Capitolo 7

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

Pier Giorgio Chiara [*]

Abstract: Il presente capitolo intende chiarire le scelte regolatorie fondative del regolamento (UE) 2024/2847 (*Cyber Resilience Act*, CRA) relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Come altri atti giuridici dell'Unione europea, soprattutto con riferimento alla regolamentazione del 'digitale', il CRA combina approcci regolatori diversi, quali: i) approccio orizzontale; ii) approccio basato sul rischio; iii) approccio di sicurezza dei prodotti. In aggiunta, l'*Explanatory Memorandum* della Commissione europea alla proposta del regolamento chiarisce che il CRA contribuisce a tutelare i diritti fondamentali. Mentre la combinazione di alcuni approcci è più risalente nella tradizione del diritto armonizzato (ad es., approccio basato sul rischio e sicurezza dei prodotti), e presenta quindi profili meno problematici, l'integrazione di un approccio basato sui diritti nelle strutture tradizionali della legislazione in materia di sicurezza dei prodotti è novità recente della tecnica legislativa dell'Unione europea e pertanto merita una riflessione critica più approfondita.

Keywords: Cyber Resilience Act – Legge sulla ciberresilienza – Diritto dell'UE – Diritto della cybersicurezza – Diritti fondamentali

Sommario: 1. Introduzione. – 2. L'approccio orizzontale. – 3. L'approccio basato sul rischio. – 4. L'approccio di sicurezza dei prodotti. – 5. Il Cyber Resilience Act e la tutela dei diritti fondamentali. – 6. Conclusione.

---

[*] Ricercatore a tempo determinato di tipo a) in informatica giuridica (IUS/20), presso CIRSFID – Alma AI e Dipartimento di Scienze Giuridiche, Università di Bologna, piergiorgio.chiara2@unibo.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 regolamento (UE) 2024/2847 [1], vale a dire la 'legge sulla ciberresilienza' o, com'è maggiormente noto in lingua inglese, *Cyber Resilience Act* o CRA, adottato sul finire del 2024, rappresenta l'approdo di un lungo processo di politica regolatoria. Già la seconda Strategia dell'Unione in materia di cybersicurezza [2], risalente al 2017, aveva evidenziato come le minacce cibernetiche nonché i cyberattacchi a prodotti connessi (c.d. *Internet of Things*), nelle loro componenti hardware e software, fossero aumentati in misura significativa, non solo da un punto di vista quantitativo, ma anche in termini di impatto e sofisticazione [3].

Il principale risultato sul piano legislativo scaturito dalla Strategia del 2017 è stato il regolamento (UE) 2019/881 (*Cybersecurity Act*), che rinforza il ruolo dell'ENISA (Agenzia Europea per la Cybersicurezza) e soprattutto introduce un quadro di certificazione a livello europeo per la cybersicurezza. Ancorché il rafforzamento della (cyber)sicurezza delle tecnologie ICT (prodotti, servizi e processi) fosse un obiettivo del *Cybersecurity Act* [4], due elementi hanno impedito, quanto meno nel breve termine, che questo si realizzasse compiutamente. In primo luogo, la certificazione rimane strumento di diritto privato caratterizzato dalla volontarietà; in secondo luogo, il summenzionato quadro normativo non contempla requisiti obbligatori circa la cybersicurezza della totalità dei prodotti digitali.

Nel 2020 la Commissione ha adottato la terza Strategia di cybersicurezza e, nel contesto della prima area di azione (resilienza, sovranità tecnologica e leadership), annuncia la possibilità di introdurre nuove norme orizzontali volte a migliorare la cibersicurezza di tutti i prodotti connessi e servizi associati presenti nel mercato interno [5], colmando quindi una lacuna significativa nel quadro normativo.

---

[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (legge sulla ciberresilienza), GU L 2024/2847, 20.11.2024. Per una disamina sulla compatibilità del CRA con il diritto del commercio internazionale si veda, in questo volume, G. ADINOLFI-R. MAGNAGHI, *Il Cyber Resilience Act nella prospettiva degli accordi commerciali dell'Unione europea*.

[2] Sul termine 'cybersicurezza', si veda, in questo volume, R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*.

[3] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017), 450 final, pp. 2-3.

[4] Considerando 65, *Cybersecurity Act*.

[5] 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, p. 10.

Nell'arco di un anno, la Commissione ha concluso che la mancanza di requisiti obbligatori di cybersicurezza per tutti i prodotti con elementi digitali è stata la causa principale del fallimento di mercato nella fornitura di prodotti digitali con adeguati livelli di cybersicurezza [6]. Le asimmetrie informative tra i produttori e i consumatori hanno contribuito a questo fallimento di mercato, dal momento che i secondi non avevano le necessarie capacità di valutare l'adeguatezza del livello di cybersicurezza di un prodotto oppure non avevano accesso a tali informazioni. Di conseguenza, i produttori non avrebbero avuto gli incentivi necessari per offrire prodotti 'più sicuri' dal momento che i consumatori non avrebbero ricompensato il costo maggiore investito in sicurezza. Il risultato pertanto è stato un livello di investimenti nella sicurezza dei prodotti digitali sub-ottimale [7].

Investimenti sub-ottimali nella sicurezza dei prodotti rappresentano un rischio non solo per il corretto funzionamento del mercato, ma anche per i diritti fondamentali e la sicurezza degli individui. Ogni ambito e settore della nostra società è digitalizzato ed interconnesso: una vulnerabilità in un prodotto, se sfruttata dagli attori della minaccia, può comportare serie compromissioni all'infrastruttura di reti e sistemi informativi ad esso collegati, potenzialmente con drammatici effetti 'spillover' per un'intera catena di approvvigionamento [8]. Inoltre, i prodotti connessi che costituiscono la cosiddetta "Internet delle 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 non solo è strumentale alla tutela dei diritti fondamentali alla riservatezza e protezione dei dati personali, ma è anche direttamente connessa all'incolumità fisica (*safety)* [9].

Da un punto di vista giuridico, rispetto al 2017, il quadro normativo dell'Unione appariva nel 2020 ancora frammentato in relazione ai requisiti di cybersicurezza per i prodotti digitali, dal momento che le diverse iniziative legislative adottate tra la seconda e la terza Strategia hanno affrontato solo in parte i problemi identificati. Oltre al già ricordato *Cybersecurity Act*, la Commissione

---

[6] COMMISSIONE EUROPEA, *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report*, 2021, p. 69, p. 73.

[7] *Ibid*., pp. 34-37.

[8] M. VAN'T SCHIP, *The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things*, in *European Journal of Law and Technology*, 2024, vol. 15, n. 1.

[9] A. VEDDER, *Safety, security and ethics*, in A. VEDDER-J. SCHROERS-C. DUCUING-P. VALCKE (a cura di), *Security and Law*, Intersentia, Cambridge, 2020, pp. 11-26; si veda inoltre, M. DURANTE, *Safety and security in the digital age. Trust, algorithms, standards, and risks*, in D. BERKICH-M.V. D'ALFONSO (a cura di), *On the cognitive, ethical, and scientific dimensions of artificial intelligence*, Springer, Berlino, 2019, p. 372.

adottò un approccio 'verticale', intervenendo cioè su alcuni atti giuridici della legislazione sulla sicurezza dei prodotti attraverso l'inclusione di requisiti essenziali in materia di cybersicurezza [10].

