DIGITAL 360
ADVISORY

Il Regolamento sicurezza generale dei prodotti.

Le comunicazioni sull'applicazione del regolamento 988 per le imprese e le caratteristiche di cibersicurezza dei servizi digitali

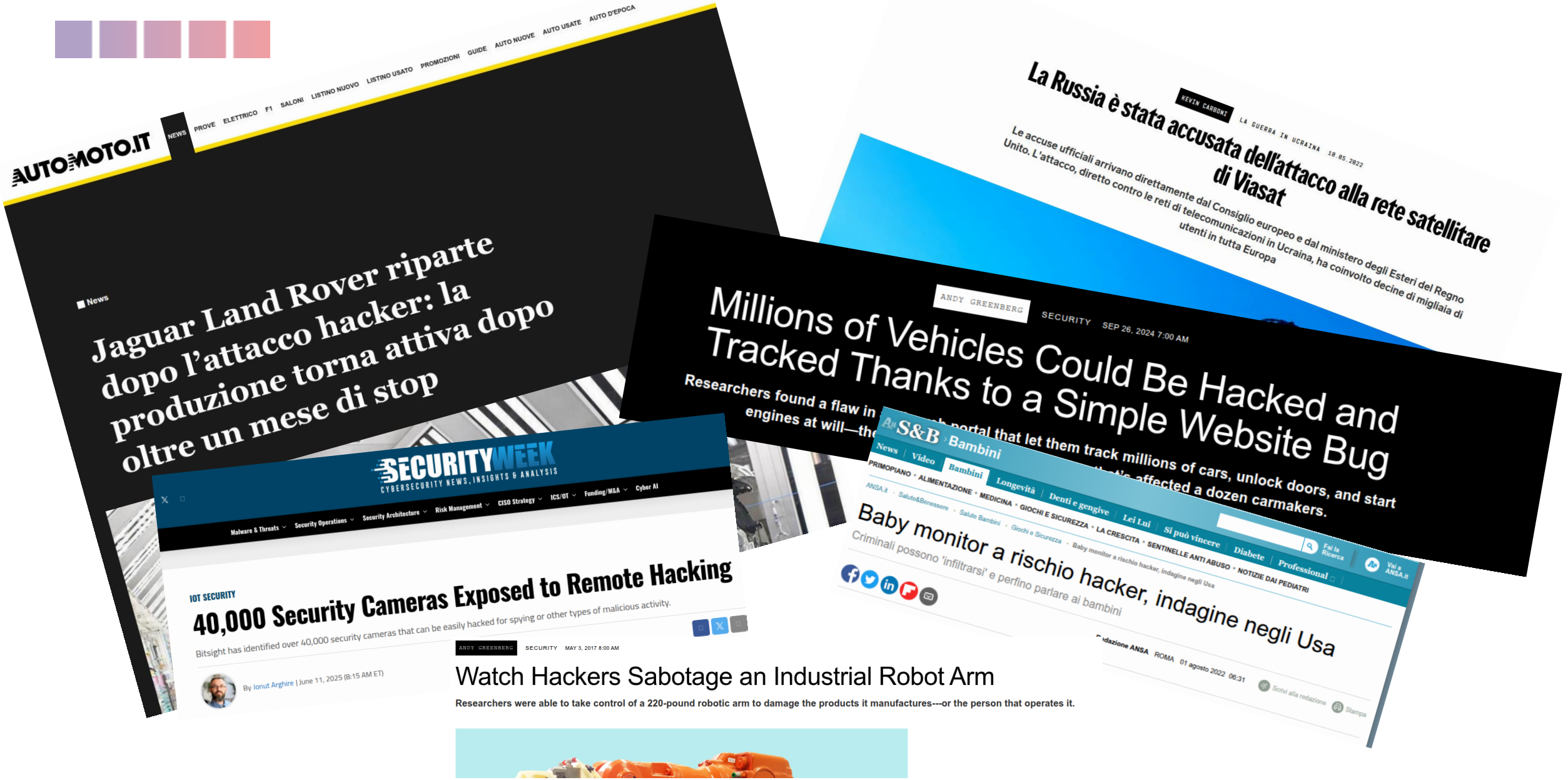
Cibersicurezza di servizi e prodotti immessi sul mercato europeo ed italiano

