

SOFTWARE ED ELEMENTI DIGITALI DIFETTOSI NEI PRODOTTI ELETTRONICI: RESPONSABILITÀ NELLA DIRETTIVA (UE) 2024/2853 E NECESSITÀ DI VERIFICHE PER LE IMPRESE

La Direttiva UE /2853/2024 - di cui ho estensivamente scritto in un precedente articolo pubblicato su un numero di Marketplace dello scorso anno - disciplina a livello UE la responsabilità del produttore per prodotti difettosi verso il consumatore finale. Essa sostituisce la precedente Direttiva 85/374/CEE, dovrà essere attuata in Italia entro il 9.12.2026 (art. 22) e si applicherà su tutti i prodotti immessi nel mercato o messi in servizio dopo il 9 dicembre 2026.

La Direttiva ribadisce ed estende regole comuni, basate sulla responsabilità oggettiva degli operatori economici per il danno causato da prodotti difettosi a persone fisiche e a cose diverse dal prodotto difettoso stesso e le relative modalità di risarcimento. Gli operatori economici possono liberarsi dalla presunzione di responsabilità che è posta loro in capo solo in determinati casi all'uopo previsti.

La nuova Direttiva estende notevolmente il campo dei prodotti possibilmente difettosi ed amplia pertanto l'ambito di potenziale responsabilità dei produttori.



MAURIZIO IORIO

Dalla partnership tra Marketplace e Andec prende vita questa rubrica, curata dall'Avvocato Maurizio Iorio nel suo duplice ruolo di Avvocato Professionista in Milano e di Presidente di Andec.

(1) Ampliamento della definizione di "Prodotto" e nuovi rischi per le imprese

Sotto la precedente Direttiva 85/374/CEE per «**Prodotto**» si intendeva qualsiasi bene mobile, anche se parte di un altro bene mobile o immobile, inclusa l'elettricità, i prodotti agricoli naturali e i giochi.

La nuova Direttiva 2024/2853/UE **amplia in modo significativo il concetto di "prodotto"**, includendo espressamente il **software, gli aggiornamenti e gli elementi digitali integrati**.

Di conseguenza, eventuali difetti derivanti da **bug software, aggiornamenti inadeguati, vulnerabilità di cybersecurity**, potranno rilevare ai fini della responsabilità oggettiva del produttore.

Il danno rilevante ai fini della responsabilità potrà inoltre consistere nella distruzione o corruzione di dati non utilizzati a fini professionali.

E' pertanto opportuno che i produttori, in previsione dell'entrata in vigore della nuova direttiva, effettuino tutte le correlative, opportune verifiche.

(2) Il software nel nuovo perimetro della responsabilità da prodotto difettoso

In Italia, la responsabilità per danno da prodotti difettosi è oggi disciplinata dagli artt. 114-127 del Codice del consumo, che recepiscono l'impianto della Direttiva 85/374/CEE. Tale disciplina pone a carico del produttore la responsabilità per il danno cagionato dal difetto del prodotto, **ma non include espressamente il software nella relativa definizione**.

La Direttiva (UE) 2024/2853, che come si è detto dovrà essere recepita entro il 9 dicembre 2026 e si applicherà ai prodotti immessi sul mercato o messi in servizio dopo tale data, modifica questo quadro. Infatti, l'art. 4 include espressamente il software nella nozione di «prodotto» e considera rilevanti anche i servizi digitali integrati o interconnessi con un bene, quando siano necessari allo svolgimento di una o più delle sue funzioni.

- Per i prodotti elettronici, ciò significa che il difetto, ai fini della responsabilità da prodotto difettoso, potrà derivare non più solo dall'hardware, ma anche dal software incorporato nel dispositivo, da un aggiornamento che ne comprometta la sicurezza o dalla mancata fornitura di un aggiornamento necessario a mantenerla, quando il prodotto sia ancora sotto il controllo del fabbricante.

- Inoltre, ai sensi dell'art. 6 della nuova direttiva, il danno risarcibile potrà consistere anche nella distruzione o corruzione di dati non utilizzati a fini professionali, come fotografie, video o documenti personali cancellati o resi inutilizzabili da un software difettoso.

(3) Software integrato e versioning

Per le imprese che fabbricano, importano o commercializzano prodotti elettronici dotati di software, il problema diviene quindi duplice: prevenire che un elemento digitale renda insicuro il prodotto e, al fine di liberarsi da eventuali responsabilità, disporre delle informazioni necessarie per ricostruire l'origine del difetto, i soggetti coinvolti e le conseguenze economiche dell'eventuale responsabilità.