La necessità di dotare l'UE di un quadro normativo unitario e coerente con precisi obblighi per gli operatori economici coinvolti nella messa a disposizione sul mercato di prodotti con elementi digitali (non solo i fabbricanti) e requisiti di cybersicurezza lungo l'intero ciclo di vita del prodotto emerge non solo dalla già ricordata terza Strategia UE in materia, ma anche dalle conclusioni del Consiglio del 2 dicembre 2020 [11] e dalla Risoluzione del Parlamento europeo del 10 giugno 2021 [12]. Così, la Presidente della Commissione europea Von der Leyen nel discorso sullo stato dell'Unione del 2021 annunciò il futuro regolamento, proposto il 15 settembre 2022. Nel novembre 2024 venne pubblicato in G.U. dell'UE il testo definitivo del regolamento.

Le scelte regolatorie alla base del CRA sono principalmente tre. Un approccio c.d. 'orizzontale', sia con riferimento all'introduzione di requisiti di cybersicurezza 'di base', che da un punto di vista dell'ambito di applicazione oggettivo (volto cioè ad includere tutti i prodotti con elementi digitali, seppure con delle eccezioni, e non invece determinate categorie merceologiche); l'approccio basato sul rischio, divenuto ormai il modello di governance standard della regolamentazione europea del digitale [13]; ed infine l'approccio di sicurezza dei prodotti, basato sul c.d. nuovo approccio, cui ora si applicano i principi del c.d. Nuovo Quadro Legislativo [14].

---

[10] È il caso del Regolamento delegato (UE) 2022/30 della Commissione del 29 ottobre 2021 che integra la direttiva 2014/53/UE del Parlamento europeo e del Consiglio per quanto riguarda l'applicazione dei requisiti essenziali di cui all'art. 3, par. 3, lett. d), e) ed f), di tale direttiva; della proposta di Regolamento relativo alle macchine (poi Regolamento (UE) 2023/1230) o della proposta di Regolamento relativo alla sicurezza generale dei prodotti (Regolamento (UE) 2023/988).

[11] CONSIGLIO DELL'UNIONE EUROPEA, *Council conclusions on the cybersecurity of connected devices*, 2020.

[12] 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)).

[13] G. DE GREGORIO-P. DUNN, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, vol. 59, n. 2, pp. 473-500; P.G. CHIARA-F. GALLI, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *MediaLaws*, 2024, no. 1, p. 105.

[14] Il Nuovo Quadro Legislativo consiste nel regolamento (CE) n. 765/2008 e la decisione n. 768/2008/CE, nonché nel regolamento (UE) 2019/ 1020 (modificato dal CRA). In breve, la legislazione in materia di sicurezza dei prodotti si limita a stabilire requisiti essenziali che i prodotti rilevanti devono rispettare per poter essere messi a disposizione sul mercato. Per dimostrare la conformità dei prodotti ai requisiti essenziali, la legislazione armonizzata prevede diverse procedure di valutazione della conformità (c.d. moduli), tra cui è prevista la possibilità per un

È opportuno un *caveat* metodologico. La combinazione di questi approcci regolatori trova nel CRA un'applicazione organica; distinguere nettamente i loro perimetri operativi nel testo del regolamento sarebbe artificioso e, comunque, di scarsa utilità nell'implementazione delle diverse disposizioni. Ciononostante, l'adozione di questa chiave interpretativa appare particolarmente utile per illustrare il funzionamento dei meccanismi ad alta complessità tecnica e giuridica del regolamento.

Anche il regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*, AIA), trova fondamento nei medesimi approcci regolatori, aggiungendo, tuttavia, meccanismi significativi di tutela dei diritti fondamentali (c.d. approccio basato sui diritti) [15].

A differenza dell'AIA, tra gli obiettivi del CRA non figura la protezione dei diritti fondamentali. Tuttavia, l'*Explanatory Memorandum* allegato alla proposta del CRA della Commissione chiarisce che il regolamento rafforzerebbe in una certa misura la protezione dei diritti e delle libertà fondamentali, come la privacy, la protezione dei dati personali, la libertà d'impresa e la protezione della proprietà o della dignità e integrità personale [16].

In questo contesto, il presente capitolo si propone di analizzare criticamente le scelte strutturali e gli equilibri sottesi al *Cyber Resilience Act*, evidenziando come l'interazione tra approcci regolatori eterogenei dia forma ad un impianto normativo ad alta complessità tecnico-giuridica. In particolare, l'attenzione sarà rivolta al modo in cui il CRA riesca (o meno) a coniugare la logica tradizionale della sicurezza dei prodotti e del rischio con l'emergente esigenza di integrare la tutela dei diritti fondamentali nell'ambito della regolazione tecnica. Attraverso un esame sistematico delle scelte regolatorie alla base delle disposizioni del regolamento, nonché dei documenti preparatori, del contesto normativo e degli strumenti di *soft-law* (es., orientamenti e linee-guida pubblicate da Autorità di settore) pertinenti, il contributo intende offrire strumenti interpretativi utili per comprendere la portata e le implicazioni di questo nuovo paradigma regolatorio, evidenziandone al contempo le potenzialità e le criticità.

---

fabbricante di usare standard tecnici armonizzati sviluppati dalle organizzazioni di standardizzazione europee (CEN, CENELEC ed ETSI) dietro mandato della Commissione europea al fine di garantire la specifica tecnica di un determinato set di requisiti essenziali. Per un approfondimento maggiore, si veda COMMISSIONE EUROPEA, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, (2022/C 247/01).

[15] T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI,* in *AIRe – Journal of AI Law and Regulation*, 2024, vol. 1, n. 1, p. 98; M. ALMADA-N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025, vol. 62, n. 1.

[16] EUROPEAN COMMISSION, *Explanatory Memorandum to the Cyber Resilience Act proposal*, (COM(2022) 454 final), p. 8.

2. L'approccio orizzontale

La mancanza di un quadro normativo completo dell'Unione, che stabilisca requisiti di cybersicurezza per tutti i prodotti con elementi digitali, è stata uno dei motivi che hanno portato il legislatore europeo ad adottare il CRA [17]. Infatti, le diverse iniziative legislative intraprese fino alla pubblicazione della proposta del CRA, sia a livello nazionale che dell'Unione, hanno affrontato i rischi di cybersicurezza solo in parte, tramite una legislazione settoriale, cioè per specifiche categorie di prodotto (ad es., il regolamento sui dispositivi medici). Il risultato di questo approccio regolatorio è stata la creazione di un 'mosaico legislativo', che ha aumentato l'incertezza del diritto, ha comportato oneri aggiuntivi per le imprese e, soprattutto, ha mostrato lacune sostanziali in termini di requisiti obbligatori di cybersicurezza per tutti i prodotti – e relative componenti – con elementi digitali, contribuendo pertanto ad uno stato diffuso di insicurezza [18].

L'approccio orizzontale si declina pertanto non solo in un novero di requisiti di cybersicurezza 'di base' [19], ma anche in un ambito di applicazione oggettivo trasversale rispetto alle categorie merceologiche dei prodotti con elementi digitali. Il CRA, infatti, si applica "ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete" [20].