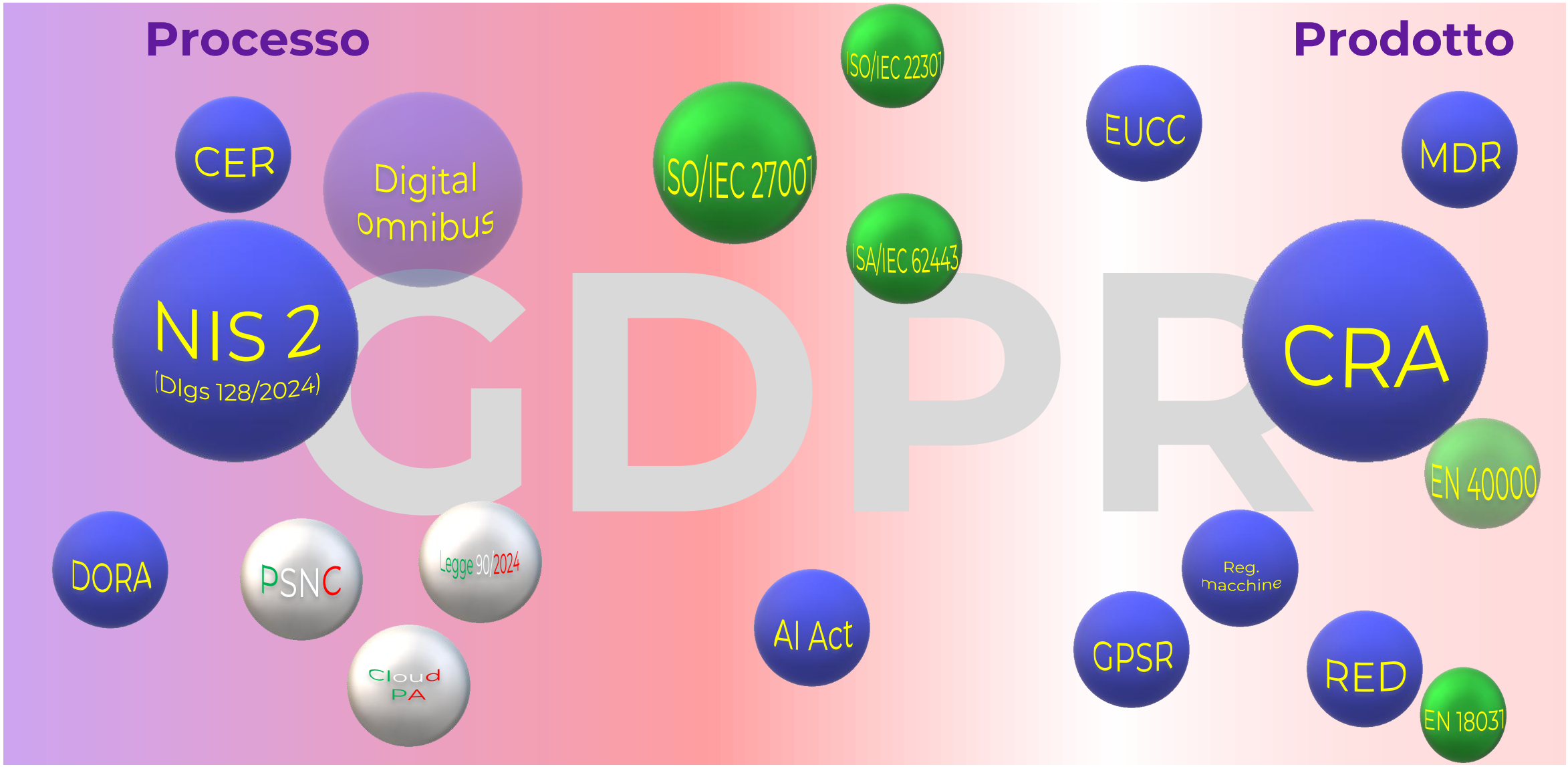
DIGITAL 360
ADVISORY

Claudio Telmon, Senior Partner - P4I, membro del comitato direttivo di Clusit

claudio.telmon@p4i.it
https://www.linkedin.com/in/telmon/

1. Il Quadro generale: perché tante normative sulla cybersecurity
2. Le principali norme di settore
3. Safety dei prodotti: requisiti e sovrapposizioni con le alter normative di settore


