C/2026/6013

17.11.2026

COMUNICAZIONE DELLA COMMISSIONE

Orientamenti della Commissione sull'applicazione del regolamento (UE) 2024/2847 (regolamento sulla ciberresilienza)

(C/2026/6013)

Indice

Pagina

1. INTRODUZIONE 3
   - 1.1. Il regolamento sulla ciberresilienza 3
   - 1.2. Scopo degli orientamenti 3
2. AMBITO DI APPLICAZIONE 4
   - 2.1. Immissione sul mercato 4
   - 2.2. Software in quanto prodotto con elementi digitali 5
   - 2.3. Codice informatico 6
   - 2.4. Combinazione di hardware e software che costituiscono un prodotto con elementi digitali 7
   - 2.5. Connessione dati 8
   - 2.6. Sistemi complessi 8
   - 2.7. Prodotti con elementi digitali progettati prima dell'entrata in applicazione del regolamento sulla ciberresilienza 9
3. SOFTWARE LIBERO E OPEN SOURCE 11
   - 3.1. Determinare su chi ricada la responsabilità di un software libero e open source 12
   - 3.2. Determinare se un software libero e open source è immesso sul mercato dell'UE 13
     - 3.2.1. Applicazione di un prezzo 13
     - 3.2.2. Monetizzazione di altri servizi o richiesta di trattamento dei dati personali 13
     - 3.2.3. Servizi di assistenza 14
     - 3.2.4. Donazioni 15
     - 3.2.5. Finanziamento dei software liberi e open source 15
     - 3.2.6. Enti senza scopo di lucro costituiti per conseguire obiettivi senza scopo di lucro 16
     - 3.2.7. Integrazione da parte di altri fabbricanti 16
   - 3.3. I gestori di software open source 16
     - 3.3.1. Sostegno duraturo e garanzia della sostenibilità economica del software libero e open source 17
   - 3.4. Contributori e usi a valle 18
   - 3.5. Scenari esemplificativi 19
4. MODIFICHE SOSTANZIALI E PEZZI DI RICAMBIO 21
   - 4.1. Riparazioni fisiche 22
   - 4.2. Pezzi di ricambio 23
   - 4.3. Aggiornamenti del software come modifiche sostanziali 24

4.4. Conseguenze di una modifica sostanziale 27
4.4.1. Modifiche sostanziali apportate da un soggetto diverso dal fabbricante originario 28
4.4.2. Modifiche sostanziali apportate dal fabbricante originario 29
5. PERIODO DI ASSISTENZA 29
5.1. Modifiche sostanziali e il periodo di assistenza 31
6. PRODOTTI CON ELEMENTI DIGITALI IMPORTANTI E CRITICI 32
6.1. Funzionalità principale 33
6.2. Valutazione della conformità per i prodotti con elementi digitali importanti e critici 36
6.3. Implicazioni per la presunzione di conformità 38
7. VALUTAZIONE DEI RISCHI DI CIBERSICUREZZA E INTEGRAZIONE DI PRODOTTI CON ELEMENTI DIGITALI E COMPONENTI 41
7.1. La valutazione e il trattamento dei rischi di cibersicurezza 41
7.2. Progettazione, sviluppo e produzione di prodotti con elementi digitali in modo da garantire un livello adeguato di cibersicurezza in base ai rischi 42
7.3. Valutazione dei rischi e dovuta diligenza in relazione alle dipendenze esterne e ai componenti integrati . 42
7.4. Riutilizzo delle valutazioni dei rischi e della documentazione di conformità per famiglie di prodotti con elementi digitali 44
8. ELABORAZIONE DATI DA REMOTO 44
8.1. Che cosa costituisce una soluzione di elaborazione dati da remoto per un prodotto con elementi digitali? 45
8.1.1. La nozione di «a distanza» 46
8.1.2. L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni? 46
8.1.3. Il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità? 47
8.2. Implicazioni pratiche e tecniche delle soluzioni di elaborazione dati da remoto e del ricorso a soluzioni di terzi 49
8.3. Casi d'uso per le soluzioni di elaborazione dati da remoto 50
8.3.1. Applicazione bancaria mobile 51
8.3.2. Termostato intelligente 52
8.3.3. Lettori elettronici 53
8.3.4. Robot industriali 53
8.3.5. Rete cellulare 53
9. ELEMENTI AGGIUNTIVI 54
9.1. Obblighi di segnalazione 54
9.2. Gestione delle vulnerabilità 56
9.2.1. Segnalazione a monte e condivisione delle correzioni di sicurezza 56
9.2.2. Vulnerabilità sfruttabili note 57
9.2.3. Prove e riesami efficaci e periodici 58
9.3. Interazione con altre normative 59
9.3.1. Regolamento (UE) 2019/2144 e regolamento (UE) n. 168/2013 59
9.3.2. Validità dei certificati di esame UE del tipo (articolo 69, paragrafo 1) 59

1. **INTRODUZIONE**

1.1. **Il regolamento sulla ciberresilienza**

1. Il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) ([1]) è entrato in vigore il 10 dicembre 2024. Il regolamento mira a rafforzare l'approccio dell'UE alla cibersicurezza, ad occuparsi della ciberresilienza a livello dell'UE e a migliorare il funzionamento del mercato interno, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersicurezza per l'immissione sul mercato dell'Unione di prodotti con elementi digitali, nonché durante il ciclo di vita di un prodotto con elementi digitali.

2. Il regolamento sulla ciberresilienza si basa sul nuovo quadro legislativo dell'UE, costituito dal regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 e dalla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione n. 93/465/CEE ([2]).

3. La vigilanza del mercato e l'applicazione delle norme sono effettuate dalle autorità nazionali di vigilanza del mercato. I prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza sono disciplinati dal regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011. La Commissione e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sostengono gli operatori economici e gli Stati membri nell'applicazione del regolamento sulla ciberresilienza.

1.2. **Scopo degli orientamenti**

4. L'articolo 26, paragrafo 1, del regolamento sulla ciberresilienza impone alla Commissione di pubblicare orientamenti per assistere gli operatori economici nell'applicazione di tale regolamento, con particolare attenzione all'agevolazione della conformità da parte delle microimprese e delle piccole e medie imprese. L'articolo 26, paragrafo 2, stabilisce gli aspetti minimi che dovrebbero essere affrontati negli orientamenti, tra cui: i) l'ambito di applicazione del regolamento sulla ciberresilienza (in particolare le soluzioni di elaborazione dati da remoto e i software liberi e open-source); ii) la nozione di «periodi di assistenza»; iii) l'interazione tra il regolamento sulla ciberresilienza e altre normative dell'UE; e iv) il concetto di «modifica sostanziale».

5. Il 3 dicembre 2025 la Commissione ha pubblicato una serie di domande frequenti (FAQ) volte ad aiutare gli operatori economici a prepararsi all'attuazione del regolamento sulla ciberresilienza ([3]).

6. I presenti orientamenti sono volti ad aiutare gli operatori economici a conformarsi al regolamento sulla ciberresilienza e a sostenere le attività delle autorità di vigilanza del mercato, delle autorità di notifica e degli organismi notificati, al fine di garantire l'applicazione armonizzata del regolamento sulla ciberresilienza in tutta l'Unione. Essi non intendono coprire l'intero ambito di applicazione del regolamento sulla ciberresilienza, ma piuttosto fornire chiarimenti sulla logica alla base di alcune disposizioni fondamentali e sulle loro possibili modalità di attuazione nella pratica. I presenti orientamenti riguardano il regolamento sulla ciberresilienza e non sono applicabili ad altre normative dell'UE.

([1]) GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Il programma di lavoro della Commissione per il 2026 prevede la presentazione di un «atto legislativo europeo sui prodotti», che preveda l'aggiornamento del nuovo quadro legislativo e delle norme sulla vigilanza del mercato e sulla normazione: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52025DC0870.

([3]) Le domande frequenti possono essere scaricate dal sito web della Commissione relativo all'attuazione del regolamento sulla ciberresilienza, dalla pagina web dedicata alle domande frequenti.

7. Nell'ambito dell'elaborazione dei presenti orientamenti è stata effettuata un'ampia consultazione dei portatori di interessi, tra cui il gruppo di esperti sulla cibersicurezza dei prodotti con elementi digitali ([4]), anche attraverso una consultazione pubblica tenutasi tra il 3 marzo e il 13 aprile 2026 ([5]).

8. I presenti orientamenti non sono vincolanti per gli operatori economici o altri attori soggetti al regolamento sulla ciberresilienza. Solo la Corte di giustizia dell'Unione europea è competente a fornire un'interpretazione autorevole del regolamento sulla ciberresilienza. I presenti orientamenti tuttavia illustrano l'interpretazione della Commissione del regolamento sulla ciberresilienza, al fine di agevolare la conformità e contribuire all'efficace attuazione del regolamento. Contengono inoltre una serie di esempi per illustrare l'applicazione di disposizioni specifiche. Tali esempi non sono tuttavia intesi a sostituire una valutazione caso per caso, che sarà sempre necessaria per tenere conto delle specificità di ogni singola fattispecie.

9. Conformemente all'articolo 26 del regolamento sulla ciberresilienza, la Commissione può prendere in considerazione la possibilità di emanare ulteriori orientamenti, compresi orientamenti destinati ai fabbricanti soggetti al regolamento sulla ciberresilienza e ad altre normative di armonizzazione dell'Unione o ad altri atti giuridici dell'Unione correlati. Tali orientamenti possono, ad esempio, affrontare questioni relative all'interazione tra il regolamento sulla ciberresilienza e il regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'IA) e il regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (regolamento DORA).

2. **AMBITO DI APPLICAZIONE**

2.1. **Immissione sul mercato**

10. Il regolamento sulla ciberresilienza si applica ai prodotti con elementi digitali messi a disposizione sul mercato dell'UE. Il concetto di messa a disposizione sul mercato è definito all'articolo 3, punto 22), del regolamento sulla ciberresilienza come «la fornitura, a titolo oneroso o gratuito, di un prodotto con elementi digitali perché sia distribuito o usato sul mercato dell'Unione nel corso di un'attività commerciale». Conformemente all'articolo 3, punto 21), un prodotto con elementi digitali è immesso sul mercato dell'UE quando è messo a disposizione per la prima volta.

11. L'ultima edizione della «Guida blu all'attuazione della normativa UE sui prodotti», pubblicata nel 2022 (di seguito «guida blu») ([6]), fornisce orientamenti volti a facilitare la comprensione della normativa UE sui prodotti e a garantirne l'applicazione uniforme nei vari quadri giuridici settoriali allineati al nuovo quadro legislativo, come ad esempio il regolamento sulla ciberresilienza. La guida blu indica che i concetti di «immissione sul mercato» e di «messa a disposizione» devono essere intesi come riferiti a «ogni singolo prodotto e non a un tipo di prodotto, a prescindere dal fatto che sia stato fabbricato in esemplare unico o in serie» (sezione 2.3).

12. Per i prodotti con elementi digitali più «tradizionali» contemplati dal nuovo quadro legislativo, come l'hardware sotto forma di macchine o apparecchiature radio con elementi digitali, il concetto di «immissione sul mercato» è ben consolidato e la guida blu fornisce ulteriori orientamenti per chiarire quando tali prodotti sono considerati immessi sul mercato. Gli «esempi in sintesi» contenuti nella sezione 2.12 della guida blu forniscono ulteriori esempi del concetto di «immissione sul mercato».

13. Tuttavia, data la natura dei prodotti intangibili con elementi digitali, come i software indipendenti (*standalone*), sono necessari ulteriori orientamenti in merito al momento in cui tali prodotti con elementi digitali si considerano immessi sul mercato. Una volta completata la fase di produzione di un software e una volta che il prodotto con elementi digitali è stato offerto ai potenziali utilizzatori sul mercato dell'UE, si può ritenere che il suo fabbricante abbia prodotto più copie dello stesso prodotto software con elementi digitali e le abbia fornite per la distribuzione o l'uso. Infatti, a differenza dei prodotti tangibili con elementi digitali, il software indipendente non è soggetto alla

([4]) Gruppo di esperti sulla cibersicurezza dei prodotti con elementi digitali nel registro dei gruppi di esperti della Commissione e di altri organismi analoghi.
([5]) Consultazione pubblica sul progetto di orientamenti della Commissione sul regolamento sulla ciberresilienza.
([6]) Comunicazione della Commissione «La guida blu all'attuazione della normativa UE sui prodotti 2022» (2022/C 247/01) (GU C 247 del 29.6.2022, pag. 1).

produzione fisica né a limiti di scorte: ogni atto di messa a disposizione del software per il download o la distribuzione comporta la creazione di una nuova copia identica per l'utilizzatore. A condizione che tale versione del software non sia modificata in modo tale da incidere sulla sua conformità al regolamento sulla ciberresilienza, l'immissione sul mercato dell'UE si considera avvenuta al momento della prima offerta per la distribuzione o l'uso. La possibilità di effettuare successivamente il download o la distribuzione di tale versione del prodotto software con elementi digitali deve pertanto essere considerata un caso in cui tale prodotto software con elementi digitali è messo a disposizione ([7]).

14. Pertanto un prodotto software indipendente con elementi digitali dovrebbe essere considerato immesso sul mercato quando la sua fase di produzione è completata e tale software è fornito per la prima volta perché sia distribuito o usato sul mercato dell'Unione nel corso di un'attività commerciale. Si dovrebbe ritenere che il fabbricante abbia immesso contemporaneamente sul mercato più copie dello stesso prodotto software con elementi digitali. Pertanto, pur rimanendo singoli prodotti con elementi digitali, le diverse copie dello stesso software sono considerate immesse sul mercato contemporaneamente, indipendentemente dal momento in cui il possesso o l'uso di ogni singola copia è trasferito a un'altra persona fisica o giuridica. Allo stesso tempo, se il fabbricante mette a disposizione software in diverse varianti che si differenziano per i componenti inclusi, le configurazioni o le funzionalità abilitate (ad esempio versioni per diversi sistemi operativi o pacchetti con serie di caratteristiche diverse), tali varianti non possono essere considerate copie multiple dello stesso prodotto software con elementi digitali. Ai fini dell'immissione sul mercato, dovrebbero pertanto essere trattate come prodotti con elementi digitali distinti.

Esempio 1: il 1º gennaio 2028 la società A fornisce per la prima volta per la distribuzione, tramite il proprio sito web, la versione 1.0.0 del suo software X. Lo stesso giorno il cliente 1 acquista una copia della versione 1.0.0 del software X. Il 15 gennaio 2028 il cliente 2 acquista una copia della versione 1.0.0 del software X. Entrambe le copie della versione 1.0.0 del software X sono immesse sul mercato il 1º gennaio 2028.

15. Dato il carattere iterativo dello sviluppo di software, è opportuno chiarire ulteriormente che le successive iterazioni di un prodotto software con elementi digitali sono considerate nuove immissioni sul mercato quando costituiscono una «modifica sostanziale» di un prodotto software con elementi digitali già immesso sul mercato, come indicato al considerando 41 del regolamento sulla ciberresilienza. Le iterazioni che non costituiscono modifiche sostanziali non impongono al fabbricante di eseguire una nuova procedura di valutazione della conformità e pertanto non modificano la data di immissione sul mercato di tale software. Per maggiori indicazioni sul concetto di modifiche sostanziali, cfr. la sezione *4 Modifiche sostanziali*.

Esempio 2: il 1º gennaio 2028, la società A fornisce per la prima volta per la distribuzione, tramite il proprio sito web, la versione 1.0.0 del software X. Lo stesso giorno, il cliente 1 acquista una copia della versione 1.0.0 del software X. Il 15 gennaio 2028, la società A rilascia una versione 1.0.1 aggiornata del software X che non costituisce una modifica sostanziale. Il 30 gennaio 2028 il cliente 2 acquista una copia della versione 1.0.1 del software X. Entrambe le copie, quella della versione1.0.0 e quella della versione 1.0.1 del software X, si considerano immesse sul mercato il 1º gennaio 2028.

16. Gli orientamenti di cui ai punti 13, 14 e 15 si applicano esclusivamente nel caso in cui il prodotto con elementi digitali sia un software indipendente. Non valgono, ad esempio, quando il software è integrato con l'hardware, come illustrato nella sezione *2.4 Combinazione di hardware e software che costituiscono un* prodotto.

2.2. **Software in quanto prodotto con elementi digitali**

17. L'articolo 3, punto 1), del regolamento sulla ciberresilienza definisce un prodotto con elementi digitali come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente». Tali prodotti con elementi digitali rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza qualora la loro finalità prevista o il loro uso ragionevolmente prevedibile includa una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.

([7]) A norma dell'articolo 13, paragrafo 11, i fabbricanti possono tenere archivi pubblici di software per migliorare l'accesso degli utilizzatori alle versioni precedenti. In questi casi, gli utilizzatori devono essere informati in modo chiaro e facilmente accessibile dei rischi associati all'uso di software privi di assistenza.

18. Il regolamento sulla ciberresilienza può pertanto riguardare una serie di prodotti con elementi digitali, tra cui: i) software indipendenti, quali applicazioni e programmi informatici, distribuiti in formato digitale o fisico; ii) hardware con software incorporato (ad esempio dispositivi dell'internet delle cose, computer portatili, tablet); iii) hardware indipendente (ad esempio circuiti integrati, schede madri); e iv) qualsiasi combinazione di hardware e software forniti separatamente ma destinati a funzionare insieme.

19. Il software indipendente rientra pertanto nell'ambito di applicazione del regolamento sulla ciberresilienza quando è immesso sul mercato come prodotto con elementi digitali. È utile distinguere tra i prodotti software con elementi digitali soggetti al regolamento sulla ciberresilienza e la fornitura da remoto di servizi che non rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza.

20. Affinché un software rientri nell'ambito di applicazione del regolamento sulla ciberresilienza, un prodotto software con elementi digitali deve essere fornito a un utilizzatore, ottenuto da quest'ultimo e utilizzato su un sistema di informazione elettronico, o come parte di esso, presso l'utilizzatore stesso. Il software scaricato, installato o altrimenti fornito all'utilizzatore e che viene eseguito sul sistema di informazione elettronico di quest'ultimo soddisfa tali criteri, anche, ad esempio, quando assume la forma di un'estensione del browser o di un'applicazione sviluppata utilizzando tecnologie web ma fornita per l'esecuzione locale.

21. Per contro, un software che viene eseguito da remoto e al quale l'utilizzatore si limita ad accedere non costituisce, solo per questo motivo, un prodotto con elementi digitali. I considerando 11 e 12 del regolamento sulla ciberresilienza operano infatti tale distinzione, spiegando che l'elaborazione o l'archiviazione a distanza rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza solo nella misura in cui sono necessari affinché un prodotto con elementi digitali svolga le sue funzioni (ossia attraverso il concetto di elaborazione dati da remoto quale definito all'articolo 3, punto 2)), e non di per sé in quanto prodotto con elementi digitali. Questo è solitamente il caso delle applicazioni web, comprese le web-app progressive, alle quali si accede esclusivamente tramite un browser web. Lo stesso vale per i siti web: sebbene dal punto di vista tecnico i siti web possano, in misura limitata, funzionare ed essere eseguiti sul dispositivo dell'utilizzatore, dal considerando 12 del regolamento sulla ciberresilienza si evince che i siti web non devono essere considerati in sé prodotti con elementi digitali, e rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza solo se supportano la funzionalità di un prodotto con elementi digitali, ossia nella misura in cui rientrano nella definizione di elaborazione dati da remoto (come ulteriormente spiegato nella sezione *8* e in particolare al punto *8.1.2 L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni?*).

Esempio 3: un'applicazione mobile che un utilizzatore scarica da un app store e installa sul proprio smartphone è fornita all'utilizzatore ed eseguita sul suo dispositivo ed è pertanto un prodotto con elementi digitali. Se è immessa sul mercato nel corso di un'attività commerciale, può rientrare nell'ambito di applicazione del regolamento sulla ciberresilienza.

Esempio 4: un'applicazione desktop realizzata utilizzando tecnologie web ma confezionata per l'installazione locale è fornita all'utilizzatore ed eseguita sul suo dispositivo ed è pertanto un prodotto con elementi digitali. Se è immessa sul mercato nel corso di un'attività commerciale, può rientrare nell'ambito di applicazione del regolamento sulla ciberresilienza.

Esempio 5: un'applicazione web a cui l'utilizzatore accede esclusivamente attraverso un browser web non è un prodotto con elementi digitali. A meno che non supporti la funzionalità di un prodotto con elementi digitali, non rientra nell'ambito di applicazione del regolamento sulla ciberresilienza. Per contro, un'applicazione fornita all'utilizzatore come client installato localmente che viene eseguita sul dispositivo dell'utilizzatore è un prodotto con elementi digitali. Se è immessa sul mercato nel corso di un'attività commerciale, può rientrare nell'ambito di applicazione del regolamento sulla ciberresilienza.

Se tale client, per svolgere una o più delle sue funzioni, utilizza un'elaborazione dati a distanza che soddisfa la definizione di elaborazione dati da remoto, anche tale elaborazione dati a distanza fa parte del prodotto con elementi digitali.

Esempio 6: un sito web che si limita a presentare informazioni ai suoi visitatori e non supporta la funzionalità di un prodotto con elementi digitali non è di per sé un prodotto con elementi digitali. Non rientra pertanto nell'ambito di applicazione del regolamento sulla ciberresilienza.

2.3. **Codice informatico**

22. È altresì utile chiarire se il codice sorgente possa costituire un prodotto software con elementi digitali. Il regolamento sulla ciberresilienza definisce un software come «la parte di un sistema di informazione elettronico costituita da un codice informatico» (articolo 3, punto 4). Il codice informatico può assumere la forma di i) codice macchina, ossia l'insieme di istruzioni eseguite direttamente dal processore di un computer, scritte in formato binario; o ii) codice sorgente, ossia l'insieme di istruzioni e dichiarazioni scritte in un linguaggio di programmazione, che devono essere compilate o interpretate per poter essere eseguite da un computer. La definizione di software contenuta nel regolamento sulla ciberresilienza comprende entrambe le forme.

23. Un'altra questione è se una determinata fornitura di codice informatico equivalga all'immissione di un prodotto con elementi digitali sul mercato dell'UE, il che richiede che la fornitura avvenga nel corso di un'attività commerciale. Nel caso del codice sorgente, spesso ciò può non verificarsi. Ad esempio, la condivisione da parte di una persona fisica o giuridica di un codice informatico libero e open source in archivi accessibili al pubblico non è generalmente considerata un'immissione di tale codice sul mercato dell'UE ai fini del regolamento sulla ciberresilienza (come illustrato più dettagliatamente nella sezione *3 Software libero e open* source). Anche il codice incompleto condiviso durante la fase di progettazione e sviluppo di un prodotto con elementi digitali (ad esempio a fini di prova o riesame) non è considerato immesso sul mercato ai fini del regolamento sulla ciberresilienza, in quanto la sua fase di fabbricazione non è completata. Analogamente, non sono considerati immessi sul mercato ai fini del regolamento sulla ciberresilienza neppure i codici campione o demo forniti nell'ambito di tutorial o di materiali formativi ([8]).

24. Per contro, quando un fabbricante fornisce ai propri clienti un codice informatico come prodotto con elementi digitali, tale codice è considerato immesso sul mercato, indipendentemente dal fatto che si tratti di un codice macchina o di un codice sorgente ([9]).

Esempio 7: la società A concede in licenza il codice sorgente alla società B per una piattaforma interna personalizzabile, fornendolo in un file di testo. Anche se il codice sorgente in questione richiede un adattamento e una compilazione ulteriori da parte della società B prima di essere utilizzato, la società A immette tale codice sorgente sul mercato ed è pertanto soggetta al regolamento sulla ciberresilienza. La società A non è responsabile della conformità al regolamento sulla ciberresilienza dei successivi adattamenti e della successiva compilazione di tale codice da parte della società B.

2.4. **Combinazione di hardware e software che costituiscono un prodotto con elementi digitali**

25. Per stabilire se un software faccia parte di un prodotto con elementi digitali non si dovrebbe considerare il modo o il momento in cui tale software è fornito all'utilizzatore, bensì se, alla luce della finalità prevista e dell'uso ragionevolmente prevedibile del prodotto, il software sia necessario affinché il prodotto con elementi digitali svolga le funzioni previste. Se un prodotto hardware con elementi digitali è progettato per funzionare in combinazione con un software specifico fornito dallo stesso fabbricante affinché possa svolgere le proprie funzioni, l'hardware e tale software insieme costituiscono il prodotto con elementi digitali. Il software necessario per far funzionare, configurare, controllare o utilizzare un prodotto con elementi digitali conformemente alla sua finalità prevista fa pertanto parte del prodotto con elementi digitali, anche se ottenuto attraverso un canale separato (ad esempio un app store, un link per il download o un altro canale digitale dopo che il prodotto hardware con elementi digitali è stato immesso sul mercato). La sua immissione sul mercato avviene quindi nello stesso momento in cui le unità dei prodotti hardware con elementi digitali sono immesse sul mercato.

Esempio 8: una stampante di rete è immessa sul mercato come prodotto hardware con elementi digitali, mentre i driver software necessari per inviare i lavori di stampa, configurare il dispositivo e gestirne il funzionamento sono messi a disposizione per il download dal sito web del fabbricante. Sebbene siano forniti attraverso canali diversi, la stampante e i driver costituiscono insieme un unico prodotto con elementi digitali, in quanto la stampante non può conseguire la finalità prevista senza i driver.

Esempio 9: un dispositivo di fitness indossabile è immesso sul mercato per misurare la frequenza cardiaca e l'attività fisica dell'utilizzatore, mentre è necessaria un'applicazione per smartphone fornita dal fabbricante per poter visualizzare i dati rilevati, consultare la cronologia e configurare il dispositivo. Sebbene l'applicazione sia scaricata separatamente attraverso un app store, il dispositivo indossabile e l'applicazione costituiscono insieme un unico prodotto con elementi digitali, in quanto sono progettati e destinati a funzionare insieme per garantire la funzionalità del prodotto con elementi digitali.

([8]) È inoltre opportuno ricordare che l'articolo 4, paragrafo 3, consente ai fabbricanti di mettere a disposizione sul mercato software non finiti non conformi al regolamento, come versioni alfa, versioni beta o *release candidate*, a condizione che il software non finito sia messo a disposizione solo per il tempo necessario a sottoporlo a prova e a raccogliere riscontri.

([9]) D'altro canto, occorre rilevare che, ai fini della normativa sulla responsabilità per danno da prodotti difettosi, il codice informatico in sé non costituisce un prodotto e pertanto i fabbricanti che immettono tale codice sul mercato non possono essere ritenuti responsabili a norma della direttiva (UE) 2024/2853 (direttiva sulla responsabilità per danno da prodotti difettosi). Il considerando 13 di tale direttiva afferma che «[l]e informazioni, invece, non devono invece essere considerate un prodotto e le norme sulla responsabilità per danno da prodotti difettosi non dovrebbero pertanto applicarsi al contenuto dei file digitali, quali file multimediali, e-book o il mero codice sorgente dei software». Ciò non esclude che i fabbricanti possano essere responsabili ai sensi del diritto nazionale in materia di responsabilità civile.

2.5. **Connessione dati**

26. L'articolo 2, paragrafo 1, stabilisce che il regolamento sulla ciberresilienza «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». L'ambito di applicazione del regolamento sulla ciberresilienza è pertanto ancorato non alla mera presenza di dispositivi elettronici, ma alla capacità di un prodotto con elementi digitali di scambiare informazioni digitali.

27. Mentre i termini «connessione logica» e «connessione fisica» sono definiti all'articolo 3, il regolamento sulla ciberresilienza non fornisce una definizione di «connessione dati» o di «dati digitali». È pertanto utile fornire un'interpretazione di cosa sia una connessione dati, al fine di chiarire il perimetro dell'ambito di applicazione del regolamento sulla ciberresilienza. Tale perimetro è particolarmente importante per distinguere i prodotti con elementi digitali che si limitano a utilizzare segnali elettrici da quelli che partecipano alla comunicazione digitale e sono pertanto esposti a rischi di cibersicurezza.

28. Al livello più elementare, una connessione dati consiste nella trasmissione di informazioni in formato binario, ossia come sequenza di 0 e 1. Il semplice fatto di attivare e disattivare un output (ossia 0/1) non costituisce di per sé una connessione dati se tali stati non sono destinati a rappresentare dati o non sono letti da un input digitale. Affinché esista una connessione dati, gli stati binari devono essere deliberatamente codificati come informazioni da una fonte e devono poter essere decodificati come informazioni a destinazione. In altre parole, deve esserci un mittente che generi deliberatamente simboli digitali secondo uno schema definito e un destinatario in grado di interpretare tali simboli come dati. Se i segnali elettrici o elettronici sono utilizzati esclusivamente per attivare o alimentare una funzione, senza trasmettere informazioni codificate digitalmente, non esiste alcuna connessione dati ai fini del regolamento sulla ciberresilienza, e pertanto il prodotto con elementi digitali non rientra nell'ambito di applicazione di cui all'articolo 2, paragrafo 1.

2.6. **Sistemi complessi**

29. I prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza possono essere costituiti non soltanto da singoli dispositivi o componenti software, ma anche da sistemi complessi, compresi i sistemi composti da molteplici elementi hardware e software che funzionano insieme per svolgere una determinata funzione. Qualora sia immesso sul mercato come un unico prodotto con elementi digitali, tale sistema costituisce un prodotto con elementi digitali ai sensi del regolamento sulla ciberresilienza.

30. Tali sistemi complessi sono spesso caratterizzati da lunghi cicli di progettazione e sviluppo, con contratti che possono essere stati firmati prima dell'applicazione del regolamento sulla ciberresilienza, da una lunga durata operativa e da un elevato grado di complessità tecnica e organizzativa. I sistemi di questo tipo, destinati a essere immessi sul mercato dopo l'entrata in applicazione del regolamento sulla ciberresilienza, possono basarsi su componenti immessi sul mercato prima dell'entrata in applicazione di tale regolamento, su architetture consolidate o su norme di interoperabilità di ampio utilizzo, comprese le norme di cui ad altre normative dell'UE o a quadri normativi settoriali. Di conseguenza potrebbe risultare difficile o sproporzionato modificare alcune caratteristiche tecniche di tali sistemi senza comprometterne la finalità prevista, la sicurezza, l'affidabilità o l'interoperabilità con l'infrastruttura esistente.

31. Tali caratteristiche non escludono di per sé i sistemi complessi dall'ambito di applicazione del regolamento sulla ciberresilienza. Sono anzi un esempio dell'applicazione dell'approccio basato sul rischio del regolamento sulla ciberresilienza, che consente di dimostrare la conformità in modi diversi a seconda delle caratteristiche e dei vincoli del prodotto con elementi digitali, conformemente all'articolo 13, paragrafo 3, del regolamento sulla ciberresilienza. Tali caratteristiche fanno parte della finalità prevista e del contesto operativo del prodotto e sono pertanto pertinenti ai fini della valutazione della conformità ai requisiti essenziali di cibersicurezza («requisiti essenziali»). In particolare, il considerando 55 riconosce esplicitamente che alcuni requisiti essenziali potrebbero non essere pienamente compatibili con la natura di un prodotto con elementi digitali. Tale caso potrebbe ad esempio presentarsi quando la conformità comprometterebbe i requisiti obbligatori in materia di interoperabilità o il corretto funzionamento del sistema.

32. Di conseguenza i fabbricanti sono tenuti ad affrontare i rischi di cibersicurezza sulla base della valutazione dei rischi di cibersicurezza di cui all'articolo 13, paragrafo 2. Come spiegato anche al considerando 55, in alcuni casi requisiti essenziali specifici non sono applicabili o non possono essere soddisfatti mediante l'attuazione di misure di

sicurezza all'avanguardia a causa, ad esempio, del fatto che la finalità prevista del sistema richiede che il prodotto con elementi digitali interagisca con dipendenze esistenti o rispetti determinati requisiti di interoperabilità. In tali casi i fabbricanti dovrebbero individuare e documentare tali vincoli specifici, valutare i rischi associati e attuare adeguate misure alternative o compensative di attenuazione dei rischi, in modo da non compromettere la sicurezza del prodotto con elementi digitali. A tal fine, sia la documentazione tecnica di cui all'articolo 31 sia le informazioni e le istruzioni per l'utilizzatore di cui all'allegato II svolgono un ruolo fondamentale nel descrivere in modo trasparente i vincoli individuati, i rischi di cibersicurezza associati e le misure di attenuazione dei rischi attuate. Conformemente all'obbligo di tenere aggiornata la valutazione dei rischi durante il periodo di assistenza, i fabbricanti dovrebbero anche riesaminare periodicamente se tali vincoli continuino a sussistere. Laddove tali vincoli possano essere eliminati o ridotti nel tempo, i fabbricanti dovrebbero aggiornare di conseguenza il prodotto con elementi digitali, in modo che possa raggiungere un livello adeguato di cibersicurezza ([10]).

Esempio 10: un fabbricante immette sul mercato un prodotto con elementi digitali che comunica con sistemi esterni utilizzando un protocollo di rete. Nell'ambito dell'applicazione dei requisiti essenziali, il fabbricante stabilisce, sulla base della valutazione dei rischi di cibersicurezza, che per garantire la riservatezza e l'integrità dei dati scambiati dal prodotto con elementi digitali è necessario l'uso di un protocollo di comunicazione sicuro.

Tuttavia la finalità prevista del prodotto comprende l'interoperabilità con sistemi esistenti che supportano solo un protocollo più vecchio o meno sicuro. In questi casi il fabbricante può applicare tale protocollo qualora ciò sia necessario per conseguire l'interoperabilità, a condizione che i rischi di cibersicurezza associati siano individuati e attenuati con altri mezzi.

Qualora sia tecnicamente fattibile che il prodotto con elementi digitali supporti sia il protocollo sicuro sia il protocollo meno sicuro, il fabbricante è tenuto a implementare il protocollo sicuro e a renderne possibile l'uso per impostazione predefinita. Il protocollo meno sicuro sarebbe consentito solo laddove necessario ai fini dell'interoperabilità.

Esempio 11: il fabbricante di un sistema di automazione industriale acquista alcuni microcontrollori prima dell'entrata in applicazione del regolamento sulla ciberresilienza. Il fabbricante effettua la valutazione dei rischi di cibersicurezza per il proprio sistema di automazione industriale, che sarà immesso sul mercato dopo l'entrata in applicazione del regolamento sulla ciberresilienza. Sulla base di tale valutazione dei rischi di cibersicurezza, il fabbricante non individua alcun rischio specifico di cibersicurezza associato all'uso di uno di tali microcontrollori. Il fabbricante lo integra nel proprio sistema di automazione industriale e garantisce che il prodotto con elementi digitali nel suo complesso (il sistema di automazione industriale) soddisfi i requisiti essenziali.