Ne consegue che la prima misura consigliata alle imprese consiste nella tracciabilità delle versioni del software integrato nel prodotto (**versioning**).

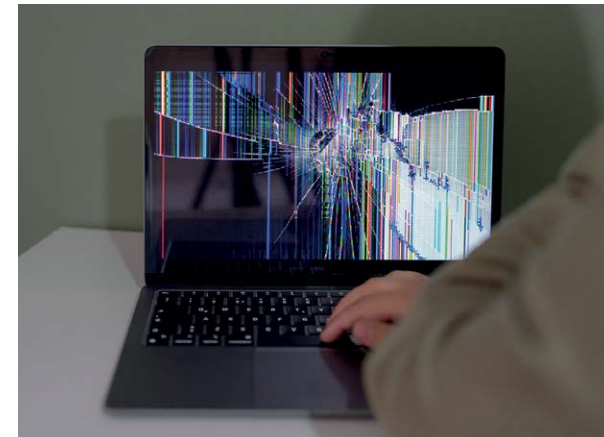
Il problema può infatti presentarsi anche dopo l'immissione sul mercato e l'art. 11, par. 1, lett. c), consente in via generale all'operatore economico di escludere la responsabilità provando che il difetto è sorto successivamente alla cessione del prodotto. Tale difesa non potrà tuttavia operare quando il prodotto sia ancora sotto il controllo del fabbricante e il difetto dipenda da software, aggiornamenti, migliorie o dalla mancanza di aggiornamenti necessari per mantenerne la sicurezza, ai sensi dell'art. 11, par. 2.

Pertanto, la registrazione e il tracciamento delle versioni software, pur non costituendo di per sé un adempimento imposto dalla direttiva né un criterio per individuare il soggetto responsabile, possono risultare utili quando, a seguito della segnalazione di incidenti o danni causati da un prodotto, sia necessario identificare tutti i prodotti sui quali sia stato installato uno specifico aggiornamento difettoso e intervenire affinché altri prodotti del medesimo modello, serie o lotto, ove esposti allo stesso problema, non restino soggetti al medesimo rischio di difettosità.

(4) Vulnerabilità informatiche e cybersecurity

Un'ulteriore area di intervento riguarda le vulnerabilità informatiche capaci di rendere non sicuro un prodotto elettronico.

La Direttiva (UE) 2024/2853 non impone, di per sé, un processo aziendale



di analisi dei rischi di cibersicurezza. Essa stabilisce, tuttavia, che un prodotto può risultare difettoso anche per effetto di una vulnerabilità informatica.

L'art. 7 della direttiva prevede infatti che un prodotto sia difettoso quando non offre la sicurezza che una persona può legittimamente attendersi o che è richiesta dal diritto dell'Unione o nazionale. Per i prodotti connessi, la sicurezza deve essere valutata considerando anche il loro funzionamento in connessione con altri dispositivi e il rispetto dei requisiti di **cibersicurezza** applicabili. Un dispositivo potrebbe quindi risultare difettoso se, ad esempio, una vulnerabilità consenta a terzi di disattivare una funzione di protezione o di alterarne il funzionamento in modo tale da provocare un danno.

La violazione di requisiti obbligatori di cibersicurezza può inoltre incidere sulla prova del difetto. Ai sensi dell'art. 10, par. 2, lett. b) della direttiva, infatti, il carattere difettoso del prodotto si presume, salvo prova contraria, quando il danneggiato dimostri che il prodotto non rispetta requisiti obbligatori di sicurezza stabiliti dal diritto dell'Unione o nazionale, purché tali requisiti siano destinati a proteggere dal rischio del danno concretamente subito.

Per i prodotti ai quali si applica il Regolamento (UE) 2024/2847, *Cyber Resilience Act* o CRA, l'analisi dei rischi di cibersicurezza costituisce anche uno specifico obbligo normativo. Salve alcune specifiche esclusioni, come da art. 2 CRA, quest'ultimo riguarda i prodotti software o hardware messi a disposizione sul mercato il cui uso previsto o ragionevolmente prevedibile comporti una connessione, anche indiretta, a un dispositivo o a una rete. Possono quindi rientrare nella disciplina numerosi prodotti elettronici connessi. Per tali prodotti, l'art. 13 CRA imporrà al fabbricante di effettuare e documentare una valutazione dei rischi di cibersicurezza, tenendone conto nella pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto e aggiornandola, se necessario, durante il periodo di assistenza. Questi obblighi si applicheranno dall'11 dicembre 2027.