AUTOMOTO.IT
NEWS PROVE ELETTRICO F1 SALONI LISTINO NUOVO LISTINO USATO PROMOZIONI GUIDE AUTO NUOVE AUTO USATE AUTO D'EPOCA
News
Jaguar Land Rover riparte dopo l'attacco hacker: la produzione torna attiva dopo oltre un mese di stop
La Russia è stata accusata dell'attacco alla rete satellitare di Viasat
KEVIN CARBONI
LA GUERRA IN UCRAINA 18.05.2022
Le accuse ufficiali arrivano direttamente dal Consiglio europeo e dal ministero degli Esteri del Regno Unito. L'attacco, diretto contro le reti di telecomunicazioni in Ucraina, ha coinvolto decine di migliaia di utenti in tutta Europa
Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug
ANDY GREENBERG SECURITY SEP 26, 2024 7:00 AM
Researchers found a flaw in
portal that let them track millions of cars, unlock doors, and start
affected a dozen carmakers.
engines at will—the
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Malware & Threats Security Operations Security Architecture Risk Management CISO Strategy ICS/OT Funding/M&A Cyber AI
IOT SECURITY
40,000 Security Cameras Exposed to Remote Hacking
Bitsight has identified over 40,000 security cameras that can be easily hacked for spying or other types of malicious activity.
By Ionut Arghire | June 11, 2025 (8:15 AM ET)
S&B Bambini
News Video Bambini Longevità Denti e gengive Lei Lui Si può vincere Diabete Professional
PRIMOPIANO ALIMENTAZIONE MEDICINA GIOCHI E SICUREZZA LA CRESCITA SENTINELLE ANTI ABUSO NOTIZIE DAI PEDIATRI
Baby monitor a rischio hacker, indagine negli Usa
Criminali possono 'infiltrarsi' e perfino parlare ai bambini
ANDY GREENBERG SECURITY MAY 3, 2017 8:00 AM
Watch Hackers Sabotage an Industrial Robot Arm
Researchers were able to take control of a 220-pound robotic arm to damage the products it manufactures---or the person that operates it.


Processo
Prodotto
CER
Digital Omnibus
NIS 2
(Dlgs 128/2024)
ISO/IEC 22301
ISO/IEC 27001
ISA/IEC 62443
EUCC
MDR
CRA
EN 40000
GDPR
DORA
PSNC
Legge 90/2024
Cloud PA
AI Act
Reg. macchine
GPSR
RED
EN 18031

Security vs Safety

Definizione e differenze tra la **sicurezza (security)** rispetto alla **sicurezza funzionale (safety)**

Security: Una condizione che deriva dall'istituzione e dal mantenimento di misure di protezione che consentono a un'organizzazione di svolgere la propria missione o funzioni critiche nonostante i rischi posti dalle minacce all'uso dei sistemi. Le misure di protezione possono comportare una combinazione di deterrenza, evitamento, prevenzione, rilevamento, recupero e correzione che dovrebbero far parte dell'approccio di gestione del rischio dell'organizzazione.

Fonte: https://csrc.nist.gov/glossary/term/security

Safety: Assenza di condizioni che possono causare morte, lesioni, malattie professionali, danni o perdita di attrezzature o proprietà o danni all'ambiente.
Aspettativa che un sistema non conduca, in determinate condizioni, a uno stato in cui la vita umana, la salute, la proprietà o l'ambiente siano in pericolo.