2.7. **Prodotti con elementi digitali progettati prima dell'entrata in applicazione del regolamento sulla ciberresilienza**

33. In alcuni casi un fabbricante potrebbe immettere sul mercato, dopo l'entrata in applicazione del regolamento sulla ciberresilienza l'11 dicembre 2027, unità di un prodotto con elementi digitali fabbricate conformemente a un tipo o modello progettato e sviluppato prima della data di applicazione del regolamento sulla ciberresilienza. In questi casi ai fini della conformità a tale regolamento non è necessariamente richiesto che le unità del prodotto con elementi digitali in questione siano riprogettate. Il fabbricante è tenuto a effettuare una valutazione dei rischi di cibersicurezza conformemente all'articolo 13, paragrafo 2, del regolamento sulla ciberresilienza al fine di determinare, sulla base della finalità prevista e dell'uso ragionevolmente prevedibile del prodotto con elementi digitali, quali dei requisiti essenziali di cui all'allegato I, parte I, siano applicabili a tale prodotto con elementi digitali e le modalità di attuazione di tali requisiti.

34. Se l'esito di tale valutazione dei rischi dimostra che il prodotto con elementi digitali comprende già misure di sicurezza adeguate ed efficaci per affrontare i rischi pertinenti, il fabbricante può basarsi su tali misure esistenti per dimostrare la conformità al regolamento sulla ciberresilienza. Il regolamento sulla ciberresilienza non impone di per sé l'obbligo di introdurre nuove caratteristiche di sicurezza o di riprogettare il prodotto con elementi digitali qualora ciò non sia necessario per affrontare i rischi individuati.

([10]) Va osservato che le considerazioni di cui al presente punto possono essere applicabili, se del caso, a tutti i prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza, e non solo ai «sistemi complessi».

35. Il fabbricante rimane tuttavia soggetto agli obblighi stabiliti nel regolamento sulla ciberresilienza. Tra questi vi è l'obbligo di garantire, prima dell'immissione sul mercato del prodotto con elementi digitali, che sia stata eseguita la procedura di valutazione della conformità applicabile, che sia stata redatta la dichiarazione di conformità UE e che sia stata apposta la marcatura CE. La conformità a tali prescrizioni è indipendente dal fatto che la progettazione del prodotto con elementi digitali abbia richiesto modifiche a seguito della valutazione dei rischi. Per i prodotti con elementi digitali progettati prima della data di applicazione del regolamento sulla ciberresilienza, ma immessi sul mercato dopo tale data, quando il fabbricante non è in grado di dimostrare in che modo la valutazione dei rischi è stata presa in considerazione durante la fase di progettazione e sviluppo del prodotto con elementi digitali, l'obbligo di cui all'articolo 13, paragrafo 2, dovrebbe essere inteso come l'obbligo per i fabbricanti di effettuare una valutazione dei rischi di cibersicurezza e di dimostrare su tale base che il prodotto con elementi digitali comprende misure di sicurezza adeguate per ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti e ridurne al minimo l'impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori.

36. Di conseguenza i prodotti con elementi digitali progettati prima dell'entrata in applicazione del regolamento sulla ciberresilienza potrebbero essere immessi sul mercato a norma di tale regolamento senza essere stati riprogettati, a condizione che il fabbricante possa dimostrare, attraverso la valutazione dei rischi di cibersicurezza e la documentazione tecnica, che il prodotto con elementi digitali raggiunge un livello adeguato di cibersicurezza in considerazione della sua finalità prevista e del suo uso ragionevolmente prevedibile ed è conforme ai requisiti essenziali di cibersicurezza.

37. È inoltre utile chiarire l'applicazione degli obblighi di valutazione della conformità che incombono ai fabbricanti di prodotti con elementi digitali immessi sul mercato dopo l'entrata in applicazione del regolamento sulla ciberresilienza, ma fabbricati conformemente a un tipo o modello progettato e sviluppato prima di tale data. A norma dell'articolo 13, paragrafo 12, il fabbricante è tenuto a dimostrare, attraverso la pertinente procedura di valutazione della conformità, che il suo prodotto con elementi digitali è conforme ai requisiti essenziali applicabili, e a includere prove in tal senso nella documentazione tecnica del prodotto (allegato VII, punto 6).

38. Tuttavia l'applicazione di tali requisiti deve essere interpretata alla luce della valutazione dei rischi di cibersicurezza e del profilo di rischio di cibersicurezza del prodotto con elementi digitali. In particolare nel caso di prodotti con elementi digitali progettati prima della data di applicazione del regolamento sulla ciberresilienza (ma immessi sul mercato dopo tale data) e soggetti alle procedure di valutazione della conformità di cui all'articolo 32, paragrafo 1, se la valutazione dei rischi dimostra che il prodotto con elementi digitali comprende già misure di sicurezza adeguate ed efficaci per affrontare i rischi di tale prodotto, l'obbligo di fornire prove nell'ambito della procedura di valutazione della conformità non dovrebbe essere inteso come un obbligo per il fabbricante di fornire i risultati delle prove relative alle fasi iniziali di progettazione e sviluppo di tali prodotti con elementi digitali. Ciò non sarebbe necessario in quanto non contribuirebbe ad aumentare la sicurezza del prodotto con elementi digitali stesso. Laddove l'effettuazione di prove dovesse comunque risultare necessaria, i fabbricanti non sono tenuti a fornire la documentazione comprovante l'esecuzione di prove su tutte le varianti del prodotto, ma possono raggruppare tali prove per famiglie di prodotti con elementi digitali, come ulteriormente illustrato nella sezione *7.4 Riutilizzo delle valutazioni dei rischi e della documentazione di conformità per famiglie di prodotti con elementi digitali*.

39. Il fabbricante dovrebbe tuttavia fornire la documentazione comprovante la conformità ai processi di gestione delle vulnerabilità di cui all'allegato I, parte II, tenere aggiornata la propria valutazione dei rischi in conformità dell'articolo 13, paragrafo 3, nonché adempiere a tutti gli altri obblighi stabiliti nel regolamento sulla ciberresilienza, anche fornendo agli utilizzatori informazioni e istruzioni conformemente all'articolo 13, paragrafo 18.

Esempio 12: un fabbricante immette sul mercato un microcontrollore che è stato progettato e sviluppato prima della data di applicazione del regolamento sulla ciberresilienza. Il microcontrollore è destinato a essere integrato in una serie di prodotti elettronici con elementi digitali, compresi prodotti con elementi digitali con funzionalità di connettività.

Prima di immettere nuove unità del microcontrollore sul mercato dopo l'applicazione del regolamento sulla ciberresilienza, il fabbricante effettua una valutazione dei rischi di cibersicurezza in conformità dell'articolo 13, paragrafo 2. Sulla base della finalità prevista del microcontrollore e del suo uso ragionevolmente prevedibile, il fabbricante individua i rischi di cibersicurezza pertinenti, quali l'accesso non autorizzato, la manipolazione di software o dati e l'uso improprio delle interfacce disponibili.

L'esito della valutazione dei rischi mostra che il microcontrollore, così come originariamente progettato, comprende già misure di sicurezza adeguate ed efficaci per affrontare i rischi individuati. Il fabbricante conclude pertanto che il prodotto con elementi digitali soddisfa i pertinenti requisiti essenziali di cui all'allegato I, parte I, e che non è necessaria una riprogettazione o l'introduzione di funzionalità di sicurezza aggiuntive.

Qualora non sia possibile dimostrare in che modo una valutazione dei rischi di cibersicurezza sia stata presa in considerazione durante la fase iniziale di progettazione e sviluppo, il fabbricante documenta una valutazione dei rischi di cibersicurezza attuale e spiega in che modo la progettazione e le misure esistenti attenuano i rischi individuati. Il fabbricante non è tenuto a ricostruire la documentazione storica relativa alla progettazione o alle prove, in quanto ciò non contribuirebbe a migliorare la cibersicurezza del prodotto con elementi digitali. Se diverse varianti del microcontrollore si basano sulla stessa progettazione e condividono lo stesso profilo di rischio di cibersicurezza, il fabbricante può anche basarsi sulla documentazione rappresentativa riguardante la pertinente famiglia di prodotti.

Il fabbricante garantisce inoltre la conformità ai requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II, anche mantenendo processi per affrontare e correggere le vulnerabilità e mantenendo aggiornata la valutazione dei rischi di cibersicurezza conformemente all'articolo 13, paragrafo 3.

In tali circostanze, il microcontrollore progettato prima della data di applicazione del regolamento sulla ciberresilienza può essere immesso sul mercato senza essere riprogettato, a condizione che il fabbricante possa dimostrare, attraverso la valutazione dei rischi di cibersicurezza e la documentazione tecnica, che esso raggiunge un livello adeguato di cibersicurezza alla luce della sua finalità prevista e del suo uso ragionevolmente prevedibile e che soddisfa i requisiti essenziali applicabili.

3. **SOFTWARE LIBERO E OPEN SOURCE**

40. Come ricordato nella sezione *2.1 Immissione sul mercato*, il regolamento sulla ciberresilienza si applica ai prodotti con elementi digitali messi a disposizione sul mercato dell'UE nel corso di un'attività commerciale per la prima volta (ossia «immessi sul mercato»), nonché a qualsiasi caso successivo che costituisca la messa a disposizione sul mercato dello stesso prodotto con elementi digitali. La guida blu (sezione 2.2) chiarisce che per «attività commerciale» s'intende la fornitura di beni, a titolo oneroso o gratuito, in un contesto commerciale e può essere valutata solamente caso per caso, tenendo conto della regolarità delle forniture, delle caratteristiche del prodotto, delle intenzioni del fornitore, ecc.

41. La fornitura nel corso di un'attività commerciale è caratterizzata da una serie di circostanze, ampiamente illustrate nella guida blu e richiamate al considerando 15 del regolamento sulla ciberresilienza. Tali circostanze possono essere costituite dall'applicazione diretta di un prezzo, come pure «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, ad esempio dalla fornitura di una piattaforma software attraverso la quale il fabbricante monetizza altri servizi, dall'imposizione, come condizione per l'utilizzo, del trattamento di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software, o dall'accettazione di donazioni che superano i costi associati alla progettazione, allo sviluppo e alla fornitura di un prodotto con elementi digitali» (considerando 15) ([11]).

42. Il regolamento sulla ciberresilienza riconosce tuttavia le specificità delle diverse modalità di sviluppo e pubblicazione del «software libero e open source» e offre alcuni orientamenti utili per stabilire se un software libero e open source sia un prodotto con elementi digitali immesso sul mercato (ossia nel corso di un'attività commerciale) ai sensi del regolamento sulla ciberresilienza. Come spiegato al considerando 18, «[l]e mere circostanze in cui il prodotto con elementi digitali è stato sviluppato o il modo in cui lo sviluppo è stato finanziato non dovrebbero […] essere presi in considerazione al fine di determinare la natura commerciale o non commerciale di tale attività». Più specificamente, «per garantire che tra la fase di sviluppo e la fase di fornitura vi sia una chiara distinzione, la fornitura di prodotti con elementi digitali che si qualificano come software liberi e open source che non sono monetizzati dai loro fabbricanti non dovrebbe essere considerata un'attività commerciale».

([11]) Va inoltre ricordato che, sebbene spesso i prodotti con elementi digitali siano monetizzati (anche) attraverso il trattamento dei dati personali, la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, come indicato al considerando 24 della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (GU L 136 del 22.5.2019, pag. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. È pertanto utile i) chiarire che cosa sia un software libero e open source; ii) quando si ritiene che rientri sotto la responsabilità di una persona fisica o giuridica; e iii) fornire esempi per aiutare i portatori di interessi a comprendere quando la distribuzione di un software libero e open source costituisce un'immissione sul mercato. Se non è immesso sul mercato, il software libero e open source non rientra nell'ambito di applicazione del regolamento sulla ciberresilienza, a meno che il soggetto che lo pubblica non sia una persona giuridica che soddisfa la definizione di «gestore di software open source» (di seguito «gestore») di cui all'articolo 3, punto 14). In tal caso, esso è soggetto unicamente agli obblighi di cui all'articolo 24.

44. L'articolo 3, punto 48), definisce un software libero e open source, come «un software il cui codice sorgente è condiviso apertamente e che è messo a disposizione nell'ambito di una licenza gratuita e open source che prevede tutti i diritti per renderlo liberamente accessibile, utilizzabile, modificabile e ridistribuibile». Sebbene i presenti orientamenti non individuino specifiche licenze gratuite e open source compatibili con la definizione di cui all'articolo 3, punto 48), dalla formulazione di tale disposizione risulta che solo i software che soddisfano cumulativamente due condizioni si qualificano come software liberi e open source ai fini del regolamento sulla ciberresilienza: i) il software deve essere messo a disposizione nell'ambito di una licenza libera e open source che conceda l'intera serie dei diritti di cui all'articolo 3, punto 48); e ii) il suo codice sorgente deve essere condiviso apertamente.

45. Il requisito secondo cui la licenza deve prevedere che il software sia «liberamente accessibile, utilizzabile, modificabile e ridistribuibile» riflette la concezione tradizionale del software aperto e open source, vale a dire che gli utenti devono poter accedere al codice sorgente, utilizzarlo senza indebite restrizioni, modificarlo e ridistribuire la versione originale o le versioni modificate. L'accesso al codice sorgente è pertanto un presupposto necessario per l'esercizio degli altri diritti: senza l'accesso al codice sorgente, non è praticamente possibile modificare o riutilizzare in modo significativo il software.

46. Tuttavia l'articolo 3, punto 48), va oltre il riferimento alle sole condizioni di licenza, in quanto prevede espressamente che il codice sorgente «sia condiviso apertamente». La nozione di «condiviso apertamente» indica che il codice sorgente deve essere reso pubblicamente disponibile («a monte» o «a valle») e non semplicemente fornito in modo limitato o a determinate condizioni. Di conseguenza i software distribuiti con licenza gratuita e open source, ma il cui codice sorgente è condiviso (o può essere condiviso) solo con clienti paganti o con un gruppo limitato di utilizzatori, non devono essere considerati software liberi e open source ai sensi dell'articolo 3, punto 48). Ai fini del regolamento sulla ciberresilienza, soltanto i software il cui codice sorgente sia pubblicamente disponibile e che siano concessi in licenza nell'ambito di una licenza gratuita e open source che garantisce l'intera serie dei diritti di cui all'articolo 3, punto 48), dovrebbero pertanto essere considerati software liberi e open source.

3.1. **Determinare su chi ricada la responsabilità di un software libero e open source**

47. Il regolamento sulla ciberresilienza attribuisce responsabilità fondamentali agli operatori economici che forniscono prodotti con elementi digitali nel mercato dell'UE. Definisce il fabbricante come la persona fisica o giuridica che fornisce un prodotto con elementi digitali con il proprio nome o marchio, e che lo fa nel corso di un'attività commerciale (immettendolo in tal modo sul mercato). Analogamente, un importatore è la persona fisica o giuridica stabilita nell'UE che fornisce il prodotto con elementi digitali di una persona stabilita al di fuori dell'UE e che lo fa nel corso di un'attività commerciale (immettendolo in tal modo sul mercato). Gli obblighi dei gestori si applicano alla persona giuridica che fornisce un software libero e open source destinato ad attività commerciali ([12]), ma non lo immette sul mercato ai sensi del regolamento sulla ciberresilienza.

48. Al fine di determinare se una persona fisica o giuridica stia immettendo un software libero e open source sul mercato dell'UE, occorre pertanto chiarire innanzitutto se tale persona fisica o giuridica stia effettivamente fornendo il software in questione. Per stabilire correttamente gli obblighi applicabili ai sensi del regolamento sulla ciberresilienza, è essenziale determinare se la persona fisica o giuridica stia effettivamente compiendo l'azione di fornire un software libero e open source. Infatti, come ricordato al considerando 18, il regolamento sulla ciberresilienza non si applica alle persone fisiche o giuridiche che contribuiscono tramite codici sorgente a prodotti con elementi digitali che si qualificano come software liberi e open source che esulano dalla loro responsabilità.

([12]) Si tratta di una condizione necessaria ma non sufficiente affinché una persona giuridica possa qualificarsi come gestore di software open source, in quanto la definizione di cui all'articolo 3, punto 14), stabilisce ulteriori condizioni affinché una persona giuridica possa essere considerato un gestore.

49. Date le specificità dello sviluppo dei software liberi e open source, che coinvolge spesso più contributori, modelli di collaborazione decentralizzati e una separazione tra il contributo e il processo decisionale, è utile chiarire che il software libero e open source è considerato «sotto la responsabilità» delle persone fisiche o giuridiche che lo pubblicano ed esercitano il controllo primario sulle decisioni relative al suo sviluppo, alle sue versioni e alla sua distribuzione (spesso denominate «responsabili della manutenzione»). I soggetti che contribuiscono tramite codici sorgente ma non controllano le versioni, le *roadmap* o le decisioni relative alla governance sono considerati «contributori»; in tali casi il software libero e open source esula dalla loro responsabilità, anche se vi hanno contribuito con il codice. La mera esistenza di permessi tecnici, come l'accesso in scrittura, non è sufficiente per stabilire che il software libero open source rientri nella responsabilità di tale soggetto; la responsabilità ricade su coloro che pubblicano e controllano il software libero e open source.

Esempio 13: uno sviluppatore autonomo o il dipendente di una società invia a un progetto open source una richiesta di «pull» o «merge» contenente una patch di sicurezza o una nuova caratteristica. I responsabili della manutenzione del progetto esaminano, accettano e integrano il codice nel repository principale, includendolo successivamente in una nuova versione. In questo scenario, la persona che ha presentato la richiesta di pull è un «contributore» e non è soggetta al regolamento sulla ciberresilienza. Sebbene tale persona abbia fornito il codice sorgente, non esercita un controllo primario sulle decisioni relative allo sviluppo, al rilascio o alla distribuzione.

3.2. **Determinare se un software libero e open source è immesso sul mercato dell'UE**

50. Una volta stabilito che un software libero e open source rientra nella responsabilità di una persona fisica o giuridica, occorre stabilire se tale persona lo fornisce nel corso di un'attività commerciale, dando luogo in tal modo a un'immissione sul mercato.

3.2.1. *Applicazione di un prezzo*

51. Se la persona fisica o giuridica che fornisce un software libero e open source applica un prezzo per il software in quanto tale (ad esempio applicando un prezzo per i binari precompilati), tale persona immette sul mercato un prodotto con elementi digitali. La persona che immette sul mercato un software libero open source è pertanto un fabbricante ai sensi del regolamento sulla ciberresilienza.

52. Spesso i fabbricanti di software liberi e open source forniscono versioni gratuite di tali software (di solito denominate versioni «della comunità»), la cui base di codice è (quasi) identica alla versione a pagamento. Tali prodotti con elementi digitali sono tuttavia prodotti diversi: la versione a pagamento è monetizzata in qualche modo (ad esempio applicando un prezzo o con altri mezzi, come illustrato nella presente sezione) ed è pertanto considerata immessa sul mercato, facendo scattare gli obblighi del fabbricante. La versione fornita gratuitamente (o la versione della comunità) non è monetizzata e pertanto non è considerata immessa sul mercato ai fini del regolamento sulla ciberresilienza. Ciò vale anche nel caso in cui la versione a pagamento sia una versione commerciale «potenziata», che estende la base di codice della versione fornita gratuitamente, o incorpora tale versione in un prodotto con elementi digitali più ampio (ad esempio, come nel caso del modello «open core»).

53. Se il soggetto che fornisce la versione della comunità è una persona giuridica, tale persona giuridica è altresì soggetta agli obblighi che incombono ai gestori per la versione che fornisce gratuitamente (versione della comunità). Se il soggetto è una persona fisica, la versione fornita gratuitamente (la versione della comunità) non rientra nell'ambito di applicazione del regolamento sulla ciberresilienza.

3.2.2. *Monetizzazione di altri servizi o richiesta di trattamento dei dati personali*

54. Una persona fisica o giuridica che pubblica un software libero e open source può altresì immetterlo sul mercato (ossia fornirlo nel corso di un'attività commerciale) nel caso in cui fornisca il software monetizzando attraverso di esso altri prodotti con elementi digitali o servizi o qualora imponga, come condizione per l'utilizzo, il trattamento dei dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software.

Esempio 14: una persona fisica o giuridica pubblica un'applicazione marketplace libera e open source. L'applicazione è disponibile gratuitamente e gli utilizzatori possono acquistare beni o servizi attraverso di essa. L'applicazione consente al soggetto che l'ha pubblicata di monetizzare altri prodotti con elementi digitali e servizi offerti attraverso di essa (ad esempio attraverso annunci pubblicitari, commissioni o quote di abbonamento). L'applicazione è pertanto considerata immessa sul mercato nel corso di un'attività commerciale.

Esempio 15: una persona fisica o giuridica pubblica una VPN libera e open source. L'applicazione è disponibile gratuitamente, ma consente agli utilizzatori di pagare per accedere a server aggiuntivi o indirizzi IP dedicati. Tale applicazione consente a tale soggetto di monetizzare altri servizi offerti attraverso di essa, pertanto è considerata immessa sul mercato nel corso di un'attività commerciale.

Esempio 16: una persona fisica o giuridica pubblica un'applicazione libera e open source per il monitoraggio dell'attività sportiva. L'applicazione è disponibile gratuitamente, ma il suo utilizzo è subordinato al trattamento dei dati personali degli utilizzatori per finalità quali pubblicità mirata o analisi non correlate alla sicurezza, alla compatibilità o all'interoperabilità del software. Richiedendo tale trattamento dei dati come condizione per l'uso, l'applicazione è pertanto considerata immessa sul mercato nel corso di un'attività commerciale.

3.2.3. *Servizi di assistenza*

55. Il semplice fatto che una persona fisica o giuridica che pubblica un software libero e open source offra anche servizi di assistenza a pagamento ad esso correlati non implica, di per sé, che il prodotto con elementi digitali sia fornito nel corso di un'attività commerciale. I servizi di assistenza possono comprendere attività quali consulenza, formazione o servizi professionali relativi all'uso, alla documentazione, alla configurazione e all'implementazione del software da parte di un cliente.

56. Come indicato al considerando 18 del regolamento sulla ciberresilienza («la fornitura di prodotti con elementi digitali che si qualificano come software liberi e open source che non sono monetizzati dai loro fabbricanti non dovrebbe essere considerata un'attività commerciale»), il fattore determinante è se l'accesso al software libero e open source in quanto tale (ossia la fornitura del prodotto con elementi digitali), compresa la sua manutenzione, sia subordinato al pagamento di un corrispettivo, e non il fatto che siano offerti servizi professionali intorno a un prodotto con elementi digitali liberamente disponibile. Se il software libero e open source può essere scaricato e installato liberamente e gli utilizzatori possono scegliere facoltativamente di acquistare servizi professionali separatamente, tale software libero e open source non è considerato immesso sul mercato.

57. Per contro, in alcuni casi l'accesso a una versione specifica del prodotto con elementi digitali, compresi determinati benefici quali l'assistenza tecnica o l'ottimizzazione delle prestazioni, è subordinato al pagamento di un corrispettivo. In questi casi tale fornitura costituisce una fornitura monetizzata di un prodotto con elementi digitali effettuata nel corso di un'attività commerciale ed è pertanto considerata un'immissione sul mercato. Ciò comprende i casi in cui un'edizione a pagamento o una versione aziendale è messa a disposizione nell'ambito di un accordo commerciale, indipendentemente dal fatto che un software equivalente dal punto di vista funzionale sia anche disponibile gratuitamente nell'ambito di una licenza gratuita e open source.

Esempio 17: una persona fisica o giuridica pubblica un sistema operativo libero e open source, offrendone una versione a pagamento che comprende servizi di assistenza, quali assistenza tecnica o ottimizzazione delle prestazioni. La versione a pagamento del sistema operativo è considerata immessa sul mercato nel corso di un'attività commerciale.

Esempio 18: una persona fisica o giuridica pubblica uno strumento a riga di comando libero e open source. Lo strumento è liberamente accessibile e chiunque può scaricarlo e installarlo. Tale persona fisica o giuridica offre separatamente servizi professionali, quali servizi facoltativi di consulenza per formare gli utilizzatori e assisterli nell'installazione e nell'utilizzo dello strumento. Tale software libero e open source non è considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza.

58. In particolare nel caso in cui il software libero e open source sia pubblicato da persone fisiche, l'offerta di assistenza tecnica direttamente associata all'accesso al prodotto con elementi digitali non sarebbe comunque considerata un'attività commerciale se, come indicato al considerando 15 del regolamento sulla ciberresilienza, il prezzo applicato è finalizzato esclusivamente a recuperare i costi effettivi. Tali costi effettivi comprendono una serie di costi relativi alla progettazione, allo sviluppo e alla manutenzione di tale software, comprese le spese di sostentamento ragionevoli della persona. Pertanto il fatto che una persona fisica pubblichi un software libero e open source e offra assistenza tecnica per coprire i propri costi e ottenere un equo corrispettivo non deve essere considerato, solo su tale base, come un'immissione di tale software sul mercato dell'UE.

59. Il fatto che una persona fisica o giuridica offra assistenza tecnica relativa a un software libero e open source che esula dalla sua responsabilità non è considerato come un'immissione di tale software sul mercato, a meno che tale persona non modifichi in modo sostanziale il software libero e open source, a norma dell'articolo 22, nell'ambito della fornitura di detta assistenza.

Esempio 19: un fornitore di servizi non pubblica un software libero e open source, ma aiuta un cliente a installarlo sul proprio server locale. Ciò avviene senza apportare alcuna modifica sostanziale a tale software libero e open source. Di conseguenza non si ritiene che il prestatore di servizi immetta il software libero e open source sul mercato.

3.2.4. *Donazioni*

60. Le persone fisiche o giuridiche che pubblicano progetti di software liberi e open source solitamente includono modalità che consentono agli utilizzatori di tale software di donare volontariamente denaro per ringraziare gli sviluppatori del progetto e anche per garantire che esso continui a essere mantenuto attivamente.

61. Come indicato al considerando 15 del regolamento sulla ciberresilienza, «[l]'atto di accettare donazioni senza fini di lucro non dovrebbe essere considerato costitutivo di un'attività commerciale». Il semplice fatto di inserire un link a una piattaforma di donazioni o a strumenti analoghi per raccogliere donazioni non dovrebbe essere considerato come un fine di lucro, anche se l'importo raccolto attraverso le donazioni supera i semplici costi associati alla progettazione, allo sviluppo e alla fornitura di un prodotto con elementi digitali. Ciò comprende un compenso ragionevole per i contributori assunti da una persona giuridica e/o le spese di sostentamento ragionevoli di una persona fisica. Le donazioni, per loro stessa natura, variano nel tempo e pertanto occorre esercitare un certo grado di flessibilità nel valutare se un software libero e open source monetizzato esclusivamente attraverso donazioni debba essere considerato immesso sul mercato. È pertanto improbabile che un software libero e open source sostenuto solo attraverso donazioni sia considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza.

Esempio 20: una persona fisica o giuridica pubblica uno strumento software libero e open source in un archivio pubblico online, consentendo a chiunque di scaricarlo, utilizzarlo, modificarlo e ridistribuirlo nell'ambito di una licenza gratuita e open source. Lo sviluppatore invita gli utenti a effettuare donazioni volontarie attraverso una piattaforma di donazioni per sostenere lo sviluppo e la manutenzione continui del progetto. L'accesso al software, al suo codice sorgente e ai suoi aggiornamenti non è subordinato all'effettuazione di una donazione. Tale software libero e open source non è considerato fornito nel corso di un'attività commerciale e non è considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza.

62. Vi sono tuttavia casi in cui un software libero e open source sostenuto mediante donazioni può essere considerato immesso sul mercato. Ciò avviene quando, sulla base di una valutazione complessiva delle circostanze, le donazioni sono di fatto equivalenti all'applicazione di un prezzo per l'accesso al prodotto con elementi digitali o ad alcune delle sue funzionalità. Ciò può verificarsi, in particolare, quando l'accesso al software libero e open source, alle funzionalità essenziali o agli aggiornamenti è subordinato di fatto all'effettuazione di una donazione, o quando le donazioni sono associate a benefici contrattuali o a vantaggi esclusivi che vanno al di là dei vantaggi offerti alla comunità.

Esempio 21: una persona fisica o giuridica pubblica un software con elementi digitali con licenza gratuita e open source, ma fornisce versioni scaricabili e aggiornamenti di sicurezza solo agli utilizzatori che effettuano una donazione. Gli utilizzatori che non effettuano donazioni non hanno accesso alla versione aggiornata del software.

In questo caso le donazioni sono di fatto una condizione per l'accesso al prodotto con elementi digitali e pertanto equivalgono all'applicazione di un prezzo. Il software libero e open source in questione è pertanto considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza.

Esempio 22: una persona fisica o giuridica rende pubblico il codice sorgente di un software libero e open source, ma fornisce binari precompilati, aggiornamenti periodici e correzioni di sicurezza garantite soltanto ai donatori. In tal caso le donazioni sono legate all'accesso ad aspetti essenziali del prodotto con elementi digitali e costituiscono un corrispettivo per la fornitura di tale prodotto. Il software libero e open source in questione è pertanto considerato immesso sul mercato nel corso di un'attività commerciale.

3.2.5. *Finanziamento dei software liberi e open source*

63. Il semplice fatto che un soggetto terzo abbia pagato per lo sviluppo di un software libero e open source, lo abbia sponsorizzato o finanziato in altro modo non è di per sé determinante per stabilire che tale software sia immesso sul mercato. È prassi comune nell'ecosistema dei software aperti e open source che singoli sviluppatori, fondazioni o comunità ricevano finanziamenti da società, enti pubblici o altri sponsor per lavorare su caratteristiche specifiche, correggere bug o mantenere componenti essenziali. Tali finanziamenti possono assumere varie forme, tra cui sovvenzioni, *bug bounty*, sponsorizzazioni, contratti di servizi o attività di sviluppo retribuite.

64. Come già ricordato, il considerando 18 del regolamento sulla ciberresilienza chiarisce che le mere circostanze in cui il prodotto con elementi digitali è stato sviluppato o il modo in cui lo sviluppo è stato finanziato non dovrebbero essere presi in considerazione al fine di determinare la natura commerciale o non commerciale di tale attività.

65. Pertanto se il software libero e open source è condiviso apertamente e liberamente accessibile, utilizzabile, modificabile e ridistribuibile da chiunque, il fatto che un soggetto commerciale possa aver pagato per tale progetto non dovrebbe costituire un elemento in base al quale determinare se il software è immesso sul mercato. Di fatto, se non è altrimenti monetizzato, tale software libero e open source non deve essere considerato immesso sul mercato. Se la società che ha finanziato lo sviluppo del software libero e open source (nonché qualsiasi altra società) lo integra in un proprio prodotto con elementi digitali, tale società deve esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5, del regolamento sulla ciberresilienza.

Esempio 23: uno sviluppatore indipendente pubblica un progetto di software libero e open source e ne cura attivamente la manutenzione. Il fabbricante A chiede allo sviluppatore indipendente di aggiungere una caratteristica specifica per tale software libero e open source e ne finanzia lo sviluppo. Lo sviluppatore aggiunge la funzione alla base di codice del software libero e open source, condividendolo apertamente e rendendolo liberamente accessibile, utilizzabile, modificabile e ridistribuibile da chiunque. Non si ritiene che lo sviluppatore indipendente abbia immesso tale software libero e open source sul mercato. Se integra il software libero e open source in un proprio prodotto con elementi digitali, il fabbricante deve esercitare la dovuta diligenza a norma dell'articolo 13, paragrafo 5.

3.2.6. *Enti senza scopo di lucro costituiti per conseguire obiettivi senza scopo di lucro*

66. Se una persona giuridica che pubblica un software libero e open source è un'organizzazione senza scopo di lucro «costituita in modo tale da garantire che tutti gli utili al netto dei costi siano utilizzati per conseguire obiettivi senza scopo di lucro» (considerando 18 del regolamento sulla ciberresilienza), il software libero e open source da essa pubblicato non è considerato immesso sul mercato. Se tale persona giuridica rientra nella definizione di «gestore», è soggetta agli obblighi corrispondenti (articolo 24 del regolamento sulla ciberresilienza).

Esempio 24: una persona giuridica pubblica un browser libero e open source che è direttamente monetizzato attraverso accordi con motori di ricerca, ma tutti i suoi utili al netto dei costi sono utilizzati per obiettivi senza scopo di lucro. Il browser non è considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza. La persona giuridica che lo pubblica è soggetta agli obblighi applicabili ai gestori.

3.2.7. *Integrazione da parte di altri fabbricanti*

67. In alcuni casi un software libero e open source è pubblicato da una persona fisica o giuridica chiaramente identificabile, ma è «destinato a essere integrato da altri fabbricanti nei rispettivi prodotti con elementi digitali». In tali casi il software libero e open source non è considerato immesso sul mercato dell'UE, a meno che non sia anche monetizzato dalla persona che lo pubblica (ossia il fabbricante originario), conformemente alle sezioni precedenti dei presenti orientamenti.

68. Laddove tale software libero e open source non sia immesso sul mercato, la persona giuridica che lo pubblica, qualora fornisca un sostegno duraturo in linea con la definizione di «gestore», sarebbe soggetta agli obblighi che incombono ai gestori.

Esempio 25: una persona giuridica pubblica una libreria software libera e open source per la creazione di interfacce utente. Non monetizza la fornitura di tale libreria, ma la integra in uno dei propri prodotti con elementi digitali (che a sua volta viene immesso sul mercato). La libreria non è considerata immessa sul mercato ai sensi del regolamento sulla ciberresilienza, ma è destinata a essere integrata in prodotti con elementi digitali. La persona giuridica che la pubblica ne è il gestore.

Esempio 26: una persona giuridica immette sul mercato un sistema operativo e pubblica anche librerie software libere e open source che fungono da implementazioni di riferimento per gli utilizzatori di tale sistema operativo. La persona giuridica non monetizza le biblioteche software libere e open source, che sono destinate a essere integrate in altri prodotti con elementi digitali. La persona giuridica che le pubblica è un gestore di tali librerie software libere e open source.

