# CYBER RESILIENCE ACT

**Proposta COM (2022) 454** del 15 settembre 2022 di **regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali** e che modifica il regolamento (UE) 2019/1020.

cep**Analisi** No. 1/2023

**VERSIONE BREVE** [ Si veda la versione estesa in lingua tedesca ]

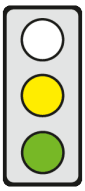
## Contesto | Obiettivo | Interessati

**Contesto:** Negli ultimi anni i prodotti software e hardware sono stati sempre più soggetti a cyberattacchi. Una delle cause principali è il basso livello di sicurezza informatica di questi prodotti. Solo nel 2021 sono state registrate perdite per 5,5 trilioni di Euro a livello mondiale. La Commissione propone quindi un *Cyber Resilience Act* (CRA).

**Obiettivo:** La Commissione intende stabilire regole uniformi di *cybersecurity* per i produttori, gli importatori e i distributori di prodotti con elementi digitali (products with digital elements - PWDE). I produttori di PWDE devono migliorare la sicurezza informatica dei loro prodotti già nella fase di progettazione e sviluppo. Inoltre, deve essere aumentata la trasparenza sulle caratteristiche di sicurezza dei PWDE.

**Interessati:** Produttori, importatori, distributori e utilizzatori di PWDE, enti di valutazione della conformità.

## Valutazione sintetica



**Pro**

- Il *Cyber Resilience* Act fornisce un contributo significativo al rafforzamento della sicurezza informatica nell'UE. Ed affronta, in modo mirato, diverse carenze nei mercati dei PWDE.
- I requisiti uniformi di cibersicurezza contrasteranno incentivi di tipo dannoso tra i produttori, gli importatori e i distributori di PWDE che ora dovranno sostenere una quota maggiore dei costi associati ai PWDE non sicuri. Sarà così più difficile trasferire i costi ai clienti ed a terzi.
- I requisiti di trasparenza renderanno più facile per gli acquirenti di PWDE valutare e confrontare le loro caratteristiche di sicurezza.
- La definizione di un calendario per la correzione delle eventuali vulnerabilità dà agli utenti dei PWDE maggiore fiducia nella qualità generale del prodotto.

**Contro**

- La classificazione dei prodotti "critici" in due classi, già effettuata dalla Commissione, non è abbastanza trasparente e non è molto coerente. Ci sono PWDE, in entrambe le classi, che non possono essere considerati di per sé "critici".
- La classificazione dei PWDE in base alla loro criticità non può essere considerata una decisione puramente tecnica e libera da considerazioni politiche. La delega di poteri alla Commissione per l'adozione di atti delegati in materia di classificazione è quindi quantomeno discutibile.
- La data di inizio prevista - 2 anni dopo l'entrata in vigore del CRA - risulta troppo ambiziosa.

## Valutazione complessiva [Nella versione estesa si veda C.1.1]

**Proposta della Commissione europea (CE):** Nell'UE sarà istituita una cornice giuridica per lo sviluppo e la distribuzione di prodotti con elementi digitali (PWDE) sicuri dal punto di vista informatico.

**Valutazione del CEP:** I produttori di PWDE presentano spesso prodotti non sicuri dal punto di vista informatico. Allo stesso tempo, è difficile per gli acquirenti dei PWDE richiedere prodotti sicuri a causa di varie carenze nei mercati dei PWDE, come i "falsi incentivi" sul lato della produzione e la mancanza di informazioni disponibili per gli acquirenti. Il CRA contribuirà in modo tangibile e significativo a colmare queste lacune del mercato.

Autori: Anastasia Kotovskaia, LL.M. e Philipp Eckhardt | kotovskaia@cep.eu Traduzione: Andrea De Petris
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Telephone +49 (0)761 38693-0 | www.cep.eu

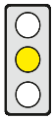
## Requisiti uniformi di cibersicurezza [Nella versione estesa si veda C.1.2]

**Proposta della CE:** Produttori, importatori e distributori di PWDE dovranno rispettare i requisiti di base in materia di cibersicurezza. Già nelle fasi di progettazione, sviluppo e produzione di un prodotto si dovrà prestare sufficiente attenzione alla sicurezza informatica.

**Valutazione del CEP:** Requisiti uniformi di cibersicurezza contrasteranno i "falsi incentivi" tra produttori, importatori e distributori di PWDE. In futuro, essi dovranno investire maggiormente nella sicurezza informatica dei loro prodotti. Ciò ridurrà i costi che finora i clienti e i terzi hanno spesso dovuto sostenere a causa di PWDE poco sicuri. Inoltre, gli svantaggi competitivi subiti dagli attori economici che sono proattivi nel fornire prodotti sicuri si ridurranno e sarà più difficile il *free-riding* tra gli acquirenti di PWDE.

