismi notificati.

5. Vigilanza del mercato e applicazione delle norme

In conformità al Regolamento (UE) 2019/1020, che si applica ai prodotti con elementi digitali nel campo di applicazione della CRA, le autorità nazionali di vigilanza del mercato designate dagli Stati membri effettuano la vigilanza del mercato nel territorio di tale Stato membro. Gli Stati membri possono designare qualsiasi autorità esistente (comprese le autorità nazionali competenti ai sensi della NIS2 e del *Cybersecurity Act*) o una nuova al fine di garantire l'effettiva attuazione del CRA[54]. Tuttavia, per i prodotti con elementi digitali che rientrano nell'ambito di applicazione del CRA e che sono classificati come sistemi di intelligenza artificiale ad alto rischio ai sensi della legge sull'intelligenza artificiale (AIA), le autorità di vigilanza del mercato designate ai fini dell'AIA sono anche le autorità responsabili delle attività di vigilanza previste dal CRA[55].

Le autorità di vigilanza del mercato designate ai sensi del CRA collaborano con altre autorità di vigilanza del mercato designate sulla base di altre normative di armonizzazione dell'Unione per altri prodotti, con le autorità nazionali di certificazione della cybersicurezza designate ai sensi del *Cybersecurity Act* e, se del caso, con le autorità garanti per la protezione dei dati personali. A questo proposito, diverse autorità di vigilanza possono realizzare attività congiunte, le quali possono anche essere proposte dalla Commissione o dall'ENISA, con l'obiettivo di garantire la cybersicurezza e la protezione dei consumatori in relazione a specifici prodotti con elementi digitali immessi o resi disponibili sul mercato[56]. Inoltre, le autorità di vigilanza possono condurre simultaneamente azioni di controllo coordinate ("indagini a tappeto") di particolari prodotti con elementi digitali, o categorie di essi, per verificare la conformità con il CRA o per individuare violazioni[57]. Salvo diversa decisione delle autorità di vigilanza interessate, tali controlli a tappeto sono coordinati dalla Commissione.

Le autorità di vigilanza del mercato riferiscono annualmente alla Commissione i risultati delle attività di vigilanza del mercato. Queste includono le valutazioni dei prodotti per quanto riguarda la loro conformità ai requisiti del CRA, che vengono effettuate se l'autorità di vigilanza ha motivi sufficienti per ritenere che i prodotti in questione presentino un rischio significativo per la cybersicurezza[58]. Se il prodotto non è conforme al regolamento, l'autorità richiede all'operatore interessato di adottare tutte le misure correttive appropriate per rendere il prodotto conforme ai requisiti, ritirarlo dal mercato o richiamarlo entro un periodo di tempo ragionevole. Se il fabbricante non adotta le azioni correttive adeguate entro il termine stabilito dall'autorità, l'autorità di vigilanza adotta misure per vietare o limitare la messa a disposizione del prodotto sul mercato nazionale, per ritirarlo da tale mercato o per richiamarlo[59]. La Commissione può avviare valutazioni da parte delle autorità nazionali ai sensi dell'art. 43 e, in circostanze eccezionali, che includono motivi per ritenere che le autorità di vigilanza non abbiano adottato misure efficaci, può chiedere all'ENISA di effettuare una valutazione della conformità[60]. Conseguentemente alle valutazioni dell'ENISA, la Commissione può adottare misure correttive o restrittive a livello dell'Unione mediante atti di esecuzione[61].

La proposta delega agli Stati membri il potere di stabilire norme sulle sanzioni – che devono essere effettive, proporzionate e dissuasive – applicabili alle violazioni del CRA[62]. Tuttavia, la discrezionalità degli Stati membri è relativa: (i) l'inosservanza dei requisiti essenziali di cybersicurezza di cui all'allegato I e degli obblighi di cui agli articoli 10 e 11 è soggetta a sanzioni amministrative pecuniarie fino a 15 milioni di euro o fino al 2,5% del fatturato mondiale annuo totale dell'esercizio precedente; (ii) l'inosservanza di qualsiasi altro obbligo previsto dal CRA è soggetta a sanzioni amministrative pecuniarie fino a 10 milioni di euro o fino al 2% del fatturato; e (iii) la fornitura

di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato è soggetta a sanzioni amministrative pecuniarie fino a 5 milioni di euro o fino all'1% del fatturato. Gli Stati membri notificano alla Commissione tali norme e misure senza indebito ritardo.