3.3. **I gestori di software open source**

69. Il regolamento sulla ciberresilienza introduce la nuova categoria di «gestore di software open source» in considerazione dell'«importanza per la cibersicurezza di molti prodotti con elementi digitali che si qualificano come software liberi e open source che sono pubblicati, ma non messi a disposizione sul mercato ai sensi del [regolamento sulla ciberresilienza]» (considerando 19 del regolamento sulla ciberresilienza).

70. In alcuni casi un software libero e open source è pubblicato, ma non messo a disposizione sul mercato ai sensi del regolamento sulla ciberresilienza, da una persona giuridica che «ha la finalità o l'obiettivo di fornire un sostegno sistematico e duraturo per lo sviluppo di [software aperti e open source] […] destinati ad attività commerciali, e che garantisce la sostenibilità economica di tali prodotti» (articolo 3, punto 14), del regolamento sulla ciberresilienza). In tali casi, la persona giuridica in questione è soggetta agli obblighi che incombono ai gestori.

71. Un gestore è definito come «una persona giuridica, diversa dal fabbricante», in quanto un fabbricante, per definizione, è la persona fisica o giuridica che immette sul mercato prodotti con elementi digitali («li commercializza») con il proprio nome o marchio. Una persona giuridica può essere un gestore soltanto per i prodotti con elementi digitali che si qualificano come software liberi e open source che sono pubblicati, ma non messi a disposizione sul mercato ai sensi del regolamento sulla ciberresilienza. Il concetto di gestore si applica pertanto a casi specifici di software liberi e open source che sono «destinati in ultima istanza ad attività commerciali, ad esempio quelli destinati all'integrazione in servizi commerciali o in prodotti monetizzati con elementi digitali» (considerando 19 del regolamento sulla ciberresilienza ([13])), ma che non sono messi a disposizione sul mercato ai sensi del regolamento sulla ciberresilienza, e per i quali la persona giuridica che pubblica il software libero e open source in questione garantisce un sostegno sistematico.

72. Il fatto che una persona giuridica sia il gestore di un determinato software libero e open source non implica necessariamente che tale persona sia anche il gestore di altri software liberi e open source da essa pubblicati. Allo stesso modo, il fatto che una persona giuridica sia il fabbricante di un determinato software libero e open source non implica che essa non possa non essere il gestore di altri software liberi e open source. Ciò comprende la fornitura di versioni «della comunità» dello stesso software libero e open source, come descritto nella sezione *3.2.1 Applicazione di un* prezzo.

73. Una persona giuridica può quindi essere al tempo stesso gestore di un determinato software libero e open source (nel qual caso fornisce un sostegno sistematico e duraturo e garantisce la sostenibilità economica del software in qualità di gestore) e fabbricante di un altro determinato software libero e open source (nel qual caso lo immette sul mercato). In altre parole, lo stesso soggetto giuridico può essere tenuto a svolgere ruoli differenti per diversi progetti di software liberi e open source.

74. Per ogni specifico software libero e open source che pubblica, la persona giuridica dovrà accertare se tale software sia considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza. In caso affermativo, ciò rende il soggetto giuridico il fabbricante del software. Se il software libero e open source non è considerato immesso sul mercato, la persona giuridica può esserne il gestore, nel caso in cui il software sia destinato ad attività commerciali e la persona giuridica fornisca un sostegno conformemente alla definizione di gestore ([14]).

3.3.1. *Sostegno duraturo e garanzia della sostenibilità economica del software libero e open source*

75. Il considerando 19 spiega che apportare un sostegno duraturo allo sviluppo di un prodotto con elementi digitali può comprendere (a titolo esemplificativo ma non esaustivo): i) l'hosting e la gestione di piattaforme di collaborazione per lo sviluppo di software; ii) l'hosting di codici sorgente o software; iii) l'amministrazione o la gestione di prodotti con elementi digitali che si qualificano come software liberi e open source; e iv) l'orientamento dello sviluppo di tali prodotti con elementi digitali.

76. Può verificarsi ad esempio che un soggetto giuridico sviluppi un software libero e open source destinato ad essere integrato nei propri prodotti con elementi digitali e poi lo pubblichi senza immetterlo sul mercato. Questo aspetto è trattato anche nella sezione *3.2.7 Integrazione da parte di altri fabbricanti*. In tal caso il soggetto giuridico non è il fabbricante del software, ma può esserne il gestore. Inoltre, come spiegato anche nelle sezioni precedenti, un soggetto giuridico che pubblica una versione libera (o della comunità) e una versione monetizzata dello stesso software libero e open source è considerato gestore della versione libera (o della comunità) e fabbricante della versione monetizzata.

77. Analogamente, una persona giuridica che monetizza un software libero e open source ma è un soggetto senza scopo di lucro i cui utili al netto dei costi sono utilizzati per conseguire obiettivi senza scopo di lucro (e pertanto il suo software libero e open source non è immesso sul mercato ai sensi della regolamento sulla ciberresilienza, come illustrato nella sezione *3.2.6 Enti senza scopo di lucro*) è il gestore del software libero e open source da essa pubblicato.

78. Inoltre alcune fondazioni offrono piattaforme di collaborazione con varie forme di amministrazione che consentono ai fabbricanti di contribuire regolarmente allo sviluppo di software liberi e open source e/o che sono regolarmente finanziate dai fabbricanti. Tali fondazioni devono essere considerate gestori in relazione a specifici software liberi e open source destinati ad attività commerciali e per i quali la fondazione offre un sostegno duraturo. Tuttavia, come spiegato nella sezione *3.3 I gestori di* software open source, qualora non fornisca un sostegno sistematico a uno specifico software libero e open source, non ne garantisca la sostenibilità economica e/o nel caso in cui tale specifico software non sia destinato ad attività commerciali, una fondazione di questo tipo potrebbe non essere soggetta ad alcun obbligo ai sensi del regolamento sulla ciberresilienza per altri specifici software liberi e open source di cui funge da host.

([13]) Questo concetto è contenuto anche nella formulazione «destinati ad attività commerciali» che figura nella definizione di «gestore di software open source» di cui all'articolo 3, punto 14), del regolamento sulla ciberresilienza.

([14]) La persona giuridica non può inoltre essere soggetta ad alcun obbligo ai sensi del regolamento sulla ciberresilienza nei casi in cui: i) uno specifico software libero e open source non è immesso sul mercato ai sensi del regolamento sulla ciberresilienza; e ii) il soggetto giuridico non soddisfa la definizione di gestore in relazione a tale specifico software libero e open source.

79. Il tipo di «sostegno duraturo» che fondazioni e organizzazioni analoghe forniscono a specifici progetti di software liberi e open source può variare notevolmente. Ad esempio, alcuni soggetti giuridici forniscono soltanto assistenza non tecnica, come la gestione del branding dei progetti, la definizione del modello di governance, l'organizzazione di eventi della comunità o la raccolta di donazioni. Altri soggetti forniscono l'infrastruttura informatica sottostante necessaria per la gestione del progetto, ad esempio tramite l'hosting degli archivi di codici sorgente, la fornitura di sistemi di controllo delle versioni o la generazione di chiavi di firma. Altri forniscono un sostegno ancora più ampio, contribuendo attivamente al progetto con risorse ingegneristiche, ad esempio assumendo sviluppatori, coordinando il lavoro di sviluppo, rivedendo o integrando il codice, gestendo le versioni o occupandosi delle segnalazioni di vulnerabilità e delle patch di sicurezza. Sebbene tutti i soggetti giuridici che si qualificano come gestori ai sensi del regolamento sulla ciberresilienza siano tenuti a rispettare gli obblighi di cui all'articolo 24, paragrafi 1 e 2, a norma dell'articolo 24, paragrafo 3, la misura in cui gli obblighi di cui all'articolo 14, paragrafi 1, 3 e 8, si applicano a tali soggetti giuridici varia a seconda del tipo di sostegno da essi fornito.

80. Ad esempio, un gestore che fornisce solo assistenza non tecnica non è, per definizione, coinvolto nello sviluppo del prodotto con elementi digitali e non è pertanto tenuto a segnalare le vulnerabilità attivamente sfruttate. Il gestore in questione non fornisce inoltre alcun sistema informativo o di rete per lo sviluppo di tali prodotti con elementi digitali e pertanto non è tenuto a segnalare incidenti gravi all'ENISA e ai CSIRT o agli utilizzatori interessati. Tuttavia, qualora venga a conoscenza di una vulnerabilità attivamente sfruttata (ad esempio tramite una segnalazione proveniente da fonti esterne, come ricercatori in materia di sicurezza), il gestore dovrebbe condividere le informazioni con i responsabili della manutenzione del prodotto con elementi digitali, conformemente alla sua politica in materia di cibersicurezza. I responsabili della manutenzione dei prodotti con elementi digitali e/o i gestori dovrebbero inoltre prendere in considerazione la possibilità di segnalare la vulnerabilità su base volontaria, conformemente all'articolo 15.

81. D'altro canto, qualora fornisca l'infrastruttura informatica sottostante per determinati prodotti con elementi digitali, un gestore è tenuto a notificare all'ENISA e ai CSIRT, conformemente all'articolo 14, paragrafo 3, qualsiasi incidente grave relativo a tale infrastruttura che abbia un impatto sulla sicurezza dei prodotti con elementi digitali. È inoltre tenuto, se del caso, a informare tutti gli utilizzatori (ad esempio mediante un annuncio generale). Come indicato al punto precedente, sebbene non sia tenuto a segnalare le vulnerabilità attivamente sfruttate di cui viene a conoscenza, il gestore dovrebbe promuovere la corretta gestione delle vulnerabilità e prendere in considerazione la segnalazione volontaria di cui all'articolo 15.

82. Infine, se fornisce anche risorse ingegneristiche a prodotti specifici con elementi digitali, un gestore è tenuto a: i) notificare, a norma dell'articolo 14, paragrafo 1, le vulnerabilità attivamente sfruttate di cui viene a conoscenza; e ii) se del caso, informare tutti gli utilizzatori. Nella misura in cui abbia anche un rapporto diretto con gli utilizzatori interessati, il gestore è altresì tenuto a informarli direttamente, conformemente all'articolo 14, paragrafo 8.

83. Qualora cessi di fornire sostegno sistematico e duraturo per uno specifico software libero e open source, un soggetto non può più soddisfare più la definizione di «gestore» e pertanto non è più soggetto agli obblighi corrispondenti. In questi casi tale soggetto è incoraggiato a comunicare chiaramente il cambiamento del proprio status per lo specifico software libero e open source in questione.

84. In determinate situazioni un soggetto che è stato il gestore di un progetto specifico può decidere di monetizzare direttamente tale progetto, immettendo in tal modo il prodotto con elementi digitali sul mercato e facendo scattare gli obblighi del fabbricante ai sensi del regolamento sulla ciberresilienza. In tali circostanze tale soggetto si qualifica come fabbricante del prodotto con elementi digitali a partire dalla data in cui lo immette sul mercato (ma non per le versioni precedenti per le quali ha agito come gestore).

3.4. **Contributori e usi a valle**

85. Come già menzionato nella sezione *3.1 Determinare su chi ricada la responsabilità di un software libero e open source*, il regolamento sulla ciberresilienza chiarisce che il suo ambito di applicazione non si estende «alle persone fisiche o giuridiche che contribuiscono tramite codici sorgente a prodotti con elementi digitali che si qualificano come software liberi e open source che esulano dalla loro responsabilità» (considerando 18).

86. Anche i fabbricanti di prodotti con elementi digitali che integrano componenti software liberi e open source nei propri prodotti con elementi digitali non diventano responsabili della conformità di tali singoli componenti al regolamento sulla ciberresilienza, anche nel caso in cui contribuiscano tramite il codice sorgente alla loro manutenzione.

87. Analogamente, il semplice fatto che i fabbricanti integrino componenti software liberi e open source nei propri prodotti (monetizzati) con elementi digitali non ha alcun impatto sullo status di tale componente open source ai sensi del regolamento sulla ciberresilienza. I responsabili della manutenzione dei componenti software liberi e open source che non sono immessi sul mercato non hanno alcun obbligo nei confronti di altri soggetti che possono integrare tali componenti nei propri prodotti con elementi digitali. L'applicabilità del regolamento sulla ciberresilienza a un determinato componente software libero e open source dipende esclusivamente dal fatto che la persona fisica o giuridica che lo pubblica lo immetta sul mercato.

88. Cionondimeno i fabbricanti di prodotti con elementi digitali che integrano componenti software liberi e open source sono tenuti a rispettare il regolamento sulla ciberresilienza per i propri prodotti con elementi digitali. Hanno inoltre l'obbligo di esercitare la dovuta diligenza, a norma dell'articolo 13, paragrafo 5, rispetto ai componenti software liberi e open source che integrano. Sono altresì tenuti a segnalare le vulnerabilità dei componenti integrati e a condividere le correzioni di sicurezza in conformità dell'articolo 13, paragrafo 6. Per ulteriori orientamenti su questo argomento, cfr. la sezione *9.2.1 Segnalazione a monte e condivisione delle correzioni di sicurezza*.

3.5. **Scenari esemplificativi**

89. Gli esempi elencati di seguito sono puramente ipotetici e intendono soltanto illustrare i diversi casi analizzati nelle sezioni precedenti.

Esempio 27: lo sviluppatore indipendente A ha sviluppato un software libero e open source. Lo sviluppatore A pubblica tale software libero e open source con il proprio nome o marchio, ma non applica un prezzo per il suo utilizzo. Il software è condiviso apertamente ed è liberamente accessibile, utilizzabile, modificabile e ridistribuibile da chiunque. Lo sviluppatore A include anche un link a una piattaforma per la raccolta di donazioni volontarie.

Le società B, C e D integrano tale software libero e open source nei propri prodotti con elementi digitali. Per sostenere la costante manutenzione, le società B, C e D effettuano donazioni volontarie in favore dello sviluppatore A. Tali donazioni consentono allo sviluppatore A di curare attivamente la manutenzione del progetto.

Tale software libero e open source non è immesso sul mercato ai sensi del regolamento sulla ciberresilienza. Lo sviluppatore A non ha obblighi ai sensi del regolamento sulla ciberresilienza. Le società B, C e D devono esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5, quando integrano tale software libero e open source nei propri prodotti con elementi digitali.

Esempio 28: la fondazione senza scopo di lucro F pubblica un componente software libero e open source destinato all'integrazione in altri prodotti commerciali con elementi digitali. La fondazione F si impegna a fornire un sostegno duraturo a tale software libero e open source, al fine di garantirne la sostenibilità economica e la diffusione. Le società A, B e C integrano tale software libero e open source nei propri prodotti con elementi digitali. Le società A e B contribuiscono volontariamente con parte del tempo dei propri sviluppatori allo sviluppo e alla manutenzione di progetti software liberi e open source all'interno della fondazione F, anche in relazione a tale software libero e open source.

Poiché la fondazione F è un soggetto senza scopo di lucro costituito in modo tale che i suoi utili al netto dei costi sono utilizzati per conseguire obiettivi senza scopo di lucro, il software libero e open source non è considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza. La fondazione F è il gestore del software libero e senza scopo di lucro ed è soggetta ai corrispondenti obblighi di cui all'articolo 24. Le società A, B e C devono esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5, quando integrano tale software libero e open source nei propri prodotti con elementi digitali.

Esempio 29: la società A ha sviluppato un componente software libero e open source da integrare nei propri prodotti con elementi digitali. Inoltre pubblica tale software libero e open source separatamente con il proprio nome o marchio e lo mantiene attivamente. Tuttavia non fa pagare per il suo utilizzo né monetizza in altri modi. Le società B, C e D integrano tale software libero e open source nei propri prodotti con elementi digitali e contribuiscono volontariamente alla sua manutenzione con parte del tempo dei propri sviluppatori.

Tale software libero e open source non è considerato immesso sul mercato ai sensi del regolamento sulla ciberresilienza. La società A non è il suo fabbricante, ma il suo gestore. Le società B, C e D devono esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5, quando integrano il software libero e open source nei propri prodotti con elementi digitali.

Esempio 30: la società A pubblica un software libero e open source con il proprio nome o marchio e lo offre come versione a pagamento, che comprende determinati benefici quali l'assistenza tecnica o l'ottimizzazione delle prestazioni. Gli sviluppatori delle società B, C e D contribuiscono alla manutenzione del software libero e open source, che rimane tuttavia sotto il controllo della società A.

La società A è considerata il fabbricante di tale software libero e open source ([15]). *Le società B, C e D non sono soggette agli obblighi previsti dal regolamento sulla ciberresilienza per lo specifico software libero e open source in questione. Se integrano tale software libero e open source nei propri prodotti con elementi digitali, esse sono tenute a esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5.*

Esempio 31: la società A pubblica un software libero e open source con il proprio nome o marchio e fornisce una manutenzione costante per garantirne la sostenibilità economica a lungo termine, al fine di consentire l'integrazione di tale software nei prodotti con elementi digitali di altre società. La società A non applica alcun costo per il suo utilizzo, non tratta i dati personali raccolti attraverso il prodotto con elementi digitali né vende servizi di assistenza associati alla pubblicazione del software libero e open source.

La società B contribuisce alla manutenzione del software libero e open source tramite il codice e il tempo degli sviluppatori dedicato a tale manutenzione, ma non lo distribuisce a fini commerciali. La società B offre servizi di assistenza tecnica indipendentemente dalla distribuzione del software libero e open source. La società A è considerata il gestore di tale software libero e open source, mentre la società B non ha obblighi ai sensi del regolamento sulla ciberresilienza per tale software.

Esempio 32: un componente software libero e open source è pubblicato da un soggetto senza scopo di lucro costituito in modo tale da garantire che tutti gli utili al netto dei costi siano utilizzati per conseguire obiettivi senza scopo di lucro. Detto soggetto fornisce un sostegno duraturo per garantire la sostenibilità economica a lungo termine del progetto. La manutenzione è finanziata con fondi pubblici, quali le sovvenzioni per la ricerca. Ulteriori sviluppi, comprese le nuove funzionalità, sono finanziati attraverso donazioni e progetti specifici, realizzati in partenariato con i fabbricanti che integrano tale software libero e open source nei propri prodotti con elementi digitali. Tali funzionalità sono integrate nella base di codici del software libero e open source.

Il soggetto senza scopo di lucro che pubblica il software libero e open source è considerato il gestore di tale componente software libero e open source. Un fabbricante che ha contribuito allo sviluppo di determinate funzionalità non diventa il fabbricante di tale componente software libero e open source. Se integra tale componente libero e open source nel proprio prodotto con elementi digitali, il fabbricante deve esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5.

Esempio 33: un soggetto senza scopo di lucro costituito in modo tale da garantire che tutti gli utili al netto dei costi siano utilizzati per conseguire obiettivi senza scopo di lucro pubblica un pacchetto di sviluppo per applicazioni (software development kit, SDK) libero e open source e ne garantisce la manutenzione costante. L'SDK è condiviso apertamente ed è liberamente accessibile, utilizzabile, modificabile e ridistribuibile da chiunque. I finanziamenti sono erogati attraverso quote associative versate al soggetto senza scopo di lucro e gli sviluppatori impiegati dalle organizzazioni aderenti contribuiscono allo sviluppo dell'SDK con codici e altre risorse. I fabbricanti utilizzano l'SDK come componente per realizzare altri prodotti con elementi digitali.

Il soggetto senza scopo di lucro che pubblica tale SDK è il suo gestore. I membri della fondazione non sono responsabili della conformità dell'SDK al regolamento sulla ciberresilienza. Qualora utilizzino l'SDK per realizzare un proprio prodotto con elementi digitali, i fabbricanti devono esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5.

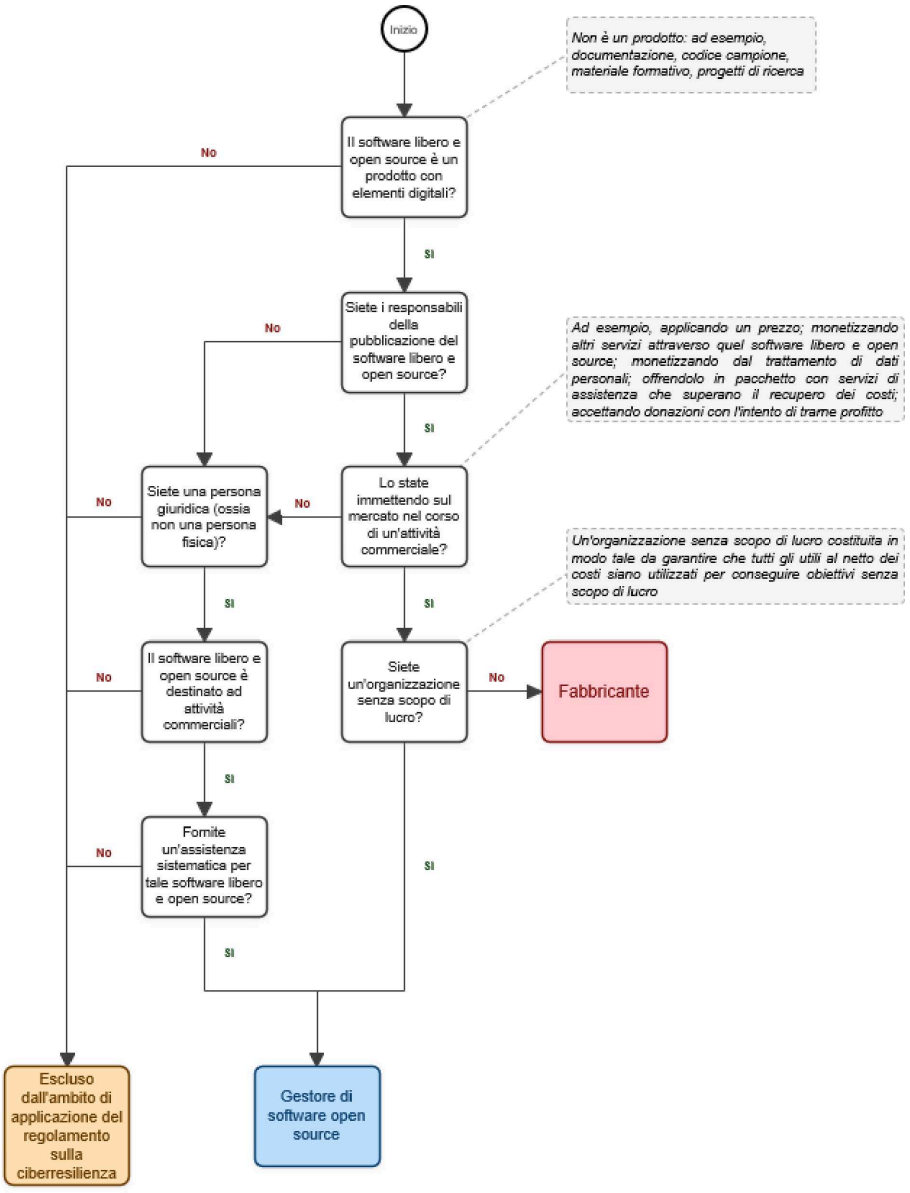
Esempio 34: uno sviluppatore indipendente pubblica una libreria software libera e open source in un archivio pubblico di pacchetti per un determinato linguaggio di programmazione e la mantiene attivamente. Nella documentazione del pacchetto, lo sviluppatore aggiunge un link per raccogliere le donazioni. Un fabbricante scarica gratuitamente tale libreria dall'archivio e la integra nel proprio prodotto con elementi digitali.

Lo sviluppatore indipendente e l'archivio dei pacchetti non hanno alcun obbligo ai sensi del regolamento sulla ciberresilienza. Il fabbricante che integra la libreria deve esercitare la dovuta diligenza conformemente all'articolo 13, paragrafo 5.

([15]) A meno che la società A non sia un soggetto senza scopo di lucro costituito in modo tale da garantire che tutti gli utili al netto dei costi siano utilizzati per conseguire obiettivi senza scopo di lucro, nel qual caso sarebbe il gestore di tale software libero e open source.

Figura 1

diagramma di flusso stilizzato relativo all'ambito di applicazione del regolamento sulla ciberresilienza in relazione ai software liberi e open source



4. **MODIFICHE SOSTANZIALI E PEZZI DI RICAMBIO**

90. L'articolo 3, punto 30), del regolamento sulla ciberresilienza definisce una «modifica sostanziale» come una modifica del prodotto con elementi digitali a seguito della sua immissione sul mercato, i) che incide sulla conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, parte I; o ii) che comporta una modifica della finalità prevista per la quale il prodotto con elementi digitali è stato valutato.

91. La nozione di modifica sostanziale è pertinente per l'accertamento degli obblighi previsti dal regolamento sulla ciberresilienza in una serie di casi, tra cui i seguenti:

a) ai sensi dell'articolo 21, un importatore o distributore che apporti una modifica sostanziale a un prodotto con elementi digitali già immesso sul mercato è considerato il suo fabbricante;

b) ai sensi dell'articolo 22, qualsiasi persona fisica o giuridica che apporti una modifica sostanziale a un prodotto con elementi digitali e metta tale prodotto a disposizione sul mercato è considerata il suo fabbricante;

c) ai sensi dell'articolo 69, paragrafo 2, qualsiasi persona fisica o giuridica che apporti una modifica sostanziale dopo l'11 dicembre 2027 a un prodotto con elementi digitali immesso sul mercato prima dell'11 dicembre 2027 e immetta tale prodotto sul mercato è considerata il suo fabbricante;

d) per i fabbricanti di prodotti con elementi digitali immessi sul mercato dopo l'11 dicembre 2027, al fine di determinare se un prodotto con elementi digitali debba essere sottoposto a una nuova procedura di valutazione della conformità a causa di modifiche apportate dopo tale data, in particolare alla luce della natura iterativa dello sviluppo di software.

92. È pertanto importante fornire orientamenti per aiutare gli operatori economici a comprendere quando le modifiche dell'hardware o del software si qualificano come modifiche sostanziali.

4.1. **Riparazioni fisiche**

93. Come indicato al considerando 42 del regolamento sulla ciberresilienza, «[s]e un prodotto con elementi digitali è soggetto a "ricondizionamento", "manutenzione" e "riparazione" quali definiti all'articolo 2, punti 18), 19) e 20), del regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio, ciò non comporta necessariamente una modifica sostanziale del prodotto, ad esempio se la finalità e le funzionalità previste non sono modificate e il livello di rischio rimane inalterato. Tuttavia il miglioramento di un prodotto con elementi digitali da parte del fabbricante potrebbe comportare modifiche nella progettazione e nello sviluppo del prodotto stesso e quindi influire sulla sua finalità prevista e sulla sua conformità ai requisiti stabiliti nel presente regolamento». Ciò è coerente con la sezione 2.1 della guida blu, che ricorda che «[i] prodotti che abbiano subito modifiche o trasformazioni consistenti dopo essere stati messi in servizio si devono considerare alla stregua di prodotti nuovi se: i) le prestazioni, la finalità o il tipo originari sono modificati, senza che ciò sia previsto nella valutazione dei rischi iniziale; ii) la natura del pericolo è cambiata o il livello di rischio è aumentato con riferimento alla pertinente normativa di armonizzazione dell'Unione; e iii) il prodotto è reso disponibile (o messo in servizio se la normativa applicabile include la messa in servizio nel proprio campo di applicazione). La situazione deve essere valutata caso per caso e in particolare alla luce degli obiettivi della normativa e del tipo di prodotti disciplinati dalla normativa in questione».

94. Le operazioni di ricondizionamento, manutenzione o riparazione che comportano modifiche fisiche di prodotti con elementi digitali già immessi sul mercato non costituiscono necessariamente modifiche sostanziali. È pertanto opportuno effettuare una valutazione caso per caso per accertare se tale modifica fisica incida sulla conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, parte I, o comporti una modifica della finalità prevista del prodotto contemplata dalla valutazione dei rischi di cibersicurezza.

95. La sostituzione di pezzi difettosi o usurati con pezzi che funzionano meglio (ad esempio a causa del progresso tecnico o perché il pezzo vecchio non è più in produzione) non comporta di per sé una modifica sostanziale del prodotto con elementi digitali riparato. Ciò si verifica solo se la modifica delle prestazioni o del funzionamento del prodotto con elementi digitali riparato i) incide sulla sua conformità ai requisiti essenziali o ii) comporta una modifica della finalità prevista che non era stata contemplata dalla valutazione dei rischi.

Esempio 35: il fabbricante di un server informatico esegue un intervento di riparazione, sostituendo una memoria RAM difettosa con una nuova dalle prestazioni migliori. La conformità del server ai requisiti essenziali non è pregiudicata. Il server funziona meglio, ma le sue nuove prestazioni rimangono nell'ambito dell'uso previsto del server, come considerato nella valutazione dei rischi di cibersicurezza. Il server informatico non è considerato modificato in modo sostanziale.

4.2. **Pezzi di ricambio**

96. L'articolo 2, paragrafo 6, del regolamento sulla ciberresilienza stabilisce che i pezzi di ricambio destinati a sostituire componenti identici e fabbricati secondo le stesse specifiche di tali componenti non sono soggetti al regolamento sulla ciberresilienza. Al considerando 29 si afferma altresì che l'esenzione riguarda sia i pezzi di ricambio per prodotti con elementi digitali messi a disposizione prima dell'entrata in applicazione del regolamento sulla ciberresilienza, sia i pezzi di ricambio che sono già stati sottoposti a una procedura di valutazione della conformità ai sensi del regolamento.

97. L'esenzione di cui all'articolo 2, paragrafo 6, del regolamento sulla ciberresilienza dovrebbe essere intesa come applicabile soltanto nei casi in cui il pezzo di ricambio sia fornito specificamente allo scopo di riparazione o di estensione della durabilità di un prodotto con elementi digitali già immesso sul mercato (prima o dopo l'11 dicembre 2027). Un prodotto con elementi digitali, se fornito come prodotto autonomo, senza alcun collegamento con la manutenzione o la riparazione di un prodotto con elementi digitali preesistente, è immesso sul mercato ai sensi del regolamento sulla ciberresilienza e non dovrebbe essere considerato un pezzo di ricambio rientrante nell'ambito di applicazione dell'articolo 2, paragrafo 6. La finalità di manutenzione o riparazione dovrebbe risultare evidente dal contesto della fornitura, ad esempio attraverso l'identificazione del prodotto con elementi digitali o della famiglia di prodotti nell'ordine o nell'offerta commerciale, oppure attraverso la fornitura tramite canali post-vendita o di servizio. È altresì opportuno tenere a disposizione delle autorità di vigilanza del mercato i documenti giustificativi a tal riguardo. In assenza di tali elementi, il fatto che un prodotto con elementi digitali possa tecnicamente essere utilizzato per sostituire un componente non è di per sé sufficiente a farlo rientrare nell'ambito di applicazione dell'esenzione.

98. Di conseguenza, laddove un pezzo di ricambio sia identico a un componente già incluso in un prodotto con elementi digitali immesso sul mercato prima della data di applicazione del regolamento sulla ciberresilienza oppure immesso sul mercato conformemente a tale regolamento, tale pezzo di ricambio non è di per sé soggetto al regolamento sulla ciberresilienza.

99. La valutazione volta a stabilire se un pezzo di ricambio debba essere considerato identico a un componente dovrebbe concentrarsi sulla funzione svolta nel prodotto con elementi digitali e sulle caratteristiche che possono essere pertinenti per la cibersicurezza. Sebbene sia sempre necessaria una valutazione caso per caso, le differenze che non incidono sulle caratteristiche di sicurezza o sul profilo di rischio di cibersicurezza del componente non impediscono, di per sé, che tale pezzo di ricambio rientri nell'ambito di applicazione dell'articolo 2, paragrafo 6, del regolamento sulla ciberresilienza.

100. Per contro, differenze nelle caratteristiche pertinenti per la cibersicurezza del componente, quali algoritmi, protocolli, meccanismi crittografici, funzioni di controllo degli accessi o altre caratteristiche rilevanti per la sicurezza, possono far sì che il pezzo nuovo non possa essere considerato identico al componente che è destinato a sostituire.

101. Se un pezzo di ricambio non è identico al componente originale, tale pezzo di ricambio costituisce un prodotto con elementi digitali a sé stante ed è pertanto soggetto al regolamento sulla ciberresilienza. In tali casi, la conformità ai requisiti essenziali deve essere valutata alla luce della finalità prevista del componente di ricambio. Di particolare rilevanza è la funzione del componente di ricambio volta a garantire la compatibilità o l'interoperabilità con un prodotto con elementi digitali esistente, anche nel caso in cui il prodotto in questione sia un prodotto con elementi digitali immesso sul mercato prima dell'entrata in applicazione del regolamento sulla ciberresilienza. Qualora determinati requisiti essenziali non possano ragionevolmente essere soddisfatti a causa di tale finalità prevista o di vincoli tecnici, il fabbricante deve tenerne conto nella valutazione dei rischi di cibersicurezza e attuare adeguate misure alternative o compensative di attenuazione dei rischi, al fine di non compromettere la sicurezza del prodotto con elementi digitali. Come illustrato anche nella sezione *2.6 Sistemi complessi*, sia la documentazione tecnica che le informazioni e le istruzioni per l'utilizzatore svolgono un ruolo fondamentale nel descrivere in modo trasparente i vincoli individuati, i rischi di cibersicurezza associati e le misure di attenuazione dei rischi messe in atto. Come spiegato nella sezione *4.1 Riparazioni fisiche*, la sostituzione di pezzi difettosi o usurati con pezzi che funzionano meglio non comporta di per sé una modifica sostanziale del prodotto con elementi digitali riparato.

Esempio 36: un fabbricante ha immesso sul mercato dell'UE dispositivi di controllo connessi. In un caso il dispositivo di controllo è stato immesso sul mercato nel 2026, prima della data di applicazione del regolamento sulla ciberresilienza. In un altro caso il dispositivo di controllo è stato immesso sul mercato nel 2028, a norma del regolamento sulla ciberresilienza. Nel 2028 un modulo di comunicazione digitale in entrambi i dispositivi si guasta. Il fabbricante fornisce come pezzo di ricambio un modulo sostitutivo identico e fabbricato secondo le stesse specifiche dell'originale.

In entrambi i casi il modulo sostitutivo rientra nell'ambito di applicazione dell'esenzione di cui all'articolo 2, paragrafo 6. Il pezzo di ricambio non è di per sé soggetto al regolamento sulla ciberresilienza, anche se si tratta di un prodotto con elementi digitali, in quanto sostituisce un componente identico in un prodotto con elementi digitali. La riparazione non costituisce una modifica sostanziale del prodotto con elementi digitali.