L'art. 14 CRA si applicherà invece dall'11 settembre 2026

e imporrà al fabbricante di notificare le vulnerabilità «attivamente sfruttate» contenute nel prodotto delle quali venga a conoscenza, nonché gli incidenti gravi aventi un impatto sulla sicurezza del prodotto. Per «vulnerabilità attivamente sfruttata» si intende una vulnerabilità per la quale esistano prove attendibili che un soggetto malintenzionato l'abbia effettivamente sfruttata in un sistema senza l'autorizzazione del proprietario. L'obbligo di notifica non riguarderà, pertanto, ogni vulnerabilità individuata, ma quelle già concretamente sfruttate in modo illecito, oltre agli incidenti gravi. Esso si applicherà anche ai prodotti immessi sul mercato prima dell'11 dicembre 2027, se soggetti al CRA.

Il CRA e la Direttiva (UE) 2024/2853 operano naturalmente su piani distinti. Il primo pone obblighi di prevenzione, gestione e segnalazione dei rischi di cibersicurezza; la seconda disciplina il risarcimento del danno causato da un prodotto difettoso.

Il richiamo al CRA è però molto pertinente perché, per i prodotti ai quali esso si applica, l'analisi e la gestione delle vulnerabilità non costituiscono soltanto misure utili a prevenire il difetto, ma obblighi normativi la cui violazione può assumere rilievo anche nel giudizio risarcitorio, alle condizioni previste dall'art. 10, par. 2, lett. b), della direttiva.

(5) Reclami, incidenti e prova del difetto

Un ulteriore profilo di cautela per gli operatori economici riguarda la corretta gestione dei reclami e degli incidenti connessi alla sicurezza del prodotto. La Direttiva (UE) 2024/2853 non introduce neppure in questo caso un obbligo aziendale di istituire procedure interne per la raccolta dei reclami. Tali obblighi possono tuttavia discendere dalla disciplina sulla sicurezza generale dei prodotti e assumere rilievo, successivamente, anche nel giudizio sulla responsabilità per danno da prodotto difettoso.

Il Regolamento (UE) 2023/988 sulla

sicurezza generale dei prodotti (GPSR), vigente ed efficace dal 13 dicembre 2024, impone al fabbricante, nei casi in cui tali disposizioni siano applicabili al prodotto considerato, di mettere a disposizione dei consumatori canali per presentare reclami e segnalare incidenti o problemi di sicurezza, di indagare sui reclami e sulle informazioni ricevute in merito agli incidenti e di tenere un registro interno dei reclami, dei richiami e delle misure correttive adottate. Obblighi analoghi gravano sull'importatore, ai sensi dell'art. 11, parr. 9, 10 e 11. Per i prodotti soggetti a specifica normativa dell'Unione, l'applicazione di tali disposizioni deve essere verificata alla luce della disciplina settoriale pertinente e dei rischi da essa già regolati.

Il GPSR disciplina, inoltre, le conseguenze di un rischio già emerso. Ai sensi dell'art. 20, il fabbricante deve notificare tramite il *Safety Business Gateway* gli incidenti causati da un prodotto che abbiano determinato la morte di una persona o gravi effetti nocivi, permanenti o temporanei, per la sua salute o sicurezza; importatori e distributori che ne vengano a conoscenza devono informare senza indebito ritardo il fabbricante. In caso di richiamo per motivi di sicurezza o qualora debbano essere diffuse informazioni necessarie all'uso sicuro del prodotto, l'art. 35 impone inoltre di informare direttamente e senza indebito ritardo i consumatori identificabili.

Questa documentazione può assumere rilievo anche nell'ipotetico contenzioso risarcitorio disciplinato dalla Direttiva (UE) 2024/2853. L'art. 7, par. 2, lett. g), include tra le circostanze rilevanti per valutare la difettosità del prodotto i richiami e gli altri interventi pertinenti adottati dalle autorità competenti o dagli operatori economici in relazione alla sicurezza. Inoltre, ai sensi dell'art. 9, il giudice potrà ordinare al convenuto di divulgare gli elementi di prova pertinenti e necessari nella sua disponibilità, quando il danneggiato abbia presentato fatti e prove sufficienti a sostenere la plausibilità della domanda. Secondo la nuova direttiva, già soltanto l'omessa "divulgazione" degli elementi di prova richiesti dal giudice può determinare la presunzione di difettosità prevista dall'art. 10, par. 2, lett. a).