## Ambito di applicazione [Nella versione estesa si veda C.1.4]

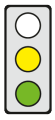
**Proposta della CE:** Il CRA si applica ai prodotti con elementi digitali (PWDE). Si tratta, in particolare, di prodotti software o hardware collegabili. I PWDE sono suddivisi in quattro gruppi: (1) PWDE "non critici", tra cui dischi rigidi e giochi per computer, (2) PWDE "critici" (Classe I), tra cui browser e gestori di password, (3) PWDE "critici" (Classe II), tra cui sistemi operativi per server, router e smartcard, e (4) PWDE "altamente critici" non ancora specificati.



**Valutazione del CEP:** Definire l'ambito di applicazione come molto ampio è appropriato perché le vulnerabilità possono verificarsi in molti PWDE, anche in quelli apparentemente non critici. Tuttavia, la classificazione dei prodotti critici in due classi, già intrapresa, manca di trasparenza. Inoltre, la classificazione è incoerente perché ci sono molti PWDE in entrambe le classi che non possono sempre essere considerati critici di per sé. Infatti, la loro criticità dipende da dove vengono utilizzati, da chi e in quali condizioni.

## Gestione delle vulnerabilità [Nella versione estesa si veda C.1.6]

**Proposta della CE:** I produttori di PWDE devono garantire che le vulnerabilità siano affrontate per la durata di vita prevista del prodotto o per cinque anni dalla data di immissione del prodotto sul mercato, a seconda di quale sia il periodo più breve.



**Valutazione del CEP:** La definizione di un periodo di tempo entro il quale i produttori devono correggere le vulnerabilità dà agli utenti dei PWDE maggiore fiducia nella qualità del prodotto. Tuttavia, la coerenza con altre normative dell'UE, per quanto riguarda la durata dell'obbligo di correggere le vulnerabilità, non è ancora raggiunta, in particolare per quanto riguarda la proposta di direttiva sulla responsabilità per i prodotti difettosi e i nuovi requisiti di progettazione ecocompatibile per smartphone, tablet e telefoni cellulari.

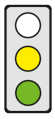
## Requisiti di trasparenza [Nella versione estesa si veda C.1.8]

**Proposta della CE:** I produttori di PWDE devono fornire informazioni agli utenti dei prodotti, come ad esempio le circostanze in cui possono verificarsi rischi per la sicurezza informatica durante l'utilizzo dei PWDE, la durata degli aggiornamenti di sicurezza e il punto di contatto dell'azienda a cui segnalare le informazioni sulle vulnerabilità.

**Valutazione del CEP:** I requisiti di trasparenza rendono più facile per i consumatori e le aziende classificare e confrontare le caratteristiche di sicurezza dei PWDE. Ciò consente loro di prendere una decisione informata sull'acquisto di un PWDE. Tali requisiti contribuiscono quindi a ridurre i malfunzionamenti del mercato causati dalle asimmetrie di informazione.

## Obblighi di segnalazione [Nella versione estesa si veda C.1.9]

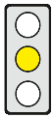
**Proposta della CE:** I produttori di PWDE devono segnalare all'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) qualsiasi incidente di sicurezza informatica o vulnerabilità attivamente sfruttata entro 24 ore.



**Valutazione del CEP:** I produttori di PWDE sono spesso riluttanti a segnalare volontariamente incidenti o vulnerabilità di cibersicurezza a causa dei rischi di immagine. Tuttavia, tali segnalazioni hanno spesso un grande vantaggio economico, in quanto è possibile adottare misure per ridurre il rischio in una fase precedente. Gli obblighi di segnalazione sono quindi appropriati. Ciononostante, l'obbligo di notificare qualsiasi vulnerabilità sfruttabile o qualsiasi incidente di sicurezza è eccessivo. Come per la linea guida NIS 2, la loro importanza deve essere tenuta in considerazione.

## Classificazione dei PWDE in base alla loro criticità [Nella versione estesa si veda C.2.3]

**Proposta della CE:** La Commissione potrà, mediante atti delegati, aggiungere nuove categorie di prodotti critici agli elenchi di PWDE critici o rimuovere categorie da tali elenchi. Pertanto, può anche creare un elenco con categorie di PWDE altamente critici. La sua decisione si basa su diversi criteri, come ad esempio il fatto che il PWDE sia utilizzato da operatori di infrastrutture critiche.



**Valutazione del CEP:** Il fatto che la Commissione possa creare elenchi di PWDE (altamente) critici tramite atti delegati significa che le sue decisioni verrebbero a mancare di trasparenza. Inoltre, non viene specificato sufficientemente il grado di soddisfazione dei criteri stessi. Tale delega di potere alla Commissione comporta il rischio che la classificazione dei PWDE possa essere influenzata da considerazioni politiche.