Esempio 37: un fabbricante ha immesso sul mercato dell'UE un dispositivo di controllo industriale connesso nel 2026, prima della data di applicazione del regolamento sulla ciberresilienza. Nel 2028 un chip di comunicazione del dispositivo si guasta. Il fabbricante, poiché non produce più tale chip, fornisce come pezzo di ricambio un chip più recente con funzionalità equivalenti, ma con un'implementazione crittografica diversa e un meccanismo di avvio sicuro aggiornato, al fine di mantenere la compatibilità e il funzionamento continuo.

In questo caso il chip sostitutivo non può essere considerato identico, in quanto le differenze nell'implementazione crittografica e nel meccanismo di avvio sicuro incidono sulle sue proprietà di cibersicurezza. Non beneficia pertanto dell'esenzione di cui all'articolo 2, paragrafo 6, e costituisce un prodotto con elementi digitali soggetto al regolamento sulla ciberresilienza. La conformità del pezzo di ricambio deve essere valutata alla luce della sua finalità prevista, compresa la sua funzione nel garantire l'interoperabilità con il prodotto con elementi digitali immesso sul mercato prima dell'entrata in applicazione del regolamento sulla ciberresilienza.

Esempio 38: nel 2028 un fabbricante immette sul mercato un dispositivo di controllo intelligente per l'edilizia in conformità con il regolamento sulla ciberresilienza. Nel 2029 il modulo senza fili di tale dispositivo si guasta. Il fabbricante, poiché non produce più tale modulo, fornisce come pezzo di ricambio un nuovo modulo che svolge la stessa funzione utilizzando gli stessi protocolli di comunicazione e gli stessi meccanismi di sicurezza, ma che è basato su un chipset diverso ed è dotato di un firmware aggiornato che non altera caratteristiche che possono essere pertinenti per la cibersicurezza.

In questo caso il modulo sostitutivo può essere considerato identico. Il modulo beneficia pertanto dell'esenzione di cui all'articolo 2, paragrafo 6, e non è soggetto al regolamento sulla ciberresilienza.

102. L'esenzione per i pezzi di ricambio si applica indipendentemente dal fatto che il pezzo di ricambio sostituisca un componente all'interno di un prodotto con elementi digitali o che sostituisca un prodotto completo con elementi digitali che a sua volta fa parte di un prodotto più grande, anche nel caso in cui tale prodotto con elementi digitali più grande sia composto da più componenti integrati, a condizione che il pezzo di ricambio sia fornito specificamente come pezzo di ricambio, come spiegato ai punti precedenti.

Esempio 39: nel 2027 un fabbricante immette sul mercato un sistema di automazione industriale che incorpora tra i suoi componenti un controllore logico programmabile (PLC). Nel 2031 l'unità centrale di elaborazione (CPU) del PLC si guasta. Il fabbricante offre due opzioni di riparazione: i) la fornitura di un'unità CPU sostitutiva che può essere considerata identica alla CPU originariamente installata; o ii) la fornitura di un PLC sostitutivo completo che può essere considerato identico al PLC originariamente installato. In ogni caso, la sostituzione è fornita attraverso il canale di assistenza post-vendita del fabbricante sotto forma di pezzo di ricambio e il sistema di automazione industriale cui è destinata la sostituzione è chiaramente identificato. In entrambi i casi la sostituzione rientra nell'ambito di applicazione dell'esenzione di cui all'articolo 2 paragrafo 6, indipendentemente dal fatto che riguardi un componente all'interno del PLC o il PLC nel suo complesso.

4.3. **Aggiornamenti del software come modifiche sostanziali**

103. Lo sviluppo di software ha una natura iterativa e i prodotti software con elementi digitali già immessi sul mercato sono aggiornati frequentemente e costantemente. In tale contesto, è utile fornire maggiori orientamenti per determinare quando il software debba essere considerato modificato in modo sostanziale. Tali orientamenti sono intesi in particolare ad aiutare i fabbricanti di prodotti software con elementi digitali che apportano modifiche ai propri prodotti a determinare se tali modifiche equivalgano a una modifica sostanziale.

104. Il considerando 39 precisa che un prodotto con elementi digitali è sostanzialmente modificato qualora una modifica alteri il livello di rischio di cibersicurezza e qualora tale rischio modificato o aggiuntivo non sia stato preso in considerazione dal fabbricante nella sua valutazione dei rischi e, di conseguenza, nell'attuazione dei requisiti essenziali. Il fabbricante dovrebbe pertanto valutare, caso per caso, se un aggiornamento del software introduca rischi di cibersicurezza nuovi o maggiori e se tali rischi siano già stati affrontati nella sua valutazione dei rischi.

105. Nel caso in cui introduca in un prodotto con elementi digitali nuove funzionalità che comportano una modifica della finalità prevista del prodotto nel suo complesso, è probabile che il fabbricante non abbia preso in considerazione tali modifiche nella propria valutazione dei rischi. In tali circostanze la modifica sarebbe di norma considerata una modifica sostanziale.

Esempio 40: un fabbricante immette sul mercato un pannello di controllo che raccoglie dati dalle macchine e mostra andamenti e allarmi, ma che non è in grado di controllare tali macchine. Il fabbricante sviluppa successivamente una nuova versione di tale pannello di controllo, introducendo funzionalità che consentono di controllare le macchine, anche tramite la regolazione dei parametri operativi e il riavvio delle macchine a seguito di condizioni di guasto. A seguito di tali modifiche, la finalità prevista del pannello di controllo si è evoluta al di là di quanto previsto nella valutazione dei rischi, passando da uno strumento di conoscenza situazionale a un prodotto con elementi digitali destinato a esercitare un controllo operativo su altri dispositivi. Il pannello di controllo è stato pertanto modificato in modo sostanziale.

Esempio 41: un fabbricante immette sul mercato un'applicazione software per consumatori destinata a organizzare e visualizzare dati personali, quali e-mail, messaggi o documenti, e a supportare funzioni di ricerca e filtraggio di base. Il fabbricante introduce successivamente un aggiornamento che consente all'applicazione di analizzare automaticamente i contenuti degli utilizzatori al fine di generare profili comportamentali e prendere decisioni automatizzate che influenzano la prioritizzazione, la soppressione o la raccomandazione dei contenuti senza l'intervento dell'utilizzatore. A seguito di tale modifica, la finalità prevista del software passa da uno strumento di gestione delle informazioni controllato dagli utilizzatori a un sistema decisionale automatizzato, che non era previsto nella valutazione dei rischi. L'applicazione è stata pertanto modificata in modo sostanziale.

106. Allo stesso tempo è tuttavia possibile che un fabbricante introduca progressivamente nuove funzionalità già considerate nella propria valutazione dei rischi o che, di per sé, non alterano il profilo di rischio di cibersicurezza del prodotto con elementi digitali. Ciò può verificarsi, ad esempio, nel caso in cui il fabbricante abbia previsto lo sviluppo di tali funzionalità, abbia già descritto e valutato i rischi associati e abbia attuato misure di attenuazione adeguate per garantire la costante conformità ai requisiti essenziali. È questo il caso anche quando le nuove funzionalità non comportano modifiche che introducono rischi nuovi o maggiori. Gli aggiornamenti di tale natura non dovrebbero pertanto essere considerati modifiche sostanziali, in quanto non aumentano il rischio di cibersicurezza e, di conseguenza, non modificano l'attuazione dei requisiti essenziali.

Esempio 42: un'applicazione di messaggistica è inizialmente rilasciata con funzionalità limitate alla messaggistica «one-to-one». La valutazione dei rischi del fabbricante prende in considerazione la successiva introduzione della messaggistica di gruppo, compresa ad esempio la maggiore complessità dell'instradamento dei messaggi. In un aggiornamento successivo, il fabbricante aggiunge una funzionalità di chat di gruppo, insieme a funzioni di controllo per gli amministratori e strumenti di moderazione che erano già stati previsti e valutati nella progettazione originale. L'aggiornamento implementa funzionalità che rientrano nell'ambito della finalità originariamente prevista e della valutazione dei rischi iniziale. L'applicazione di messaggistica non è stata pertanto modificata in modo sostanziale.

Esempio 43: un sistema di monitoraggio della produzione è immesso sul mercato con l'abilitazione di pannelli di controllo in sola lettura, mentre le funzionalità di controllo automatizzato, pur essendo presenti nell'architettura del sistema, rimangono disabilitate. La valutazione dei rischi del fabbricante copre esplicitamente la futura attivazione di circuiti di controllo automatizzati, compresi i rischi di cibersicurezza associati al controllo a circuito chiuso, nonché misure di protezione quali i meccanismi di esclusione manuale e stati di sicurezza in caso di guasto (fail-safe). In un aggiornamento successivo il fabbricante abilita le funzioni di controllo automatizzato e attiva le misure di protezione come inizialmente valutate. Il sistema di controllo della produzione non è stato pertanto modificato in modo sostanziale.

107. Per contro, nuove funzionalità anche limitate o apparentemente minori possono introdurre rischi significativi di cibersicurezza che incidono sulla conformità ai requisiti essenziali. La valutazione del carattere sostanziale di una modifica non dovrebbe pertanto basarsi sulla portata o sulla complessità della modifica stessa, bensì sul suo potenziale impatto negativo sul profilo di rischio di cibersicurezza del prodotto con elementi digitali e di conseguenza sull'attuazione dei requisiti essenziali.

Esempio 44: un fabbricante introduce un aggiornamento a un'applicazione software che aggiunge una funzione «ricordami» o una funzionalità di login permanente che memorizza localmente i token di autenticazione a fini di una maggiore praticità per gli utilizzatori. Sebbene sia di entità limitata, la funzionalità introduce nuovi rischi connessi al furto di token, all'accesso non autorizzato e al dirottamento di sessione che non sono stati presi in considerazione nella valutazione dei rischi. L'aggiornamento incide pertanto sulla conformità ai requisiti essenziali. L'applicazione software è stata modificata in modo sostanziale.

Esempio 45: un fabbricante aggiunge una nuova funzionalità di registrazione e diagnostica a un prodotto software con elementi digitali esistente, che consente l'esportazione di log dettagliati del sistema a fini di risoluzione dei problemi. Sebbene appaia minore, la funzionalità comporta la raccolta e la conservazione di dati operativi sensibili in un formato non criptato, introducendo rischi di esposizione dei dati che non erano stati precedentemente valutati o attenuati. La modifica può pertanto avere un impatto significativo sul profilo di rischio di cibersicurezza del prodotto con elementi digitali. Il prodotto software con elementi digitali è stato modificato in modo sostanziale.

108. In linea con il considerando 39 del regolamento sulla ciberresilienza, gli aggiornamenti di sicurezza non devono essere generalmente considerati modifiche sostanziali, in quanto il loro scopo principale è ridurre il livello di rischio di cibersicurezza associato al prodotto con elementi digitali. Un aggiornamento di sicurezza che non modifica la finalità prevista di tale prodotto e non introduce nuovi rischi di cibersicurezza non dovrebbe pertanto essere considerato una modifica sostanziale, anche se tale aggiornamento può introdurre modifiche tecniche significative. Ciò comprende il caso in cui determinate funzionalità siano modificate o limitate al solo scopo di attenuare le vulnerabilità individuate e garantire la costante conformità ai requisiti essenziali.

Esempio 46: un fabbricante implementa un aggiornamento di sicurezza per affrontare una vulnerabilità nella base di codice di un prodotto con elementi digitali correggendo un errore di convalida dell'input che potrebbe determinare un sovraccarico del buffer o correggendo un difetto logico che consente di aggirare l'autenticazione attraverso una convalida impropria del token di sessione. L'aggiornamento modifica l'implementazione interna del software senza influire sulla finalità prevista né introdurre nuove vulnerabilità. Tale aggiornamento è inteso esclusivamente a ridurre il rischio di cibersicurezza. L'aggiornamento di sicurezza non dovrebbe essere considerato una modifica sostanziale.

Esempio 47: un fabbricante introduce un aggiornamento di sicurezza che rafforza le configurazioni di sicurezza esistenti, ad esempio rendendo più rigorose le regole del firewall, disattivando le porte di rete inutilizzate, modificando le politiche predefinite in materia di password dell'amministratore o rendendo obbligatoria l'autenticazione a più fattori qualora tale funzionalità fosse già disponibile o prevista. Sebbene possa incidere sul modo in cui gli utilizzatori configurano il prodotto con elementi digitali o vi accedono, l'aggiornamento non ne altera la finalità prevista e serve unicamente a rafforzarne la postura di sicurezza. L'aggiornamento di sicurezza non dovrebbe essere considerato una modifica sostanziale.

Esempio 48: un fabbricante immette sul mercato un prodotto software con elementi digitali che garantisce la sicurezza delle comunicazioni tramite un sistema di cifratura configurabile che supporta diversi algoritmi crittografici e diverse dimensioni delle chiavi, come descritto nella documentazione tecnica e nella valutazione dei rischi del prodotto. La valutazione dei rischi copre tutte le opzioni crittografiche offerte dal prodotto con elementi digitali e prevede la futura deprecazione di determinati algoritmi. La valutazione dei rischi comprende anche misure di attenuazione, quali l'agilità crittografica, la gestione delle chiavi interne e prove di compatibilità. In seguito a nuovi orientamenti in materia di crittografia, il fabbricante implementa un aggiornamento di sicurezza che disabilita un algoritmo predefinito deprecato e attiva un'alternativa più forte e già supportata, senza introdurre nuove dipendenze esterne o alterare i flussi di dati. Poiché l'aggiornamento attua una misura di sicurezza prevista e valutata nell'ambito della progettazione iniziale e non introduce nuovi rischi di cibersicurezza, l'aggiornamento di sicurezza non dovrebbe essere considerato una modifica sostanziale.

109. Per contro, un aggiornamento di sicurezza può essere considerato una modifica sostanziale se, pur avendo come obiettivo la sicurezza, determina una modifica della finalità prevista del prodotto con elementi digitali al di là di quanto inizialmente previsto o introduce rischi di cibersicurezza nuovi o maggiori. Ciò può verificarsi, ad esempio, quando un aggiornamento modifica sostanzialmente il perimetro o la struttura di dipendenza di tale prodotto in un modo non previsto nella valutazione dei rischi, ad esempio alterando in misura significativa i flussi di dati o aggiungendo nuove interfacce accessibili dall'esterno.

Esempio 49: un fabbricante immette sul mercato un prodotto software con elementi digitali destinato a garantire la cifratura locale dei file memorizzati sul dispositivo di un utilizzatore, che consente agli utilizzatori di criptare e decriptare i file a richiesta. A seguito della scoperta di una vulnerabilità nel flusso di lavoro di cifratura, il fabbricante implementa un aggiornamento di sicurezza che elimina la funzionalità di cifratura locale e prevede invece che tutti i file vengano caricati, archiviati ed elaborati da un servizio di cifratura da remoto gestito dal fabbricante stesso. A seguito di tale modifica, il prodotto con elementi digitali non esegue più la cifratura locale come originariamente previsto, ma funziona come un servizio di cifratura ed elaborazione dati da remoto. Sebbene introdotto per motivi di sicurezza, l'aggiornamento modifica radicalmente la finalità prevista del prodotto in un modo non previsto nella valutazione dei rischi e si configura pertanto come una modifica sostanziale.

Esempio 50: un fabbricante immette sul mercato un prodotto software con elementi digitali che utilizza un protocollo di cifratura consolidato e un ciclo di vita delle chiavi gestito internamente per garantire la sicurezza delle comunicazioni tra i componenti del prodotto con elementi digitali. In seguito all'individuazione di nuove vulnerabilità crittografiche, il fabbricante introduce un aggiornamento di sicurezza che sostituisce il meccanismo di cifratura esistente con un protocollo diverso che richiede l'uso di un servizio esterno di gestione delle chiavi gestito da terzi. A seguito di tale modifica, le dipendenze e i flussi di dati del prodotto con elementi digitali risultano sostanzialmente alterati, con l'introduzione di nuove interfacce esterne e il ricorso a servizi di terzi non considerati nella valutazione dei rischi. Sebbene sia orientato alla sicurezza, l'aggiornamento introduce nuovi rischi di cibersicurezza e si configura pertanto come una modifica sostanziale.

110. Come indicato al punto 104, la questione se un aggiornamento del software costituisca una modifica sostanziale dovrebbe essere valutata caso per caso. Nell'effettuare tale valutazione, i fabbricanti possono considerare, a mero titolo esemplificativo, se l'aggiornamento del software:

a) introduce nuovi vettori di minacce, quali interfacce aggiuntive, canali di comunicazione, ambienti di esecuzione o dipendenze esterne attraverso i quali potrebbero concretizzarsi eventuali minacce;

b) rende possibili nuovi scenari di attacco, compresi ad esempio nuovi modi in cui potrebbero plausibilmente verificarsi accessi non autorizzati, manipolazioni, interferenze o usi impropri del prodotto con elementi digitali o dei dati da esso elaborati;

c) modifica la probabilità che si verifichino scenari di attacco precedentemente individuati, ad esempio riducendo gli sforzi o le competenze necessari per sfruttarli, aumentando l'esposizione ad attori non fidati o indebolendo le misure di protezione esistenti;

d) modifica il potenziale impatto di scenari di attacco precedentemente individuati, comprese ad esempio la portata dei dati o delle funzioni interessati, la gravità delle conseguenze operative, economiche o di sicurezza o la capacità di rilevare un incidente, contenerlo o riprendersi da esso.

111. In alcuni casi un aggiornamento del software non introduce nuovi vettori di minacce, non consente nuovi scenari di attacco e non modifica in modo sostanziale la probabilità o l'impatto di scenari di attacco precedentemente individuati. Ciò può indicare che l'aggiornamento non introduce nuovi o maggiori rischi di cibersicurezza, a condizione che le i presupposti e le misure di attenuazione su cui si basa la valutazione dei rischi rimangano validi ed efficaci. È pertanto probabile che l'aggiornamento non si configuri come una modifica sostanziale.

112. Per contro, un aggiornamento del software potrebbe introdurre nuovi vettori di minacce, rendere possibili nuovi scenari di attacco o alterare in modo sostanziale la probabilità o l'impatto degli scenari di attacco esistenti. In tali casi il fabbricante dovrebbe effettuare una nuova valutazione dei rischi di cibersicurezza del prodotto con elementi digitali e determinare se i requisiti essenziali continuino a essere soddisfatti, nonché se l'aggiornamento introduca rischi nuovi o maggiori non previsti nella valutazione dei rischi.

113. Il fatto che un aggiornamento del software possa essere considerato o meno una modifica sostanziale è rilevante ai fini della determinazione dell'applicabilità di determinati obblighi previsti dal regolamento sulla ciberresilienza, come indicato al punto 91. Tuttavia, a prescindere da tale considerazione, i fabbricanti restano responsabili di garantire la sicurezza degli aggiornamenti del software e del proprio prodotto con elementi digitali durante il periodo di assistenza, conformemente ai requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II, del regolamento sulla ciberresilienza. Inoltre, indipendentemente dal fatto che gli aggiornamenti del software costituiscano o meno modifiche sostanziali, i fabbricanti sono tenuti a provvedere affinché la valutazione dei rischi e la documentazione tecnica siano accurate, complete e costantemente aggiornate, in conformità dell'articolo 13, paragrafo 7, e dell'articolo 31, paragrafo 2.

4.4. **Conseguenze di una modifica sostanziale**

114. Le conseguenze di una modifica sostanziale effettuata da un soggetto diverso dal fabbricante originario di un prodotto con elementi digitali già immesso sul mercato sono trattate agli articoli 21 e 22 del regolamento sulla ciberresilienza. L'articolo 21 riguarda gli importatori e i distributori, mentre l'articolo 22 riguarda qualsiasi persona fisica o giuridica diversa dal fabbricante, dall'importatore o dal distributore.

115. Se la modifica sostanziale è effettuata dal fabbricante originario del prodotto con elementi digitali, le conseguenze derivano dal concetto generalmente riconosciuto di modifica sostanziale di cui al considerando 41 del regolamento sulla ciberresilienza e sono ulteriormente esaminate nella sezione 2.1 della guida blu. Tale sezione precisa che i prodotti che abbiano subito modifiche o trasformazioni significative dopo essere stati immessi sul mercato devono essere considerati alla stregua di prodotti nuovi se le prestazioni, la finalità o il tipo originari del prodotto sono stati modificati, la natura del pericolo è cambiata o il livello di rischio è aumentato e il prodotto con elementi digitali è messo a disposizione sul mercato.

116. La conseguenza generalmente riconosciuta è pertanto che, qualora una modifica di un prodotto con elementi digitali costituisca una modifica sostanziale e il prodotto con elementi digitali modificato sia messo a disposizione sul mercato, tale prodotto deve essere trattato come un prodotto con elementi digitali nuovo ai fini del regolamento sulla ciberresilienza. Di conseguenza, l'atto di mettere a disposizione sul mercato il prodotto modificato in modo sostanziale costituisce una nuova immissione sul mercato. Ciò vale indipendentemente dal fatto che la modifica sostanziale sia apportata dal fabbricante originario o da un altro soggetto. Al fine di garantire che il regolamento sulla ciberresilienza sia applicato in modo uniforme e proporzionato alle diverse categorie di soggetti che possono apportare una modifica sostanziale, nelle sottosezioni seguenti sono illustrati gli obblighi conseguenti a carico della persona che apporta la modifica sostanziale quando il prodotto con elementi digitali modificato in modo sostanziale è immesso sul mercato. Le conseguenze per quanto riguarda il periodo di assistenza del prodotto con elementi digitali sono trattate nella sezione 5 *Periodo di* assistenza.

4.4.1. *Modifiche sostanziali apportate da un soggetto diverso dal fabbricante originario*

117. A norma degli articoli 21 e 22, qualora una modifica sostanziale di un prodotto con elementi digitali già immesso sul mercato sia apportata da una persona fisica o giuridica diversa dal fabbricante del prodotto con elementi digitali, il soggetto che apporta la modifica sostanziale e mette a disposizione sul mercato il prodotto con elementi digitali modificato deve essere considerato il fabbricante del prodotto con elementi digitali modificato, indipendentemente dal fatto che tale soggetto abbia preso parte alla progettazione o all'immissione sul mercato originarie di tale prodotto.

118. L'articolo 22 chiarisce inoltre che la persona che apporta la modifica è soggetta agli obblighi di cui agli articoli 13 e 14 solo in relazione alla parte del prodotto con elementi digitali interessata dalla modifica sostanziale, se tale modifica non incide sulla cibersicurezza del prodotto con elementi digitali nel suo complesso.

119. Se una modifica sostanziale incide sulla conformità ai requisiti essenziali ma non incide negativamente sulla cibersicurezza del prodotto con elementi digitali nel suo complesso, il soggetto che effettua la modifica è soggetto agli articoli 13 (compreso l'obbligo di garantire la conformità ai requisiti essenziali e di eseguire una procedura di valutazione della conformità) e 14 (obblighi di segnalazione) solo in relazione alla parte del prodotto con elementi digitali che è stata modificata in modo sostanziale ([16]). Inoltre gli obblighi del fabbricante originario a norma del regolamento sulla ciberresilienza continuano ad applicarsi al prodotto con elementi digitali originario immesso sul mercato, garantendo la continuità nella gestione delle vulnerabilità e la conformità per le parti invariate.

120. Un caso di modifica sostanziale non dovrebbe essere confuso con i casi di integrazione, in cui un soggetto assembla componenti (anche, se del caso, modificandoli) in un nuovo prodotto con elementi digitali che immette esso stesso sul mercato. In tali casi l'integratore non sta modificando un prodotto con elementi digitali già immesso sul mercato da un altro fabbricante; sta piuttosto immettendo sul mercato un nuovo prodotto con elementi digitali. L'integratore è il fabbricante di tale nuovo prodotto con elementi digitali ai fini del regolamento sulla ciberresilienza ed è tenuto a rispettare il regolamento nella sua interezza per quanto riguarda il prodotto con elementi digitali nel suo complesso. Qualora integri componenti soggetti al regolamento sulla ciberresilienza, il fabbricante può avvalersi delle attività relative alla conformità svolte dai fabbricanti dei componenti per facilitare la propria conformità al regolamento sulla ciberresilienza.

Esempio 51: una società acquista da fornitori terzi moduli di microcontrollori e componenti di connettività pronti all'uso, sviluppa firmware proprietari e un pacchetto di sensori e li assembla in un prodotto con elementi digitali connesso per il monitoraggio agricolo, che immette sul mercato a proprio nome. Sebbene abbia modificato i moduli di microcontrollori sottostanti e li abbia combinati con altri componenti, la società non sta modificando in modo sostanziale un prodotto con elementi digitali già immesso sul mercato; sta piuttosto immettendo sul mercato un nuovo prodotto con elementi digitali. La società è il fabbricante del sistema di monitoraggio agricolo ai fini del regolamento sulla ciberresilienza ed è tenuta a rispettare il regolamento per quanto riguarda il sistema di monitoraggio agricolo nel suo complesso.

([16]) In linea con la sezione 2.1 della guida blu «[n]on occorre ripetere prove e produrre nuova documentazione in relazione ad aspetti che non hanno risentito della modifica. Spetta alla persona fisica o giuridica che apporta o fa apportare modifiche al prodotto dimostrare che non occorre aggiornare tutti gli elementi della documentazione tecnica. La persona fisica o giuridica che apporta o fa apportare modifiche al prodotto è responsabile della conformità del prodotto modificato e deve redigere una dichiarazione di conformità, anche se utilizza prove e documentazione tecnica già esistenti».

121. Se una modifica sostanziale effettuata da un soggetto diverso dal fabbricante originario incide negativamente sulla cibersicurezza del prodotto con elementi digitali nel suo complesso, ad esempio perché non si tratta più di una modifica mirata o limitata a un componente o sottosistema specifico, il prodotto con elementi digitali modificato messo a disposizione sul mercato dovrebbe essere trattato come un prodotto con elementi digitali nuovo soggetto al regolamento sulla ciberresilienza. In tali casi il profilo generale di rischio di cibersicurezza di tale prodotto è cambiato e la modifica non può essere valutata senza considerare il prodotto con elementi digitali nel suo complesso. Il soggetto che effettua la modifica è tenuto ad adempiere agli obblighi del fabbricante di cui agli articoli 13 e 14 in relazione al prodotto con elementi digitali modificato nel suo complesso.

4.4.2. *Modifiche sostanziali apportate dal fabbricante originario*

122. Se la modifica sostanziale è apportata dal fabbricante originario, anche nel contesto dello sviluppo iterativo di prodotti software con elementi digitali, tale fabbricante rimane il fabbricante ai fini del regolamento sulla ciberresilienza. Tuttavia il prodotto con elementi digitali modificato in modo sostanziale deve essere considerato alla stregua di un nuovo prodotto immesso sul mercato.

123. Conformemente alla sezione 2.1 della guida blu, il fabbricante originario che immette sul mercato prodotti con elementi digitali modificati in modo sostanziale può riutilizzare la documentazione e le prove esistenti per aspetti del prodotto con elementi digitali che non hanno risentito della modifica sostanziale. In particolare se il fabbricante immette sul mercato versioni modificate in modo sostanziale dello stesso prodotto con elementi digitali, la procedura di valutazione della conformità dovrebbe concentrarsi sulle parti del prodotto con elementi digitali modificate in modo sostanziale. Allo stesso modo, qualora sia effettuata una valutazione della conformità da parte di terzi, l'organismo di valutazione della conformità dovrebbe concentrare la propria valutazione sulle parti modificate in modo sostanziale. Per le parti del prodotto con elementi digitali rimaste invariate, può riutilizzare la documentazione e i risultati delle prove esistenti.

124. Le considerazioni relative alla proporzionalità di cui alla sottosezione precedente si applicano anche alle modifiche sostanziali effettuate dal fabbricante originario di un prodotto con elementi digitali immesso sul mercato prima dell'11 dicembre 2027. In questo caso l'apporto di una modifica sostanziale da parte del fabbricante originario non comporta di per sé l'obbligo per quest'ultimo di rendere l'intero prodotto con elementi digitali immesso sul mercato prima di tale data pienamente conforme al regolamento sulla ciberresilienza, a meno che la modifica non incida negativamente sulla cibersicurezza del prodotto con elementi digitali nel suo complesso. Se la modifica non incide sulla cibersicurezza del prodotto con elementi digitali nel suo complesso, gli obblighi del fabbricante originario in relazione alla modifica dovrebbero essere limitati alle parti modificate in modo sostanziale.

5. **PERIODO DI ASSISTENZA**

125. L'articolo 13, paragrafo 8, del regolamento sulla ciberresilienza impone ai fabbricanti di determinare il periodo di assistenza durante il quale le vulnerabilità del prodotto, compresi i suoi componenti, sono gestite in modo efficace e in conformità dei requisiti essenziali di cibersicurezza di cui all'allegato I, parte II. Il periodo di assistenza riflette il periodo di tempo durante il quale si prevede che il prodotto con elementi digitali sarà in uso (la durata di utilizzo prevista) e dovrebbe essere determinato tenendo conto dei criteri di cui all'articolo 13, paragrafo 8, in particolare delle ragionevoli aspettative degli utilizzatori, della natura del prodotto con elementi digitali, compresa la sua finalità prevista, nonché del pertinente diritto dell'Unione che determina la durata di vita dei prodotti con elementi digitali ([17]). Nel complesso, tali criteri devono essere presi in considerazione in modo da garantire la proporzionalità nella determinazione del periodo di assistenza.

([17]) Tra gli ulteriori criteri che possono essere presi in considerazione a norma dell'articolo 13, paragrafo 8, figurano i periodi di assistenza dei prodotti con elementi digitali che offrono funzionalità analoghe immessi sul mercato da altri fabbricanti, la disponibilità dell'ambiente operativo, i periodi di assistenza dei componenti integrati che forniscono funzioni essenziali e che provengono da terzi, nonché gli orientamenti pertinenti forniti dall'apposito gruppo di cooperazione amministrativa (ADCO) istituito a norma del regolamento sulla ciberresilienza e dalla Commissione.

126. L'articolo 13, paragrafo 8, prevede inoltre che il periodo di assistenza sia di almeno cinque anni, a meno che non si preveda che il prodotto con elementi digitali sarà utilizzato per meno di cinque anni, nel qual caso il periodo di assistenza corrisponderà alla durata di utilizzo prevista. Il periodo minimo di assistenza funge quindi soltanto da misura di salvaguardia, garantendo che le vulnerabilità siano gestite per un periodo sufficientemente lungo, consentendo nel contempo ai fabbricanti di tenere conto dei prodotti con elementi digitali con durate di utilizzo previste effettivamente più brevi. Il considerando 60 fornisce maggiori orientamenti al riguardo, chiarendo che i prodotti con elementi digitali che si prevede ragionevolmente rimarranno in uso per più di cinque anni dovrebbero di conseguenza avere periodi di assistenza più lunghi. Non si dovrebbe pertanto considerare un periodo di assistenza predefinito di cinque anni per tutti i prodotti con elementi digitali. Il fabbricante dovrebbe invece determinare il periodo di assistenza adeguato alla luce dei criteri di cui all'articolo 13, paragrafo 8.

127. L'articolo 13, paragrafo 19, impone ai fabbricanti di indicare in modo chiaro e comprensibile la data finale del periodo di assistenza (almeno il mese e l'anno) al momento dell'acquisto. Impone inoltre ai fabbricanti, ove tecnicamente fattibile alla luce della natura del prodotto con elementi digitali, di inviare una notifica agli utilizzatori alla scadenza del periodo di assistenza. Tale obbligo è inteso a garantire la trasparenza nei confronti degli utilizzatori per quanto riguarda la durata dell'assistenza di sicurezza che possono aspettarsi.

128. Nel caso di prodotti software con elementi digitali, che sono spesso sviluppati e rilasciati in modo iterativo e per i quali, nel corso del tempo, possono essere immesse sul mercato con frequenza versioni sostanzialmente modificate, il periodo di assistenza deve essere inteso alla luce di tale modello di sviluppo. Ogni versione sostanzialmente modificata di un prodotto software con elementi digitali immessa sul mercato deve disporre di un periodo di assistenza dichiarato conforme all'articolo 13, paragrafo 8. Ciò comprende il periodo minimo di assistenza di almeno cinque anni, a meno che non sia dimostrabile che il tempo di utilizzo previsto di tale versione è più breve, come chiarito anche nel considerando 60. La sezione *5.1 Modifiche sostanziali e il periodo di* assistenza chiarisce inoltre che, se la modifica sostanziale non comporta cambiamenti nei fattori che hanno originariamente determinato la durata di utilizzo prevista del prodotto con elementi digitali, il periodo di assistenza originario rimane invariato (ossia anche nei casi in cui il restante periodo di assistenza sia inferiore a cinque anni).

129. L'articolo 13, paragrafo 10, offre un certo grado di flessibilità per i prodotti software con elementi digitali consentendo ai fabbricanti, a determinate condizioni, di garantire la conformità al requisito di gestione delle vulnerabilità di cui all'allegato I, parte II, punto 2 (affrontare e correggere le vulnerabilità), solo per l'ultima versione del prodotto software con elementi digitali immessa sul mercato. Ciò è consentito se gli utilizzatori delle versioni precedentemente immesse sul mercato hanno accesso gratuito all'ultima versione immessa sul mercato e non devono sostenere costi aggiuntivi per adeguare l'ambiente hardware e software in cui utilizzano la versione originale di tale prodotto.

130. Ai fini dell'articolo 13, paragrafo 10, il concetto di «costi aggiuntivi» dovrebbe essere interpretato in modo pratico e proporzionato, tenendo conto delle pratiche normali e previste nell'ambito della manutenzione e del funzionamento del software. Non comprende gli sforzi operativi ragionevoli inerenti all'applicazione degli aggiornamenti software o al mantenimento di un ambiente operativo sicuro, quali il tempo dedicato dal personale, le prove di routine, le modifiche alla configurazione o gli aggiornamenti delle dipendenze software sottostanti necessari per gestire i componenti giunti a fine vita o le vulnerabilità di sicurezza note. Per contro, per «costi aggiuntivi» si intendono gli oneri che vanno al di là di quanto normalmente previsto nel contesto degli aggiornamenti software, quali l'acquisto obbligatorio di nuovo hardware, la sostituzione dell'infrastruttura o modifiche fondamentali dell'ambiente operativo.

