Luiss
Libera Università Internazionale
degli Studi Sociali Guido Carli

Il Cyber Resilience Act: impatti e implementazione nell'industria italiana

Inquadramento normativo e cenni di disciplina

Ministero delle Imprese e del Made in Italy – 30 settembre 2024

Avv. Luca D'Agostino

LUISS

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Sommario

1. Il Cyber Resilience Act. Uno sguardo d’insieme

2. Oggetto e ambito di applicazione

3. Obblighi di compliance in capo agli operatori economici

4. Conformità dei prodotti con elementi digitali, organismi di valutazione della conformità e vigilanza del mercato

5. Apparato sanzionatorio

1. Il Cyber Resilience Act. Uno sguardo d’insieme

Perché il Cyber Resilience Act?

1. **Aumento delle minacce informatiche**: La crescita esponenziale del numero e della varietà di dispositivi connessi nei prossimi anni rende le minacce informatiche una questione sempre più centrale. Gli attacchi informatici hanno un impatto critico sull'economia dell'Unione, e minacciano anche la democrazia, la sicurezza dei consumatori e la salute pubblica. Pertanto, è necessario rafforzare l'approccio dell'Unione alla sicurezza informatica, migliorando la resilienza a livello dell'Unione e il funzionamento del mercato interno attraverso un quadro giuridico uniforme per i requisiti essenziali di sicurezza informatica per i prodotti con elementi digitali
2. **Basso livello di sicurezza dei prodotti digitali**: Attualmente, esistono due principali problemi che aumentano i rischi per gli utenti e la società: un basso livello di sicurezza dei prodotti con elementi digitali, e la fornitura insufficiente e incoerente di aggiornamenti di sicurezza per affrontarle. Inoltre, vi è una comprensione insufficiente e un accesso limitato alle informazioni da parte degli utenti, che impedisce loro di scegliere prodotti con proprietà di sicurezza informatica adeguate o di utilizzarli in modo sicuro.

Perché il Cyber Resilience Act? (2)

3. **Inadeguatezza delle normative esistenti**: Le leggi attuali dell'Unione in materia di sicurezza informatica non coprono direttamente i requisiti obbligatori per la sicurezza dei prodotti con elementi digitali. Anche se esistono diverse normative settoriali e orizzontali, come il Regolamento (UE) 2019/881 e la Direttiva (UE) 2022/2555, queste affrontano solo parzialmente i problemi legati alla sicurezza informatica, creando un mosaico normativo che aumenta l'incertezza legale per i produttori e gli utenti e impone un onere inutile sulle imprese e le organizzazioni.

4. **Necessità di un quadro normativo uniforme:** L'assenza di un quadro normativo uniforme a livello di Unione Europea per stabilire requisiti di sicurezza informatica per tutti i prodotti con elementi digitali ha portato a una legislazione frammentata che aumenta l'incertezza giuridica per i produttori e gli utenti. Un quadro uniforme aiuterà a migliorare la sicurezza e la trasparenza del mercato, garantendo che i prodotti con elementi digitali siano progettati e sviluppati in modo sicuro, minimizzando le vulnerabilità e garantendo aggiornamenti di sicurezza regolari durante l'intero ciclo di vita del prodotto.

Entrata in vigore e applicazione del Cyber Resilience Act

- Il regolamento **entrerà in vigore** il ventesimo giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea.
- Tuttavia, le disposizioni del regolamento **saranno applicabili** a partire da 36 mesi dalla data della sua entrata in vigore.

DEROGA: l'**art. 14** sarà applicabile a partire da 21 mesi dalla data di entrata in vigore. La disposizione è particolarmente significativa, perché introduce obblighi di notifica relativi alle vulnerabilità e agli incidenti di sicurezza dei prodotti con elementi digitali. Quali i motivi?