6. Interazione con le altre normative dell'Unione

Come già affermato *supra* nell'Introduzione, il CRA intende colmare una lacuna nella normativa dell'UE per quanto riguarda i requisiti di cybersicurezza dei prodotti digitali; finora, l'approccio di governance adottato dalla Commissione è stato "verticale", cioè settoriale[63]. Il CRA è il pezzo rimanente del puzzle che creerebbe un'interfaccia tra tutti gli atti legislativi che affrontano il tema della cybersicurezza dei prodotti, direttamente o indirettamente, come le direttive e i regolamenti in vigore o proposti nell'alveo della legislazione sulla sicurezza dei prodotti, l'AIA, il *Cybersecurity Act*, il regolamento delegato (UE) 2022/30 e la direttiva NIS2.

Il raccordo tra il CRA e altre norme dell'Unione che stabiliscono requisiti di cybersicurezza per i prodotti con elementi digitali è disciplinato dall'articolo 2, paragrafo 4, del CRA. Questa disposizione può essere interpretata come una regola di prevalenza, in quanto stabilisce i criteri in base ai quali altri quadri giuridici dell'UE – che affrontano tutti o alcuni dei rischi coperti dai requisiti essenziali di cui all'allegato I del CRA – possono prevalere sul CRA. Pertanto, l'applicazione del CRA può essere limitata o esclusa se le norme settoriali che si applicano ai prodotti conseguano lo stesso livello di protezione previsto dal CRA e se tale prevalenza è coerente con il quadro normativo complessivo che si applica a tali prodotti. La Commissione può specificare, mediante atti delegati, se tale limitazione o esclusione sia necessaria, quali siano i prodotti interessati, nonché la portata della limitazione.

Le sezioni che seguono presenteranno alcune osservazioni preliminari relative all'interazione tra la proposta CRA e altri atti giuridici dell'Unione pertinenti.

6.1. Interazione tra il CRA e la proposta di legge sull'intelligenza artificiale

I prodotti che rientrano nell'ambito di applicazione del CRA e che sono anche classificati come sistemi di intelligenza artificiale ad alto rischio ai sensi dell'art. 6 della proposta di legge sull'intelligenza artificiale devono essere conformi ai requisiti essenziali di cui all'allegato I del CRA[64]. Quando tali sistemi di intelligenza artificiale ad alto rischio soddisfano i requisiti essenziali del CRA sono considerati conformi ai requisiti di cybersicurezza di cui all'articolo 15 della proposta di legge sull'IA, nella misura in cui il conseguimento del livello di protezione previsto da tali requisiti sia dimostrato dalla dichiarazione di conformità UE rilasciata ai sensi del CRA.

Al contrario, per quanto riguarda le procedure di valutazione della conformità, l'art. 43 della legge sull'IA prevale sulle rispettive disposizioni del CRA, come precedentemente trattato *supra* nel paragrafo 4. Di conseguenza, gli organismi notificati che controllano la conformità dei sistemi di IA ad alto rischio ai sensi della legge sull'IA sono anche autorizzati a controllare la conformità ai requisiti essenziali di cui all'Allegato I del CRA[65]. Tuttavia, se i sistemi di IA ad alto rischio sono anche qualificati come prodotti critici ai sensi del CRA, sono soggetti alle regole di valutazione della conformità del CRA[66].