La portata reale e l'impatto sul mercato interno di tale approccio sono chiariti dalla definizione di 'prodotto con elementi digitali', cioè "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi sul mercato separatamente" [21]. A fronte della notevole estensione della nozione di prodotto contenuta nel regolamento, in linea peraltro con altri atti giuridici dell'Unione, come la direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi [22], ponendo fine ad un dibattito che tanto ha animato la letteratura soprattutto con riferimento

[17] Cons. 4, CRA.

[18] COMMISSIONE EUROPEA, *Relazione alla proposta di regolamento CRA, 2022/0272 (COD)*, COM(2022) 454 final, p. 3.

[19] L'art. 5, par. 1, CRA lascia impregiudicata infatti la possibilità per gli Stati membri di prevedere requisiti di cybersicurezza supplementari per l'acquisto o l'uso di prodotti con elementi digitali per finalità specifiche, anche nel caso in cui tali prodotti siano acquistati o utilizzati per scopi di sicurezza nazionale o di difesa.

[20] Art. 2, par. 1, CRA.

[21] Art. 3, punto 1, CRA.

[22] Art. 4, punto 1, Direttiva (UE) 2024/2853.

alle questioni inerenti alla responsabilità civile [23], è opportuno chiarire fino a che punto i requisiti e gli obblighi del CRA si applichino al software.

Il regolamento non solo ricomprende a pieno titolo il software 'incorporato', ma anche le componenti software immesse sul mercato separatamente, nonché le c.d. soluzioni di elaborazioni dati da remoto [24], vale a dire il software sviluppato dal fabbricante, o per suo conto, ai fini del trattamento o dell'archiviazione a distanza di dati la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni, come ad esempio un'applicazione mobile che richieda l'accesso a un'interfaccia per programmi applicativi [25].

Solo a queste condizioni, quindi, una soluzione di elaborazione dati da remoto rientra nell'ambito di applicazione del CRA. Ne consegue che ad un servizio cloud la cui progettazione esuli dalla responsabilità del fabbricante di un prodotto, o ad un sito web che non supporti le funzionalità di un prodotto con elementi digitali, non si applica il CRA [26]. D'altronde, gli aspetti di cybersicurezza dei modelli di servizi di cloud quali il c.d. *software-as-a-service* sono già adeguatamente coperti dalla direttiva (UE) 2022/2555 (c.d. direttiva NIS2).

Sotto altro profilo, nonostante le doglianze della comunità di riferimento, anche il software libero ed open-source rientra nell'ambito di applicazione del CRA, a patto che sia messo a disposizione sul mercato, vale a dire, fornito per essere distribuito o utilizzato nel corso di un'attività commerciale [27], in ragione

---

[23] Si veda *ex multis* G. WAGNER, *Software as a product*, in S. LOHSSE-R. SCHULZE-D. STAUDENMAYER (a cura di), *Smart products: Münster colloquia on EU law and the digital economy VI*, Nomos, 2022, pp. 157-179.

[24] DIGITALEUROPE, commentando la proposta CRA, sosteneva che il regolamento non avrebbe dovuto comprendere il 'software generico', dal momento che opera indipendentemente da uno specifico prodotto e pertanto non è adatto allo stesso trattamento legislativo; si veda DIGITALEUROPE, *Building blocks for a scalable cyber resilience act*, in https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf, 2022, pp. 7-8. *Contra*, Eurosmart, BEUC e ANEC ritenevano che l'ambito di applicazione del CRA avrebbe dovuto includere non solo il software 'non incorporato' ma anche i servizi cloud. Cfr. EUROSMART, *Cyber Resilience Act (CRA)-new cybersecurity rules for digital products and ancillary services*, 2022, pp. 8-9; ANEC, *Anec response to EC Call for evidence for an impact assessment on the cyber resilience act (CRA) initiative*, 2022, pp. 3-5; BEUC, *Cyber resilience act: cybersecurity of digital products and ancillary services-BEUC response to public consultation*, 2022, p. 7.

[25] Cons. 11; art. 3, punto 2, CRA.

[26] Cons. 12, CRA.

[27] Cons. 18, CRA. Il considerando 15 specifica che il requisito dell'attività commerciale è soddisfatto non solo dall'applicazione di un prezzo per il prodotto, ma anche dall'applicazione di un prezzo per i servizi di assistenza tecnica quando ciò non è finalizzato esclusivamente a recuperare i costi effettivi, dall'intenzione di monetizzare altri servizi, dall'imposizione, come condizione per l'utilizzo, del trattamento di dati personali per motivi diversi dal solo miglioramento

dei drammatici impatti all'intera catena di approvvigionamento a seguito di attacchi di sicurezza a componenti open-source (eg., Log4Shell, XZ Utils) [28].

La portata dell'ambito di applicazione oggettivo del CRA conosce comunque dei limiti. Alcuni prodotti con elementi digitali sono infatti esclusi in ragione del fatto che atti giuridici settoriali dell'Unione loro applicabili si occupano dei rischi di cybersicurezza e sicurezza delle informazioni assicurando il medesimo livello di protezione del CRA. È il caso dei dispositivi medici e medico-diagnostici in vitro, dei veicoli a motore, dei prodotti aeronautici certificati in conformità al regolamento (UE) 2018/1139, nonché dell'equipaggiamento marittimo a cui si applica la direttiva 2014/90/UE [29]. Inoltre, il regolamento non si applica ai pezzi di ricambio per sostituire componenti identici in prodotti con elementi digitali, a condizione che siano fabbricati secondo le stesse specifiche, e neanche ai prodotti con elementi digitali sviluppati o modificati esclusivamente per scopi di sicurezza nazionale o difesa.

Alla luce del complicato quadro che emerge, la Commissione pubblicherà orientamenti per agevolare l'attuazione del regolamento, in particolare, chiarendo fino a che punto l'ambito di applicazione del CRA si estenda al software (quindi, le soluzioni di elaborazione dati da remoto e software libero e open-source) [30].

Per quanto attiene all'ambito di applicazione soggettivo, i destinatari degli obblighi del CRA sono tutti gli operatori economici coinvolti lungo l'intera catena di valore di un prodotto con elementi digitali (fabbricanti, distributori, importatori, rappresentanti autorizzati, fornitori di servizi di logistica), ancorché con regimi di responsabilità diversi [31]. Come si vedrà nella prossima sezione, la diversa modulazione di tali obblighi è informata da un approccio basato sul diverso rischio che il singolo operatore economico gestisce con riguardo alla fabbricazione o alla messa a disposizione sul mercato del prodotto.

---

della sicurezza, della compatibilità o dell'interoperabilità del software, o dall'accettazione di donazioni che superano i costi associati alla progettazione.

[28] L. COLONNA, *The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive*, in *Computer Law & Security Review*, 2025, vol. 56, pp. 4-5; J. TRIDGELL, *Open or Closing Doors? The Influence of 'Digital Sovereignty' in the EU's Cybersecurity Strategy on Cybersecurity of Open-Source Software*, in *Computer Law & Security Review*, 2025, vol. 56.

[29] Art. 2, CRA.

[30] Art. 26, par. 2, lett. a), CRA.

[31] Gli obblighi dei fabbricanti si estendono anche all'importatore o al distributore che immetta un prodotto sul mercato con il proprio nome o marchio o effettui una modifica sostanziale del prodotto.