1) Urgenza di affrontare le vulnerabilità critiche: dato che le vulnerabilità nei prodotti digitali possono essere sfruttate rapidamente dai threat actors, è essenziale implementare al più presto un sistema di notifica obbligatorio per ridurre i rischi per la sicurezza e proteggere gli utenti finali.
2) Coordinamento efficace e tempestivo: l'implementazione di una piattaforma centralizzata e di obblighi di notifica migliora il coordinamento tra le autorità di cybersecurity nell'UE, permettendo una risposta più rapida ed efficace alle minacce emergenti.
3) Incentivazione alla compliance: l'applicazione anticipata delle regole di notifica aiuta a incentivare i produttori a conformarsi rapidamente ai requisiti di sicurezza, promuovendo una maggiore responsabilità e trasparenza da parte delle aziende

Entrata in vigore e applicazione del Cyber Resilience Act (2)

- Il **Capitolo IV** (Articoli 35-51) sarà applicabile a partire da 18 mesi dalla data di entrata in vigore. Per quale motivo?

Il Capitolo IV contiene disposizioni cruciali relative alla sorveglianza del mercato e alle misure di conformità, fondamentali per garantire l'effettiva attuazione del regolamento e la protezione contro i rischi di sicurezza informatica associati ai prodotti con elementi digitali.

La scelta di applicare il Capitolo IV a partire da 18 mesi dalla data di entrata in vigore riflette l'urgenza di garantire una sorveglianza efficace del mercato e l'adozione di misure correttive quanto prima possibile. Dato il crescente numero di prodotti connessi e le minacce alla sicurezza informatica, è fondamentale che le autorità siano pronte a monitorare, identificare e affrontare i rischi in modo tempestivo. L'applicazione anticipata consente di stabilire rapidamente le basi per un'efficace governance della sicurezza informatica a livello dell'UE, proteggendo così meglio consumatori, imprese e infrastrutture critiche.

Disposizioni transitorie (art. 69): i prodotti con elementi digitali immessi sul mercato prima di 36 mesi dalla data di entrata in vigore del Regolamento (ndr, dal ventesimo giorno dalla pubblicazione in Gazzetta) saranno soggetti ai requisiti del regolamento solo se, da quella data, tali prodotti subiranno modifiche sostanziali. *Quid iuris* rispetto ai prodotti immessi sul mercato nei mesi precedenti alla data di applicabilità?

2. Oggetto e ambito di applicazione

Capo I CRA

A chi/cosa si applica il Regolamento?

- Il Cyber Resilience Act definisce i requisiti di sicurezza informatica per i prodotti con elementi digitali. L'obiettivo è migliorare la sicurezza di questi prodotti sul mercato dell'Unione Europea, riducendo le vulnerabilità e garantendo che i produttori prendano in considerazione la sicurezza durante l'intero ciclo di vita del prodotto.

Ambito di applicazione: il Regolamento si applica a tutti i prodotti con elementi digitali immessi sul mercato dell'Unione Europea. Questo include sia hardware (come dispositivi elettronici) che software (come applicazioni e programmi) che sono venduti o resi disponibili agli utenti all'interno dell'UE. Ambito di applicazione che potremmo definire *«product-oriented»* (che non si focalizza sul soggetto, bensì sull'oggetto).

Esclusioni: Vi sono tuttavia numerose esclusioni dall'ambito di applicazione del Regolamento.

1. **Prodotti regolati da specifiche normative UE**: Il regolamento non si applica ai prodotti con elementi digitali già coperti da altre leggi dell'UE, tra cui:

- Regolamento (UE) 2017/745 (dispositivi medici) e Regolamento (UE) 2017/746 (*dispositivi medico-diagnostici* in vitro), che stabiliscono requisiti specifici di sicurezza, inclusa la sicurezza informatica;

- Regolamento (UE) 2019/2144 (*sicurezza dei veicoli a motore*), che include norme per la gestione della sicurezza informatica nei veicoli.

A chi/cosa si applica il Regolamento?

2. **Prodotti certificati secondo il Regolamento (UE) 2018/1139**: Esclusi i prodotti con elementi digitali già certificati per *la sicurezza dell'aviazione civile*, che seguono regole specifiche per affrontare le minacce alla sicurezza informatica nel settore aeronautico.
3. **Attrezzature marittime**: Esclusi i prodotti rientranti nella Direttiva 2014/90/UE (*attrezzature marittime*), che prevede requisiti di sicurezza per le apparecchiature utilizzate a bordo delle navi.
4. **Prodotti per scopi di sicurezza nazionale o difesa**: Esclusi i prodotti sviluppati per scopi di *sicurezza nazionale o difesa*, nonché quelli progettati per *gestire informazioni classificate*.
5. **Prodotti per uso personale, non commerciale**: Esclusi i prodotti con elementi digitali sviluppati da persone fisiche *per uso personale, senza scopi commerciali*.