Fonte: https://csrc.nist.gov/glossary/term/safety

Le norme europee tendono ad usare il termine **cybersecurity** (cibersicurezza), riducendo la confusione

Security nel GPSR

(23) La sicurezza di un prodotto dovrebbe essere valutata alla luce di tutti gli aspetti pertinenti del prodotto, in particolare le sue caratteristiche, quali le caratteristiche fisiche, meccaniche e chimiche, e la sua presentazione, nonché le esigenze e i rischi specifici che il prodotto rappresenta per talune categorie di consumatori che probabilmente lo utilizzeranno, in particolare i bambini, gli anziani e le persone con disabilità. Tali rischi possono includere anche i rischi ambientali nella misura in cui il prodotto rappresenti un rischio per la salute e la sicurezza dei consumatori. Tale valutazione dovrebbe tenere conto dei rischi per la salute posti dai prodotti digitalmente connessi, anche per quanto riguarda i rischi per la salute mentale, specialmente dei consumatori vulnerabili e in particolare dei minori. Pertanto, nel valutare la sicurezza dei prodotti digitalmente connessi che possono avere un impatto sui minori, i produttori dovrebbero assicurarsi che i prodotti che mettono a disposizione sul mercato soddisfino le più rigorose norme in materia di protezione, ***security*** e riservatezza sin dalla progettazione nell'interesse dei minori. Inoltre, laddove siano necessarie informazioni specifiche per rendere i prodotti sicuri per una determinata categoria di persone, la valutazione della sicurezza dei prodotti dovrebbe tenere anche conto della presenza di tali informazioni e della loro accessibilità. La sicurezza di tutti i prodotti dovrebbe essere valutata tenendo conto che il prodotto deve essere sicuro durante tutta la sua vita utile.

(24) Gli articoli che si collegano ad altri articoli o gli articoli non integrati che influenzano il funzionamento di un altro articolo possono presentare un rischio per la sicurezza del prodotto. È opportuno tenere debitamente conto di tale aspetto quale rischio potenziale. I collegamenti e le interrelazioni che un articolo potrebbe presentare con articoli esterni non dovrebbero comprometterne la sicurezza.

(25) Le nuove tecnologie potrebbero determinare nuovi rischi per la salute e la sicurezza dei consumatori o modificare il modo in cui i rischi esistenti potrebbero concretizzarsi, ad esempio un prodotto potrebbe subire un attacco informatico o altro intervento esterno che ne modifichi le caratteristiche. Le nuove tecnologie potrebbero modificare sostanzialmente il prodotto originale, ad esempio attraverso aggiornamenti del software, che dovrebbero quindi essere oggetto di una nuova valutazione del rischio se tale modifica sostanziale dovesse avere un impatto sulla sicurezza del prodotto.

(26) Specifici rischi di **cibersicurezza** che incidono sulla sicurezza dei consumatori nonché su protocolli e certificazioni possono essere affrontati dalla normativa settoriale. Tuttavia è opportuno garantire che, nei casi in cui non si applica la normativa settoriale, gli operatori economici pertinenti e le autorità nazionali prendano in considerazione i rischi legati alle nuove tecnologie rispettivamente al momento della progettazione dei prodotti e della loro valutazione, al fine di assicurare che le modifiche apportate ai prodotti non ne compromettano la sicurezza.