6.2. Interazione tra il CRA e la proposta di regolamento sulla sicurezza generale dei prodotti

L'articolo 7 del CRA mira a chiarire il raccordo tra il CRA e il (proposto) regolamento relativo alla sicurezza generale dei prodotti (*General Product Safety Regulation*, GPSR). Quest'ultimo si applicherà come *lex generalis* ai prodotti non armonizzati e ai prodotti di consumo armonizzati per gli aspetti non coperti dalla legislazione armonizzata[67]. L'art. 7 CRA recita: «In deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento [Regolamento relativo alla sicurezza generale dei prodotti], qualora i prodotti con elementi digitali non siano soggetti a requisiti specifici imposti da altre normative di armonizzazione dell'Unione ai sensi dell'[articolo 3, punto 25, del Regolamento sulla sicurezza generale dei prodotti], il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento [Regolamento relativo alla sicurezza generale dei prodotti] si applicano a tali prodotti per quanto riguarda i rischi di sicurezza non contemplati dal presente regolamento».

Una lettura combinata del considerando 28 CRA e degli articoli pertinenti del GPSR può aiutare a districare il dettato di questa disposizione. Il considerando 28 CRA chiarisce che i prodotti con elementi digitali possono presentare altri rischi per la sicurezza oltre a quelli legati alla cybersicurezza. Tali rischi sono disciplinati da altre normative dell'Unione in materia di sicurezza dei prodotti. Se non è applicabile nessun'altra normativa armonizzata dell'Unione, i prodotti saranno allora soggetti al quadro giuridico

del GPSR, coerentemente con il suo ruolo di "rete di sicurezza". D'altra parte, l'articolo 2, paragrafo 1, del GPSR stabilisce che se i prodotti rientrano nell'ambito di applicazione della legislazione dell'Unione in materia di sicurezza dei prodotti, le norme stabilite dal GPSR si applicano solo agli aspetti e ai rischi non coperti da tali requisiti; in particolare, non si applicano il capo III, sezione 1, i capi V e VII e i capi IX-XI del GPSR.

Secondo il considerando 28 del CRA, la deroga alla regola generale prescritta dall'art. 2, para. 1, del GPSR trova la sua ragion d'essere nell'ambito di applicazione del CRA limitato ai soli aspetti di cybersicurezza, senza disciplinare allo stesso tempo requisiti generali di salute e sicurezza come gli altri atti giuridici della legislazione UE sui prodotti. Pertanto, il legislatore ha ritenuto necessario estendere la copertura del capitolo III, sezione 1, dei capitoli V e VII e dei capitoli IX-XI del GPSR ai prodotti con elementi digitali per quanto riguarda i rischi per la sicurezza non coperti dal CRA.

6.3. Interazione tra il CRA e la proposta di regolamento sui prodotti macchina

L'interazione tra il CRA e la proposta di regolamento sui prodotti macchina è regolata dall'art. 9 CRA, in particolare, con riguardo alle sovrapposizioni delle valutazioni di conformità previste dai due strumenti giuridici. In tal senso, se i prodotti macchina sono anche prodotti con elementi digitali ai sensi del CRA, e per i quali è stata rilasciata una dichiarazione di conformità UE sulla base del CRA, sono considerati conformi ai requisiti essenziali di salute e sicurezza di cui all'allegato III, punti 1.1.9 e 1.2.1, della proposta di regolamento sui prodotti macchina.

6.4. Interazione tra il CRA e il regolamento delegato (UE) 2022/30

Il regolamento delegato (UE) 2022/30 è stato adottato il 29 ottobre 2021 al fine di specificare a quali categorie o classi di apparecchiature radio si applicano i requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere (d) (relativo ai danni alla rete e uso improprio delle risorse di rete), (e) (relativo alla protezione dei dati personali e della vita privata) e (f) (relativo alla protezione da frodi) della direttiva 2014/53/UE sulle apparecchiature radio (RED).

I requisiti essenziali stabiliti dal CRA comprendono tutti gli elementi dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) ed f) della RED[68]. Inoltre, i requisiti essenziali del CRA sono anche allineati con gli obiettivi delle norme armonizzate incluse nella richiesta di standardizzazione della Commissione agli organismi europei di standardizzazione per dimostrare la conformità ai suddetti requisiti della RED[69].