Ratio: Queste esclusioni evitano sovrapposizioni normative e garantiscono che in ambiti specifici si seguano regole adatte a specifiche esigenze settoriali.

Definizioni rilevanti

‘Prodotto con elementi digitali’: un prodotto software o hardware e le sue soluzioni di elaborazione dati a distanza, inclusi i componenti software o hardware immessi sul mercato separatamente;

‘Operatore economico’: il fabbricante, il rappresentante autorizzato, l'importatore, il distributore o altra persona fisica o giuridica soggetta a obblighi in relazione alla fabbricazione di prodotti con elementi digitali o alla messa a disposizione di prodotti sul mercato in conformità al presente Regolamento;

‘Produttore’: una persona fisica o giuridica che sviluppa o produce prodotti con elementi digitali o fa progettare, sviluppare o produrre tali prodotti, e li commercializza sotto il proprio nome o marchio, sia a pagamento, per monetizzazione o gratuitamente;

‘Rischio di sicurezza informatica’: la possibilità di perdita o interruzione causata da un incidente, espressa come una combinazione della gravità di tale perdita o interruzione e della probabilità che l'incidente si verifichi;

‘Incidente’: un incidente come definito nell'articolo 6, punto (6), della Direttiva (UE) 2022/2555 → un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.

Contratti pubblici per l’acquisto di beni ICT e requisiti ulteriori di sicurezza

- L'**Articolo 5** del *Cyber Resilience Act* consente agli Stati membri dell'UE di imporre requisiti di sicurezza informatica aggiuntivi per l'acquisto o l'uso di prodotti con elementi digitali per scopi specifici, come la sicurezza nazionale o la difesa, purché tali requisiti siano conformi al diritto dell'Unione e siano necessari e proporzionati. Inoltre, quando questi prodotti vengono acquistati, gli Stati membri devono garantire che il processo di appalto consideri la conformità ai requisiti essenziali del regolamento, inclusa la capacità dei produttori di gestire le vulnerabilità in modo efficace, senza pregiudicare le direttive UE sugli appalti pubblici (2014/24/UE e 2014/25/UE).

- L'Articolo 5 del *Cyber Resilience Act* non preclude dunque l'applicazione della disciplina italiana prevista dal D.L. 105/2019 per gli acquisti di beni ICT per il Perimetro di Sicurezza Nazionale Cibernetica, anzi, è compatibile con essa, permettendo all'Italia di mantenere o introdurre ulteriori misure di sicurezza, in linea con le proprie esigenze e nel rispetto del diritto dell'Unione Europea.

Obblighi fondamentali per l'immissione sul mercato dei prodotti con elementi digitali

I prodotti con elementi digitali potranno essere immessi sul mercato solo se rispettano **due condizioni fondamentali**:

1. Devono soddisfare i requisiti essenziali di sicurezza indicati nell'**Allegato I, Parte I**, a condizione che siano installati, mantenuti e utilizzati correttamente per il loro scopo previsto, o in condizioni ragionevolmente prevedibili, e che siano stati installati gli aggiornamenti di sicurezza necessari.
2. I processi implementati dal produttore devono conformarsi ai requisiti essenziali indicati nell'**Allegato I, Parte II,** che riguardano specificamente le pratiche di sicurezza del produttore durante tutto il ciclo di vita del prodotto.

- L'**Annex I, Parte I** del *Cyber Resilience Act* elenca i requisiti essenziali di sicurezza per i prodotti con elementi digitali, che devono essere progettati, sviluppati e prodotti per garantire un adeguato livello di sicurezza informatica in base ai rischi identificati. I principali requisiti sono:

1. Assenza di vulnerabilità note: I prodotti devono essere immessi sul mercato senza vulnerabilità note che possano essere sfruttate.

2. Configurazione sicura di default: Devono avere impostazioni di sicurezza predefinite, con possibilità di ripristino allo stato originale.

Obblighi fondamentali per l’immissione sul mercato dei prodotti con elementi digitali (2)

3. Aggiornamenti di sicurezza: Devono poter ricevere aggiornamenti di sicurezza tempestivi, inclusi aggiornamenti automatici con opzioni di rinvio e disattivazione.