Security nel GPSR

Articolo 6 - Aspetti della valutazione della sicurezza del prodotto

1. Nel valutare se un prodotto è sicuro, si prendono in considerazione in particolare gli aspetti seguenti:

a) le caratteristiche del prodotto, tra cui la sua progettazione, le sue caratteristiche tecniche, la sua composizione, il suo imballaggio, le sue istruzioni per l'assemblaggio e, se del caso, per l'installazione, per l'uso e per la manutenzione;
b) l'effetto del prodotto su altri prodotti, qualora sia ragionevolmente prevedibile che il prodotto sarà utilizzato con altri prodotti, compresa l'interconnessione di tali prodotti;
c) l'effetto che altri prodotti potrebbero avere sul prodotto da valutare, qualora sia ragionevolmente prevedibile l'utilizzo di altri prodotti con tale prodotto, compreso l'effetto di elementi non integrati destinati a determinare, modificare o completare il funzionamento del prodotto da valutare, di cui si deve tener conto nella valutazione della sicurezza del prodotto da valutare;
d) la presentazione del prodotto, la sua etichettatura, compresa l'etichettatura relativa all'età di idoneità per i bambini, le eventuali avvertenze e istruzioni per l'uso e lo smaltimento sicuri nonché qualsiasi altra indicazione o informazione relativa al prodotto;
e) le categorie di consumatori che utilizzano il prodotto, in particolare valutando i rischi per i consumatori vulnerabili come i bambini, gli anziani e le persone con disabilità, nonché l'impatto delle differenze di genere sulla salute e la sicurezza;
f) l'aspetto del prodotto quando può indurre i consumatori a utilizzarlo in modo diverso da quello per cui è stato progettato, in particolare:
    i. se un prodotto, pur non essendo un prodotto alimentare, vi assomiglia e può essere confuso con un prodotto alimentare per la sua forma, odore, colore, aspetto, imballaggio, etichettatura, volume, dimensioni o altre caratteristiche, e i consumatori, in particolare i bambini, potrebbero pertanto portarli alla bocca, succhiarli o ingerirli;
    ii. se un prodotto, pur non progettato per essere utilizzato da bambini, né destinato a esserlo, può essere utilizzato dai bambini o assomiglia per la sua progettazione, il suo imballaggio o le sue caratteristiche a un oggetto comunemente riconosciuto come attraente per i bambini o destinato a un utilizzo da parte di questi;
g) laddove lo imponga la natura del prodotto, le adeguate caratteristiche di cibersicurezza necessarie per proteggere il prodotto da influenze esterne, compresi terzi malintenzionati, se tale influenza potrebbe avere un impatto sulla sicurezza del prodotto, compresa la possibile perdita di interconnessione;

CRA: una normativa orizzontale sulla cybersicurezza dei prodotti

Cyber Resilience Act

1. Perché

Il **Regolamento (UE) 2024/2847** cerca di aumentare il livello di sicurezza informatica dei prodotti con **elementi digitali** e le conoscenze delle imprese e dei consumatori sulla sicurezza dei prodotti.

Sono state definite sanzioni in caso di non-compliance

2. Cosa

Un **quadro normativo orizzontale dell'UE** basato su una serie completa di requisiti di cibersicurezza per i prodotti **con elementi digitali**, tra cui il software "tangibile" (hardware) e non incorporato. Introduce norme per proteggere i prodotti digitali che non sono coperti da alcuna regolamentazione precedente.

3. Quando

Dal 11 dicembre 2024, gli operatori economici e gli Stati membri avranno **36 mesi di tempo** (**Dicembre 2027**) per adeguarsi ai nuovi requisiti.

21 mesi (**Settembre 2026**) nel caso di **obblighi di segnalazione** di vulnerabilità sfruttate e incidenti, e **18 mesi** per definire i processi di notifica alle autorità responsabili (applicazione solo a autorità nazionali).

4. Chi

Fabbricanti, importatori, distributori di prodotti con elementi digitali

5. Come

Definendo e imponendo requisiti essenziali di cibersicurezza (comprese le norme armonizzate) da soddisfare **prima dell'immissione** dei prodotti **sul mercato** e **durante l'intero ciclo di vita** del prodotto.

Ambito di applicazione e definizioni

AMBITO DI APPLICAZIONE

Nell'art. 2, paragrafo 1, si fa riferimento a:

«*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*.»

V. Regolamento del Parlamento Europeo e del Consiglio del 23 Ottobre 2024 sui requisiti orizzontali di cybersecurity per i prodotti dotati di elementi digitali e in rettifica dei Regolamenti UE 168/2013 e 2019/1020 e della Direttiva UE 2020/1828 (Cyber Resilience Act) art. 3

LA DEFINIZIONE DI «***PRODOTTI CON ELEMENTI DIGITALI***» DELL'ART.3 DEL CRA:

1) «prodotto con elementi digitali»: qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi sul mercato separatamente

2) «elaborazione dati da remoto»: 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 le sue funzioni

8) «connessione logica»: una rappresentazione virtuale di una connessione dati realizzata attraverso un'interfaccia software

9) «connessione fisica»: qualsiasi connessione tra sistemi di informazione elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche, ottiche o meccaniche, fili od onde radio

10) «connessione indiretta»: una connessione a un dispositivo o a una rete che non avviene direttamente ma piuttosto nell'ambito di un sistema più ampio che è direttamente collegabile a tale dispositivo o rete

Prodotti con elementi digitali

Il Cyber Resilience Act (CRA) **classifica i prodotti** con elementi digitali in **tre categorie** basate sul loro **potenziale rischio e impatto** sulla sicurezza informatica:

Prodotti con elementi digitali

Categoria "*predefinita*" che comprende prodotti che non rientrano nelle definizioni specifiche di "*importante*" o "*critico*".