131. Per i prodotti software con elementi digitali in continua evoluzione, i fabbricanti possono immettere sul mercato versioni successive sostanzialmente modificate a intervalli relativamente brevi e aspettarsi che gli utilizzatori effettuino aggiornamenti regolari. In tali casi il periodo di assistenza dichiarato per ciascuna versione sostanzialmente modificata deve essere conforme all'articolo 13, paragrafo 8, al momento dell'immissione sul mercato. In altre parole, il fabbricante deve dichiarare un nuovo periodo di assistenza per tale versione sostanzialmente modificata. I fabbricanti possono tuttavia avvalersi dell'articolo 13, paragrafo 10, per cessare di affrontare e correggere le vulnerabilità per le versioni precedenti una volta che gli utilizzatori siano in grado di

passare a una versione successiva gratuitamente e senza incorrere nei costi aggiuntivi di cui sopra, anche se ciò si traduce in un periodo di assistenza effettivo più breve per le versioni precedenti in questione ([18]). Il fabbricante rimane soggetto agli altri requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II, nonché agli obblighi di segnalazione di cui all'articolo 14. Come spiegato anche al considerando 40, tali obblighi comprendono, tra l'altro, per tutte le successive versioni del prodotto software con elementi digitali immesso sul mercato che sono state modificate in modo sostanziale: i) il mantenimento di una politica in materia di divulgazione coordinata delle vulnerabilità; e ii) misure volte ad agevolare la condivisione di informazioni sulle potenziali vulnerabilità ([19]).

Esempio 52: un fabbricante immette sul mercato dell'UE un modello di smartphone e dichiara un periodo di assistenza di X anni dalla data di immissione sul mercato, durante il quale fornirà aggiornamenti di sicurezza volti ad affrontare le vulnerabilità. Durante tale periodo, il fabbricante rilascia aggiornamenti periodici del software e versioni sostanzialmente modificate del sistema operativo, che gli utenti possono installare gratuitamente senza bisogno di un nuovo hardware.

A norma dell'articolo 13, paragrafo 10, il fabbricante può affrontare e correggere le vulnerabilità dell'ultima versione del sistema operativo messa a disposizione per tale modello di smartphone, a condizione che le versioni precedenti possano essere aggiornate gratuitamente e senza costi aggiuntivi. Per la durata del periodo di assistenza, il fabbricante rimane soggetto agli altri requisiti di gestione delle vulnerabilità, quali la divulgazione coordinata delle vulnerabilità e le misure di condivisione delle informazioni.

Esempio 53: un fabbricante immette sul mercato un prodotto software aziendale con elementi digitali e rilascia versioni sostanzialmente modificate ogni pochi mesi, che rispecchiano miglioramenti in termini di sicurezza, nuove caratteristiche e compatibilità con sistemi operativi e piattaforme aggiornati. Ciascuna versione è immessa sul mercato con un periodo di assistenza dichiarato in conformità dell'articolo 13, paragrafo 8. Il fabbricante si aspetta che gli utilizzatori effettuino aggiornamenti regolari nell'ambito del normale funzionamento e fornisce gratuitamente l'accesso all'ultima versione. L'applicazione di aggiornamenti può richiedere uno sforzo operativo ragionevole, come prove o adeguamenti della configurazione, ma non comporta costi aggiuntivi, come l'acquisto di nuovo hardware o modifiche fondamentali dell'infrastruttura. In tale contesto, il fabbricante può avvalersi dell'articolo 13, paragrafo 10, per cessare di affrontare e correggere le vulnerabilità per le versioni precedenti una volta che gli utilizzatori possono passare all'ultima versione, continuando nel contempo a rispettare gli altri requisiti di gestione delle vulnerabilità per tutte le successive versioni modificate in modo sostanziale.

5.1. **Modifiche sostanziali e il periodo di assistenza**

132. Come indicato nella sezione *4.4 Conseguenze di una modifica sostanziale*, quando la modifica di un prodotto con elementi digitali si configura come una modifica sostanziale e il prodotto con elementi digitali modificato è messo a disposizione sul mercato, tale prodotto deve essere trattato alla stregua di un nuovo prodotto ai fini del regolamento sulla ciberresilienza e l'atto di mettere a disposizione sul mercato il prodotto con elementi digitali modificato in modo sostanziale costituisce una nuova immissione sul mercato. È pertanto utile chiarire in che modo questa nuova immissione sul mercato incida sul periodo di assistenza del prodotto con elementi digitali modificato in modo sostanziale.

133. Il periodo di assistenza di un prodotto con elementi digitali modificato in modo sostanziale dovrebbe essere determinato con riferimento alla durata di utilizzo prevista di tale prodotto, in considerazione dei criteri di cui all'articolo 13, paragrafo 8, del regolamento sulla ciberresilienza. Una modifica sostanziale dovrebbe pertanto richiedere una nuova valutazione tenendo conto di tali criteri, ma non comporta automaticamente il riavvio del periodo di assistenza né tantomeno la sua proroga. La questione rilevante è se la modifica sostanziale incida sui fattori che hanno originariamente determinato la durata di utilizzo prevista di tale prodotto e pertanto il periodo di assistenza originario.

([18]) È opportuno ricordare che l'articolo 13, paragrafo 19, impone ai fabbricanti, ove tecnicamente fattibile alla luce della natura del prodotto con elementi digitali, di inviare una notifica agli utilizzatori per informarli che il loro prodotto con elementi digitali ha raggiunto la fine del periodo di assistenza. Pertanto qualora non si provveda più ad affrontare e correggere le vulnerabilità per le versioni precedenti, è previsto che gli utilizzatori che non hanno effettuato l'aggiornamento alla versione più recente ne siano informati, se tecnicamente fattibile.

([19]) Va osservato che, qualora gli utilizzatori possano effettuare l'aggiornamento alla versione più recente del software senza costi aggiuntivi, i fabbricanti possono comunque scegliere di continuare ad affrontare e correggere le vulnerabilità nelle versioni precedenti di tale software, anche a pagamento o nell'ambito di altri accordi commerciali. Il regolamento sulla ciberresilienza non impone ai fabbricanti di fornire gratuitamente aggiornamenti di sicurezza per tali versioni precedenti.

134. Qualora la modifica sostanziale non incida su tali fattori, i criteri di cui all'articolo 13, paragrafo 8, continuano a indicare la stessa durata di utilizzo prevista inizialmente determinata e il periodo di assistenza del prodotto con elementi digitali modificato dovrebbe allinearsi alla durata di utilizzo prevista residua del prodotto originariamente immesso sul mercato. Ciò si verifica in genere quando la durata di utilizzo prevista è stata determinata principalmente da fattori che non sono alterati dalla modifica, quali la durabilità fisica dei componenti hardware, qualora la modifica sostanziale riguardi esclusivamente le funzionalità del software o i servizi di back-end.

Esempio *54: un fabbricante immette sul mercato un robot aspirapolvere con una durata di utilizzo prevista di X anni, determinata sulla base della natura del prodotto con elementi digitali, comprese la durabilità fisica e le caratteristiche di usura dei componenti hardware, e tenendo conto delle ragionevoli aspettative degli utilizzatori in merito alla durata di vita di tale prodotto. Il costruttore fissa un periodo di assistenza di X anni. Dopo Y anni, il fabbricante rilascia un aggiornamento del software che si configura come una modifica sostanziale, aggiungendo nuove modalità di pulizia e funzioni di navigazione. L'aggiornamento del software non incide sulla durabilità fisica dell'hardware e non altera le ragionevoli aspettative degli utilizzatori in merito alla durata di vita di tale prodotto. Di conseguenza, in base ai criteri di cui all'articolo 13, paragrafo 8, la durata di utilizzo prevista rimane invariata. Il periodo di assistenza del prodotto con elementi digitali modificato corrisponde alla restante durata di utilizzo prevista, come originariamente determinata.*

Esempio 55: un fabbricante immette sul mercato un macchinario industriale, ossia un prodotto con elementi digitali complesso con back-end sul cloud che costituisce una soluzione di elaborazione dati da remoto. La durata di utilizzo prevista è di X anni, determinata tenendo conto delle ragionevoli aspettative degli utilizzatori e della natura del prodotto con elementi digitali, quali la durabilità fisica dell'hardware della macchina e l'usura prevista. Il periodo di assistenza è fissato in modo da corrispondere a tale durata di utilizzo prevista, ossia X anni. Dopo Y anni, il fabbricante riprogetta l'architettura del back-end sul cloud (la soluzione di elaborazione dati da remoto), introducendo nuove API e nuovi flussi di dati, in un modo che si configura come una modifica sostanziale del prodotto con elementi digitali ma non altera la natura di tale prodotto né incide sulle aspettative degli utilizzatori. Di conseguenza, in base ai criteri di cui all'articolo 13, paragrafo 8, la durata di utilizzo prevista rimane invariata. Il periodo di assistenza del prodotto con elementi digitali modificato corrisponde alla restante durata di utilizzo prevista, come originariamente determinata.

135. Se la modifica sostanziale incide sui fattori che hanno originariamente determinato la durata di utilizzo prevista del prodotto con elementi digitali, il fabbricante dovrebbe ricalcolare il periodo di assistenza per riflettere la nuova durata di utilizzo prevista, applicando di conseguenza i criteri di cui all'articolo 13, paragrafo 8. Ciò può verificarsi, ad esempio, nel caso di modifiche hardware volte a rinnovare il prodotto e a prolungarne la vita operativa, oppure nel caso di una riprogrammazione o riscrittura sostanziale del software di base di tale prodotto che ne modifichi sostanzialmente la durata di utilizzo prevista ([20]).

Esempio 56: un fabbricante immette sul mercato un controllore logico programmabile (PLC) con una durata di utilizzo prevista di X anni, determinata principalmente in base alla natura del prodotto con elementi digitali e alla durabilità dell'hardware sottostante. Il periodo di assistenza è fissato di conseguenza. Diversi anni dopo la prima immissione sul mercato, il fabbricante apporta una modifica sostanziale consistente nella sostituzione della piattaforma informatica integrata del PLC, che comprende il processore, la memoria e l'ambiente di esecuzione, con una nuova generazione di componenti progettati per una durata operativa notevolmente più lunga. A seguito della modifica, cambiano le ragionevoli aspettative degli utilizzatori e la natura del prodotto con elementi digitali: l'utilizzatore del PLC può ora ragionevolmente aspettarsi che il PLC continui a essere utilizzato in modo produttivo oltre il periodo di utilizzo previsto inizialmente dichiarato, grazie al supporto della nuova piattaforma informatica. In base ai criteri di cui all'articolo 13, paragrafo 8, il periodo di utilizzo previsto risulta pertanto più lungo e il fabbricante ricalcola di conseguenza il periodo di assistenza per lo specifico PLC in questione.

6. **PRODOTTI CON ELEMENTI DIGITALI IMPORTANTI E CRITICI**

136. L'articolo 7, paragrafo 1, del regolamento sulla ciberresilienza stabilisce che i prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti di cui all'allegato III del regolamento sono considerati «prodotti con elementi digitali importanti». L'allegato III suddivide inoltre i prodotti con elementi digitali importanti in classi (classe I e classe II). Analogamente, l'articolo 8, paragrafo 1, stabilisce che i prodotti con elementi digitali che hanno la funzionalità principale di una categoria di prodotti di cui all'allegato IV del regolamento sulla ciberresilienza sono considerati «prodotti con elementi digitali critici» ([21]).

([20]) È opportuno ricordare che, come indicato nella sezione *4.1 Riparazioni fisiche*, le operazioni di ricondizionamento, manutenzione o riparazione non sono generalmente considerate modifiche sostanziali.

([21]) Il regolamento di esecuzione (UE) 2025/2392 della Commissione stabilisce la descrizione tecnica delle categorie di prodotti importanti e critici.

137. La classificazione di un prodotto con elementi digitali come importante o critico oppure, al contrario, come appartenente alla categoria «predefinita» ([22]), è rilevante ai fini della determinazione della procedura di valutazione della conformità che il fabbricante è tenuto a seguire, ai sensi dell'articolo 32, prima di poter immettere sul mercato tale prodotto con elementi digitali. In particolare, per i prodotti con elementi digitali appartenenti alla categoria predefinita è sempre possibile applicare la procedura di controllo interno basata sul modulo A («autovalutazione») ([23]). I prodotti con elementi digitali importanti di classe I o II e i prodotti con elementi digitali critici sono soggetti a procedure di valutazione della conformità più rigorose. Sono esclusi i prodotti con elementi digitali importanti di classe I o II che si qualificano come software liberi e open source immessi sul mercato, per i quali, in conformità dell'articolo 32, paragrafo 5, i fabbricanti sono autorizzati a seguire le procedure previste per la categoria predefinita.

138. Il concetto di funzionalità principale è pertanto essenziale affinché il fabbricante possa determinare il regime di valutazione della conformità applicabile. Si tratta tuttavia di un concetto che non è definito in modo esplicito nel regolamento sulla ciberresilienza. I prodotti con elementi digitali possono svolgere una serie di funzioni, alcune delle quali possono essere ausiliarie alla funzionalità principale del prodotto e non dovrebbero incidere sulla classificazione del prodotto come predefinito/importante di classe I/importante di classe II/critico. È pertanto utile fornire maggiori orientamenti per aiutare i fabbricanti a eseguire correttamente le pertinenti procedure di valutazione della conformità e per assistere le autorità di vigilanza del mercato nel garantire l'applicazione armonizzata del regolamento sulla ciberresilienza in tutta l'UE.

6.1. **Funzionalità principale**

139. La funzionalità principale di un prodotto con elementi digitali si riferisce alle principali caratteristiche e capacità tecniche di tale prodotto, senza le quali esso non sarebbe in grado di conseguire la sua finalità prevista. Questo aspetto può essere valutato alla luce del contesto e delle condizioni d'uso specifici di tale prodotto, tenendo conto, tra l'altro, delle informazioni fornite dal fabbricante nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica.

Esempio 57: un prodotto software con elementi digitali fornisce un livello di astrazione sull'hardware sottostante e gestisce l'esecuzione di componenti software. Le sue caratteristiche principali comprendono l'inizializzazione dell'hardware e delle periferiche, la gestione dei processi e della memoria, il controllo input/output, lo scheduling, l'assegnazione delle risorse e la messa a disposizione dei servizi di sistema e delle interfacce di programmazione delle applicazioni (API), attraverso le quali le applicazioni interagiscono con le risorse hardware e software del dispositivo. La documentazione tecnica indica che il prodotto con elementi digitali orchestra le risorse di calcolo, applica le configurazioni di sistema e fornisce interfacce standardizzate per i moduli software e le periferiche collegate. Il fabbricante sottolinea che tali capacità consentono alla piattaforma di fungere da ambiente software centrale su cui le applicazioni possono funzionare in modo affidabile. Il prodotto con elementi digitali ha la funzionalità principale di un sistema operativo, come descritto nell'allegato I, punto 11, del regolamento di esecuzione (UE) 2025/2392.

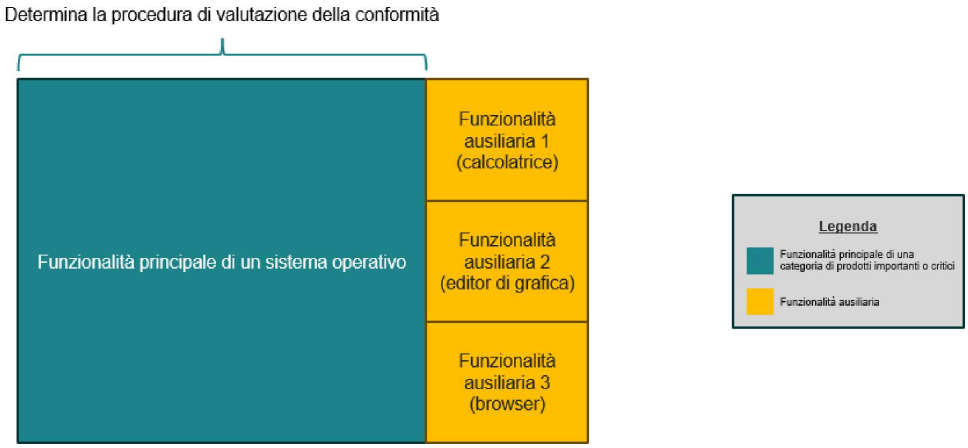
140. La funzionalità di un prodotto con elementi digitali è raramente limitata esclusivamente alla sua funzionalità principale, in quanto i prodotti con elementi digitali spesso, se non sempre, svolgono funzioni aggiuntive che non contribuiscono alla funzionalità principale del prodotto. Ciò può includere anche l'incorporazione di componenti che hanno essi stessi la funzionalità di un altro prodotto con elementi digitali importante o critico. Tuttavia il fatto che un prodotto con elementi digitali svolga funzioni diverse o aggiuntive rispetto a quelle dettagliate nelle descrizioni tecniche dei prodotti con elementi digitali importanti o critici non esclude di per sé che il prodotto abbia una di tali funzionalità principali.

([22]) Il termine «predefinito» non è un termine definito nel regolamento sulla ciberresilienza. Nel presente documento il termine è utilizzato in riferimento ai prodotti con elementi digitali che non hanno la funzionalità principale di una categoria di prodotti di cui agli allegati III o IV del regolamento sulla ciberresilienza e che, di conseguenza, sono soggetti al regime di valutazione della conformità di cui all'articolo 32, paragrafo 1.

([23]) Il fabbricante può tuttavia sempre scegliere di applicare una procedura di valutazione della conformità più rigorosa, come stabilito all'articolo 32, paragrafo 1.

Figura 2

rappresentazione grafica di come sia la funzionalità principale, e non le funzionalità ausiliarie, a determinare la procedura di valutazione della conformità applicabile



141. Un prodotto con elementi digitali può essere in grado di svolgere le funzioni di una categoria di prodotti importanti o critici, ma avere comunque una funzionalità principale diversa da quella di tale categoria di prodotti. In tali casi il prodotto con elementi digitali non si qualificherebbe quindi come un prodotto con elementi digitali importante o critico. Come indicato esplicitamente all'articolo 7, paragrafo 1, del regolamento sulla ciberresilienza per i prodotti con elementi digitali importanti (e applicando la stessa logica per i prodotti con elementi digitali critici), la semplice integrazione di un prodotto con elementi digitali importante o critico non rende di per sé il prodotto con elementi digitali un prodotto con elementi digitali importante o critico.

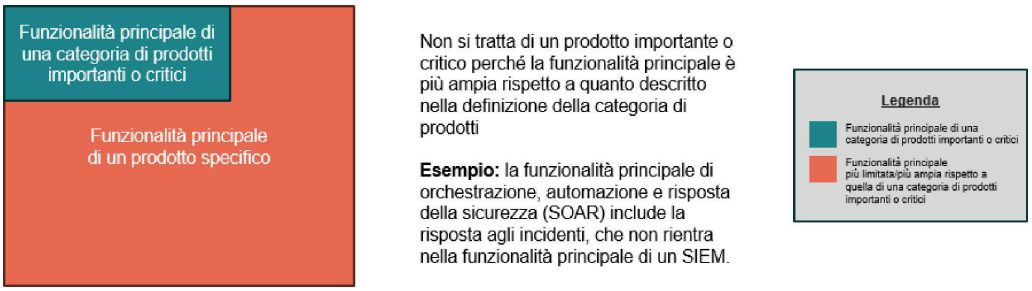
Esempio 58: uno smartphone integra un sistema operativo che fornisce le funzionalità descritte nell'allegato I, punto 11, del regolamento di esecuzione (UE) 2025/2392. Mentre il sistema operativo consente la gestione delle risorse hardware e l'esecuzione di applicazioni software, lo smartphone nel suo complesso ha una funzionalità principale diversa (ossia quella di consentire agli utilizzatori di comunicare e accedere a informazioni e servizi). La semplice integrazione di un sistema operativo non significa che lo smartphone abbia la funzionalità principale di un sistema operativo.

142. Alcuni prodotti con elementi digitali possono essere simili a una categoria di prodotti importanti o critici o appartenere alla stessa famiglia generale di prodotti, ma la loro funzionalità principale può essere sostanzialmente superiore o sostanzialmente inferiore rispetto alla funzionalità principale di tale categoria. Ciò non si verifica nel caso in cui un prodotto con elementi digitali includa funzionalità aggiuntive che si limitano a integrare o migliorare la funzionalità principale, che a sua volta corrisponde a quella di una categoria di prodotti importanti o critici; in questi casi il prodotto con elementi digitali mantiene la funzionalità principale di tale categoria ed è classificato di conseguenza. Tale valutazione dovrebbe basarsi sulle principali caratteristiche e capacità tecniche di tale prodotto, considerate oggettivamente alla luce della sua finalità prevista, e non sul modo in cui il prodotto con elementi digitali è descritto o commercializzato, qualora tale descrizione non rispecchi le effettive caratteristiche tecniche del prodotto.

Esempio 59: un software di orchestrazione, automazione e risposta della sicurezza (SOAR) è spesso in grado di svolgere le funzioni di prodotti con elementi digitali appartenenti alla categoria «sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM)», ossia raccogliere dati provenienti da diverse fonti, analizzarli e correlarli e presentarli come informazioni utilizzabili a fini di sicurezza. Tuttavia la funzionalità principale del software è notevolmente più ampia di quella di un SIEM e include servizi quali la risposta agli incidenti come elementi fondamentali delle sue capacità tecniche. Pertanto in genere non si ritiene che i software SOAR abbiano la funzionalità principale di un sistema SIEM.

Figura 3

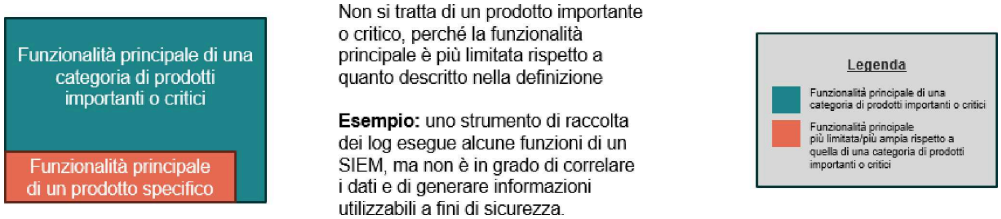
rappresentazione grafica del caso di funzionalità principale di un prodotto con elementi digitali sostanzialmente più ampia rispetto alla definizione di una categoria di prodotti importanti o critici



Esempio 60: alcuni strumenti di raccolta e visualizzazione dei log sono in grado di acquisire i dati dei log e di presentare dashboard di base che mostrano gli eventi del sistema. Sebbene possano supportare le attività di monitoraggio della sicurezza, la funzionalità principale di questi strumenti è più limitata rispetto a quella dei sistemi SIEM, in quanto essi non effettuano la correlazione dei dati né forniscono informazioni utilizzabili a fini di sicurezza. Pertanto tali strumenti non sono generalmente da considerarsi come aventi la funzionalità principale di un sistema SIEM.

Figura 4

rappresentazione grafica del caso di funzionalità principale di un prodotto con elementi digitali sostanzialmente più limitata rispetto alla definizione di una categoria di prodotti importanti o critici

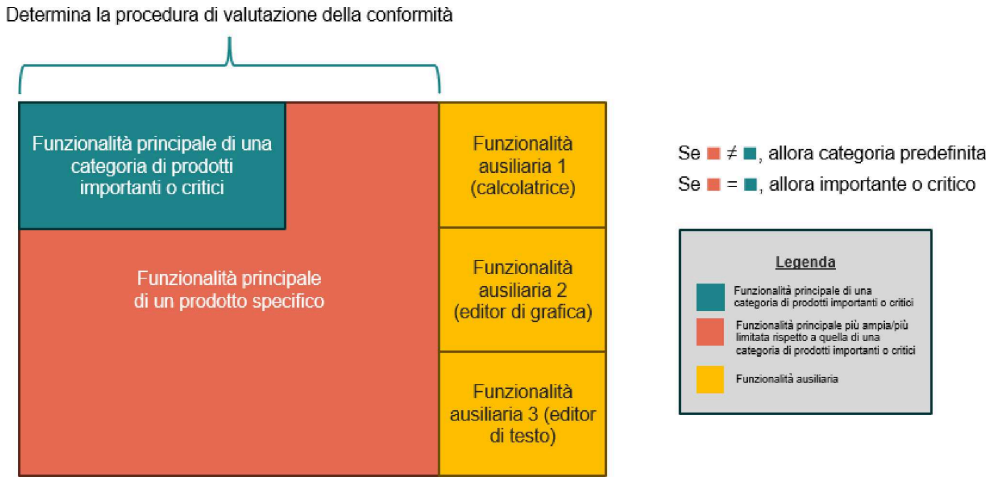


143. Un fabbricante non può fornire informazioni fuorvianti sulla funzionalità principale del proprio prodotto con elementi digitali al fine di eludere il regime di valutazione della conformità applicabile ai prodotti con elementi digitali importanti o critici, ad esempio sottolineando o sminuendo eccessivamente il ruolo di determinate funzionalità, in modo che il prodotto risulti sostanzialmente superiore o inferiore rispetto a una determinata funzionalità principale. Ciò si verificherebbe, ad esempio, qualora sussistessero evidenti incongruenze tra il materiale promozionale, le istruzioni per l'uso e la documentazione tecnica.

144. Un prodotto con elementi digitali non può avere più di una funzionalità principale ai fini della determinazione del regime di valutazione della conformità applicabile. Conformemente all'allegato VII del regolamento sulla ciberresilienza, nella documentazione tecnica di un prodotto, i fabbricanti sono tenuti a descrivere la finalità prevista del loro prodotto con elementi digitali e la procedura di valutazione della conformità che hanno seguito. La funzionalità principale del prodotto dovrebbe pertanto essere chiaramente identificata. Ciò consente la corretta individuazione del regime di valutazione della conformità applicabile e consente alle autorità di vigilanza del mercato di controllare e verificare che il regolamento sia applicato correttamente.

Figura 5

rappresentazione grafica del modo in cui la funzionalità principale di uno specifico prodotto con elementi digitali determina la classe del prodotto e quindi la procedura di valutazione della conformità applicabile



145. Alcuni prodotti con elementi digitali sono immessi sul mercato come un unico prodotto con elementi digitali, ma sono composti da moduli distinti con funzionalità distinte. Qualora un fabbricante metta tali moduli a disposizione sul mercato anche separatamente, ad esempio nel caso in cui essi siano offerti per l'acquisto, la concessione in licenza o l'abbonamento a titolo separato, tali moduli costituiscono prodotti autonomi (*standalone*) con elementi digitali a sé stanti. Di conseguenza devono essere classificati sulla base delle rispettive funzionalità principali (e pertanto sono soggetti al regime di valutazione della conformità appropriato sulla base della funzionalità principale di ciascun modulo). Fermo restando che, nei casi in cui i moduli sono forniti esclusivamente come componenti di un prodotto con elementi digitali integrato e non sono messi a disposizione separatamente, la funzionalità principale è determinata a livello del prodotto con elementi digitali integrato.

Esempio 61: un fabbricante immette sul mercato una suite di sicurezza unificata che combina più moduli, tra cui un SIEM, un sistema di rilevamento delle intrusioni e un modulo di analisi. Il fabbricante offre tali moduli anche con abbonamenti separati. In questo scenario, ciascun modulo è un prodotto con elementi digitali distinto ed è classificato in base alla propria funzionalità principale. Il modulo SIEM è soggetto al regime di valutazione della conformità per i prodotti con elementi digitali importanti di classe I, in quanto la sua funzionalità principale è quella dei «sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)». Il sistema di rilevamento delle intrusioni è soggetto al regime di valutazione della conformità per i prodotti con elementi digitali importanti di classe II, in quanto la sua funzionalità principale è quella di «Firewall, sistemi di rilevamento e prevenzione delle intrusioni». Il modulo di analisi è soggetto al regime di valutazione della conformità per i prodotti con elementi digitali «predefiniti», in quanto la sua funzionalità principale non è quella di una categoria di prodotti importanti o critici.

146. La non conformità agli obblighi di cui all'articolo 32 del regolamento sulla ciberresilienza può comportare sanzioni amministrative pecuniarie a norma dell'articolo 64, paragrafo 3.

6.2. Valutazione della conformità per i prodotti con elementi digitali importanti e critici

147. Una volta determinata la funzionalità principale del proprio prodotto con elementi digitali, il fabbricante deve eseguire una delle procedure di valutazione della conformità applicabili. Il fabbricante deve garantire che il prodotto con elementi digitali nel suo complesso soddisfi i requisiti essenziali, tenendo conto, se del caso, della sicurezza dei componenti integrati o delle funzionalità integrate.

148. Per i prodotti con elementi digitali importanti di classe II (ad eccezione di quelli che si qualificano come software liberi e open source, in conformità dell'articolo 32, paragrafo 5) e per i prodotti con elementi digitali critici ([24]) è obbligatoria una procedura di valutazione della conformità più rigorosa, con il coinvolgimento di terzi (basata sul modulo B+C, sul modulo H o sui sistemi di certificazione della cibersicurezza). Per contro, i prodotti con elementi digitali importanti di classe I (ad eccezione di quelli che si qualificano come software liberi e open source, in conformità dell'articolo 32, paragrafo 5) devono essere sottoposti a una procedura di valutazione della conformità da parte di terzi solo se il fabbricante non ha applicato o ha applicato solo in parte le norme armonizzate pertinenti i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* (di seguito «norme armonizzate»), specifiche comuni o sistemi europei di certificazione della cibersicurezza con un livello di affidabilità almeno «sostanziale» ([25]).

149. Pertanto, affinché un prodotto con elementi digitali importante di classe I sia ammissibile alla procedura di controllo interno, i) devono essere applicati tutti i requisiti applicabili di una norma armonizzata pertinente; e ii) l'ambito di applicazione della norma deve coprire almeno tutti i rischi di cibersicurezza associati alla funzionalità principale di tale prodotto.

150. La gamma di funzioni del prodotto con elementi digitali può essere più ampia di quella prevista dalla pertinente norma armonizzata e tali funzioni aggiuntive possono presentare rischi di cibersicurezza diversi o aggiuntivi. Il fabbricante è sempre tenuto a effettuare una valutazione dei rischi a norma dell'articolo 13, paragrafo 2, e dovrebbe di conseguenza verificare se l'attuazione di una norma armonizzata copra tutti i rischi associati al prodotto con elementi digitali. Qualora l'attuazione della norma non copra tutti i rischi, il fabbricante dovrebbe garantire con altri mezzi che il proprio prodotto con elementi digitali sia conforme ai requisiti essenziali.

151. Pertanto il fabbricante di un prodotto con elementi digitali importante di classe I, qualora abbia applicato una norma armonizzata pertinente che contempla i rischi associati alla funzionalità principale di tale prodotto, può decidere di avvalersi della procedura di controllo interno per dimostrare la conformità del proprio prodotto. Nell'ambito delle proprie attività di valutazione della conformità, il fabbricante sarà comunque tenuto a dimostrare che tutti i rischi applicabili al proprio prodotto con elementi digitali siano stati affrontati. Pertanto, qualora vi sia un divario tra la copertura della norma armonizzata e la gamma di funzioni del prodotto con elementi digitali nel suo complesso, il fabbricante deve comunque documentare quali misure supplementari ha messo in atto per trattare tali rischi.

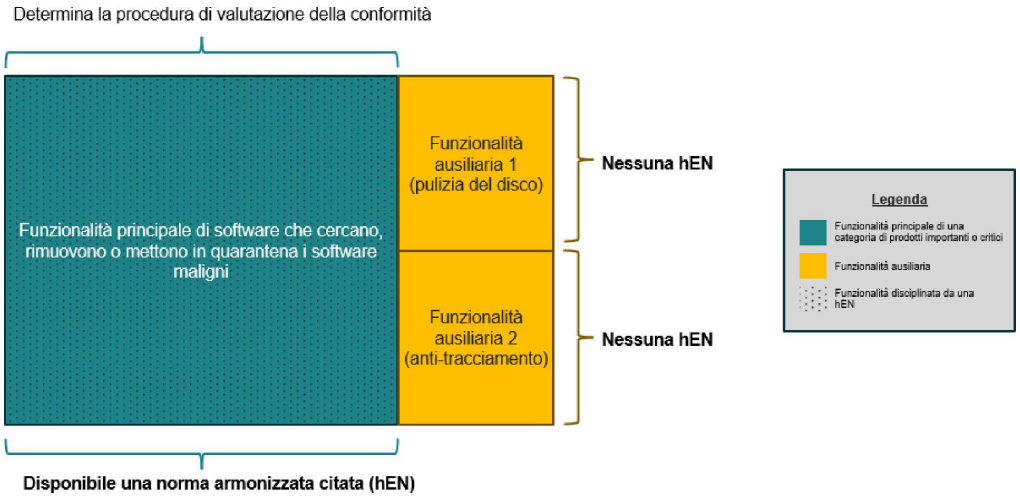
Esempio 62: un software antivirus ha la funzionalità principale di un software che cerca, rimuove o mette in quarantena i software maligni, come descritto nell'allegato I, punto 4, del regolamento di esecuzione (UE) 2025/2392. Tale prodotto con elementi digitali comprende anche caratteristiche aggiuntive, vale a dire una funzione di pulizia del disco e una funzione di anti-tracciamento che protegge l'utilizzatore durante la navigazione sul web. Il fabbricante effettua una valutazione dei rischi che riguarda il prodotto con elementi digitali nella sua interezza, comprese la funzionalità principale dell'antivirus, e le funzioni di pulizia del disco e di anti-tracciamento. Applica una norma armonizzata che contempla i rischi associati alla funzionalità principale dell'antivirus e misure supplementari per affrontare i rischi derivanti dalle funzioni aggiuntive. Il fabbricante è autorizzato ad avvalersi della procedura di controllo interno per la sua valutazione della conformità, che copre il prodotto con elementi digitali nel suo complesso, comprese le funzioni di pulizia del disco e di anti-tracciamento.

([24]) Ciò vale anche quando si ricorre a un sistema europeo di certificazione della cibersicurezza con un livello di affidabilità almeno «sostanziale», in quanto è richiesto l'intervento di un organismo di certificazione terzo.

([25]) Per brevità, il resto della presente sezione fa riferimento soltanto alle norme armonizzate i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*. Tuttavia gli stessi orientamenti si applicano anche alle specifiche comuni adottate a norma dell'articolo 27, paragrafo 2, e ai sistemi europei di certificazione della cibersicurezza, ove specificato dalla Commissione mediante atti delegati a norma dell'articolo 27, paragrafo 9.