4. Protezione dall'accesso non autorizzato: Misure di controllo, come autenticazione e gestione degli accessi, devono essere implementate.

5. Protezione della riservatezza dei dati: I dati devono essere protetti tramite meccanismi avanzati di crittografia.

6. Integrità dei dati: Devono essere protetti contro modifiche non autorizzate e segnalare eventuali corruzioni.

7. Minimizzazione dei dati: Devono trattare solo i dati personali necessari per il loro scopo previsto.

8. Continuità delle funzioni essenziali: Devono garantire la disponibilità delle funzioni anche dopo un incidente.

9. Resilienza agli incidenti: Devono includere meccanismi per ridurre l'impatto di un incidente.

10. Registrazione delle attività di sicurezza: Registrare e monitorare le attività interne rilevanti.

Prodotti importanti e critici

- I **"prodotti importanti con elementi digitali"** sono quelli appartenenti a una categoria specificata nell'Allegato III, che richiedono procedure di valutazione della conformità. Questi prodotti sono classificati in due classi (I e II) e devono soddisfare almeno uno dei seguenti criteri:

- Svolgono funzioni critiche per la sicurezza informatica di altri prodotti, reti o servizi, come l'autenticazione, la prevenzione delle intrusioni o la protezione delle reti.

- Esercitano funzioni con un rischio significativo di effetti negativi, come la gestione di sistemi centrali o il trattamento di dati personali. La Commissione Europea può modificare l'Allegato III tramite atti delegati per aggiungere, modificare o rimuovere categorie di prodotti, considerando il rischio per la sicurezza informatica.

- I **"prodotti critici con elementi digitali**" richiederanno una certificazione europea di cybersicurezza ad un livello di garanzia "sostanziale" o superiore (Allegato IV). La Commissione può adottare atti delegati per identificare quali prodotti necessitano di questa certificazione, considerando l'uso previsto. Prima di adottare tali atti, la Commissione valuta l'impatto sul mercato e consulta le parti interessate. Inoltre, la Commissione può modificare l'Allegato IV per aggiungere o rimuovere categorie di prodotti critici, tenendo conto della dipendenza critica e dei potenziali rischi per le catene di approvvigionamento.

3. Obblighi di compliance in capo agli operatori economici

Capo II CRA

Obblighi dei produttori

- Progettazione e Sviluppo Sicuro: I produttori devono garantire che i prodotti con elementi digitali siano progettati, sviluppati e prodotti secondo i requisiti di sicurezza essenziali (Annex I, Parte I). Devono effettuare una valutazione dei rischi di sicurezza informatica e tenerne conto in tutte le fasi (pianificazione, sviluppo, produzione, consegna e manutenzione).
- Gestione delle Vulnerabilità: Devono identificare e risolvere le vulnerabilità, anche quelle nei componenti open source, notificandole alle parti responsabili e fornendo correzioni o documentazione adeguata.
- Supporto Continuativo e Documentazione: I produttori devono garantire la gestione delle vulnerabilità per almeno cinque anni o per il periodo di supporto determinato. Devono documentare sistematicamente gli aspetti di sicurezza e aggiornare la valutazione dei rischi. La documentazione tecnica e la dichiarazione di conformità UE devono essere mantenute disponibili per almeno 10 anni.
- Informazioni ai Consumatori: Devono fornire informazioni chiare e accessibili agli utenti sul periodo di supporto, inclusa la data di fine, e garantire che ogni aggiornamento di sicurezza sia disponibile per almeno 10 anni.
- Segnalazione di Incidenti: Devono notificare le vulnerabilità sfruttate attivamente e gli incidenti gravi sia al CSIRT designato come coordinatore che a ENISA tramite una piattaforma unica di segnalazione.

Obblighi degli importatori e dei distributori

Obblighi degli Importatori

- Verifica di Conformità: Gli importatori devono assicurarsi che i prodotti siano conformi ai requisiti di sicurezza prima di immetterli sul mercato, verificando che siano state completate le valutazioni di conformità e che la documentazione richiesta sia corretta e completa.
- Comunicazione delle Non-Conformità: Se un prodotto non è conforme, gli importatori devono astenersi dal commercializzarlo e informare il produttore e le autorità competenti. In caso di rischio significativo per la sicurezza informatica, devono agire immediatamente per adottare misure correttive.
- Informazioni e Cooperazione: Devono mantenere la documentazione e collaborare con le autorità di sorveglianza, fornendo tutte le informazioni necessarie per dimostrare la conformità.