Alla luce di quanto detto sopra, si può concludere che il contenuto e gli obiettivi dell'atto delegato della RED si sovrappongono completamente alla proposta CRA. Infatti, il considerando 15 CRA prevede esplicitamente la possibilità di abrogare o modificare il regolamento delegato (UE) 2022/30. Se così fosse, la Commissione e gli organismi di standardizzazione «dovrebbero tenere conto dei lavori di normazione svolti nel contesto della decisione di esecuzione C(2022)5637 della Commissione relativa ad una richiesta di normazione per il regolamento delegato (UE) 2022/30 che integra la direttiva sulle apparecchiature radio nella preparazione e nello sviluppo di norme armonizzate per facilitare l'attuazione del presente regolamento»[70].

6.5. Interazione tra il CRA e la direttiva NIS2

Vista la natura generale e introduttiva del presente articolo, questa sezione commenta le disposizioni del CRA che costituiscono un'interfaccia con la direttiva NIS2, senza perciò addentrarsi in un'analisi critica dettagliata delle potenziali sfide giuridiche derivanti dall'applicazione dei due quadri normativi.

La direttiva NIS2, che abrogherà la direttiva NIS, mira a modernizzare l'attuale quadro giuridico dell'UE in materia di cybersicurezza, affrontando diverse problematiche che hanno impedito alla direttiva NIS di esprimere tutto il suo potenziale. Ai fini del presente articolo, vengono prese in considerazione tre aree di interazione con il CRA. Esse riguardano: (i) l'ambito di applicazione dei due atti giuridici; (ii) le norme che regolano i rapporti lungo la catena di approvvigionamento; (iii) gli obblighi di segnalazione di incidenti e vulnerabilità.

Il *software-as-a-service*, con alcune eccezioni, come detto, non rientra nell'ambito di applicazione del CRA. La NIS2 sarebbe quindi complementare rispetto al CRA, dal momento che si applicherà ai servizi di cloud computing e ai modelli di servizi cloud, come il *SaaS*, in quanto tutti i soggetti che forniscono servizi di cloud computing nell'Unione e che raggiungono o superano la soglia delle medie imprese rientrano nell'ambito di applicazione di tale direttiva[71]. Inoltre, un criterio di cui la Commissione dovrà tenere conto nel determinare le categorie di prodotti altamente critici è se una categoria di prodotti con elementi digitali sia utilizzata dai soggetti essenziali ai sensi della NIS2, sia una categoria di prodotti su cui detti soggetti fanno affidamento, oppure possa avere un'importanza futura per le attività di tali soggetti[72].

Inoltre, il CRA integrerebbe efficacemente il quadro NIS garantendo i prerequisiti per una maggiore sicurezza della catena di approvvigionamento[73]. Pertanto, la conformità dei soggetti NIS2 alle misure di gestione dei rischi di cybersicurezza relative alla catena di approvvigionamento di cui agli articoli 21, para. 2, lettera d), 21, para. 3 e 22 della NIS2 sarebbe facilitata dalla garanzia che i prodotti con elementi digitali che i soggetti essenziali e importanti utilizzano nella fornitura dei loro servizi siano progettati e fabbricati secondo controlli di cybersicurezza allo stato dell'arte. Inoltre, l'approccio dinamico, lungo il ciclo di vita dei prodotti adottato dal CRA assicura che i soggetti NIS2 abbiano accesso a tempestivi aggiornamenti di sicurezza per tali prodotti[74].

Un'ulteriore area di intersezione è rappresentata dagli obblighi di segnalazione. Come si è visto *supra* nel paragrafo 3, gli obblighi di notifica dei fabbricanti riguardano principalmente le vulnerabilità sfruttate attivamente e qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali (art. 11 CRA). Il modello centralizzato di governance del CRA pone l'ENISA al centro del quadro procedurale di queste notifiche. Sullo sfondo degli obblighi di segnalazione di incidenti e vulnerabilità da parte di entità essenziali e importanti ai sensi della NIS2, sarà fondamentale garantire una comunicazione efficiente e tempestiva tra l'ENISA e il punto di contatto unico degli Stati membri interessati, per quanto riguarda gli incidenti, e il CSIRT designato ai fini della divulgazione coordinata delle vulnerabilità ai sensi dell'art. 12 NIS2. L'inclusione della rete EUCyCLONe, istituita dall'art. 16 NIS2, in questo quadro coordinato[75] suggerisce la volontà di costruire un ecosistema europeo coerente di sicurezza e resilienza digitale.