3. L'approccio basato sul rischio

Come altri atti giuridici dell'Unione in materia digitale, anche il CRA segue un approccio basato sul rischio [32]. Tale approccio permea ogni aspetto del regolamento, dalla classificazione dei prodotti nell'ambito di applicazione, agli obblighi, passando per le procedure di applicazione delle norme. Pertanto, come ricordato nell'Introduzione, diverse considerazioni svolte in questa sezione necessariamente intersecheranno con gli istituti tipici della legislazione armonizzata in materia di sicurezza dei prodotti, analizzati nella sezione successiva (par. 4).

Il regolamento definisce il "rischio di cybersicurezza" secondo lo schema classico della teoria di gestione del rischio [33]: il rischio si quantifica in un danno potenziale (perdita o perturbazione), causato da un incidente. Tale prodotto è dato dalla combinazione di due fattori, vale a dire la gravità del danno e la probabilità che questo si verifichi in un incidente [34]. Un rischio di cybersicurezza è invece considerato "significativo" se, in base alle sue caratteristiche tecniche, la probabilità che provochi un incidente sia *elevata* e l'impatto negativo che potrebbe cagionare *grave* (in termini di perdite materiali e immateriali) [35].

Il regolamento tutela così diversi beni giuridici dai diversi rischi di cybersicurezza che possono interessare i prodotti con elementi digitali, non limitandosi al novero classico dell'approccio in materia di sicurezza dei prodotti (par. 4), vale a dire la salute, la sicurezza o l'incolumità degli utilizzatori [36], ma includendo anche gli stessi prodotti con elementi digitali che potrebbero potenzialmente essere danneggiati, controllati o perturbati da altri prodotti [37], la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti da parte dei soggetti essenziali di cui alla direttiva NIS2, la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali (si veda par. 5), nonché altri aspetti della tutela dell'interesse pubblico largamente inteso [38]. Siffatta prospettiva ampia e 'strumentale' risulta peraltro allineata alla definizione di cybersicurezza fornita dal regolamento UE 2019/881 (*Cybersecurity Act*), quale insieme delle attività necessarie per proteggere la rete e i sistemi

[32] G. De Gregorio-P. Dunn, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, vol. 59, n. 2, pp. 473-500.

[33] Si veda *ex multis* lo standard ISO 31000 in tema di gestione del rischio: International Standardisation Organisation, *ISO 31000:2018 Risk Management – Guidelines*, 2018.

[34] Art. 3, punto 37, CRA.

[35] Art. 3, punto 38, CRA.

[36] Cons. 10, CRA.

[37] Cons. 43, CRA.

[38] Art. 57, CRA.

informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche [39].

In relazione al diverso rischio di cybersicurezza posto in essere dalle funzionalità dei prodotti, il regolamento distingue diverse categorie di prodotti con elementi digitali. Oltre ad una categoria di prodotti con elementi digitali 'standard', il CRA distingue prodotti con elementi digitali 'importanti' e 'critici'. La prima categoria include i prodotti che hanno la funzionalità principale di una delle categorie elencate nell'Allegato III: conformemente al concetto di rischio suesposto, una funzione è elencata nell'Allegato III se è essenziale per la cibersicurezza di altri prodotti, e/o se comporta un rischio significativo di avere effetti negativi su altri prodotti o sulla salute, la sicurezza o l'incolumità dei suoi utenti [40]. Questa categoria è ulteriormente divisa in due classi: la classe I ricomprende prodotti meno rischiosi (browser autonomi e incorporati; sistemi di gestione delle password; VPN; sistemi operativi; ecc.), mentre la classe II include prodotti aventi un livello maggiore di rischio (ipervisori; firewall; microprocessori e microcontrollori).

I prodotti con elementi digitali 'critici', invece, la cui funzionalità principale rientra tra le categorie elencate all'Allegato IV (dispositivi hardware con cassette di sicurezza; gateway per contatori intelligenti; carte intelligenti), sono tali in quanto la loro funzione, oltre a soddisfare i due criteri caratterizzanti i prodotti 'importanti', è in una relazione di dipendenza critica dei soggetti essenziali della direttiva NIS2 o, alternativamente, potrebbe causare gravi perturbazioni delle catene di approvvigionamento critiche in tutto il mercato interno se si verificasse un incidente o se una vulnerabilità venisse sfruttata [41]. Come si avrà modo di vedere nella prossima sezione, la ricaduta operativa di questa tassonomia è data dalle diverse procedure di valutazione di conformità che i fabbricanti devono seguire con riguardo alle diverse tipologie di prodotti.

Come nel regolamento UE 2024/1689 (AI Act), il legislatore predetermina il livello di rischiosità di un prodotto, o sistema di IA, adottando quindi una logica anticipatoria imperniata su un modello di governance *top-down* che non lascia spazio ad una rideterminazione del rischio *ex post*, diversamente dalla scelta regolatoria fatta in materia di protezione dei dati personali con un modello di governance "co-regolatoria", esemplificata soprattutto dal principio di responsabilizzazione *ex* art. 5 GDPR [42]. A differenza dell'AI Act, tuttavia, il CRA

[39] Art. 2, punto 1, *Cybersecurity Act*.

[40] Art. 7, par. 2, CRA.

[41] Art. 8, par. 2, CRA.

[42] U. PAGALLO-P. CASANOVAS-R. MADELIN, *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, in *The Theory and Practice of Legislation*, 2019, vol. 7, n. 1.

impone a tutti i prodotti con elementi digitali rientranti nel suo ambito di applicazione il rispetto dei requisiti essenziali, mentre solo una categoria di sistemi di IA – quelli ad alto rischio – deve essere conforme ai requisiti essenziali di cui al capo 3, sezione 2, dell'AI Act.

Sotto altro profilo, l'approccio basato sul rischio del CRA è visibile nei diversi obblighi posti in capo all'ampio ventaglio di operatori economici coinvolti nell'ambito di applicazione soggettivo del regolamento (fabbricanti, distributori, importatori, rappresentanti autorizzati), a seconda del loro ruolo e della responsabilità nella catena di approvvigionamento [43].

Il primo obbligo dei fabbricanti consiste nell'effettuare una valutazione dei rischi di cybersicurezza associati al prodotto [44], il risultato della quale deve essere tenuto conto in tutte le fasi dell'intero ciclo-vita del prodotto (dalla pianificazione alla manutenzione), non solo per identificare i rischi, ma anche i requisiti essenziali relativi al prodotto (Allegato I, sezione I, si veda par. 4) pertinenti [45]. Alcuni requisiti essenziali di cybersicurezza potrebbero non essere applicabili ad un prodotto; in questo caso il fabbricante dovrebbe fornire una chiara giustificazione nella valutazione dei rischi [46]. Questo implicito 'principio di responsabilizzazione' del fabbricante non contraddice quanto detto prima in ordine alla differenza tra CRA ed AI Act: la valutazione circa la compatibilità dei requisiti essenziali del CRA con la natura di un prodotto specifico deve essere effettuata per tutti i prodotti con elementi digitali, senza distinzioni in relazione ai rischi introdotti nel mercato.