Obblighi dei Distributori

- Due Diligence: I distributori devono agire con attenzione verificando la conformità dei prodotti prima di metterli in commercio. Se scoprono che un prodotto non è conforme o rappresenta un rischio, devono immediatamente informare il produttore e le autorità competenti.
- Gestione delle Vulnerabilità: Come gli importatori, devono segnalare le vulnerabilità scoperte nei prodotti e garantire che vengano adottate le misure correttive necessarie.

Obblighi per gestori di software Open Source

Per “gestore di software open-source” si intende una persona giuridica, diversa da un produttore, che ha lo scopo o l'obiettivo di fornire sistematicamente un sostegno duraturo allo sviluppo di prodotti specifici con elementi digitali, qualificati come software libero e open-source e destinati ad attività commerciali, e che garantisce la redditività di tali prodotti.

Obblighi per gestori di Software Open Source

- Politiche di Sicurezza: I gestori del software open source devono implementare e documentare politiche di sicurezza per favorire lo sviluppo sicuro dei prodotti e la gestione delle vulnerabilità. Devono incoraggiare la segnalazione volontaria delle vulnerabilità.
- Cooperazione con le Autorità: Devono collaborare con le autorità di sorveglianza per mitigare i rischi e fornire la documentazione richiesta.

Obblighi generali di segnalazione

- **Segnalazioni Volontarie**: Tutti gli operatori possono notificare volontariamente vulnerabilità e incidenti alle autorità competenti.
- La **notifica obbligatoria** è richiesta per le vulnerabilità sfruttate attivamente e per incidenti gravi che possono compromettere la sicurezza.
- Ai fini dell'assolvimento dell'obbligo di notifica, un incidente che incide sulla sicurezza del prodotto con elementi digitali si considera grave quando:

(a) pregiudica o è in grado di pregiudicare la capacità di un prodotto con elementi digitali di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o delle funzioni sensibili o importanti; oppure

(b) ha provocato o è in grado di provocare l'introduzione o l'esecuzione di codice dannoso in un prodotto con elementi digitali o nei sistemi di rete e informazione di un utente del prodotto con elementi digitali.

4. Conformità dei prodotti con elementi digitali, organismi di valutazione della conformità e vigilanza del mercato

Capi III-V CRA

Disposizioni in materia di conformità dei prodotti con elementi digitali

Capo III – Definisce come i prodotti digitali debbano dimostrare la conformità ai requisiti di sicurezza dell'UE, stabilendo standard, procedure di conformità, e supporto per le PMI

Presunzione di conformità: I prodotti digitali conformi agli standard armonizzati dell'UE, pubblicati nella *Gazzetta Ufficiale*, sono considerati conformi ai requisiti di sicurezza essenziali. Se non esistono standard armonizzati, la Commissione può stabilire specifiche tecniche comuni per garantire la conformità.

Dichiarazione di conformità UE: I produttori devono redigere una dichiarazione di conformità UE, che confermi il rispetto dei requisiti di sicurezza. La dichiarazione deve essere aggiornata e disponibile nelle lingue richieste dallo Stato membro in cui il prodotto è commercializzato.

Marchio CE: Il marchio CE deve essere apposto in modo visibile e leggibile sui prodotti, indicando la conformità ai requisiti di sicurezza dell'UE. Può essere accompagnato da un numero identificativo dell'organismo notificato coinvolto nella valutazione della conformità.

Disposizioni in materia di conformità dei prodotti con elementi digitali (2)

Documentazione tecnica: I produttori devono fornire una documentazione tecnica dettagliata per dimostrare la conformità del prodotto ai requisiti essenziali. Questa documentazione deve essere aggiornata durante il periodo di supporto del prodotto.

Procedure di valutazione della conformità: I produttori devono seguire specifiche procedure di valutazione della conformità, che includono il controllo interno della produzione, esami UE del tipo, l'assicurazione completa della qualità, o schemi di certificazione della cybersicurezza. Prodotti importanti e critici devono seguire procedure più rigorose.