6.6. Interazione tra il CRA e il *Cybersecurity Act*

La proposta CRA mira a sfruttare le sinergie con il CSA soprattutto per quanto riguarda la procedura di valutazione della conformità. L'articolo 18, paragrafi 3 e 4, del CRA funge da raccordo tra i due quadri giuridici al fine di promuovere i sistemi europei di certificazione della cybersicurezza (*European Cybersecurity Certification Schemes*, ECCS) e facilitare la valutazione della conformità dei prodotti con elementi digitali, se coperti da una dichiarazione di conformità UE o da un certificato nell'ambito di un ECCS ai sensi del Regolamento (UE) 2019/881.

La Commissione può specificare, mediante atti di esecuzione: (i) gli ECCS che possono essere utilizzati per la presunzione di conformità ai requisiti essenziali di CRA; (ii) se un certificato di cybersicurezza rilasciato nell'ambito di tali sistemi elimina l'obbligo per un fabbricante di effettuare una valutazione di conformità da parte di terzi per i requisiti corrispondenti. Inoltre, alla Commissione è conferito il potere di adottare atti delegati per specificare le categorie di prodotti con elementi digitali "altamente critici" per i quali i fabbricanti sono tenuti a ottenere un certificato nell'ambito di un ECCS per dimostrare la conformità ai requisiti essenziali stabiliti nel CRA, rendendo di conseguenza obbligatorio ricorrere allo strumento – in teoria volontario – della certificazione.

Infine, è interessante notare come il considerando 39 della proposta CRA ritagli *prima facie* un ruolo di riferimento per il CRA in relazione ai futuri ECCS: «la necessità di nuovi sistemi europei di certificazione della cybersicurezza per i prodotti con elementi digitali dovrebbe essere valutata alla luce del presente regolamento. Tali futuri sistemi europei di certificazione della cybersicurezza relativi ai prodotti con elementi digitali dovrebbero tenere conto dei requisiti essenziali stabiliti nel presente regolamento e facilitare la conformità a quest'ultimo».

7. Conclusione

Una legislazione armonizzata in materia di cybersicurezza a livello comunitario è l'opzione strategica più efficace per aumentare il livello di fiducia degli utenti, l'attrattiva dei prodotti con elementi digitali dotati di marcatura CE e il livello generale di cyberresilienza. Il CRA andrebbe inoltre a vantaggio degli operatori economici, fornendo certezza giuridica e creando condizioni di parità per i venditori e sviluppatori di prodotti hardware e software. Questo atto giuridico, atipico nella legislazione dell'UE sulla sicurezza dei prodotti, giacché coprirebbe esclusivamente gli aspetti legati alla cybersicurezza per una categoria molto ampia di prodotti senza tenere conto di più ampie considerazioni in materia di salute e sicurezza, giustifica lo strumento del regolamento da un punto di vista di policy, in quanto affronterebbe in modo più efficace i problemi individuati.

Inoltre, il CRA contribuirebbe al processo in corso di definizione di un concetto di cybersicurezza nel diritto dell'UE[76]. La cybersicurezza si è progressivamente trasformata in una sfida sociale, economica e multidisciplinare[77]; una concettualizzazione che ricomprenda i soli obiettivi tradizionali di protezione della sicurezza informatica sarebbe oggi anacronistica. In questo contesto, la proliferazione dei prodotti connessi e la digitalizzazione di tutti i settori della società amplia il perimetro dei valori e degli asset da proteggere. I fattori di rischio e le minacce nell'odierno ambiente digitale iperconnesso vanno oltre l'infrastruttura tecnologica dei sistemi informativi,

delle reti e delle informazioni sottostanti. Un attacco informatico potrebbe comportare degli impatti anche significativi per i diritti fondamentali degli individui, compromettere la sicurezza fisica delle persone e, per quanto riguarda le infrastrutture critiche, avere gravi conseguenze per le comunità e le istituzioni.