La valutazione dei rischi deve essere inclusa dal fabbricante nella documentazione tecnica, gli elementi minimi della quale sono contenuti nell'allegato VII, e messa a disposizione del pubblico. Altri obblighi di documentazione riguardano la gestione delle vulnerabilità e delle informazioni fornite da terze parti. I fabbricanti devono rispettare ulteriori obblighi nelle fasi antecedenti la messa a disposizione sul mercato: di *due diligence* per quanto riguarda l'integrazione nel prodotto con elementi digitali di componenti forniti da terze parti, di adozione delle politiche e procedure adeguate (es., politiche di divulgazione coordinata delle vulnerabilità o per assicurare la conformità dei prodotti in serie), nonché informativi (es., dati identificativi del fabbricante e del prodotto, come numero di tipo, di lotto o serie, nonché designazione di un punto di contatto unico per le comunicazioni con gli utilizzatori ed istruzioni per gli utilizzatori).

---

[43] Gli obblighi dei fabbricanti si estendono anche all'importatore o al distributore che immetta un prodotto sul mercato con il proprio nome o marchio o effettui una modifica sostanziale del prodotto.

[44] Art. 13, par. 2, CRA.

[45] Cons. 54, CRA.

[46] Cons. 55; art. 13, par. 3, CRA.

Le responsabilità dei fabbricanti non terminano una volta che il prodotto è stato immesso sul mercato. Infatti, per l'intera durata del periodo di assistenza [47], i fabbricanti garantiscono di gestire in modo efficace le vulnerabilità, come anche di rendere disponibili per almeno 10 anni dal rilascio del prodotto gli aggiornamenti di sicurezza [48].

Nel periodo di assistenza, i fabbricanti devono poi rispettare diversi obblighi di segnalazione, in particolare, delle vulnerabilità attivamente sfruttate e degli incidenti gravi che abbiano un impatto sulla sicurezza del prodotto. Incidenti e vulnerabilità vanno notificati simultaneamente al CSIRT competente e all'ENISA, nonché agli utilizzatori del prodotto con l'indicazione di qualsiasi misura correttiva che questi possono adottare per attenuare l'impatto pregiudizievole della minaccia o dell'evento [49]. Sotto altro profilo, i fabbricanti sono tenuti a segnalare eventuali vulnerabilità scoperte nei componenti (anche open-source) integrati nel prodotto ai soggetti che li producono o mantengono.

A questo si legano anche altri obblighi "cooperativi": se i fabbricanti "correggono" le vulnerabilità scoperte nei componenti, devono condividere la *patch* con il soggetto responsabile del componente. Queste misure evidenziano come il CRA operazionalizzi il principio di sicurezza della supply-chain, stabilendo regole relative alla cybersicurezza per i diversi rapporti intercorrenti tra i fornitori e i clienti lungo l'intera catena di approvvigionamento dei prodotti con elementi digitali, un aspetto che in precedenza era regolato da clausole contrattuali basate sulle migliori pratiche di sicurezza.

Sempre sul fronte cooperativo, i fabbricanti sono tenuti a collaborare con le autorità di vigilanza del mercato, fornendo, su richiesta motivata, tutte le informazioni necessarie per dimostrare la conformità del prodotto, e, se necessario, in merito a qualsiasi misura adottata per eliminare i rischi di cybersicurezza posti dal prodotto.

---

[47] Il periodo di assistenza è determinato dal fabbricante in modo da riflettere la durata di utilizzo prevista del prodotto, tenendo conto di diversi fattori quali le ragionevoli aspettative degli utilizzatori e la natura del prodotto. Tale periodo è almeno di 5 anni salvo che il fabbricante non ritenga che il prodotto sarà utilizzato per meno di 5 anni.

[48] A tutela del consumatore, il CRA prevede che gli utilizzatori possano avere accesso all'ultima versione del software in modo gratuito se il fabbricante intenda fornire aggiornamenti di sicurezza solo all'ultima versione modificata sostanzialmente.

[49] Il fabbricante presenta una notifica di preallarme di una vulnerabilità sfruttata o di un incidente grave entro 24 ore dal momento in cui ne è venuto a conoscenza; quindi, entro 72 ore dal momento della scoperta, il fabbricante dettaglia il preallarme attraverso una notifica completa; infine, il fabbricante presenta una relazione finale entro 14 giorni dalla messa a disposizione di una misura correttiva della vulnerabilità e un mese dalla trasmissione della notifica di incidente.

4. L'approccio di sicurezza dei prodotti

L'approccio di sicurezza dei prodotti, aderente a logiche di regolazione *ex ante*, mira ad assicurare che i prodotti con elementi digitali, come gli altri prodotti oggetto della legislazione armonizzata conforme al c.d. 'Nuovo Quadro Legislativo' [50], siano sicuri (e quindi meritevoli di fiducia da parte degli utilizzatori) prima che siano immessi sul mercato.

In breve, l'attuale normativa armonizzata prevede che il contenuto della legislazione si limiti ad individuare dei "requisiti essenziali" (funzionali o prestazionali) lasciando la definizione dei dettagli tecnici a norme armonizzate europee (standard tecnici) elaborate dagli organismi europei di normazione (CEN, CENELEC ed ETSI) sulla base di una richiesta di normazione da parte della Commissione. Un prodotto, per poter essere immesso sul mercato interno, deve essere conforme ai requisiti essenziali [51]. Il prodotto si presume conforme ai requisiti essenziali se il fabbricante sceglie di applicare le norme armonizzate rilevanti nella procedura di valutazione della conformità [52].

In linea con gli istituti del Nuovo Quadro Legislativo, il CRA dispone che i prodotti con elementi digitali possano essere messi a disposizione sul mercato a condizione che rispettino i requisiti essenziali di cui all'Allegato I. Nel contesto del CRA, poi, la presunzione di conformità vista poc'anzi opera anche nel caso in cui il fabbricante abbia applicato le "specifiche comuni" rilevanti stabilite in atti di esecuzione adottati dalla Commissione nel caso in cui non siano disponibili le norme armonizzate [53]. Parimenti un prodotto con elementi digitale si presume conforme ai requisiti essenziali dell'Allegato I per il quale sono stati

---

[50] Il 'Nuovo Quadro Legislativo', adottato nel luglio 2008, e basato sul 'Nuovo Approccio' del 1985, consiste nel Regolamento (UE) 765/2008, nella Decisione 768/2008, e nel Regolamento (UE) 2019/1020.

[51] Sul funzionamento della normativa di armonizzazione dell'UE si veda COMMISSIONE EUROPEA, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022, 2022/C 247/01.

[52] Ancorché gli standard tecnici armonizzati rimangano strumenti di diritto privato di natura volontaria, il meccanismo della presunzione di conformità di cui godono i prodotti sviluppati in conformità alle norme armonizzate ha portato alcuni commentatori a ritenere che abbiano una natura *de facto* obbligatoria, giacché i fabbricanti si ritroverebbero senza reali alternative. Cfr. I. KAMARA, *Standardizing Personal Data Protection*, Oxford University Press, 2025, p. 76. In generale, sulla legislazione armonizzata UE si vedano *ex multis* H. HOFMANN, *European regulatory Union? The role of agencies and standards*, in P. KOUTRAKOS-J. SNELL (a cura di), *Research handbook on the EU's internal market*, Elgar Publishing, Cheltenham, 2016; E. AL MUREDEN, *La sicurezza dei prodotti e la responsabilità del produttore: Casi e materiali*, Giappichelli, Torino, 2017.