Supporto per le PMI e Accordi di riconoscimento reciproco: Gli Stati membri devono supportare le PMI attraverso formazione, comunicazione dedicata, e accesso a "sandbox regolatorie" per testare i prodotti. L'UE può inoltre concludere accordi con paesi terzi per riconoscere reciprocamente le valutazioni di conformità.

Disposizioni sugli organismi di valutazione della conformità

Capo IV – Stabilisce un quadro chiaro per la designazione, il monitoraggio e la notifica degli organismi di valutazione della conformità, garantendo che questi enti operino in modo imparziale, competente e coordinato in tutta l'Unione Europea.

Notifica degli Organismi di Valutazione della Conformità: Gli Stati membri devono notificare alla Commissione e agli altri Stati membri gli organismi autorizzati a svolgere valutazioni di conformità. Devono garantire un numero sufficiente di organismi notificati per evitare ostacoli all'ingresso nel mercato.

Autorità di Notifica: Gli Stati membri devono designare un'autorità di notifica responsabile dell'accreditamento e della supervisione degli organismi di valutazione della conformità. L'autorità deve essere indipendente, imparziale e organizzata per evitare conflitti di interesse. Può delegare compiti a enti esterni, purché siano legalmente riconosciuti e abbiano misure per coprire eventuali responsabilità.

Requisiti per gli Organismi: Gli organismi notificati devono essere terze parti indipendenti, libere da conflitti di interesse con i prodotti che valutano. Devono possedere personale qualificato, capacità tecniche e risorse adeguate per svolgere le valutazioni di conformità, mantenendo riservatezza, imparzialità e integrità.

Disposizioni sugli organismi di valutazione della conformità (2)

Presunzione di conformità degli organismi notificati: gli organismi di valutazione della conformità che rispettano gli standard armonizzati pubblicati sono presunti conformi ai requisiti del regolamento.

Procedure di notifica e obblighi operativi: gli Organismi devono presentare domanda per la notifica e fornire prove documentali della loro competenza. Le autorità gestiscono la notifica e assicurano che gli organismi notificati rispettino costantemente i requisiti. Le autorità devono anche informare la Commissione in caso di cambiamenti rilevanti o criticità.

Coordinamento e Cooperazione: Gli Stati membri devono assicurare procedure di ricorso contro le decisioni dei corpi notificati e promuovere la cooperazione tra i corpi notificati per garantire una valutazione coerente e uniforme.

Sorveglianza del mercato ed enforcement (2)

Capo V - Delinea un sistema di sorveglianza e applicazione coordinato a livello nazionale e dell'UE per garantire che i prodotti con elementi digitali rispettino i requisiti di sicurezza informatica, promuovendo una risposta efficace e armonizzata alle minacce alla sicurezza.

Sorveglianza del mercato e controllo dei prodotti con elementi digitali: Gli Stati membri devono designare una o più autorità di sorveglianza del mercato per garantire l'applicazione efficace del regolamento. Queste autorità possono cooperare con le autorità di certificazione della cybersicurezza e con i CSIRT (Computer Security Incident Response Teams) per scambiarsi informazioni e fornire supporto tecnico. Devono inoltre fornire risorse adeguate, inclusi strumenti di automazione e personale qualificato in cybersicurezza.

Accesso a dati e documentazione: Le autorità di sorveglianza del mercato possono richiedere accesso a tutti i dati necessari per valutare la conformità dei prodotti digitali, inclusa la documentazione interna degli operatori economici.

Prodotti che presentano rischi significativi di sicurezza informatica: Quando un'autorità di sorveglianza ritiene che un prodotto presenti un rischio significativo, deve condurre una valutazione e, se necessario, richiedere all'operatore economico di prendere misure correttive. Se l'operatore non interviene, l'autorità può adottare misure per vietare, ritirare o richiamare il prodotto dal mercato. La Commissione può intervenire se un prodotto presenta un rischio significativo di sicurezza informatica a livello dell'Unione. La Commissione può consultare le autorità nazionali e, se necessario, adottare misure correttive o restrittive, come il ritiro del prodotto dal mercato.