Questa prospettiva, definita altrove come "infraetica"[78], è riconosciuta dalla proposta CRA: «proteggendo i consumatori e le organizzazioni dai rischi di cybersicurezza, i requisiti essenziali di cybersicurezza stabiliti nel presente regolamento dovrebbero inoltre contribuire a migliorare la protezione dei dati personali e della vita privata delle persone»[79]. In altre parole, la cybersicurezza può anche essere concepita come un valore strumentale necessario per sostenere valori fondamentali, come i diritti e le libertà fondamentali e la sicurezza individuale.

Note

[1] Enisa, *Enisa Threat Landscape*, 2021.

[2] A. Vedder, *Safety, Security and Ethics*, in A. Vedder, J. Schroers, C. Ducuing, P. Valcke (eds.), "Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security", Intersentia, 2019, pp. 11-26.

[3] M. Durante, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. Berkich, M.V. d'Alfonso (eds.), "On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence", Springer, 2019, p. 372.

[4] J.M. Blythe, S.D. Johnson, M. Manning, *What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices*, in "Crime Science", vol. 9, 2020, n. 1, pp. 1-9.

[5] S. Georgiev, A. Thirriot, C. Meziat et al., *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715. Final Study Report*, 2021, pp. 34-36.

[6] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.

[7] Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final.

[8] Consiglio dell'Unione europea, *Council conclusions on the cybersecurity of connected devices*, 2020.

[9] Parlamento europeo, Risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, (2021/2568(RSP)).

[10] 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, COM(2022) 454, del 15 settembre 2022.

[11] Art. 2, para. 1, proposta CRA.

[12] Art. 3, para. 1, proposta CRA.

[13] Digitaleurope, *Building blocks for a scalable cyber resilience act*, 2022, pp. 7-8.

[14] Eurosmart, *Cyber Resilience Act (CRA) – New cybersecurity rules for digital products and ancillary services*, 2022, pp. 8-9; si veda anche Anec, *Anec response to EC Call for evidence for an impact assessment on the cyber resilience act (CRA) initiative*, 2022, pp. 3-5.

[15] Beuc, *Cyber resilience act: cybersecurity of digital products and ancillary services—BEUC response to public consultation*, 2022, p. 7.

[16] Si veda *ex multis* G. Wagner, *Software as a product*, in S. Lohsse, R. Schulze, D. Staudenmayer (eds.), "Smart products: Münster colloquia on EU law and the digital economy VI", Nomos, 2022, pp. 157-179.

[17] Relazione alla proposta CRA, p. 1.

[18] *Ivi*, p. 8.

[19] Considerando 10, proposta CRA.

[20] Art. 2, para. 5, proposta CRA.

[21] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in "Common Market Law Review", vol. 59, 2022, n. 2, pp. 473-500.

[22] Art. 6, para. 2, proposta CRA.

[23] Art. 6, para. 5, proposta CRA.

[24] Art. 6, para. 4, proposta CRA.

[25] Art. 6, para. 5, proposta CRA.

[26] Art. 10, para. 4, proposta CRA.

[27] Art. 5, punto 1, proposta CRA.

[28] Art. 10; Art. 5, punto 1, proposta CRA.

[29] Art. 5, punto 2, proposta CRA.

[30] Art. 10, para. 2, proposta CRA.

[31] Art. 10, para. 3, proposta CRA.

[32] Art. 10, para. 5, proposta CRA.

[33] Art. 10, para. 8, proposta CRA.

[34] Art. 10, para. 13, proposta CRA.

[35] Art. 10, para. 14, proposta CRA.

[36] Art. 10, para. 10, proposta CRA.

[37] Art. 10, para. 11, proposta CRA.

[38] S. Schmitz, S. Schiffner, *Responsible vulnerability disclosure under the NIS 2.0 proposal*, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", vol. 12, 2021, n. 5, pp. 448-457.