Figura 6

rappresentazione grafica di come l'utilizzo di una norma armonizzata citata che contempla solo la funzionalità principale determini la procedura di valutazione della conformità applicabile



152. Ciò vale anche quando il prodotto con elementi digitali integra una funzione aggiuntiva che è di per sé quella di un altro prodotto con elementi digitali importante o critico. Infatti è la funzionalità principale del prodotto con elementi digitali nel suo complesso, e non la funzionalità dei componenti integrati considerati isolatamente, a determinare l'eventuale appartenenza di un prodotto con elementi digitali alla categoria di prodotti importanti o critici (e quindi il regime di valutazione della conformità applicabile). Ad esempio, se un prodotto con elementi digitali ha la funzionalità principale di un prodotto con elementi digitali importante di classe I, tale prodotto nel suo complesso è soggetto al regime di valutazione della conformità applicabile ai prodotti con elementi digitali importanti di classe I, anche se integra un componente che è a sua volta un prodotto con elementi digitali critico. In questi casi, qualora applichi una norma armonizzata che contempla i rischi associati alla funzionalità principale di tale prodotto, il fabbricante può avvalersi della procedura di controllo interno.

Esempio 63: un prodotto hardware con elementi digitali ha la funzionalità principale di un router, come descritta nell'allegato I, punto 12, del regolamento di esecuzione (UE) 2025/2392. Tale prodotto con elementi digitali comprende anche funzionalità aggiuntive, comprese capacità di firewall, in quanto integra un componente firewall. Il fabbricante effettua una valutazione dei rischi che riguarda il prodotto con elementi digitali nella sua interezza, comprese la funzionalità principale di router e la funzionalità di firewall. Applica una norma armonizzata che contempla i rischi associati alla funzionalità principale di router e misure supplementari per affrontare i rischi derivanti dalle funzioni aggiuntive. Ad esempio, il fabbricante può applicare la norma armonizzata per i firewall per coprire i rischi associati alla funzionalità di firewall. Il fabbricante è autorizzato ad avvalersi della procedura di controllo interno per la propria valutazione della conformità, che riguarda il prodotto con elementi digitali nel suo complesso, compresa la funzionalità di firewall.

6.3. Implicazioni per la presunzione di conformità

153. A norma dell'articolo 27, paragrafo 1, del regolamento sulla ciberresilienza, i prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono 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 di cibersicurezza di cui all'allegato I oggetto di tali norme o parti di esse ([26]). L'articolo 27, paragrafo 5, estende la

([26]) Come chiaramente indicato nella sezione 4.1.2.2 della guida blu, «nella normativa di armonizzazione relativa ai rischi [...] i fabbricanti, anche quando ricorrono a norme armonizzate, i cui riferimenti sono pubblicati nella *Gazzetta ufficiale dell'Unione europea*, restano sempre pienamente responsabili della valutazione di tutti i rischi del loro prodotto al fine di stabilire quali requisiti essenziali (o altri) siano pertinenti. Dopo questa valutazione il fabbricante può scegliere di applicare le specifiche tecniche indicate nelle norme armonizzate, i cui riferimenti sono pubblicati nella *Gazzetta ufficiale dell'Unione europea*, per attuare "misure di riduzione del rischio" specificate da norme armonizzate».

stessa presunzione di conformità ai prodotti con elementi digitali e ai processi messi in atto dal fabbricante che sono conformi alle specifiche comuni adottate dalla Commissione mediante atti di esecuzione, e l'articolo 27, paragrafo 8, prevede la presunzione di conformità per i prodotti con elementi digitali e i processi messi in atto dal fabbricante per i quali sono stati rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881, se ciò è stato specificato mediante atti delegati conformemente all'articolo 27, paragrafo 9 ([27]).

154. Pertanto, qualora abbia applicato una norma armonizzata i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, il fabbricante beneficia di una presunzione di conformità per i rischi contemplati da tale norma. Ciò potrebbe verificarsi, ad esempio, nel caso in cui la norma armonizzata di riferimento affronti tutti i rischi associati alla funzionalità principale di un prodotto con elementi digitali e non vi siano funzionalità aggiuntive che presentino rischi di cibersicurezza. Ad esempio, ci si aspetta che la norma armonizzata per i router affronti almeno i rischi associati alla funzionalità principale di tali prodotti con elementi digitali. Se tale prodotto non contiene funzionalità aggiuntive o se tali funzionalità aggiuntive non presentano rischi non affrontati dalla norma, il prodotto con elementi digitali può beneficiare della presunzione di conformità.

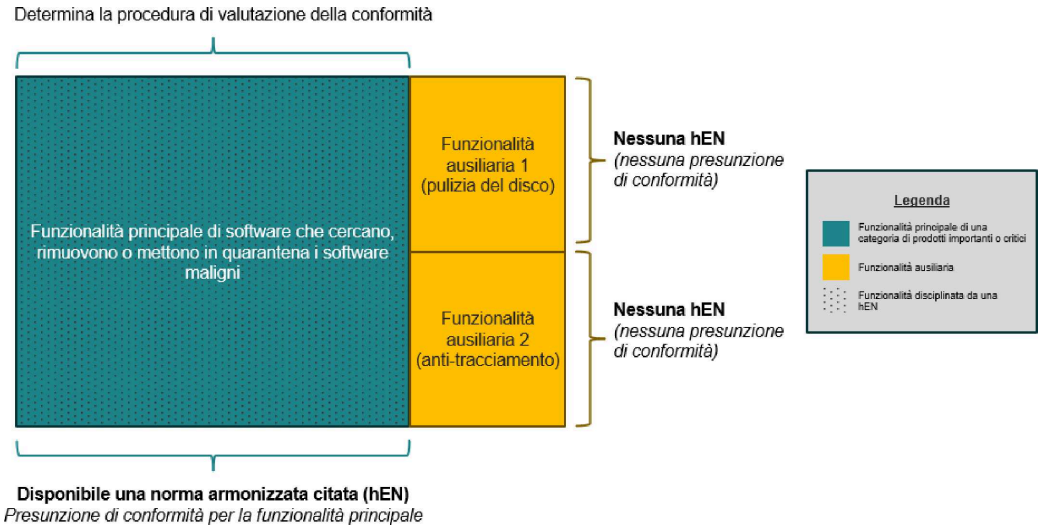
155. Nei casi di cui ai punti 151 e 152, il fabbricante è autorizzato a utilizzare la procedura di controllo interno in quanto la norma armonizzata contempla i rischi associati alla funzionalità principale del prodotto con elementi digitali. Tuttavia i prodotti con elementi digitali descritti in tali esempi potrebbero avere una gamma di funzioni più ampia rispetto a quella oggetto delle norme armonizzate, e le funzionalità aggiuntive potrebbero comportare rischi per la sicurezza informatica non contemplati da tale norma armonizzata. Tali prodotti con elementi digitali non possono pertanto beneficiare della presunzione di conformità per tali funzionalità aggiuntive.

Esempio 64: un software antivirus ha la funzionalità principale di un software che cerca, rimuove o mette in quarantena i software maligni, e i rischi associati a tale funzionalità principale sono contemplati dalla norma armonizzata. Tale prodotto con elementi digitali comprende anche funzionalità aggiuntive, vale a dire una funzione di pulizia del disco e una funzionalità anti-tracciamento che protegge l'utilizzatore durante la navigazione sul web, i cui rischi non sono contemplati dalla norma armonizzata. Se è applicata la norma armonizzata, il fabbricante è autorizzato ad avvalersi della procedura di controllo interno per la valutazione della conformità. Beneficerà della presunzione di conformità per i rischi associati alla funzionalità principale del prodotto, ma non per i rischi associati alle funzionalità aggiuntive.

([27]) Come sopra, per brevità, nel resto della presente sezione si fa riferimento soltanto alle norme armonizzate i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*. Tuttavia gli stessi orientamenti si applicano anche alle specifiche comuni e ai sistemi europei di certificazione della cibersicurezza.

Figura 7

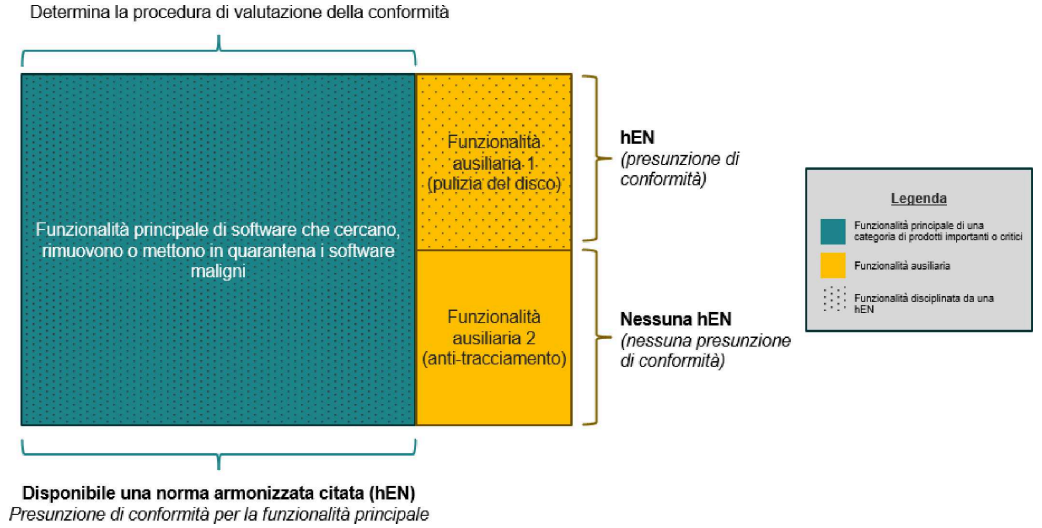
la norma armonizzata conferisce la presunzione di conformità per la funzionalità principale, in quanto affronta tutti i rischi associati a tale funzionalità principale, ma non per le funzionalità ausiliarie



Esempio 65: nello stesso scenario dell'esempio precedente, la norma armonizzata è stata aggiornata per contemplare anche i rischi associati a una delle funzionalità aggiuntive, ossia la funzione di pulizia del disco, ma non all'altra (ossia la funzione di anti-tracciamento). Se è applicata la norma armonizzata, il fabbricante è autorizzato ad avvalersi della procedura di controllo interno per la valutazione della conformità. Beneficerà di una presunzione di conformità per i rischi associati alla funzionalità principale di tale prodotto e per la funzionalità di pulizia del disco, ma non per i rischi connessi alla funzionalità di anti-tracciamento.

Figura 8

la norma armonizzata conferisce la presunzione di conformità per la funzionalità principale e la funzionalità ausiliaria 1, in quanto affronta tutti i rischi associati a queste due funzionalità, ma non per la funzionalità ausiliaria 2



7. VALUTAZIONE DEI RISCHI DI CIBERSICUREZZA E INTEGRAZIONE DI PRODOTTI CON ELEMENTI DIGITALI E COMPONENTI

7.1. La valutazione e il trattamento dei rischi di cibersicurezza

156. La valutazione dei rischi di cibersicurezza di cui all'articolo 13, paragrafo 2, del regolamento sulla ciberresilienza impone ai fabbricanti di individuare i rischi pertinenti e di valutarne il potenziale impatto sul prodotto con elementi digitali. I fabbricanti devono inoltre attuare misure adeguate per affrontare tali rischi, conformemente ai requisiti essenziali di cui all'allegato I.

157. Nella gestione dei rischi a livello di organizzazione, i rischi sono generalmente valutati sulla base di criteri di accettazione derivanti dagli obiettivi interni o dalla propensione al rischio dell'organizzazione. Per contro, nell'ambito del regolamento sulla ciberresilienza, il rischio residuo di cibersicurezza dovrebbe essere valutato alla luce del requisito secondo cui il prodotto con elementi digitali immesso sul mercato deve garantire un livello adeguato di cibersicurezza in base ai rischi, tenendo conto della sua finalità prevista e del suo uso ragionevolmente prevedibile.

158. Di conseguenza la tolleranza al rischio interna del fabbricante, la sua strategia commerciale o le semplici considerazioni di costo non sono pertinenti per determinare se i rischi siano stati affrontati. Ai fini dell'articolo 13, paragrafi 2 e 3, i fabbricanti devono essere in grado di determinare se i rischi di cibersicurezza individuati siano stati affrontati in misura sufficiente attraverso l'attuazione dei requisiti essenziali di cui all'allegato I, parte I, alla luce della finalità prevista, dell'uso ragionevolmente prevedibile e delle condizioni d'uso, compresi, se del caso, l'ambiente operativo (ad esempio gli utilizzatori cui il prodotto con elementi digitali è destinato) e gli attivi da proteggere, tenendo conto della durata di utilizzo prevista del prodotto con elementi digitali.

159. Il rischio residuo di cibersicurezza è un risultato intrinseco della valutazione e del trattamento dei rischi. Si riconosce che i rischi di cibersicurezza non possono, nella pratica, essere completamente eliminati. Tuttavia l'esistenza di un rischio residuo non implica che possa essere accettato qualsiasi rischio a discrezione del fabbricante. Un prodotto con elementi digitali può essere immesso sul mercato solo se i rischi residui, una volta adottate misure adeguate, sono stati affrontati in misura sufficiente attraverso l'attuazione dei requisiti essenziali, tenendo conto della finalità prevista e dell'uso ragionevolmente prevedibile del prodotto con elementi digitali.

160. Conformemente all'articolo 13, paragrafo 3, qualora siano individuati rischi di cibersicurezza, i fabbricanti sono tenuti ad affrontarli mediante misure adeguate, anche a livello di prodotto. A seconda delle circostanze, ciò può comportare, ad esempio, la riduzione della superficie di attacco, l'attuazione di garanzie tecniche, la limitazione o l'adeguamento della funzionalità o una definizione più precisa della finalità prevista del prodotto con elementi digitali. I fabbricanti possono inoltre adottare misure volte a orientare l'uso ragionevolmente prevedibile del prodotto con elementi digitali, ad esempio attraverso la comunicazione dei rischi, istruzioni per l'uso o la progettazione dell'interfaccia utente, al fine di orientare il comportamento degli utilizzatori verso modelli d'uso sicuri.

161. Il regolamento sulla ciberresilienza non consente di trasferire il rischio o la responsabilità in materia di cibersicurezza agli utilizzatori o a terzi per compensare le carenze nella progettazione dei prodotti o per giustificare il fatto che i rischi di cibersicurezza non siano stati affrontati. L'obbligo di immettere sul mercato un prodotto con elementi digitali sicuro e di dimostrare la conformità ai requisiti essenziali spetta al fabbricante.

162. Le informazioni e le istruzioni fornite agli utilizzatori possono essere utilizzate per sostenere la diffusione e il funzionamento sicuri del prodotto con elementi digitali, anche nel caso in cui il fabbricante abbia scelto di limitare la finalità prevista di tale prodotto ad ambienti sicuri, nonché per informare gli utilizzatori dei rischi residui, in modo adeguato alla natura del prodotto con elementi digitali e agli utilizzatori cui il prodotto è destinato.

Esempio 66: un fabbricante sviluppa un sensore industriale da utilizzare in ambienti sicuri. Affinché il sensore funzioni correttamente, il produttore non adotta misure di protezione contro gli attacchi fisici diretti al sensore stesso. Per attenuare i rischi associati individuati nella valutazione dei rischi, il fabbricante limita la finalità prevista del sensore all'uso in ambienti sicuri in cui è impedito l'accesso fisico non autorizzato al prodotto con elementi digitali. Le informazioni e le istruzioni per gli utilizzatori forniscono informazioni chiare su tali limitazioni relative all'uso del sensore, in modo adeguato alla natura del prodotto con elementi digitali e agli utilizzatori cui esso è destinato.

Esempio 67: un fabbricante sviluppa un'applicazione software per uso professionale su desktop e dispositivi mobili gestiti. L'applicazione elabora dati sensibili memorizzati localmente e contenuti generati dagli utilizzatori. Durante la valutazione dei rischi, il fabbricante individua il rischio di accesso non autorizzato a tali dati qualora fossero memorizzati in chiaro sul dispositivo. Anziché progettare e implementare un meccanismo di cifratura proprietario all'interno dell'applicazione stessa, il produttore sceglie di affidarsi alle funzioni di crittografia e gestione delle chiavi fornite in modo nativo dal sistema operativo su cui l'applicazione è destinata a funzionare, poiché i servizi crittografici integrati nel sistema operativo sono consolidati e sottoposti a regolare manutenzione.

163. Se la valutazione dei rischi di cibersicurezza individua rischi che non possono essere adeguatamente affrontati mediante opportune misure, ai fini della conformità al regolamento sulla ciberresilienza, può essere necessario apportare modifiche alla progettazione, alla funzionalità o alla finalità prevista del prodotto con elementi digitali. Considerazioni relative esclusivamente al costo o alla fattibilità commerciale non costituiscono motivi sufficienti per non trattare tali rischi qualora ciò impedisca al prodotto con elementi digitali di soddisfare i requisiti essenziali.

7.2. Progettazione, sviluppo e produzione di prodotti con elementi digitali in modo da garantire un livello adeguato di cibersicurezza in base ai rischi

164. Il requisito essenziale di cibersicurezza di cui all'allegato I, parte I, punto 1, del regolamento sulla ciberresilienza prevede che i prodotti con elementi digitali siano progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi.

165. Questo requisito essenziale è volto ad affrontare tutti i rischi di cibersicurezza individuati nell'ambito della valutazione dei rischi di cibersicurezza. In particolare, ciò comprende i rischi di cibersicurezza che non sono altrimenti adeguatamente affrontati nell'ambito dell'attuazione dei requisiti essenziali di cui all'allegato I, parte I, diversi dal quello di cui al punto 1. Questo requisito essenziale è diverso dall'obbligo giuridico di effettuare una valutazione dei rischi di cibersicurezza, che deve essere effettuata a norma dell'articolo 13, paragrafo 2.

166. Se tutti i rischi di cibersicurezza pertinenti relativi a un prodotto con elementi digitali sono trattati attuando misure adeguate per soddisfare i requisiti essenziali applicabili diversi da quello di cui al punto 1, il requisito essenziale di cui all'allegato I, parte I, punto 1, si considera soddisfatto. Per contro, se la valutazione dei rischi di cibersicurezza individua rischi aggiuntivi non pienamente affrontati da tali misure, i fabbricanti sono tenuti ad attuare misure adeguate sul prodotto con elementi digitali per affrontare tali rischi, in modo da conformarsi al requisito essenziale di cui all'allegato I, parte I, punto 1. Nella pratica, nella maggior parte dei casi, la conformità agli altri requisiti essenziali dovrebbe comportare la conformità a tale requisito.

7.3. Valutazione dei rischi e dovuta diligenza in relazione alle dipendenze esterne e ai componenti integrati

167. Il regolamento sulla ciberresilienza stabilisce due obblighi distinti ma complementari per i fabbricanti in relazione alla gestione dei rischi di cibersicurezza. In primo luogo, l'articolo 13, paragrafo 2, impone ai fabbricanti di effettuare una valutazione dei rischi di cibersicurezza per il prodotto con elementi digitali stesso. In secondo luogo, l'articolo 13, paragrafo 5, impone l'obbligo di esercitare la dovuta diligenza in relazione ai componenti integrati. Insieme, questi due obblighi sono concepiti per garantire che il prodotto con elementi digitali rimanga sicuro, anche quando si basa su soluzioni di elaborazione dati da remoto, servizi da remoto o componenti software o hardware di terzi.

168. La valutazione dei rischi di cibersicurezza riguarda l'individuazione e la gestione dei rischi pertinenti che possono incidere sul prodotto con elementi digitali, compresi i rischi che hanno origine al di fuori del prodotto stesso, quali reti esterne, fattori ambientali o altri aspetti esterni che potrebbero incidere sul prodotto con elementi digitali o da cui il prodotto dipende. Per tali rischi esterni, il regolamento sulla ciberresilienza non impone ai fabbricanti di controllare o gestire l'ambiente esterno. I fabbricanti sono invece tenuti a individuare tali rischi e ad attenuarli attraverso la progettazione e lo sviluppo del prodotto con elementi digitali stesso. Ciò comporterà l'attuazione degli opportuni requisiti essenziali di cui all'allegato I, parte I, e, se necessario, la fornitura di informazioni e istruzioni agli utilizzatori sui rischi di integrazione o implementazione.

169. Ad esempio, un fabbricante può individuare il rischio che persone non autorizzate possano avere accesso a sistemi back-end che non fanno parte del prodotto con elementi digitali stesso mentre il prodotto è in funzione e tentare di inviare comandi malevoli al prodotto con elementi digitali. Tali sistemi back-end, se non sono progettati e sviluppati dal fabbricante o sotto la sua responsabilità, o se non supportano una delle funzioni del prodotto con elementi digitali, non costituiscono soluzioni di elaborazione dati da remoto e pertanto non rientrano nella definizione di prodotto con elementi digitali ai fini del regolamento sulla ciberresilienza. Tuttavia il regolamento sulla ciberresilienza impone al fabbricante di affrontare il rischio che essi possono comportare attraverso misure a livello di prodotto, ad esempio richiedendo l'autenticazione crittografica dei comandi da remoto, verificando l'integrità delle modifiche di configurazione o generando log o allarmi rilevanti per la sicurezza quando viene rilevato un comportamento anomalo. Analogamente, qualora un fabbricante individui un rischio derivante dall'indisponibilità di tale servizio esterno, ad esempio a causa di interruzioni di corrente o guasti dell'infrastruttura, il regolamento sulla ciberresilienza può richiedere misure di attenuazione a livello di prodotto contro tali rischi di cibersicurezza, ad esempio misure volte a fare in modo che l'interruzione di corrente non provochi il passaggio del prodotto con elementi digitali a stati non sicuri. In questi tali casi il regolamento sulla ciberresilienza disciplina il modo in cui il prodotto con elementi digitali risponde a tali rischi esterni; non impone obblighi sul modo in cui l'infrastruttura back-end è organizzata, dotata di personale o gestita, né tratta tale infrastruttura come parte del prodotto con elementi digitali.

170. Il dovere di diligenza riguarda gli elementi che fanno parte del prodotto con elementi digitali stesso, in particolare i componenti software o hardware integrati forniti da terzi. I fabbricanti sono tenuti ad adottare misure adeguate per garantire che tali componenti non compromettano la conformità del prodotto con elementi digitali ai requisiti essenziali. Tale obiettivo può essere conseguito soltanto determinando ciò che il prodotto con elementi digitali richiede ai propri componenti per raggiungere i suoi obiettivi di cibersicurezza e verificando, secondo un approccio basato sul rischio, che tali componenti siano adeguati alle esigenze del prodotto, come indicato anche al considerando 34.

171. Alla luce della propria valutazione dei rischi di cibersicurezza, il fabbricante deve individuare i requisiti che il componente integrato dovrebbe soddisfare. Ad esempio, se il prodotto con elementi digitali si basa su funzioni crittografiche, meccanismi di aggiornamento o comunicazioni sicure forniti da un componente, il fabbricante deve, nell'ambito della dovuta diligenza, individuare tali esigenze e verificare che il componente le soddisfi. Le prove a tal fine possono consistere nella documentazione ottenuta dal fabbricante del componente, come le specifiche tecniche, la documentazione di sicurezza o la pertinente documentazione sulla conformità o sulla garanzia. Se del caso, il fabbricante può anche effettuare prove per verificare che tali componenti svolgano adeguatamente le funzioni pertinenti. Sebbene sia un obbligo giuridico a sé stante, la dovuta diligenza sostiene e rafforza la capacità del fabbricante di dimostrare la conformità ai requisiti essenziali per il prodotto con elementi digitali nel suo complesso.

172. Nel valutare i rischi relativi al prodotto con elementi digitali nel suo complesso è necessario prendere in considerazione, nell'ambito della valutazione dei rischi di cibersicurezza, gli elementi esterni al prodotto, quali gli elementi ambientali, le infrastrutture esterne, altri sistemi o reti e, se del caso, affrontarli attraverso misure a livello di prodotto per garantire la conformità del prodotto con elementi digitali ai requisiti essenziali. Nell'ambito della valutazione dei rischi devono essere considerati anche i componenti fisicamente o logicamente integrati nel prodotto con elementi digitali ma provenienti da terzi. Tuttavia, ai fini della conformità, il fabbricante dovrebbe trattare tali componenti alla stregua di componenti forniti dall'esterno le cui proprietà sono verificate esercitando la dovuta diligenza al momento dell'integrazione, poiché il fabbricante potrebbe non averli riprogettati o sviluppati ex-novo.

173. La stessa logica si applica durante lo sviluppo e l'integrazione dei componenti. Il fabbricante, qualora sviluppi esso stesso le funzionalità, deve attuare direttamente i requisiti essenziali. Qualora integri componenti sviluppati da altri, il fabbricante deve garantire, esercitando la dovuta diligenza, che tali componenti possano essere utilizzati in modo da far sì che il prodotto con elementi digitali nel suo complesso sia conforme. In entrambi i casi l'obiettivo è lo stesso: che il prodotto con elementi digitali, quale immesso sul mercato, raggiunga un livello adeguato di cibersicurezza come richiesto dal regolamento sulla ciberresilienza, tenendo conto dei rischi individuati nella valutazione dei rischi di cibersicurezza.

7.4. **Riutilizzo delle valutazioni dei rischi e della documentazione di conformità per famiglie di prodotti con elementi digitali**

174. I fabbricanti possono immettere sul mercato prodotti con elementi digitali simili, ad esempio diverse varianti, modelli o configurazioni differenti della stessa famiglia di prodotti. Qualora tali prodotti con elementi digitali condividano la stessa architettura, la stessa progettazione volta alla sicurezza e la stessa finalità prevista e siano esposti agli stessi rischi di cibersicurezza, il regolamento sulla ciberresilienza non impone ai fabbricanti di trattare ciascuna variante come un prodotto con elementi digitali completamente distinto ai fini della valutazione dei rischi e della valutazione della conformità.

175. In tali casi, a condizione che tutte le varianti interessate siano adeguatamente coperte in termini di rischi e requisiti essenziali pertinenti, i fabbricanti possono basarsi su: i) un'unica valutazione dei rischi di cibersicurezza effettuata conformemente all'articolo 13, paragrafo 2, del regolamento sulla ciberresilienza; ii) un'unica documentazione tecnica; e iii) un'unica procedura di valutazione della conformità. Ciò consente inoltre di rilasciare un'unica dichiarazione di conformità UE per il gruppo di prodotti con elementi digitali, a condizione che siano chiaramente identificate le varianti del prodotto cui essa si applica.

176. Il fattore decisivo è se le differenze tra le varianti siano rilevanti per la cibersicurezza. Le variazioni che non incidono sulle proprietà di cibersicurezza del prodotto con elementi digitali, quali differenze di colore, del fattore di forma, della capacità di memoria o di altre caratteristiche non rilevanti per la sicurezza, non richiedono valutazioni dei rischi o valutazioni della conformità separate. Per contro, in alcuni casi le varianti possono differire in modi che incidono sull'attuazione dei requisiti essenziali, ad esempio attraverso interfacce di comunicazione, stack di software, meccanismi di aggiornamento o connettività remota differenti. In questi casi tali differenze devono trovare riscontro nella valutazione dei rischi e, se necessario, nella valutazione della conformità e nella documentazione tecnica.

177. Spetta ai fabbricanti garantire che la valutazione dei rischi e la relativa documentazione rispecchino accuratamente i prodotti con elementi digitali immessi sul mercato. Qualora una nuova variante introduca nuovi rischi di cibersicurezza o modifichi le modalità di attuazione dei requisiti essenziali, la valutazione dei rischi e la documentazione di conformità esistenti devono essere aggiornate di conseguenza. Il ricorso a un'unica valutazione della conformità è possibile solo nella misura in cui i prodotti con elementi digitali non presentano differenze per quanto riguarda le proprietà di cibersicurezza.

8. **ELABORAZIONE DATI DA REMOTO**

178. L'articolo 3, punto 1), del regolamento sulla ciberresilienza definisce un prodotto con elementi digitali come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente». In quest'ottica, il fabbricante deve considerare il prodotto con elementi digitali nella sua interezza, comprese le relative soluzioni di elaborazione dati da remoto. Ad esempio, nel dimostrare che il prodotto con elementi digitali è conforme ai requisiti essenziali di cui all'allegato I, occorre tenere conto delle soluzioni di elaborazione dati da remoto, a partire dalla valutazione dei rischi (articolo 13, paragrafo 2). Lo stesso vale per gli obblighi relativi al ciclo di vita, come la segnalazione di vulnerabilità attivamente sfruttate e incidenti gravi (articolo 14).

179. Lo scopo dei presenti orientamenti è offrire ulteriori indicazioni ai fabbricanti per aiutarli a determinare se un proprio prodotto con elementi digitali comprenda soluzioni di elaborazione dati da remoto quali definite nel regolamento sulla ciberresilienza e come adempiere ai rispettivi obblighi di conformità a tale riguardo. Dopo un'analisi iniziale delle definizioni e dei considerando contenuti nel regolamento sulla ciberresilienza, i presenti orientamenti forniranno alcune domande volte ad aiutare i fabbricanti a capire se il proprio prodotto con elementi digitali comprenda una soluzione di elaborazione dati da remoto (cfr. sezione *8.1* Che *cosa costituisce una soluzione di elaborazione dati da remoto per un prodotto con elementi digitali?*). Saranno quindi illustrate le implicazioni tecniche delle soluzioni di elaborazione dati da remoto e le modalità di valutazione della conformità al regolamento sulla ciberresilienza (cfr. sezione *8.2 Implicazioni pratiche e tecniche delle soluzioni di elaborazione dati da remoto e del ricorso* a soluzioni di terzi).

180. Il concetto di «elaborazione dati da remoto» è di fatto definito all'articolo 3, punto 2), come «qualsiasi elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità e la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni». Le soluzioni di elaborazione dati da remoto sono pertanto definite come gli elementi software («la parte di un sistema di informazione elettronico costituita da un codice informatico», quale definito all'articolo 3, punto 4)) dell'elaborazione dei dati a distanza. Non si intende pertanto includere nell'ambito della definizione di prodotto con elementi digitali l'hardware su cui può basarsi l'elaborazione remota dei dati.

181. I considerando 11 e 12 forniscono ulteriori spiegazioni sul modo in cui tale concetto dovrebbe essere interpretato. Il considerando 11 chiarisce che l'obiettivo di comprendere le soluzioni di elaborazione dati da remoto è che «i prodotti siano protetti adeguatamente nella loro interezza dai fabbricanti, indipendentemente dal fatto che i dati siano trattati o conservati localmente sul dispositivo dell'utente o a distanza dal fabbricante». Il considerando precisa inoltre che «[i] requisiti relativi alle soluzioni di elaborazione dati da remoto che rientrano nell'ambito di applicazione del presente regolamento non comportano pertanto misure tecniche, operative o organizzative volte a gestire i rischi posti alla sicurezza dei sistemi informativi e di rete di un fabbricante nel loro complesso».

182. Pertanto dal considerando 11 si evince che l'intento non è che i requisiti del regolamento sulla ciberresilienza coprano l'intera infrastruttura informatica di un'organizzazione, ma solo i componenti software che consentono l'esecuzione della soluzione di elaborazione dati. Ad esempio, i sistemi interni relativi alle risorse umane proprie del fabbricante stesso, alle relative buste paga, alla sua gestione delle relazioni con i clienti, alle pipeline di integrazione continua/distribuzione continua (CI/CD) e alla distribuzione di aggiornamenti di sicurezza alle proprie sedi periferiche non dovrebbero essere considerati soluzioni di elaborazione dati da remoto. Analogamente, i sistemi legati alle attività di audit e test, quali i test di penetrazione, la ricerca delle minacce e il red teaming, non rientrano nell'ambito della definizione di prodotto con elementi digitali disciplinato dal regolamento sulla ciberresilienza. È importante osservare che, sebbene l'effettuazione di prove e riesami efficaci e periodici della sicurezza del prodotto con elementi digitali sia un requisito essenziale di cui all'allegato I, parte II, punto 3, del regolamento sulla ciberresilienza, ciò non significa che tali attività debbano essere considerate soluzioni di elaborazione dati da remoto per il prodotto con elementi digitali.

183. Il considerando 12 si concentra sui servizi cloud e approfondisce le circostanze in cui i servizi cloud possono essere considerati soluzioni di elaborazione dati da remoto. Il considerando si conclude ricordando che i servizi di cloud computing e i modelli di servizi cloud rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 (NIS 2) ([28]), che stabilisce requisiti di gestione dei rischi di cibersicurezza per i fornitori di servizi di cloud computing. Tali requisiti sono ulteriormente specificati dal regolamento di esecuzione (UE) 2024/2690 della Commissione ([29]).

8.1. **Che cosa costituisce una soluzione di elaborazione dati da remoto per un prodotto con elementi digitali?**

184. La definizione di elaborazione dati da remoto cui all'articolo 3, punto 2), si basa su tre elementi: i) il fatto che l'elaborazione avvenga «a distanza»; ii) il fatto che l'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni; e iii) il fatto che il software sia progettato e sviluppato dal fabbricante o sotto la sua responsabilità. Nelle tre sottosezioni seguenti ciascuno di questi elementi è esaminato in modo più dettagliato.

([28]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Regolamento di esecuzione (UE) 2024/2690 della Commissione, del 17 ottobre 2024, recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari (GU L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *La nozione di «a distanza»*

185. La nozione di «a distanza» di cui all'articolo 3, punto 2), è pertinente ma non sufficiente per determinare se un prodotto con elementi digitali comprenda una soluzione di elaborazione dati da remoto. Inoltre, data la varietà di soluzioni che potrebbero rientrare in tale concetto, non è possibile fornire una definizione esaustiva di «a distanza». È necessaria una valutazione caso per caso da parte del fabbricante.

186. Il considerando 11 del regolamento sulla ciberresilienza menziona i dati trattati o conservati «a distanza dal fabbricante» rispetto ai dati trattati o conservati «localmente sul dispositivo dell'utente». L'elaborazione dei dati da remoto avviene generalmente al di fuori dell'ambiente utente di un prodotto con elementi digitali o dell'ambiente operativo di un'organizzazione (per un utente professionale). Ciò non impedisce tuttavia che il trattamento avvenga anche in prossimità del dispositivo («nell'*edge*»). La trasmissione di dati può essere cablata (ad esempio cavo ethernet) o senza fili (ad esempio Wi-Fi, Bluetooth). Il cloud computing, compreso l'edge computing, è un tipico esempio di elaborazione dati effettuata «a distanza». Ad esempio, nel caso di una funzione basata sul cloud a cui l'utente accede da un'applicazione mobile, parte del trattamento dei dati avviene sul cloud, al di fuori dell'ambiente dell'utente.