5. Apparato sanzionatorio

Capo VII CRA

Le sanzioni amministrative pecuniarie

Gli Stati membri devono stabilire le norme relative alle sanzioni applicabili alle violazioni del Regolamento e adottare tutte le misure necessarie per garantirne l'applicazione. Le sanzioni previste devono essere efficaci, proporzionate e dissuasive. Gli Stati membri devono notificare senza indugio alla Commissione tali norme.

Il Capo VII del Cyber Resilience Act stabilisce i limiti edittali delle sanzioni per le imprese che non rispettano i requisiti del regolamento.

1. **Sanzioni per la mancata conformità ai requisiti essenziali di sicurezza informatica (Annex I)** e agli obblighi di gestione delle vulnerabilità (Articoli 13 e 14):

Le imprese che non rispettano questi requisiti possono essere soggette a sanzioni amministrative fino a 15 milioni di euro o, se l'impresa è un'azienda, fino al 2,5% del fatturato mondiale annuo dell'esercizio precedente, a seconda di quale sia l'importo maggiore.

Le sanzioni amministrative pecuniarie (2)

2. Sanzioni per la mancata conformità ad altri obblighi specifici (Articoli 18-23, 28, 30(1)-(4), 31(1)-(4), 32(1)-(3), 33(5), 39, 41, 47, 49 e 53). In questi casi le multe possono arrivare fino a 10 milioni di euro o, per un'azienda, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, a seconda di quale sia l'importo maggiore.

- Articoli 18-23: Stabiliscono obblighi per rappresentanti autorizzati, importatori e distributori. Questi operatori economici devono assicurare che i prodotti con elementi digitali siano conformi ai requisiti essenziali di cybersecurity e tenere documentazione tecnica disponibile per le autorità di sorveglianza del mercato.
- Articolo 28: Richiede che i produttori preparino una dichiarazione di conformità UE per dimostrare il rispetto dei requisiti essenziali del Regolamento. La dichiarazione deve essere aggiornata e disponibile in tutte le lingue richieste dagli Stati membri.
- Articolo 30(1)-(4): Stabilisce le regole per l'apposizione del marchio CE sui prodotti con elementi digitali, indicando che il marchio deve essere visibile, leggibile e indelebile.
- Articolo 31(1)-(4): Richiede che i produttori mantengano una documentazione tecnica che dimostri la conformità del prodotto ai requisiti essenziali. Tale documentazione deve essere disponibile per almeno 10 anni.
- Articolo 32(1)-(3): Regola le procedure di valutazione della conformità, specificando che i prodotti devono essere soggetti a valutazione interna del controllo della produzione o al controllo della conformità da parte di un organismo notificato.Articoli 39, 41, 47, 49 e 53: Dettano ulteriori requisiti per la sorveglianza del mercato, l'accesso ai dati e la cooperazione tra gli operatori economici e le autorità di sorveglianza del mercato per garantire che i prodotti con elementi digitali siano sicuri e conformi alle normative.

Le sanzioni amministrative pecuniarie (2)

3. **Sanzioni per informazioni errate, incomplete o fuorvianti:** l'operatore che fornisce informazioni false o ingannevoli agli organismi notificati o alle autorità di sorveglianza del mercato può essere punito con sanzioni amministrative pecuniarie fino a 5 milioni di euro o, se l'impresa è un'azienda, fino all'1% del fatturato mondiale annuo dell'esercizio precedente, a seconda di quale sia l'importo maggiore.

Criteri di determinazione delle sanzioni:

- Natura, gravità e durata della violazione e le sue conseguenze.
- Eventuali sanzioni amministrative precedenti imposte dallo stesso o da altri enti di sorveglianza del mercato per una violazione simile
- Dimensioni dell'operatore economico, con particolare attenzione a microimprese, piccole e medie imprese, comprese le start-up, e la quota di mercato dell'operatore che ha commesso la violazione.

Eccezioni:

Le sanzioni amministrative **non si applicano** nei seguenti casi:

• Ai produttori che si qualificano come microimprese o piccole imprese per il mancato rispetto di alcune scadenze specifiche (Articolo 14(2), punto (a), e Articolo 14(4), punto (a)).

• Alle violazioni del regolamento da parte dei gestori di *software open-source*.

THE END

Grazie per l’attenzione!

Avv. Luca D’Agostino

ldagostino@luiss.it

studio@dagostinolex.com