Per un prodotto elettronico dotato di software, la gestione dei reclami e degli incidenti deve quindi permettere di individuare il prodotto interessato, il problema di sicurezza segnalato e le misure eventualmente adottate. Quando il problema possa dipendere dal software o da un aggiornamento, potrà inoltre essere utile ricostruire la configurazione digitale del prodotto coinvolto.

(6) Software sviluppato da terzi e responsabilità nella filiera

Un altro profilo da considerare da parte dei produttori riguarda i prodotti nei quali il software che incide sulla sicurezza dell'apparecchio sia sviluppato o fornito da un soggetto diverso dal fabbricante del prodotto finale. In tali casi, occorre distinguere la responsabilità legale verso il

danneggiato dai rapporti contrattuali interni alla filiera.

Quanto alla responsabilità ex lege, se un software difettoso, integrato o interconnesso con un prodotto sotto il controllo del fabbricante, rende difettoso il prodotto finale, l'art. 8 della Direttiva (UE) 2024/2853 individua come responsabili del danno il fabbricante del prodotto difettoso e il fabbricante del componente software difettoso. Quando il fabbricante del prodotto o del componente software sia stabilito fuori dall'Unione, rispondono inoltre, alle condizioni previste dalla medesima disposizione, l'importatore del prodotto o del componente difettoso e il rappresentante autorizzato del fabbricante; in mancanza di un importatore o di un rappresentante autorizzato stabiliti nell'Unione, risponde il fornitore di servizi di logistica. Se più operatori sono responsabili del medesimo danno, l'art. 12, par. 1, prevede che possano essere chiamati a risponderne in solido.

Quanto ai rapporti contrattuali, il contratto tra produttore e fornitore del software non può modificare la posizione del danneggiato, in quanto, ai sensi dell'art. 15, la responsabilità prevista dalla direttiva non può essere limitata o esclusa mediante accordi contrattuali. **Il contratto può però disciplinare i rapporti interni tra gli operatori**, stabilendo chi debba correggere o aggiornare il software, comunicare vulnerabilità o incidenti, conservare e rendere disponibili test e documentazione tecnica e cooperare in caso di contenzioso.

La disciplina contrattuale assume rilievo anche rispetto alla rivalsa. In linea generale, l'art. 14 riconosce all'operatore che abbia risarcito il danneggiato il diritto di agire, secondo il diritto nazionale, contro un altro operatore responsabile. Tuttavia, l'art. 12, par. 2, prevede una specifica eccezione per il software: il fabbricante che abbia integrato nel proprio prodotto un componente software difettoso non ha diritto di rivalsa verso il fabbricante del software, qualora quest'ultimo sia una

microimpresa o una piccola impresa al momento dell'immissione sul mercato del componente e il fabbricante del prodotto abbia contrattualmente rinunciato alla rivalsa.

(7) Coperture assicurative: un presidio economico, non un'esimente

L'ultima verifica riguarda le coperture assicurative. Per le imprese diviene infatti opportuno accertare se le polizze di *product liability* stipulate comprendano anche i danni cagionati da prodotti resi difettosi da software preinstallato, aggiornamenti difettosi, vulnerabilità informatiche o servizi digitali correlati, nonché la distruzione o corruzione di dati non utilizzati a fini professionali, che l'art. 6 della nuova direttiva include tra i danni risarcibili. La copertura assicurativa non evita, né limita verso il danneggiato, la responsabilità prevista dalla direttiva. Può soltanto stabilire, secondo le condizioni, i limiti e le esclusioni della polizza, se il costo economico dell'eventuale risarcimento rimanga a carico dell'impresa o possa essere trasferito, in tutto o in parte, all'assicuratore.

In breve...

con il futuro regime previsto dalla Direttiva (UE) 2024/2853, la responsabilità per prodotto difettoso potrà riguardare espressamente anche i difetti riconducibili al software, agli aggiornamenti e ai servizi digitali dai quali dipende la sicurezza del prodotto, nonché i danni consistenti nella distruzione o corruzione di dati non utilizzati a fini professionali.

Per le imprese dell'elettronica di consumo, sarà pertanto necessario estendere i controlli sul rischio agli elementi digitali, verificando le misure di prevenzione applicabili, i rapporti con i fornitori di software e l'effettiva copertura economica dell'eventuale responsabilità.

Riproduzione riservata ©Maurizio Iorio

N.B. Le immagini utilizzate a corredo di questo articolo sono solo a puro scopo illustrativo