[53] Art. 27, par. 5, CRA.

rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cybersicurezza [54].

I requisiti essenziali di cybersicurezza relativi alle proprietà dei prodotti (parte I dell'Allegato I) mettono ancora una volta in luce la complementarità tra l'approccio al rischio e gli istituti del Nuovo Quadro Legislativo. Se il primo requisito richiede che i prodotti con elementi digitali debbano essere progettati, sviluppati e prodotti in modo da *garantire un livello adeguato di cibersicurezza in base ai rischi* (enfasi mia), l'applicazione dei rimanenti 13 requisiti, di dettaglio maggiore [55], è effettuata sulla base della *valutazione dei rischi* e *ove applicabili*, testimoniando quindi un certo grado di scalabilità – caratteristica tipica dell'approccio al rischio [56] – nel regime degli obblighi imposti ai fabbricanti. Di contro, i fabbricanti sono chiamati a soddisfare tutti gli 8 requisiti di gestione delle vulnerabilità [57] di cui alla parte II dell'Allegato I [58].

Il 3 febbraio 2025, la Commissione europea ha fatto ufficialmente richiesta agli organismi di normazione europei (CEN, CENELEC ed ETSI) di elaborare nuovi standard europei per assicurare la conformità ai requisiti essenziali del Cyber Resilience Act [59], con termini differenziati per l'adozione, a partire dal 30 agosto 2026. A supporto delle attività di standardizzazione, ENISA ha svolto due mappature al fine di identificare, nella prima, il grado di copertura offerta dagli standard di cybersicurezza esistenti più rilevanti per ogni requisito

---

[54] Art. 27, par. 8, CRA.

[55] Sono messi a disposizione sul mercato senza vulnerabilità note, e con una configurazione sicura per impostazione predefinita; garantiscono che le vulnerabilità possano essere affrontate mediante aggiornamenti di sicurezza e la protezione dall'accesso non autorizzato mediante meccanismi di controllo; proteggono la riservatezza dei dati personali o di altro tipo; ecc.

[56] Si veda nel contesto della protezione dei dati personali *ex multis* N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, vol. 10, n. 1.

[57] I fabbricanti identificano e documentano le vulnerabilità e i componenti contenuti nel prodotto; affrontano e correggono tempestivamente le vulnerabilità; effettuano prove e riesami efficaci e periodici della sicurezza; condividono e divulgano pubblicamente informazioni sulle vulnerabilità risolte; ecc.

[58] Cons. 54, CRA.

[59] COMMISSIONE EUROPEA, *Commission implementing legislation of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*, C(2025) 618 final.

essenziale del CRA, evidenziando le possibili lacune da colmare [60]; nella seconda, la certificazione nel contesto del sistema europeo di certificazione della cybersicurezza basato sui criteri comuni è stata analizzata per capire fino a che punto possa essere usata per ottenere la conformità ai requisiti CRA [61].

I fabbricanti, quindi, dimostrano che i prodotti sono conformi ai requisiti essenziali attraverso la c.d. procedura di valutazione della conformità [62]. Al termine della procedura di valutazione della conformità, i fabbricanti redigono una 'dichiarazione di conformità UE che fornisca le informazioni richieste dall'Allegato V e attesti la conformità dei prodotti con elementi digitali ai requisiti essenziali di cybersicurezza *ex* Allegato I e da altri atti pertinenti della normativa di armonizzazione dell'Unione applicabili [63]. Infine, appongono la marcatura CE sul prodotto con elementi digitali in modo visibile, leggibile e indelebile [64].

A seconda del livello di rischio di cybersicurezza del prodotto con elementi digitali, il CRA impone ai fabbricanti di seguire determinate procedure di valutazione della conformità. Se, infatti, i fabbricanti hanno la piena possibilità di scegliere tra la procedura di auto-valutazione (basata sul modulo A di cui alla Decisione n. 768/2008/CE) o una svolta da terze parti (esame UE del tipo basata sul modulo B; controllo interno della produzione basata sul modulo C; garanzia della qualità totale basata sul modulo H; oppure un sistema europeo di certificazione della cybersicurezza con un livello di affidabilità almeno 'sostanziale') per i prodotti con elementi digitali "standard" [65] (vale a dire, né importanti né critici), che secondo la Commissione rappresenteranno circa il 90% dei prodotti in *scope* al regolamento [66], per i prodotti importanti e critici il CRA limita la discrezionalità dei fabbricanti.

Per quanto riguarda i prodotti importanti di classe I, il fabbricante può scegliere di applicare le norme armonizzate, le specifiche comuni o sistemi europei di certificazione della cybersicurezza con livello di affidabilità almeno "sostanziale". Se, tuttavia, questi strumenti non sono applicati (anche perché

---

[60] ENISA, *Cyber Resilience Act Requirements Standards Mapping*, 2024.

[61] ENISA, *Cyber Resilience Act implementation via EUCC and its applicable technical elements*, 2025.

[62] Decisione n. 768/2008/CE.

[63] Art. 13, par. 12; art. 28, CRA.

[64] Art. 30, CRA.

[65] Art. 32, par. 1, CRA.

[66] COMMISSIONE EUROPEA, *Directorate-General for Communications Networks, Content and Technology, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products*, 2022, in https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products.

indisponibili), o vengono applicati solo in parte, allora il fabbricante è tenuto a scegliere una procedura da parte di terze parti, vale a dire modulo B seguito dal modulo C oppure modulo H [67].

In ragione del maggior rischio di cybersicurezza, per i prodotti importanti di classe II è esclusa l'autovalutazione del fabbricante. Infatti, il fabbricante può scegliere tra le due procedure di valutazione della conformità da parte di terzi viste sopra o, ancora, un sistema europeo di certificazione della cybersicurezza con livello di affidabilità almeno "sostanziale"[68].

Eccezionalmente, i fabbricanti di prodotti con elementi digitali "importanti", che si qualifichino come software libero e open source, possono scegliere tra le procedure disponibili ai fabbricanti dei prodotti "standard"[69].

Similmente, nel caso di prodotti con elementi digitali critici, il fabbricante deve applicare i rilevanti sistemi di certificazione della cybersicurezza se richiesto, per quella categoria di prodotto critico, da uno specifico atto delegato adottato dalla Commissione a norma dell'art. 8; in mancanza di siffatto atto di implementazione, il fabbricante può scegliere una delle procedure applicabili ai prodotti importanti di classe II [70].

Infine, il capo IV del regolamento definisce le regole relative agli organismi di valutazione della conformità. In linea con il Nuovo Quadro Legislativo, gli Stati membri designano un'autorità di notifica responsabile di istituire ed eseguire le procedure necessarie per la valutazione, la notifica degli organismi di valutazione della conformità e il monitoraggio degli stessi.

5. Il Cyber Resilience Act e la tutela dei diritti fondamentali

Nella fase di presentazione della proposta legislativa, la Commissione europea ha evidenziato come tale intervento normativo orizzontale avrebbe migliorato la tutela dei diritti e delle libertà fondamentali, come la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della proprietà o la dignità e l'integrità della persona [71]. In particolare, aumentando il livello di cybersicurezza e resilienza dei prodotti con elementi digitali,

[67] Art. 32, par. 2, CRA.

[68] Art. 32, par. 3, CRA.

[69] Art. 32, par. 5, CRA.