187. È importante notare che le soluzioni di elaborazione dati da remoto non sono necessariamente gestite su infrastrutture cloud di terzi. Anche l'elaborazione dati da remoto in esecuzione su server locali presso la sede del fabbricante può costituire una soluzione di elaborazione dati da remoto. In altre parole, una soluzione in esecuzione in loco e su un cloud privato può essere considerata una soluzione di elaborazione dati da remoto tanto quanto una soluzione in esecuzione su un cloud pubblico e fuori sede.

188. Le due domande decisive e cumulative che determinano se l'elaborazione dati rientri nell'ambito di applicazione del regolamento sulla ciberresilienza in quanto soluzione di elaborazione dati da remoto sono illustrate di seguito, nelle sezioni *8.1.2* e *8.2*. Se la risposta a entrambe le domande è affermativa, l'elaborazione dati da remoto si qualifica come soluzione di elaborazione dati da remoto.

8.1.2. *L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni?*

189. Come stabilito nella definizione di «elaborazione dati da remoto» di cui all'articolo 3, punto 2), affinché l'elaborazione dati a distanza possa essere considerata una soluzione di elaborazione dati da remoto, la sua assenza dovrebbe impedire al prodotto con elementi digitali di svolgere una delle sue funzioni. La nozione di «funzioni» inclusa in questa definizione non si limita alla «funzionalità principale» o alla «finalità prevista» del prodotto con elementi digitali, in quanto il regolamento sulla ciberresilienza non impone tale limitazione. Le funzioni che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza sono sia quelle volte a realizzare direttamente alla finalità prevista del prodotto con elementi digitali dal punto di vista dell'esperienza dell'utilizzatore sia quelle che supportano le prestazioni complessive del prodotto.

190. Tra gli esempi di funzioni in cui potrebbe verificarsi un'elaborazione dei dati a distanza e che impedirebbero a un prodotto con elementi digitali di svolgere una delle sue funzioni figurano: i) invio di comandi a un dispositivo; ii) sincronizzazione dei file; iii) onboarding dell'utente; iv) configurazione (personalizzazione del prodotto con elementi digitali); v) distribuzione automatizzata degli aggiornamenti, compresi l'aggiornamento delle funzioni e le patch di sicurezza; vi) gestione dell'identità e dell'accesso.

191. In alcuni casi l'utente può utilizzare una funzione sia a distanza che manualmente (ad esempio accendendo una lampadina con un'app o manualmente). Questa opzione non esclude che l'elaborazione dei dati associata all'esecuzione a distanza della funzione possa essere considerata una soluzione di elaborazione dati da remoto. Anche l'esecuzione di tale funzione a distanza è considerata parte delle funzioni offerte dal prodotto con elementi digitali.

192. Per contro, qualora l'assenza di una determinata elaborazione dati non impedisca al prodotto con elementi digitali di svolgere una delle sue funzioni, tale elaborazione non è considerata una soluzione di elaborazione dati da remoto ai sensi del regolamento sulla ciberresilienza. Ciò comprende, ad esempio, l'analisi a distanza dei dati di telemetria raccolti a fini puramente statistici o per lo sviluppo di prodotti futuri.

193. Tuttavia anche quando l'elaborazione dei dati non supporta una funzione di un prodotto con elementi digitali, i fabbricanti potrebbero dover considerare, nell'ambito della propria valutazione dei rischi di cibersicurezza, se tali componenti remoti introducano rischi per il prodotto con elementi digitali (ad esempio alla luce dell'ambiente operativo del prodotto) e attenuare di conseguenza tali rischi (ad esempio attraverso misure di attenuazione a livello di prodotto).

194. I siti web rappresentano un caso specifico meritevole di ulteriori chiarimenti, come spiegato anche nella *sezione 2.1 Immissione sul mercato*. Come spiegato al considerando 11 del regolamento sulla ciberresilienza, i siti web non rientrano nella definizione di soluzione di elaborazione dati da remoto se non supportano una funzione di un prodotto con elementi digitali. Il fatto che un sito web contenga informazioni su un prodotto con elementi digitali non è sufficiente per ritenere che tale sito rientri nella definizione di soluzione di elaborazione dati da remoto, anche se il prodotto reindirizza ad esso. Ad esempio, il reindirizzamento degli utenti su una pagina web esterna che contiene le informazioni e le istruzioni per gli utilizzatori non costituisce una soluzione di elaborazione dati da remoto. Per contro, un sito web può rientrare nella definizione di soluzione di elaborazione dati da remoto se consente o supporta una funzione di un prodotto con elementi digitali. Ad esempio, un portale di autenticazione che rilascia le credenziali o i token necessari per il funzionamento del prodotto con elementi digitali sarebbe considerato una soluzione di elaborazione dati da remoto (a condizione che siano soddisfatti anche gli altri criteri della definizione).

8.1.3. *Il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità?*

195. La definizione di «elaborazione dati da remoto» di cui all'articolo 3, punto 2), del regolamento sulla ciberresilienza specifica inoltre che il software di tale elaborazione dati a distanza deve essere progettato e sviluppato dal fabbricante o sotto la sua responsabilità. L'elaborazione dati da remoto interamente sviluppata e progettata dal fabbricante (internamente) rientrerebbe naturalmente nella definizione di soluzione di elaborazione dati da remoto. Lo stesso varrebbe anche nel caso in cui i fabbricanti si affidassero a un fornitore esterno di servizi per lo sviluppo e la progettazione di una soluzione (ossia «sotto la sua responsabilità»). L'espressione «sotto la responsabilità del fabbricante» si riferisce a soluzioni di elaborazione da remoto realizzate su misura per il fabbricante. Si tratta dei casi in cui il fabbricante non si limita a concedere in licenza un prodotto con elementi digitali o un servizio esistente che un fornitore di servizi offre ai suoi clienti o le relative versioni leggermente modificate. «Sotto la responsabilità del fabbricante» significa che il software è realizzato esclusivamente dal fabbricante o per suo conto, sulla base dei progetti e delle specifiche da esso forniti.

196. Ai fini della comprensione del concetto di soluzione di elaborazione dati da remoto, la questione di «chi gestisce la soluzione» non costituisce un fattore determinante, in quanto la definizione contenuta nel regolamento sulla ciberresilienza si riferisce soltanto alla progettazione e allo sviluppo della soluzione di elaborazione dati da remoto. Ciò è coerente con l'approccio del regolamento sulla ciberresilienza in base al quale i requisiti e gli obblighi ricadono sui fabbricanti e non riguardano il funzionamento del prodotto con elementi digitali. Quando progettano e sviluppano soluzioni che sono poi gestite da terzi, i fabbricanti rimangono responsabili della conformità ai requisiti essenziali stabiliti dal regolamento sulla ciberresilienza per il prodotto con elementi digitali che immettono sul mercato.

197. È necessario distinguere tra i casi in cui la progettazione e lo sviluppo sono effettuati dai fabbricanti (o sotto la loro responsabilità) e i casi di ricorso a soluzioni di terzi non progettate e sviluppate dai fabbricanti (o sotto la loro responsabilità). A titolo di esempio, è utile considerare i modelli più comuni di servizi cloud che prevedono diversi gradi di controllo da parte degli utenti e che sono citati anche al considerando 12 del regolamento sulla ciberresilienza, ossia il servizio a livello di software (*Software-as-a-Service* – SaaS), il servizio a livello di piattaforma (*Platform-as-a-Service* – PaaS) e il servizio a livello di infrastruttura (*Infrastructure-as-a-Service* – IaaS).

198. Nel caso di una soluzione IaaS di terzi, il fabbricante non gestisce né controlla le risorse fisiche e virtuali sottostanti (come l'hardware sottostante e l'ipervisore (*hypervisor*) del fornitore di servizi cloud), ma è in grado di implementare ed eseguire software a propria discrezione utilizzando tali risorse, quali sistemi operativi e applicazioni. Tale software è progettato e sviluppato dal fabbricante, o sotto la sua responsabilità, e può pertanto essere considerato una soluzione di elaborazione dati da remoto (se soddisfa gli altri elementi della definizione).

199. Nel caso di una soluzione PaaS di terzi, il fabbricante implementa una propria applicazione (creata o acquisita) utilizzando linguaggi di programmazione e ambienti di esecuzione forniti dal fornitore di servizi cloud e integra l'applicazione nel proprio prodotto con elementi digitali. Il fabbricante ha il controllo dell'applicazione ed eventualmente delle impostazioni di configurazione per l'ambiente di esecuzione. L'applicazione è pertanto progettata e sviluppata dal fabbricante, o sotto la sua responsabilità, e può pertanto essere considerata una soluzione di elaborazione dati da remoto (se soddisfa gli altri elementi della definizione).

200. Nel caso di una soluzione SaaS di terzi, il fornitore di SaaS offre al fabbricante un'applicazione completamente sviluppata da integrare nel prodotto con elementi digitali del fabbricante. Il fabbricante ha una capacità limitata di gestire le impostazioni di configurazione delle applicazioni specifiche dell'utente. L'applicazione non è pertanto progettata e sviluppata dal fabbricante o sotto la sua responsabilità.

201. Cionondimeno, laddove alcuni elementi non siano considerati una soluzione di elaborazione dati da remoto (ad esempio l'ipervisore nel caso di un'infrastruttura IaaS di terzi, il sistema operativo nel caso di una soluzione PaaS di terzi o l'applicazione SaaS di terzi), ma siano integrati nel prodotto con elementi digitali in modo tale da incidere sulla sua sicurezza, tali soluzioni dovrebbero essere considerate alla stregua di componenti di terzi. Il fabbricante è tenuto a individuare e valutare i rischi connessi all'integrazione di tali elementi e ad affrontarli applicando i requisiti essenziali al prodotto con elementi digitali stesso. A tal fine, se del caso, è possibile avvalersi delle funzioni di sicurezza messe a disposizione dal fornitore di servizi cloud attraverso il suo modello di responsabilità condivisa, qualora il fabbricante utilizzi o configuri tali funzioni per affrontare i rischi individuati. Inoltre il fabbricante è tenuto ad adempiere un obbligo analogo a quello di esercitare la dovuta diligenza di cui all'articolo 13, paragrafo 5, in relazione alla sicurezza di tali componenti, in modo proporzionato al rischio che la soluzione da remoto comporta per la sicurezza del prodotto con elementi digitali.

202. Pertanto riassumendo:

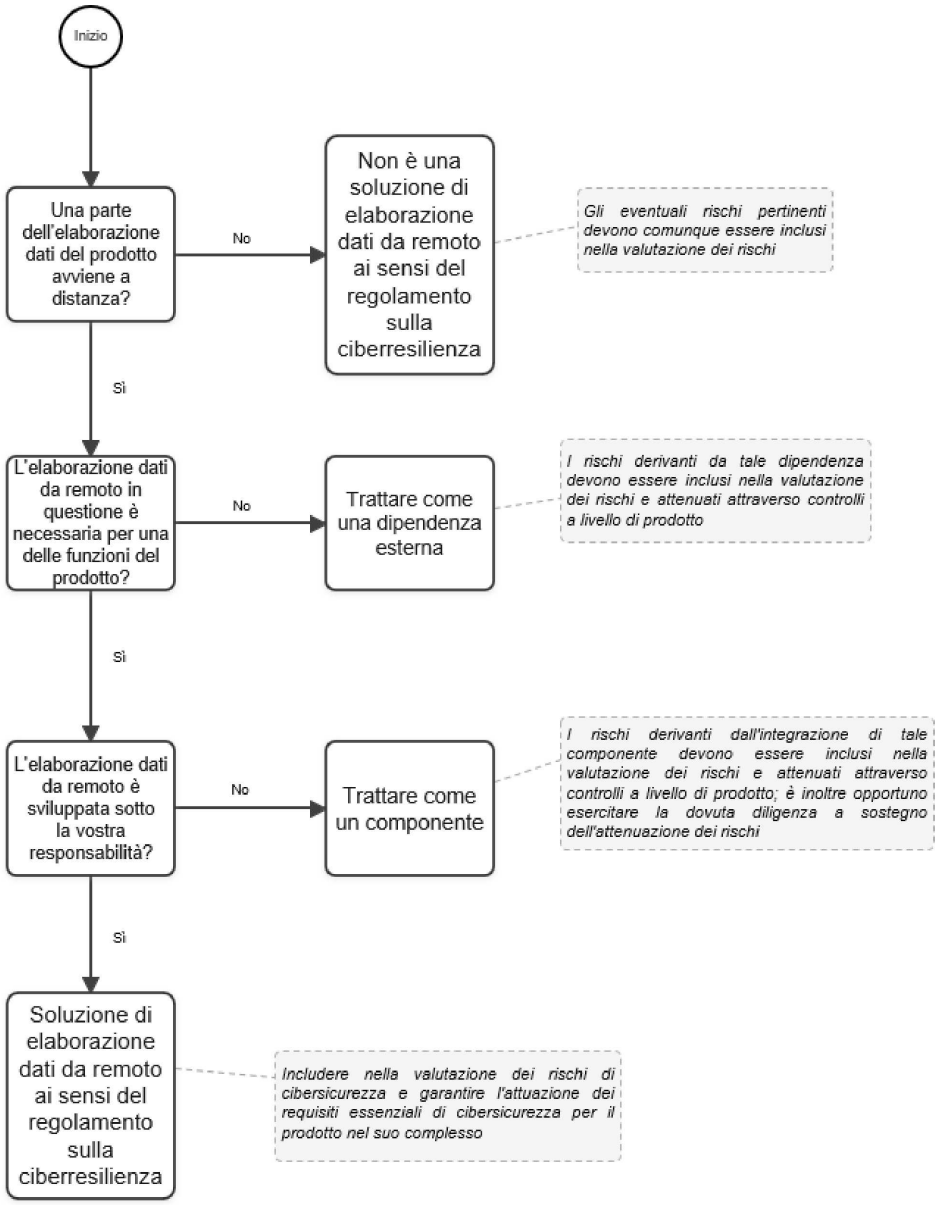
a) affinché l'elaborazione dei dati possa essere considerata una soluzione di elaborazione dati da remoto, la risposta a entrambe le domande poste nelle sezioni *8.1.2 L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni?* e *8.1.3 Il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità?* deve essere affermativa;

b) se la risposta alla domanda di cui alla sezione *8.1.2 L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni?* è negativa, i fabbricanti dovrebbero valutare i rischi derivanti dall'esistenza di tale elaborazione dati nell'ambito della propria valutazione dei rischi;

c) se la risposta alla domanda della sezione *8.1.2 L'assenza di tale elaborazione dati impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni?* è affermativa, ma la risposta alla domanda nella sezione *8.1.3 Il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità?* è negativa, i fabbricanti dovrebbero trattare la soluzione fornita da terzi alla stregua di un componente. Nell'ambito della valutazione dei rischi, i fabbricanti dovrebbero valutare i rischi derivanti dall'integrazione di tale soluzione e attenuarli di conseguenza. I fabbricanti dovrebbero inoltre esercitare la dovuta diligenza.

Figura 9

diagramma di flusso stilizzato per determinare se un prodotto con elementi digitali contiene soluzioni di elaborazione dati da remoto



8.2. Implicazioni pratiche e tecniche delle soluzioni di elaborazione dati da remoto e del ricorso a soluzioni di terzi

203. Il regolamento sulla ciberresilienza segue un approccio basato sul rischio, sancito dall'articolo 13, paragrafi 2 e 3, nonché dal primo requisito essenziale di cui all'allegato I, parte I, in base al quale «[i] prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi». Di conseguenza, nell'applicare i requisiti del regolamento sulla ciberresilienza alle soluzioni di elaborazione dati da remoto e nel trattare i rischi derivanti dai servizi di terzi integrati nel prodotto con elementi digitali dovrebbe essere adottato un approccio basato sul rischio.

204. In primo luogo, i fabbricanti dovrebbero i) indicare nella documentazione tecnica che il loro prodotto con elementi digitali comprende una soluzione di elaborazione dati da remoto o si basa su soluzioni da remoto di terzi e ii) descrivere tali soluzioni. Se la stessa soluzione di elaborazione dati da remoto supporta diversi prodotti con elementi digitali, la soluzione di elaborazione dati da remoto deve essere dichiarata nella documentazione tecnica di ciascun prodotto. La documentazione relativa a una soluzione di elaborazione dati da remoto che supporta diversi prodotti con elementi digitali può essere riutilizzata da una valutazione della conformità di un prodotto a quella di un altro.

205. Come indicato al considerando 11, le soluzioni di elaborazione dati da remoto che fanno parte del prodotto con elementi digitali e sono pertanto soggette alla valutazione della conformità del prodotto dovrebbero essere limitate ai moduli software responsabili della funzionalità del prodotto con elementi digitali e alle interfacce che tali moduli utilizzano con servizi esterni. Altri sistemi back-end che effettuano un trattamento successivo e con i quali il prodotto con elementi digitali non interagisce direttamente non sono considerati soluzioni di elaborazione dati da remoto.

206. Tuttavia tali sistemi back-end rimangono dipendenze esterne che devono essere prese in considerazione nell'ambito della valutazione dei rischi di cibersicurezza e sottoposte a misure di attenuazione a livello di prodotto. Di fatto la valutazione dei rischi effettuata dal fabbricante dovrebbe prendere in considerazione: i) i rischi connessi alle soluzioni di elaborazione dati da remoto; ii) i rischi connessi al ricorso a soluzioni da remoto di terzi (assimilabili a componenti di terzi); e iii) i rischi connessi all'ambiente del prodotto (ad esempio hardware sottostante). I fabbricanti dovrebbero effettuare controlli di sicurezza sul prodotto con elementi digitali stesso per attenuare tali rischi.

207. Inoltre nell'ambito della valutazione della conformità e/o dell'adempimento degli obblighi di dovuta diligenza relativi ai servizi da remoto di terzi, a sostegno della valutazione del fabbricante è possibile riutilizzare i documenti relativi alla garanzia di cui al seguente elenco non esaustivo:

a) documentazione comprovante l'adempimento degli obblighi di cui al regolamento di esecuzione (UE) 2024/2690 della Commissione;

b) documentazione comprovante l'adempimento degli obblighi di cui al regolamento (UE) 2022/2554 (DORA);

c) dichiarazione di conformità o certificato ottenuti nell'ambito di un sistema europeo di certificazione della cibersicurezza (adottato a norma del regolamento (UE) 2019/881, il regolamento sulla cibersicurezza);

d) documentazione comprovante la conformità alle norme ISO/IEC 27017: 2015 o ISO/IEC 27001: 2022.

208. Infine, nelle loro interazioni con i fornitori terzi di servizi da remoto, i fabbricanti devono attuare le misure di sicurezza più adeguate sulla base della propria valutazione dei rischi (e, se del caso, con il ricorso al modello di responsabilità condivisa del fornitore). Tali misure di attenuazione dovrebbero includere controlli di sicurezza per i propri prodotti con elementi digitali e la verifica delle misure di sicurezza fornite dagli stessi fornitori terzi (dovuta diligenza). Uno strumento per attenuare tali rischi può consistere nell'inserire garanzie di sicurezza negli accordi sul livello dei servizi con fornitori terzi, comprese garanzie che i fornitori gestiscano adeguatamente le vulnerabilità. Una modifica importante apportata alle soluzioni fornite dai fornitori terzi di servizi da remoto non dovrebbe essere considerata una modifica sostanziale del prodotto con elementi digitali, in quanto tali elementi non sono sotto la responsabilità del fabbricante. Tuttavia nell'ambito dei loro obblighi di dovuta diligenza e al fine di attenuare correttamente i rischi derivanti dal ricorso a fornitori terzi i fabbricanti sono incoraggiati ad assicurarsi che i propri fornitori terzi di servizi cloud li tengano adeguatamente informati in merito alle modifiche apportate alle proprie soluzioni. Sulla base di tali informazioni, i fabbricanti potrebbero dover rivedere la propria valutazione dei rischi. Nell'ambito della valutazione aggiornata dei rischi si dovrebbe verificare se i fornitori terzi di servizi continuino a fornire garanzie sufficienti in termini di cibersicurezza e se i controlli di sicurezza a livello di prodotto siano ancora adeguati. In alcuni casi, i fabbricanti potrebbero dover modificare tali controlli o cambiare fornitori terzi di servizi.

8.3. **Casi d'uso per le soluzioni di elaborazione dati da remoto**

Al fine di fornire ulteriori orientamenti pratici ai fabbricanti, in questa sezione è presentata una serie di casi d'uso fittizi, in cui sono descritti prodotti archetipici con elementi digitali che si basano sull'elaborazione dei dati da remoto ed è spiegato se tale elaborazione possa essere considerata una soluzione di elaborazione dati da remoto ai sensi del regolamento sulla ciberresilienza.

8.3.1. *Applicazione bancaria mobile*

Un'entità finanziaria immette sul mercato un'applicazione bancaria mobile. I sistemi back-end dell'applicazione supportano, tra l'altro, l'autenticazione, l'autorizzazione, la gestione dei conti e i pagamenti. L'entità finanziaria utilizza una strategia ibrida che si avvale sia di infrastrutture interne sia di soluzioni da remoto di terzi per supportare le funzionalità dell'applicazione. Queste includono:

un'infrastruttura self-hosted sviluppata dall'entità finanziaria:

— il cliente apre l'applicazione bancaria mobile ed è autenticato attraverso l'interfaccia bancaria, una soluzione self-hosted sviluppata dall'entità finanziaria che riceve le richieste dell'applicazione e restituisce le risposte corrispondenti. L'interfaccia bancaria verifica l'identità del cliente interrogando il sistema di gestione dei conti e consente l'accesso all'applicazione;

— il cliente dispone un bonifico tramite l'applicazione. L'applicazione trasmette l'istruzione all'interfaccia bancaria, che presenta una richiesta corrispondente al sistema di registro;

— il sistema di gestione dei conti e il sistema di registro, entrambi self-hosted ma logicamente separati dall'interfaccia bancaria, registrano l'operazione;

— il sistema di registro restituisce lo stato dell'operazione all'interfaccia bancaria, che presenta il risultato al cliente;

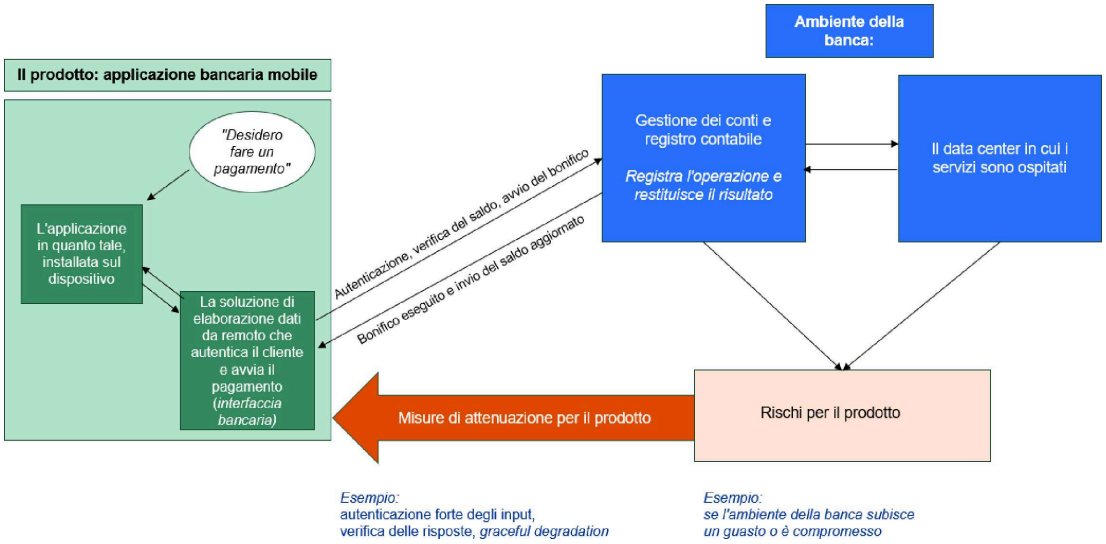
implicazioni per quanto riguarda le soluzioni di elaborazione dati da remoto:

— l'interfaccia bancaria è necessaria affinché l'applicazione possa svolgere le sue funzioni, vale a dire autenticare il cliente, trasmettere le istruzioni del cliente, comprese le istruzioni di pagamento e di trasferimento, e restituire lo stato risultante. L'interfaccia bancaria è progettata e sviluppata sotto la responsabilità del fabbricante. Poiché la risposta a entrambe le domande presentate nelle sezioni precedenti è affermativa, l'interfaccia bancaria deve essere considerata una soluzione di elaborazione dati da remoto. Deve pertanto essere inclusa nella valutazione dei rischi di cibersicurezza e nell'attuazione dei requisiti essenziali per il prodotto con elementi digitali nel suo complesso. La successiva elaborazione di un ordine una volta inviato, in particolare la registrazione dell'operazione nei sistemi di gestione dei conti e di registro, la liquidazione e la compensazione, è effettuata da sistemi con i quali l'applicazione non interagisce direttamente e, su questa base, non costituisce una soluzione di elaborazione dati da remoto;

— il sistema di gestione dei conti e il sistema di registro non si qualificano come soluzioni di elaborazione dati da remoto per l'applicazione bancaria. L'applicazione non interagisce direttamente con essi (ma interagisce invece con l'interfaccia bancaria, che a sua volta si avvale di essi). Sebbene la loro disponibilità possa essere necessaria per completare una funzione, nell'ambito di applicazione del regolamento sulla ciberresilienza rientrano soltanto le parti del sistema che interagiscono direttamente con il prodotto con elementi digitali. Essi non rientrano pertanto nella definizione di soluzione di elaborazione dati da remoto ai fini del regolamento sulla ciberresilienza. Tali sistemi rimangono tuttavia dipendenze esterne che possono comportare rischi significativi di cibersicurezza per il prodotto con elementi digitali. Ad esempio, la compromissione del sistema di registro potrebbe consentire a un soggetto malintenzionato di influenzare i risultati delle operazioni che vengono successivamente visualizzati nell'applicazione. Il fabbricante è pertanto tenuto a individuare e valutare tali rischi nell'ambito della valutazione dei rischi di cibersicurezza e ad attenuarli attraverso misure a livello di prodotto, quali un'autenticazione forte delle interfacce back-end, la protezione dell'integrità dei dati sulle operazioni, canali di comunicazione sicuri e la verifica delle risposte ricevute dall'applicazione;

Figura 10

rappresentazione stilizzata di un'applicazione bancaria basata su una soluzione di elaborazione dati da remoto



SaaS di terzi per l'assistenza ai clienti:

— l'entità finanziaria integra nella propria applicazione una soluzione di chat di assistenza alla clientela sviluppata e gestita da un fornitore terzo; il fornitore terzo ha scritto il codice del server di chat, ha realizzato l'interfaccia utente e gestisce l'infrastruttura in cui è implementata la chat (ossia il modello SaaS);

— quando il cliente invia una richiesta di assistenza, l'applicazione collega il cliente al servizio di terzi per avviare una sessione di chat e gestire il flusso di messaggistica, senza fornire a tale fornitore terzo l'accesso ai sistemi bancari di base;

implicazioni per quanto riguarda le soluzioni di elaborazione dati da remoto:

— la soluzione di chat di assistenza è necessaria affinché il prodotto con elementi digitali svolga una delle sue funzioni, ma non è progettata e sviluppata dall'entità finanziaria o sotto la sua responsabilità; non si tratta quindi di una soluzione di elaborazione dati da remoto. Dovrebbe però essere trattata come un componente di terzi. Il ricorso a tale servizio di terzi può creare rischi di cibersicurezza per l'applicazione bancaria, ad esempio nel caso in cui un soggetto malintenzionato utilizzasse il canale di chat per spacciarsi per la banca o per inviare contenuti malevoli agli utenti. L'entità finanziaria deve tenere conto di tali rischi nell'ambito della propria valutazione dei rischi di cibersicurezza e attenuarli attraverso misure a livello di prodotto, quali l'isolamento della funzione di chat dalle funzioni bancarie fondamentali, il controllo dei flussi di dati e la convalida dei contenuti. È inoltre opportuno esercitare la dovuta diligenza sul servizio a livello di software (SaaS).

8.3.2. *Termostato intelligente*

Un termostato intelligente consente agli utilizzatori di controllare la temperatura delle proprie abitazioni attraverso un'applicazione mobile. L'applicazione mobile e il termostato intelligente utilizzano l'elaborazione dei dati da remoto per lo scambio di dati (ad esempio la richiesta di aumentare la temperatura) e la memorizzazione di dati (ad esempio le preferenze dell'utilizzatore). Queste funzioni sono state sviluppate e progettate sotto la responsabilità del fabbricante, ma sono eseguite su un'infrastruttura fisica e virtuale sottostante fornita da terzi (IaaS di terzi).

Poiché il termostato intelligente non sarebbe in grado di svolgere le sue funzionalità intelligenti senza tale elaborazione dati da remoto, la sua assenza impedirebbe al prodotto con elementi digitali di svolgere una o più delle sue funzioni. Inoltre il software è stato sviluppato e progettato sotto la responsabilità del fabbricante del termostato intelligente. Pertanto l'elaborazione dei dati da remoto rientra nella definizione di soluzione di elaborazione dati da remoto ai sensi del regolamento sulla ciberresilienza.

Ai fini della conformità al regolamento sulla ciberresilienza, il fabbricante del termostato intelligente deve documentare la soluzione di elaborazione dati da remoto e il ricorso all'IaaS di terzi nella documentazione tecnica del prodotto con elementi digitali, compresi i dettagli del servizio appaltato. Il fabbricante deve tenere conto di tali elementi nella valutazione dei rischi, che comprende la finalità prevista e l'uso ragionevolmente prevedibile del prodotto con elementi digitali. Il fabbricante attua i requisiti essenziali del regolamento sulla ciberresilienza sulla base dei rischi inerenti alla soluzione di elaborazione dati da remoto. Per quanto riguarda il servizio IaaS di terzi, il fabbricante deve garantire che le misure di sicurezza fornite dal fornitore terzo siano adeguate e/o adottare misure pertinenti rispetto all'infrastruttura. Per le prime, il fabbricante potrebbe, ad esempio, chiedere la documentazione comprovante l'adempimento degli obblighi previsti dalla direttiva NIS 2.

8.3.3. *Lettori elettronici*

Il produttore di un software di lettura elettronica utilizza un servizio di archiviazione SaaS di terzi per archiviare i libri elettronici acquistati dai clienti e consentire loro di accedere ai propri libri. L'assenza di tale servizio di archiviazione impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni, ma il servizio di archiviazione SaaS di terzi non è sviluppato dal fabbricante o sotto la sua responsabilità; il fornitore del SaaS lo mette a disposizione dei clienti per qualsiasi caso d'uso.

Il servizio di archiviazione SaaS non soddisfa la definizione di soluzione di elaborazione dati da remoto. Tuttavia il fabbricante di lettori elettronici si affida a tale servizio esterno per il funzionamento del proprio prodotto con elementi digitali e deve pertanto tenere conto dei rischi associati nella sua valutazione dei rischi di cibersicurezza. Il fabbricante di lettori elettronici deve trattare il SaaS come un componente. Il fabbricante deve attuare adeguate misure di sicurezza a livello di prodotto, quali l'autenticazione sicura, la cifratura e la protezione dell'integrità delle comunicazioni con il servizio di memorizzazione. Inoltre l'esercizio della dovuta diligenza nella selezione e nell'integrazione del fornitore di SaaS faciliterà l'adempimento degli obblighi del fabbricante, affinché il prodotto con elementi digitali nel suo complesso possa soddisfare i requisiti essenziali.

8.3.4. *Robot industriali*

Un robot industriale ha il compito di prelevare componenti. Il robot invia le informazioni raccolte tramite telecamere a un servizio remoto progettato e sviluppato dal fabbricante. Questo servizio funziona su un'infrastruttura fisica e virtuale sottostante fornita da un fornitore terzo di servizi (IaaS di terzi). Il servizio cloud calcola la posizione di un componente sulla base delle immagini di una telecamera e invia comandi al robot affinché prelevi i componenti.

L'assenza di tale elaborazione dei dati impedirebbe al robot industriale di prelevare i componenti e quindi di svolgere una delle sue funzioni. Inoltre il software che gira sull'infrastruttura è stato progettato e sviluppato dal fabbricante. Il software progettato e sviluppato dal fabbricante soddisfa la definizione di soluzione di elaborazione dati da remoto.

Il fabbricante del robot industriale deve documentare la soluzione di elaborazione dati da remoto e il ricorso all'IaaS di terzi nella documentazione tecnica del prodotto con elementi digitali (compresi i dettagli del servizio appaltato). Il fabbricante deve inoltre tenere conto di tali elementi nella valutazione dei rischi, che comprende la finalità prevista e l'uso ragionevolmente prevedibile del prodotto con elementi digitali. Il fabbricante attua i requisiti essenziali del regolamento sulla ciberresilienza per il prodotto con elementi digitali, compresa la relativa soluzione di elaborazione dati da remoto, sulla base dei rischi. Inoltre l'esercizio della dovuta diligenza nella selezione del fornitore IaaS contribuirà all'adempimento degli obblighi del fabbricante. Ad esempio, il fabbricante potrebbe chiedere la documentazione comprovante l'adempimento degli obblighi previsti dalla direttiva NIS 2.

8.3.5. *Rete cellulare*

Uno smartphone si basa su una rete 5G per fornire agli utenti connessione internet, chiamate telefoniche e messaggi (connettività mobile). La rete cellulare è sviluppata e progettata da operatori di telecomunicazioni. La rete comprende piccole celle e torri cellulari e altre apparecchiature di rete.

Il prodotto con elementi digitali dovrebbe essere in grado di connettersi correttamente a una rete; questa è una delle sue funzioni. Tuttavia il fatto che tale rete sia in funzione o meno non è pertinente per accertare se il prodotto con elementi digitali funzioni correttamente. La rete è solo un canale di comunicazione e non è necessaria affinché il prodotto con elementi digitali svolga la sua funzione di «connettersi correttamente a una rete». Analogamente, un cavo ethernet, un router o un segnale Wi-Fi non è considerato un'elaborazione dati la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni, ma piuttosto un elemento che consente la comunicazione/connettività.

Di conseguenza, la rete cellulare non soddisfa la definizione di soluzione di elaborazione dati da remoto. La rete non dovrebbe essere considerata un componente di terzi, poiché non vi è un software integrato nel prodotto con elementi digitali, ma il prodotto semplicemente utilizza tale rete. Pertanto non è necessario che il fabbricante eserciti gli obblighi di dovuta diligenza nei confronti del fornitore della rete.