[39] Art. 11, para. 4, proposta CRA.

[40] Art. 11, para. 7, proposta CRA.

[41] Art. 15, proposta CRA.

[42] Art. 16, proposta CRA.

[43] H.C.H. Hofmann, *A European Regulatory Union - The Role of Agencies and Standards*, in P. Koutrakos, J. Snell (eds.), "Research handbook on the EU's internal market", Elgar Publishing, 2016, pp. 1-20.

[44] Art. 18, proposta CRA.

[45] Art. 18, para. 3, proposta CRA.

[46] Art. 18, para. 4, proposta CRA.

[47] Art. 19, proposta CRA.

[48] Art. 18, para. 2, proposta CRA.

[49] Art. 20, proposta CRA.

[50] Art. 24, para. 1, proposta CRA.

[51] Art. 24, para. 2 e 3, proposta CRA.

[52] Art. 24, para. 2, proposta CRA.

[53] Art. 22, para. 1, proposta CRA.

[54] Art. 41, proposta CRA.

[55] Art. 41, para. 10, proposta CRA.

[56] Art. 48, proposta CRA.

[57] Art. 49, proposta CRA.

[58] Art. 43, para. 1, proposta CRA.

[59] Art. 43, para. 4, proposta CRA.

[60] Art. 45, proposta CRA.

[61] Art. 45, para. 4, proposta CRA.

[62] Art. 53, proposta CRA.

[63] P.G. Chiara, *The IoT and the new EU cybersecurity regulatory landscape*, in "International Review of Law Computers and Technology", vol. 36, 2022, n. 2.

[64] Art. 8, proposta CRA.

[65] Art. 8, para. 2, proposta CRA.

[66] Art. 8, para. 3, proposta CRA.

[67] Commissione europea, *Sintesi della relazione sulla valutazione d'impatto che accompagna il documento Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 87/357/CEE del Consiglio e la direttiva 2001/95/CE del Parlamento europeo e del Consiglio*, SWD(2021) 169 final, p. 10.

[68] Considerando 15, proposta CRA.

[69] *Ibidem*.

[70] *Ibidem*.

[71] Considerando 9, proposta CRA.

[72] Art. 6, para. 5, lett. a, proposta CRA.

[73] P.G. Chiara, *The IoT and the new EU cybersecurity*, cit., p. 12.

[74] Considerando 11, proposta CRA.

[75] Art. 11, para. 3, proposta CRA.

[76] V. Papakonstantinou, *Cybersecurity as* praxis *and as a* state*: The EU law path towards acknowledgement of a new right to cybersecurity?*, in "Computer Law & Security Review", vol. 44, 2022.

[77] M. Veale, I. Brown, *Cybersecurity*, in "Internet Policy Review", vol. 9, 2020, n. 4.

[78] P.G. Chiara, *The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: A Critique to Traditional "Security&Privacy" Surveys*, in "European Data Protection Law Review", vol. 7, 2021, n. 1; si veda inoltre L. Floridi, *Infraethics–on the Conditions of Possibility of Morality*, in "Philosophy & Technology", vol. 30, 2017, pp. 391-394.

[79] Considerando 17, proposta CRA.

* * *

The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements

Abstract: The EU Commission presented on 15 September 2022 the proposal for a "Regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020" (Cyber Resilience Act, CRA). This article sheds light on the "horizontal" character of the CRA proposal by highlighting its main pillars. In particular, the contribution takes into account the new set of obligations placed on economic operators, the conformity assessment procedures as well as the market surveillance framework and the interplay with other legislative initiatives, both in the policy area and outside EU cybersecurity law. Against the backdrop of the sectoral regulatory approach adopted thus far by the Commission vis-à-vis cybersecurity requirements for products, horizontal intervention is needed not only to ensure higher standard of cybersecurity of products with digital elements, but also to ensure legal certainty, avoiding duplicative obligations and further market fragmentation.

Keywords: Cyber Resilience Act – EU law – Cybersecurity Law