[70] Art. 32, par. 4, CRA.

[71] COMMISSIONE EUROPEA, *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 final, p. 9.

il numero e la gravità degli incidenti si sarebbero ridotti, con impatti positivi per la sicurezza dei dati personali trattati dai prodotti nell'ambito di applicazione del CRA.

Una visione strumentale della cybersicurezza alla protezione dei dati personali, peraltro, è stata da sempre sostenuta dal Garante europeo della protezione dei dati personali [72] e dal Comitato europeo per la protezione dei dati personali [73], nonché dalle corti europee [74] e nazionali [75], che hanno progressivamente contribuito al radicamento della cybersicurezza nel quadro costituzionale dell'Unione con riguardo alla protezione dei diritti fondamentali [76]. Ad esempio, la crittografia è riconosciuta come una delle principali misure tecniche di cybersicurezza non solo dal CRA [77], ma anche dal GDPR [78] e dalla direttiva NIS2 [79]. Con particolare riferimento alla crittografia end-to-end, la Corte EDU ha esplicitamente riconosciuto il ruolo cruciale giocato da questa tecnologia nella tutela del diritto alla riservatezza e alla libertà di espressione, ritenendo che obblighi statutari di fornire alle autorità i mezzi per decrittare le comunicazioni cifrate end-to-end non siano proporzionati agli obiettivi legittimi perseguiti [80].

---

[72] G. BUTTARELLI, *Encryption protects security and privacy*, keynote speech all'Assemblea Nazionale francese, 21 novembre 2016; W. WIEWIÓROWSKI, *The Future of Encryption in the EU*, 2020, keynote speech del webinar ISOC 2020, p. 3; W. WIEWIÓROWSKI, *Cybersecurity and Data Protection: a necessary and powerful duo*, 28 settembre 2023.

[73] EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 2021.

[74] Per quanto riguarda la giurisprudenza della CGUE si veda, ad esempio, la decisione in *Digital Rights Ireland c. Minister for Communications & Others* del 2014 (cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238), par. 40 e, più recentemente, *VB v Natsionalna agentsia za prihodite* del 2024 (causa C-340/21, ECLI:EU:C:2023:986), par. 55. Per quanto riguarda la Corte EDU si veda, ad esempio, la sentenza del caso *Podchasov c. Russia*, 13 febbraio 2024, n. 33696/19.

[75] Si veda la decisione della Corte Costituzionale Federale tedesca del 27 febbraio 2008, 1 BvR 370/07 (ECLI:DE:BVerfG:2008:rs20080227.1bvr037007), che riconosce un 'diritto fondamentale alla tutela della confidenzialità ed integrità dei sistemi informativi' come parte dei diritti della personalità tutelati dalla Costituzione tedesca (par. 166 ss.).

[76] L.A. BYGRAVE, *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes*, in *Computer Law & Security Review*, 2024, vol. 56, pp. 4-5.

[77] Allegato I, Parte I, punto 2), lett. e).

[78] Art. 32, par. 1, lett. a), GDPR. Cfr. L.A. BYGRAVE, *Article 32. Security of processing*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation: A Commentary (2nd edition)*, forthcoming Oxford University Press, p. 71.

[79] Art. 21, par. 2, lett. h).

[80] *Podchasov c. Russia*, cit., parr. 76-79.

Al di là della tutela dei diritti fondamentali offerta *indirettamente* dagli obblighi e dai requisiti essenziali del CRA, il testo finale del regolamento non prevede *direttamente* dei meccanismi volti ad assicurare che i prodotti con elementi digitali rispettino i diritti fondamentali, come nel caso dell'AI Act – dove l'approccio basato sui diritti informa l'intero impianto di questo atipico strumento di sicurezza dei prodotti, a partire dalla base giuridica aggiunta durante i negoziati del trilogo per regolamentare la protezione dei dati personali ai sensi dell'art. 16 TFUE [81].

Infatti, oltre a migliorare il funzionamento del mercato interno e promuovere l'adozione di un'intelligenza artificiale antropocentrica e affidabile, l'AI Act ha l'obiettivo di garantire un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta [82]. Inoltre, l'impatto negativo sui diritti fondamentali è uno dei criteri che la Commissione deve seguire nel modificare la tassonomia dei sistemi di IA ad alto rischio elencati nell'Allegato III [83]. Ancora, diversi requisiti essenziali per i sistemi di IA ad alto rischio tengono conto dei rischi per i diritti fondamentali [84] e, in aggiunta, per determinati utilizzatori, è previsto l'obbligo di condurre una valutazione d'impatto sui diritti fondamentali [85]. Infine, la Commissione può sottoporre specifici sistemi di IA ad alto rischio a una valutazione di conformità da parte di terzi, tenendo conto dell'efficacia dell'autovalutazione nel minimizzare i rischi per i diritti fondamentali [86].

Nel testo finale del CRA, invece, i pochi riferimenti espliciti ai diritti fondamentali sono rinvenibili nelle regole relative all'applicazione delle norme (*enforcement*) di cui al Capo V. L'autorità di vigilanza del mercato designata da ogni Stato membro ai fini dell'attuazione del CRA può effettuare una valutazione del prodotto con elementi digitali per quanto riguarda la sua conformità ai requisiti essenziali del CRA se ha motivi sufficienti per ritenere che tale prodotto presenti un rischio di cybersicurezza significativo, tenendo conto anche dei fattori di rischio non tecnici. Se, all'esito dell'indagine, il prodotto risulta non conforme, l'autorità chiede all'operatore economico di adottare le opportune misure correttive. Qualora l'operatore economico non dovesse collaborare,

---

[81] M. ALMADA-N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025, vol. 62, n. 1; cfr. T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe – Journal of AI Law and Regulation*, 2024, vol. 1, no. 1, p. 98.

[82] Art. 1, AI Act.

[83] Artt. 6, par. 3; 7, AI Act.

[84] Artt. 9, par. 2, lett. a); 10, par. 2, lett. f); 13, par. 3, lett. b), punto iii); 14, par. 2, AI Act.

[85] Art. 27, AI Act.

[86] Art. 43, par. 6, AI Act.

l'autorità adotta adeguate misure restrittive di natura provvisoria (es., divieto o limitazione della messa a disposizione, ritiro o richiamo): per considerarsi definitive, è necessario il decorso di 3 mesi senza obiezioni dalla Commissione e dagli altri Stati membri che hanno ricevuto la comunicazione da parte dell'autorità procedente della procedura [87].

Dopo aver effettuato l'indagine di cui sopra, l'autorità, pur rilevando la conformità del prodotto al regolamento, può tuttavia ravvisare un rischio di cybersicurezza significativo oppure, *inter alia*, un "rischio per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali"[88]. In tal caso, l'operatore economico pertinente è tenuto ad adottare le misure correttive del caso nel termine assegnato dall'autorità, che comunica le misure adottate alla Commissione e agli altri Stati membri.