9. **ELEMENTI AGGIUNTIVI**

9.1. **Obblighi di segnalazione**

209. A norma dell'articolo 14, paragrafi 1, e 3, del regolamento sulla ciberresilienza, un fabbricante è tenuto a notificare contemporaneamente al CSIRT designato come coordinatore e all'ENISA i) qualsiasi vulnerabilità attivamente sfruttata contenuta nel proprio prodotto con elementi digitali di cui viene a conoscenza; e ii) qualsiasi incidente grave che abbia un impatto sulla sicurezza del prodotto con elementi digitali di cui viene a conoscenza.

210. Conformemente all'articolo 69, paragrafo 3, e all'articolo 71, paragrafo 2, secondo comma, l'obbligo di rispettare l'articolo 14 si applica a decorrere dall'11 settembre 2026 a tutti i prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sulla ciberresilienza, compresi i prodotti con elementi digitali immessi sul mercato prima dell'11 dicembre 2027. Inoltre, a differenza degli obblighi di gestione delle vulnerabilità, che continuano ad applicarsi solo per la durata del periodo di assistenza di un prodotto, gli obblighi di segnalazione continuano ad applicarsi oltre il termine del periodo di assistenza di un prodotto con elementi digitali. Se un prodotto con elementi digitali è stato immesso sul mercato prima dell'11 dicembre 2027 o se il suo periodo di assistenza è terminato, il fabbricante non è tenuto a rispettare gli obblighi di gestione delle vulnerabilità di cui all'allegato I, parte II.

211. È opportuno ricordare che l'obbligo di segnalare tali eventi scatta nel momento in cui il fabbricante viene a conoscenza del fatto che una vulnerabilità è attivamente sfruttata o che si è verificato un incidente grave che ha compromesso la sicurezza del suo prodotto con elementi digitali. Pertanto gli orientamenti sul momento in cui si ritiene che un fabbricante sia venuto a conoscenza dovrebbero aiutare i fabbricanti a determinare il momento in cui iniziano a decorrere i termini di segnalazione applicabili.

212. I fabbricanti possono essere soggetti a obblighi di segnalazione comparabili a norma di diversi atti dell'UE. Per garantire che il concetto di «venire a conoscenza» sia interpretato in modo coerente e per agevolare il rispetto di tali obblighi da parte dei fabbricanti, i presenti orientamenti sono allineati al considerando 31 del regolamento di esecuzione (UE) 2024/2690 della Commissione e alla sezione II, lettera A, delle linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR).

213. In alcuni casi un fabbricante potrebbe rilevare un evento sospetto, oppure un terzo, come una persona fisica, un cliente, un soggetto, un'autorità, organizzazione mediatica o un'altra fonte, potrebbe sottoporre alla sua attenzione un possibile incidente o una potenziale vulnerabilità. In questi casi il fabbricante dovrebbe valutare tempestivamente l'evento sospetto per determinare se costituisca una vulnerabilità attivamente sfruttata o un incidente grave avente un impatto sulla sicurezza del prodotto con elementi digitali. Il fabbricante è quindi da ritenersi a conoscenza del fatto se, dopo tale valutazione iniziale, è ragionevolmente certo che: i) una vulnerabilità contenuta nel suo prodotto con elementi digitali sia attivamente sfruttata; o ii) si sia verificato un incidente grave che ha compromesso la sicurezza del suo prodotto con elementi digitali.

214. Pertanto il momento in cui si può ritenere che un fabbricante sia a conoscenza dipenderà dalle circostanze della specifica vulnerabilità attivamente sfruttata o dell'incidente grave. In alcuni casi il fatto che una vulnerabilità sia attivamente sfruttata o che un incidente grave stia avendo un impatto sulla sicurezza di un prodotto con elementi digitali risulterà relativamente evidente fin dall'inizio. In altri può essere necessario un certo tempo per stabilire se un prodotto con elementi digitali sia interessato da una vulnerabilità e se tale vulnerabilità sia sfruttata da un soggetto malintenzionato o se un incidente incida sulla sicurezza di un prodotto con elementi digitali. Occorre tuttavia porre l'accento sulla necessità di agire in modo tempestivo per effettuare la valutazione iniziale al fine di determinare se tali condizioni siano effettivamente soddisfatte, in particolare quando la vulnerabilità può rappresentare un rischio significativo, e, in tal caso, per adottare misure correttive e notificarle in conformità del regolamento sulla ciberresilienza.

215. Inoltre la struttura degli obblighi di segnalazione impone ai fabbricanti di aggiornare progressivamente le proprie notifiche man mano che le indagini interne procedono e la loro conoscenza della vulnerabilità attivamente sfruttata o dell'incidente diventa più dettagliata. In particolare, i fabbricanti sono tenuti a presentare una notifica di preallarme contenente informazioni limitate senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui sono venuti a conoscenza. Ulteriori informazioni sono successivamente richieste nell'ambito della notifica da presentare senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui sono venuti a conoscenza («notifica entro 72 ore»). La relazione completa deve essere presentata entro 14 giorni dalla messa a disposizione di una misura correttiva o di attenuazione per le vulnerabilità attivamente sfruttate, oppure entro un mese dalla notifica entro 72 ore per gli incidenti gravi.

216. Come ricordato anche nella sezione *3.3.1 Sostegno duraturo e garanzia della sostenibilità economica* del software libero e open source, a norma dell'articolo 24, paragrafo 3, anche i gestori di software open source sono tenuti a segnalare le vulnerabilità attivamente sfruttate ([30]). Tale obbligo scatta nel momento in cui si viene a conoscenza di una vulnerabilità attivamente sfruttata, e non semplicemente nel caso in cui esista una vulnerabilità nel codice sorgente di un software libero e open source di cui tale soggetto è il gestore. In pratica, poiché i componenti software liberi e open source sono generalmente integrati a valle in altri prodotti con elementi digitali, è probabile che un gestore venga a conoscenza dello sfruttamento attivo attraverso segnalazioni di terzi, che individuano lo sfruttamento nei componenti software liberi e open source integrati in altri prodotti con elementi digitali. Ciò può verificarsi, ad esempio, nel caso in cui il fabbricante di un prodotto con elementi digitali rilevi lo sfruttamento attivo di un componente software libero e open source integrato nel proprio prodotto e lo segnali al gestore di tale componente; oppure qualora un utilizzatore o un ricercatore nel settore della sicurezza riscontri prove dello sfruttamento di un componente software libero e open source integrato in un prodotto con elementi digitali e segnali tale sfruttamento attivo al gestore del componente.

217. È inoltre opportuno chiarire che, poiché l'obbligo di segnalare le vulnerabilità attivamente sfruttate si applica nel momento in cui il fabbricante viene a conoscenza di tale sfruttamento, quest'ultimo non è tenuto a segnalare le vulnerabilità del cui sfruttamento attivo era già venuto a conoscenza prima dell'11 settembre 2026 (data in cui inizia ad applicarsi l'obbligo di segnalazione). Il regolamento sulla ciberresilienza non richiede pertanto la segnalazione retroattiva di tali vulnerabilità. Per contro, l'obbligo si applica qualora il fabbricante fosse a conoscenza di una vulnerabilità prima dell'11 settembre 2026, ma non fosse, in quel momento, a conoscenza di uno sfruttamento attivo della stessa (perché non si era ancora verificato o perché il fabbricante non ne era venuto a conoscenza). Se, successivamente all'11 settembre 2026, si verifica uno sfruttamento attivo o il fabbricante ne viene a conoscenza, la vulnerabilità è considerata una vulnerabilità attivamente sfruttata soggetta all'obbligo di segnalazione.

218. Analogamente, un fabbricante è tenuto solo a segnalare le vulnerabilità attivamente sfruttate contenute nel proprio prodotto con elementi digitali. Se un prodotto con elementi digitali contiene una vulnerabilità attivamente sfruttata derivante da un componente di terzi, il fabbricante del prodotto con elementi digitali è tenuto a notificare tale vulnerabilità attivamente sfruttata. Tuttavia, se un fabbricante è a conoscenza del fatto che un componente di terzi contiene una vulnerabilità, ma tale vulnerabilità i) non può essere sfruttata nel suo prodotto con elementi digitali (ad esempio perché il codice vulnerabile non è accessibile) oppure ii) non è stata sfruttata nel suo prodotto con elementi digitali, tale vulnerabilità non è considerata una vulnerabilità attivamente sfruttata contenuta nel suo prodotto con elementi digitali e pertanto non è soggetta alla segnalazione obbligatoria da parte di tale fabbricante. A norma dell'articolo 15 del regolamento sulla ciberresilienza, Il fabbricante in questione può comunque notificare tale vulnerabilità su base volontaria. È inoltre tenuto a rispettare i requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II, del medesimo regolamento, nonché a segnalare la vulnerabilità alla persona o al soggetto che si occupa della fabbricazione o della manutenzione del componente, conformemente all'articolo 13, paragrafo 6, e come ulteriormente spiegato nella sezione *9.2.1 Segnalazione a monte e condivisione delle* correzioni di sicurezza.

([30]) Nella misura in cui il gestore è coinvolto nello sviluppo di un prodotto con elementi digitali.

219. Dopo essere venuti a conoscenza di una vulnerabilità attivamente sfruttata o di un incidente grave, i fabbricanti sono inoltre tenuti, a norma dell'articolo 14, paragrafo 8, a informare gli utilizzatori interessati e, se del caso, tutti gli utilizzatori. Qualora non vi provvedano tempestivamente, i CSIRT che hanno ricevuto la notifica possono fornire tali informazioni agli utilizzatori quando ciò sia ritenuto proporzionato e necessario per prevenire o attenuare l'impatto di tale vulnerabilità o incidente.

220. In linea con l'approccio basato sul rischio del regolamento sulla ciberresilienza, l'obbligo di informare gli utilizzatori di cui all'articolo 14, paragrafo 8, deve essere applicato in modo proporzionato e basato sul rischio. In particolare, la comunicazione di informazioni su una vulnerabilità attivamente sfruttata o su un incidente grave non implica che tali informazioni debbano essere rese pubbliche o divulgate indiscriminatamente. Se del caso, e tenuto conto della natura del prodotto con elementi digitali, degli utilizzatori interessati e della vulnerabilità o del potenziale impatto dell'incidente, i fabbricanti possono limitare la divulgazione di informazioni dettagliate agli utilizzatori o ai clienti interessati. Ciò vale in particolare per i prodotti con elementi digitali utilizzati in ambienti sensibili o essenziali, in cui la divulgazione al pubblico di dettagli tecnici potrebbe di per sé aumentare i rischi di cibersicurezza o facilitare un ulteriore sfruttamento.

221. Una volta che la vulnerabilità sia stata adeguatamente affrontata o attenuata, potrebbe essere opportuna una divulgazione più ampia. Ciò sarebbe opportuno ad esempio qualora la divulgazione contribuisse a sensibilizzare l'opinione pubblica o consentisse agli utilizzatori di verificare che i propri prodotti con elementi digitali non siano più interessati dalla vulnerabilità. In questi casi il livello di dettaglio e la tempistica di un'eventuale divulgazione più ampia dovrebbero rimanere proporzionati e tenere conto dei rischi residui di sfruttamento, della natura del prodotto con elementi digitali e degli interessi degli utilizzatori interessati. Inoltre l'allegato I, parte II, punto 4, impone ai fabbricanti di divulgare pubblicamente informazioni sulle vulnerabilità risolte una volta reso disponibile un aggiornamento di sicurezza.

9.2. **Gestione delle vulnerabilità**

9.2.1. *Segnalazione a monte e condivisione delle correzioni di sicurezza*

222. L'articolo 13, paragrafo 6, del regolamento sulla ciberresilienza impone ai fabbricanti di segnalare le vulnerabilità dei componenti integrati alla persona o al soggetto che si occupa della fabbricazione o della manutenzione di tale componente («segnalazione a monte»).

223. I fabbricanti sono tenuti a effettuare la segnalazione a monte solo in relazione alla versione del componente che integrano. Qualora la persona o il soggetto che si occupa della fabbricazione o della manutenzione del componente abbia stabilito politiche di sicurezza, processi di divulgazione coordinata delle vulnerabilità o canali designati per segnalare le vulnerabilità, i fabbricanti dovrebbero effettuare la segnalazione conformemente a tali politiche, in particolare quando la divulgazione prematura di vulnerabilità non risolte potrebbe aumentare i rischi di cibersicurezza. Inoltre, al fine di ridurre l'onere per i responsabili della manutenzione a monte, in particolare nei progetti open source, i fabbricanti non sono tenuti a effettuare la segnalazione a monte qualora possano confermare che la persona o il soggetto che si occupa della fabbricazione o della manutenzione di un componente è a conoscenza dell'esistenza di una vulnerabilità. I fabbricanti sono incoraggiati ad adottare misure ragionevoli per evitare la presentazione di doppie segnalazioni, ad esempio controllando le banche dati delle vulnerabilità accessibili al pubblico, gli avvisi di sicurezza specifici per progetto o i sistemi consolidati di tracciamento dei problemi prima di effettuare segnalazioni a monte.

224. I fabbricanti sono tenuti a segnalare a monte solo le vulnerabilità esistenti nel componente integrato in quanto tale, e non quelle derivanti dall'integrazione tra il componente e un altro codice sviluppato dal fabbricante o dall'integrazione di altri componenti. Possono tuttavia verificarsi situazioni in cui l'integrazione di un componente in uno specifico prodotto con elementi digitali mette in luce determinati comportamenti, interazioni o caratteristiche rilevanti per la sicurezza di tale componente che, se considerato isolatamente, non erano evidenti, o non erano facilmente identificabili. In questi casi i fabbricanti sono incoraggiati a comunicare tali informazioni alla persona o al soggetto che si occupa della fabbricazione o della manutenzione del componente, al fine di promuovere buone pratiche di gestione delle vulnerabilità volte a facilitare una correzione efficace e a migliorare la sicurezza complessiva dell'ecosistema dei componenti.

225. Infine i fabbricanti non sono tenuti a segnalare la vulnerabilità a monte anche nel caso in cui il componente non abbia più un responsabile della manutenzione oppure quando il fabbricante non si affida più al responsabile della manutenzione originale per le nuove versioni o le correzioni di sicurezza. In questi casi il fabbricante è comunque incoraggiato a informare gli utilizzatori di tale componente attraverso misure alternative ragionevoli, ad esempio attraverso i meccanismi esistenti a livello di comunità (quali mailing list o creazione di ticket) o attraverso registri pubblici delle vulnerabilità.

226. Inoltre, a norma dell'articolo 13, paragrafo 6, i fabbricanti che hanno sviluppato una modifica del software per affrontare una vulnerabilità in un componente integrato sono tenuti a condividere tale modifica del software («correzione di sicurezza») con la persona o il soggetto che si occupa della fabbricazione o della manutenzione del componente («condivisione a monte»).

227. Qualora i fabbricanti siano tenuti a condividere una correzione di sicurezza a norma dell'articolo 13, paragrafo 6, la correzione dovrebbe, se del caso, essere fornita in un formato leggibile da un dispositivo automatico, in modo che possa essere facilmente verificata e, se del caso, integrata dalla persona o dal soggetto che si occupa della fabbricazione o della manutenzione del componente. Nel caso di un componente libero e open source, la correzione di sicurezza dovrebbe essere condivisa in modo compatibile con la licenza di tale componente, ad esempio condividendola nell'ambito della stessa licenza o con una licenza che consenta al responsabile della manutenzione di distribuire la correzione con la propria licenza. Se il responsabile della manutenzione di tale componente dispone di orientamenti sulle modalità di condivisione delle correzioni di sicurezza, il fabbricante dovrebbe seguire tali orientamenti.

228. A norma del regolamento sulla ciberresilienza, i fabbricanti non sono tuttavia tenuti a garantire che le correzioni di sicurezza siano necessariamente accettate dalla persona o dal soggetto che si occupa della fabbricazione o della manutenzione del componente. Né sono tenuti ad assicurarsi che tali correzioni siano necessariamente integrate nell'archivio dei codici dei componenti, ad esempio nel caso in cui il responsabile della manutenzione preferisca un'opzione diversa per risolvere il problema. Allo stesso modo, i fabbricanti non sono tenuti ad accettare una soluzione proposta sviluppata dal responsabile della manutenzione dei componenti e potrebbero preferire attenuare il problema in altri modi adeguati.

229. In alcuni casi è possibile che la persona o il soggetto che si occupa della fabbricazione o della manutenzione del componente abbia già fornito una correzione di sicurezza per risolvere la vulnerabilità, ma che il fabbricante adotti una strategia di attenuazione diversa (ad esempio modificando una diversa configurazione). In questi casi il regolamento sulla ciberresilienza non impone al fabbricante di condividere la modifica di un'altra parte del sistema a monte. Il fabbricante è tuttavia incoraggiato a farlo qualora ciò possa essere utile alla persona o al soggetto che si occupa della manutenzione del componente.

9.2.2. *Vulnerabilità sfruttabili note*

230. Uno dei requisiti essenziali di cui all'allegato I, parte I, del regolamento sulla ciberresilienza prevede che, sulla base della valutazione dei rischi di cibersicurezza di cui all'articolo 13, paragrafo 2, e ove applicabile, i prodotti con elementi digitali debbano essere messi a disposizione sul mercato senza vulnerabilità sfruttabili note.

231. L'articolo 3, punto 41), definisce «vulnerabilità sfruttabile» «una vulnerabilità che può essere utilizzata efficacemente da un avversario in condizioni operative pratiche». Non tutte le vulnerabilità sono sfruttabili in condizioni operative pratiche, e alcune possono essere sfruttate solo in condizioni teoriche (ad esempio in laboratorio o in una simulazione) e/o non in condizioni che si verificherebbero nell'ambiente operativo di un prodotto con elementi digitali.

232. Il regolamento sulla ciberresilienza impone ai fabbricanti di disporre di politiche e procedure adeguate per gestire e correggere potenziali vulnerabilità segnalate da fonti interne o esterne (articolo 13, paragrafo 8). Non specifica tuttavia esplicitamente quando una vulnerabilità sfruttabile debba essere considerata nota al fabbricante, facendo così scattare l'obbligo di conformarsi a tale requisito essenziale al momento dell'immissione sul mercato.

233. Una vulnerabilità dovrebbe essere considerata nota quando è elencata nelle pertinenti banche dati delle vulnerabilità accessibili al pubblico, come la banca dati europea delle vulnerabilità istituita dall'articolo 12, paragrafo 2, della direttiva (UE) 2022/2555 o altre importanti banche dati delle vulnerabilità.

234. Inoltre una vulnerabilità può essere nota anche quando il fabbricante ne è venuto a conoscenza attraverso informazioni non pubbliche, ad esempio attraverso la divulgazione coordinata da parte di un ricercatore in materia di sicurezza o attraverso prove e analisi interne condotte dal fabbricante, anche, ad esempio, nell'ambito dell'utilizzo di servizi basati sull'IA. Allo stesso modo, una vulnerabilità può essere nota quando è stata segnalata pubblicamente e in modo visibile in organi di informazione affidabili, comprese pubblicazioni specializzate in materia di cibersicurezza o mezzi di comunicazione di massa generali.

235. Tuttavia il semplice fatto che una vulnerabilità sia segnalata o riscontrata non significa, di per sé, che sia sfruttabile nella pratica o applicabile allo specifico prodotto con elementi digitali in questione. Il fabbricante dovrà approfondire e confermare la veridicità di tali informazioni e l'applicabilità al proprio prodotto con elementi digitali. Di conseguenza tra la prima segnalazione della vulnerabilità e la sua conferma potrebbe intercorrere un periodo di tempo limitato. Come indicato nella sezione *9.1 Obblighi di* segnalazione, l'accento dovrebbe essere posto sulla necessità di agire in modo tempestivo per indagare e reagire.

236. Inoltre, a norma dell'articolo 13, paragrafo 1, l'obbligo per i fabbricanti di conformarsi ai requisiti essenziali di cui all'allegato I, parte I, si applica al momento dell'immissione sul mercato. In pratica, può accadere che vengano scoperte nuove vulnerabilità potenzialmente sfruttabili durante le fasi finali del ciclo di vita di sviluppo del prodotto con elementi digitali, anche poco prima che esso entri nella catena di distribuzione (e sia pertanto immesso sul mercato).

237. Poiché l'obbligo di immettere sul mercato prodotti con elementi digitali senza vulnerabilità sfruttabili note è un obbligo basato sul rischio, spetta al fabbricante determinare se, sulla base della valutazione dei rischi di cibersicurezza, il prodotto con elementi digitali possa essere immesso sul mercato in modo sicuro, in conformità del regolamento sulla ciberresilienza. In alternativa il fabbricante potrebbe decidere che una nuova vulnerabilità diventata nota debba essere corretta prima che il prodotto con elementi digitali possa essere immesso sul mercato. Nel prendere tale decisione, i fabbricanti dovrebbero tenere conto della gravità, della sfruttabilità e del potenziale impatto della vulnerabilità, nonché dei rischi che sorgono per il prodotto con elementi digitali una volta in uso. Possono anche tenere conto dei rischi legati al rinvio del rilascio del prodotto fino a quando la vulnerabilità non sia stata risolta, ad esempio perché la nuova versione corregge anche altre vulnerabilità sfruttabili o è necessaria per il funzionamento continuo di sistemi critici. In ogni caso, una volta che un prodotto con elementi digitali è immesso sul mercato, il fabbricante rimane soggetto all'obbligo di gestire le vulnerabilità in modo efficace e conformemente ai requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II.

9.2.3. *Prove e riesami efficaci e periodici*

238. L'allegato I, parte II, punto 3, impone ai fabbricanti di effettuare prove e riesami efficaci e periodici del prodotto con elementi digitali per tutto il relativo periodo di assistenza. L'esecuzione di prove periodiche non richiede la ripetizione meccanica, a intervalli fissi, di una campagna di prove invariata. Significa riesaminare periodicamente se nuovi elementi, quali l'individuazione di nuove minacce o la scoperta di nuove vulnerabilità, richiedano un aggiornamento delle prove esistenti, ed eseguire le prove di conseguenza.

239. La frequenza, il grado di approfondimento e il contenuto del riesame dovrebbero essere proporzionati al profilo di rischio di cibersicurezza del prodotto con elementi digitali, alla sua evoluzione nel tempo e allo stato del panorama delle minacce. Qualora il riesame individui nuovi elementi pertinenti che incidono sulla serie di prove, dovrebbero essere ideate ed eseguite prove nuove o modificate sul prodotto, al fine di garantire che nessuna vulnerabilità rimanga irrisolta. Ciò può includere la riesecuzione di prove esistenti qualora una modifica del prodotto con elementi digitali renda appropriati tali tipi di prove, come le prove di regressione.

240. Se il riesame non individua tale elementi, non è necessario ideare prove supplementari. Gli altri obblighi di gestione delle vulnerabilità, compreso quello di affrontare e correggere le vulnerabilità in relazione ai rischi posti, continuano ad applicarsi in parallelo.

9.3. **Interazione con altre normative**

9.3.1. *Regolamento (UE) 2019/2144 e regolamento (UE) n. 168/2013*

241. L'articolo 2, paragrafo 2, lettera c), del regolamento sulla ciberresilienza stabilisce che il regolamento non si applica ai prodotti con elementi digitali a cui si applica il regolamento (UE) 2019/2144. Il regolamento (UE) 2019/2144 si applica ai «veicoli delle categorie M, N e O, come definiti all'articolo 4 del regolamento (UE) 2018/858 e ai sistemi, componenti ed entità tecniche concepiti e costruiti per tali veicoli».

242. Analogamente, il regolamento delegato (UE) 2025/1535 della Commissione ha escluso dall'ambito di applicazione del regolamento sulla ciberresilienza i prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) n. 168/2013. Il regolamento (UE) n. 168/2013 si applica ai veicoli della categoria L e «a sistemi, componenti ed entità tecniche indipendenti, nonché parti e equipaggiamenti, progettati e fabbricati per tali veicoli» (articolo 2, paragrafo 1).

243. I veicoli cui si applicano tali regolamenti non sono soggetti al regolamento sulla ciberresilienza. Sono altresì necessari ulteriori chiarimenti per quanto riguarda l'ambito di applicazione dell'esenzione per i sistemi, i componenti, le entità tecniche indipendenti, le parti e gli equipaggiamenti (di seguito denominati, ai fini della presente sezione, «componenti») progettati e fabbricati per tali veicoli che sono considerati prodotti con elementi digitali ai sensi del regolamento sulla ciberresilienza.

244. Tali componenti non sono considerati soggetti al regolamento sulla ciberresilienza, a condizione che siano progettati e fabbricati esclusivamente per essere integrati nei veicoli disciplinati dai regolamenti (UE) 2019/2144 e (UE) n. 168/2013. Ciò vale indipendentemente dal fatto che il fabbricante di tale componente lo venda direttamente al costruttore del veicolo o a un altro operatore economico della catena di approvvigionamento del settore automobilistico, a condizione che il componente sia chiaramente destinato e idoneo solo all'integrazione finale all'interno di tali veicoli.

245. Per contro, un fabbricante che vende componenti generici che sono prodotti con elementi digitali che possono essere integrati in diversi tipi di prodotti, e non esclusivamente in veicoli disciplinati da tali regolamenti, è soggetto al regolamento sulla ciberresilienza.

246. Per stabilire se un componente sia immesso sul mercato ai sensi del regolamento sulla ciberresilienza occorre basarsi sulle condizioni oggettive alle quali tale componente è messo a disposizione. Se un fabbricante offre un componente che non è esclusivamente idoneo all'integrazione finale all'interno di tali veicoli attraverso canali di distribuzione aperti a clienti esterni alla catena di approvvigionamento del settore automobilistico, quali punti vendita al dettaglio generali o canali di vendita online che accettano ordini dal grande pubblico, tale componente rientra nell'ambito di applicazione del regolamento sulla ciberresilienza, indipendentemente da eventuali dichiarazioni relative al suo uso previsto. In tali circostanze, il componente non può essere considerato progettato e fabbricato esclusivamente per essere integrato nei veicoli disciplinati dai regolamenti (UE) 2019/2144 e (UE) n. 168/2013 e il fabbricante è tenuto a conformarsi al regolamento sulla ciberresilienza. Per contro, l'uso di canali di distribuzione riservati agli scambi tra imprese, limitati alla catena di approvvigionamento del settore automobilistico, potrebbe indicare che il componente è progettato e fabbricato esclusivamente per tale integrazione.

9.3.2. *Validità dei certificati di esame UE del tipo (articolo 69, paragrafo 1)*

247. L'articolo 69, paragrafo 1, del regolamento sulla ciberresilienza stabilisce che «[i] certificati di esame UE del tipo e le decisioni di approvazione rilasciati in relazione ai requisiti di cibersicurezza per i prodotti con elementi digitali soggetti ad altra normativa di armonizzazione dell'Unione diversa dal presente regolamento rimangono validi fino all'11 giugno 2028, a meno che non scadano prima di tale data o non sia altrimenti disposto in tali altre normative di armonizzazione dell'Unione, nel qual caso rimangono validi come indicato in tali normative».

248. Il mantenimento della validità di tali certificati e decisioni di approvazione dovrebbe essere inteso come limitato ai rischi di cibersicurezza e ai corrispondenti requisiti disciplinati dalla rispettiva normativa di armonizzazione dell'Unione sulla base della quale sono stati rilasciati. Per tali rischi, i fabbricanti non sono tenuti a valutare o dimostrare nuovamente la conformità ai soli fini del regolamento sulla ciberresilienza durante il periodo di validità di cui all'articolo 69, paragrafo 1, per i prodotti con elementi digitali che intendono immettere sul mercato a partire dall'11 dicembre 2027 (compreso) e fino all'11 giugno 2028 ([31]). Ciò vale per i certificati e le decisioni di approvazione rilasciati nei casi in cui la normativa di armonizzazione dell'Unione applicabile imponga al fabbricante di eseguire la procedura di valutazione della conformità tramite un organismo notificato, nonché nei casi in cui il fabbricante abbia scelto volontariamente di procedere in tal senso.

249. Di conseguenza l'esistenza di un certificato o di una decisione di approvazione in corso di validità a norma di altre normative di armonizzazione dell'Unione non esenta i fabbricanti dall'effettuazione di una valutazione completa dei rischi di cibersicurezza a norma del regolamento sulla ciberresilienza (o da altri obblighi previsti da tale regolamento). Consente loro invece di avvalersi delle certificazioni esistenti come prova di conformità per la propria procedura di valutazione della conformità, nella misura in cui i corrispondenti rischi di cibersicurezza siano già contemplati. Qualora la validità del certificato o della decisione di approvazione a norma di un'altra normativa di armonizzazione dell'Unione si estenda oltre l'11 giugno 2028, il fabbricante può tuttavia avvalersi di tale certificato o decisione ai fini del regolamento sulla ciberresilienza solo fino all'11 giugno 2028.

250. Qualora la valutazione dei rischi di cibersicurezza effettuata conformemente all'articolo 13, paragrafo 2, individui rischi aggiuntivi non contemplati dai requisiti di cibersicurezza su cui si basa il certificato o la decisione di approvazione esistente, i fabbricanti sono tenuti ad affrontare tali rischi conformemente al regolamento sulla ciberresilienza. In tali casi, ai fini della conformità, le lacune individuate devono essere valutate e attenuate, indipendentemente dal fatto che il certificato o la decisione di approvazione esistente sia ancora in corso di validità.

251. Si consideri ad esempio il caso in cui un prodotto con elementi digitali sia soggetto ai requisiti di cibersicurezza di cui al regolamento delegato (UE) 2022/30 della Commissione che integra la direttiva 2014/53/UE (regolamento delegato della direttiva sulle apparecchiature radio) e in cui il rilascio di un certificato di esame UE del tipo o di una decisione di approvazione sia avvenuto sulla base di tali requisiti. In tal caso, conformemente all'articolo 69, paragrafo 1, il certificato o la decisione mantiene la sua validità per i rischi di cibersicurezza contemplati da tale certificato e in relazione ai requisiti essenziali di cibersicurezza della direttiva 2014/53/UE (direttiva sulle apparecchiature radio).

252. In tali casi i fabbricanti non sono tenuti, ai fini del regolamento sulla ciberresilienza, a effettuare una nuova valutazione o a dimostrare nuovamente la conformità in relazione ai rischi già affrontati da tali certificati finché il certificato o la decisione di approvazione pertinente mantiene la sua validità e, in ogni caso, non oltre l'11 giugno 2028. Sono inclusi, ad esempio, i rischi di cibersicurezza connessi alla protezione della rete, alla protezione dei dati personali e della vita privata o alla prevenzione delle frodi (nella misura in cui tali rischi sono contemplati dal certificato in questione) relativi ai requisiti di cibersicurezza della direttiva sulle apparecchiature radio e rispecchiati nella valutazione della conformità.

253. Tuttavia qualora la valutazione dei rischi di cibersicurezza effettuata conformemente all'articolo 13, paragrafo 2, del regolamento sulla ciberresilienza individui ulteriori rischi per la cibersicurezza non contemplati da tali certificati, i fabbricanti sono tenuti ad affrontare tali rischi conformemente al regolamento sulla ciberresilienza. Ciò può includere, ad esempio, i rischi connessi ai processi di gestione delle vulnerabilità, alla minimizzazione dei dati e alla riduzione della superficie di attacco, o altri aspetti di cibersicurezza specifici del prodotto non affrontati da tali certificati o, in ogni caso, non contemplati dai requisiti essenziali di cibersicurezza della direttiva sulle apparecchiature radio.

254. Di conseguenza l'esistenza di un certificato di esame UE del tipo o di una decisione di approvazione in corso di validità a norma della direttiva sulle apparecchiature radio per i requisiti essenziali relativi alla cibersicurezza di tale direttiva non dimostra, di per sé, la piena conformità al regolamento sulla ciberresilienza. Consente invece ai fabbricanti di avvalersi di tale certificato o decisione come prova di conformità per i rischi corrispondenti, garantendo nel contempo che eventuali rischi rimanenti o recentemente individuati siano valutati e attenuati conformemente al regolamento sulla ciberresilienza.

([31]) I prodotti con elementi digitali immessi sul mercato prima dell'11 dicembre 2027 sono soggetti alla normativa dell'Unione applicabile al momento dell'immissione sul mercato e, se conformi, possono essere venduti e messi in funzione, a meno che, all'11 dicembre 2027 o successivamente a tale data, non siano sottoposti a modifiche sostanziali. Per i concetti di «immissione sul mercato» e «messa a disposizione sul mercato», cfr. anche la sezione *2.1 Immissione sul mercato* del presente documento e il capitolo 2 della guida blu.

255. Analogamente, se un prodotto con elementi digitali è soggetto ai requisiti essenziali di sicurezza e di tutela della salute connessi alla cibersicurezza di cui al regolamento (UE) 2023/1230 (regolamento relativo alle macchine), pienamente applicabile a decorrere dal 20 gennaio 2027, e se sulla base di tali requisiti è stato rilasciato un certificato di esame UE del tipo o una decisione di approvazione, tale certificato o decisione di approvazione mantiene la propria validità, a norma dell'articolo 69, paragrafo 1, del regolamento sulla ciberresilienza, per i rischi di cibersicurezza contemplati dal regolamento relativo alle macchine.

256. Ciò riguarda in particolare gli aspetti di cibersicurezza relativi alla protezione dall'alterazione e alla sicurezza e affidabilità dei sistemi di comando, di cui all'allegato III, punti 1.1.9 e 1.2.1, del regolamento relativo alle macchine. Per tali rischi i fabbricanti non sono tenuti, ai fini del regolamento sulla ciberresilienza, a effettuare una nuova valutazione o a dimostrare nuovamente la conformità finché il certificato o la decisione di approvazione pertinenti mantiene la sua validità e, in ogni caso, non oltre l'11 giugno 2028. Ciò vale a condizione che tali rischi siano stati affrontati nell'ambito della valutazione della conformità a norma del regolamento relativo alle macchine.

257. Come nel caso dei requisiti essenziali di cibersicurezza della direttiva sulle apparecchiature radio di cui sopra, qualora la valutazione dei rischi di cibersicurezza effettuata a norma dell'articolo 13, paragrafo 2, del regolamento sulla ciberresilienza individui ulteriori rischi di cibersicurezza che non sono contemplati dal pertinente certificato rilasciato a norma del regolamento relativo alle macchine e che sono connessi ai requisiti di cibersicurezza di tale regolamento, i fabbricanti sono tenuti ad affrontare tali rischi in conformità del regolamento sulla ciberresilienza.