È importante sottolineare il potere della Commissione di 'stimolare' la valutazione da parte delle autorità nazionali competenti se ha motivi per ritenere che un prodotto, sebbene conforme al CRA, presenti i rischi suesposti. Come nella procedura a livello dell'Unione nei confronti di prodotti non conformi di cui all'art. 56, la Commissione può effettuare la valutazione del rischio in luogo delle autorità nazionali, con il supporto dell'ENISA, a condizione che: i) vi siano circostanze che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno; ii) non siano state adottate misure efficaci da parte dell'autorità nazionale competente; iii) la Commissione abbia motivi sufficienti per ritenere che il prodotto continui a presentare rischi per tali valori fondamentali; e, iv) informi le autorità nazionali interessate [89]. La Commissione può quindi imporre una misura correttiva o restrittiva a livello dell'Unione [90].

Da un punto di vista procedurale, tuttavia, il CRA non chiarisce i criteri affinché le condizioni che permettono l'azione della Commissione possano considerarsi soddisfatte. Per quanto riguarda la prima condizione, ci si può chiedere infatti quali siano le circostanze eccezionali che giustificano l'intervento immediato della Commissione. Infatti, il considerando 112 risulta essere ben poco d'aiuto, dal momento che fa unicamente riferimento alla situazione in cui un fabbricante metta a disposizione, in diversi Stati membri, un prodotto non conforme che è utilizzato anche in settori essenziali dai soggetti NIS2 e che contenga vulnerabilità note sfruttate da soggetti malintenzionati. Nulla dice invero circa situazioni ben più problematiche relative a prodotti conformi che, al tempo stesso, presentano rischi di cybersicurezza significativi e ad altri rischi ai beni fondamentali di cui al primo paragrafo dell'art. 57 CRA.

---

[87] Art. 54, CRA.

[88] Art. 57, par. 1, CRA.

[89] Art. 57, par. 7, CRA.

[90] Art. 57, par. 8, CRA.

La seconda condizione pone altri problemi. Com'è misurata l'efficacia di una misura adottata da parte di un'autorità nazionale? Quanto tempo deve passare prima che la Commissione intervenga? Altri atti giuridici del diritto digitale UE prevedono scenari in cui, a determinate condizioni, vi è un trasferimento dei poteri di *enforcement* dalle autorità nazionali alla Commissione, si veda ad esempio il regolamento (UE) 2022/2065 (Digital Services Act). Tuttavia, l'art. 59 DSA stabilisce termini precisi per un tale trasferimento di poteri. Questa mancanza di termini lascia ancora più sorpresi se la procedura di cui all'art. 57 viene confrontata con la procedura di salvaguardia dell'Unione prevista dall'art. 55. In quel caso, la Commissione decide se le misure correttive o restrittive adottate dalle autorità nazionali siano giustificate o meno entro un termine specifico, ossia nove mesi dalla notifica da parte dell'autorità competente.

Sotto il profilo sostanziale, uno sguardo attento alla formulazione dell'art. 57 rivela come il rischio presentato dai prodotti non sia ai diritti fondamentali di per sé, come nel caso dell'AI Act [91], bensì al *rispetto degli obblighi previsti dal diritto dell'Unione o nazionale volti a tutelare i diritti fondamentali*. Se, nel primo caso, l'enfasi della valutazione risiede nel grado di violazione di uno o più diritti fondamentali, nel secondo la valutazione concerne la conformità ad una norma di secondo livello volta ad implementare i diritti fondamentali.

Ne consegue che l'esito della valutazione a cui è chiamata l'autorità procedente sembrerebbe essere binario: gli obblighi sono rispettati oppure no. Tuttavia, la linea di demarcazione tra situazioni che comportino la conformità e la non-conformità non è sempre ben definita [92]; pertanto, queste analisi *ex-ante* [93] spesso implicano valutazioni normative, a seconda dell'obbligo in questione e del contesto applicativo del prodotto sotto indagine [94]. Così, un assistente virtuale per *smart homes*, prodotto importante di classe I ai sensi dell'Allegato III CRA, che registri e analizzi ininterrottamente *by default* tutte le interazioni dell'ambiente (es., casa privata) in cui è posto, presenta *prima facie* un rischio per la conformità ai principi e obblighi del GDPR.

L'interazione tra CRA e GDPR aumenterebbe la tutela degli interessati dal momento che le autorità per la protezione dei dati non dispongono delle misure di *enforcement* delle autorità di vigilanza del mercato in caso di violazioni degli

---

[91] Art. 82, AI Act.

[92] G. MALGIERI-C. SANTOS, *Assessing the (severity of) impacts on fundamental rights*, in *Computer Law & Security Review*, 2025, vol. 56, p. 5. Cfr. R. GELLERT, *Understanding the Notion of Risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, vol. 34.

[93] Prima, cioè, che una violazione occorra.

[94] Si veda, *ex multis*, K. YEUNG-L.A. BYGRAVE, *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in *Regulation & Governance*, 2022, vol. 16, p. 146.

obblighi del GDPR, sebbene alcune misure restrittive, come la limitazione definitiva del trattamento *ex* art. 58(2)(f) GDPR, possano avere effetti simili a quelle previste dal CRA (es., divieto di messa a disposizione sul mercato). Nonostante ciò, le autorità di vigilanza del mercato non sembrano i soggetti pubblici più adatti a condurre valutazioni eminentemente normative basate su valori e diritti fondamentali, ambito in cui le autorità per la protezione dei dati personali hanno storicamente maggiore esperienza.

6. Conclusione

Il presente contributo si è confrontato con l'elevato livello di complessità tecnico-giuridica del regolamento europeo Cyber Resilience Act, provando a fornire una rielaborazione dei pilastri principali dello strumento attraverso le diverse scelte regolatorie effettuate dal legislatore europeo. Come detto nell'introduzione, una separazione netta e compartimentata tra i diversi approcci regolatori (orizzontale, basato sul rischio e di sicurezza dei prodotti) che vengono implementati da questo atto giuridico, ancorché utile ai fini esplicativi del saggio, rischia di esporsi a fraintendimenti. L'analisi ha infatti mostrato come in realtà questi approcci normativi trovino uno sviluppo organico e, soprattutto, compenetrato nel testo giuridico. Così, gli istituti tipici della legislazione in materia di sicurezza dei prodotti presenti nel CRA (es., requisiti essenziali, obblighi degli operatori economici, procedure di valutazione della conformità) risultano perfettamente integrati con l'approccio al rischio, che sempre di più informa la normativa europea in materia digitale. Peraltro, se, da una parte, la combinazione degli approcci orizzontale, *risk-based* e di sicurezza dei prodotti non risulta essere una novità significativa nel contesto del diritto europeo, l'ibridizzazione di questi con un approccio più marcatamente *rights-based* presenta, invero, dei rilievi di novità e, in subordine, aspetti *prima facie* problematici.

Il CRA tutela i diritti fondamentali da una duplice prospettiva, 'strumentale' e 'diretta'. Sotto il primo aspetto, una maggior resilienza dei prodotti con elementi digitali agli attacchi informatici e agli incidenti aumenta la protezione di alcuni diritti fondamentali quali la protezione dei dati personali, la riservatezza e la libertà di espressione. In secondo luogo, come visto nella sezione 5, il CRA dispiega specifici meccanismi di *enforcement* consentendo alle autorità procedenti – siano le autorità nazionali di vigilanza del mercato o, in determinate circostanze, la Commissione europea – di utilizzare importanti poteri correttivi e restrittivi nei confronti di prodotti che, seppur anche conformi al regolamento, comportano dei rischi alla conformità alla legislazione UE o nazionale che protegge i diritti fondamentali, come ad esempio il GDPR.