Questi prodotti sono comunque soggetti ai requisiti di sicurezza come la gestione delle vulnerabilità, le configurazioni sicure predefinite e le misure di protezione dei dati.

Prodotti con elementi digitali importanti

Prodotti la cui funzionalità principale comporta un rischio informatico più elevato, in quanto svolge principalmente funzioni essenziali per la cibersicurezza, o a causa del potenziale impatto negativo su altri prodotti, reti, servizi.

L'Allegato III elenca categorie specifiche di prodotti, suddividendole in Classe I e Classe II in base alla gravità dei potenziali effetti avversi.

Prodotti con elementi digitali critici

I prodotti critici con elementi digitali sono quelli con il più alto rischio di sicurezza informatica a causa del loro ruolo vitale e della potenziale causa di gravi perturbazioni alle catena di approvvigionamento se compromessi. La Commissione Europea può richiedere la certificazione europea per la sicurezza informatica per questi prodotti, imponendo un livello di affidabilità almeno "*sostanziale*".

L'**Allegato IV** elenca le categorie di prodotti critici

Prodotti con elementi digitali

DIGITAL 360
ADVISORY

Prodotti con elementi digitali «importanti»

1. I **Prodotti** con elementi digitali **importanti** sono:
   I prodotti importanti sono quelli la cui compromissione potrebbe causare rischi significativi su altri sistemi o sulle persone. Tali prodotti sono definiti nell'**Allegato III** e si dividono in:

   - **Classe I:** Prodotti che svolgono funzioni vitali per la sicurezza, come sistemi di gestione delle identità e browser, con un impatto potenziale meno grave.

   - **Classe II:** Prodotti come firewall e sistemi di rilevamento delle intrusioni, con un rischio maggiore di effetti avversi significativi.

2. Valutazione della Conformità:
   - **I prodotti di Classe I** possono sottoporsi a un'autovalutazione attraverso la procedura di controllo interno (Modulo A) se il fabbricante applica standard armonizzati, specifiche comuni o schemi di certificazione europea per la sicurezza informatica. Se questi non vengono applicati, è obbligatoria una valutazione della conformità da parte di terzi.

   - **I prodotti di Classe II** richiedono sempre una valutazione della conformità da terzi parti, indipendentemente dall'applicazione di standard armonizzati o altre specifiche.

Prodotti in **Classe I:**

1. Gestione delle identità
2. Browser
3. Gestori di password
4. Antivirus
5. Virtual Private Network (VPN)
6. Gestione delle reti
7. SIEM
8. Boot Managers
9. Public Key Infrastructure (PKI)
10. Interfacce di rete
11. Sistemi operativi
12. Router, modem per la connessione a Internet e switch
13. Microprocessori per la sicurezza
14. Microcontrollori per la sicurezza
15. ASIC & FPGA per la sicurezza
16. Assistenti virtuali per la casa
17. Prodotti per Smart House: serrature intelligenti, telecamere di sicurezza, sistemi di monitoraggio per bambini e sistemi di allarme
18. Giocattoli connessi a Internet
19. Prodotti indossabili che monitorano la salute

Prodotti in **Classe II:**

1. Hypervisor e sistemi di runtime per container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili
2. Firewall, sistemi di rilevamento e prevenzione delle intrusioni
3. Microprocessori a prova di manomissione
4. Microcontrollori a prova di manomissione

DIGITAL 360 ADVISORY

Prodotti con elementi digitali «critici»

1. I **Prodotti** con elementi digitali **critici** sono:
    - I prodotti critici hanno **funzionalità legate alla sicurezza informatica** e svolgono ruoli vitali per la sicurezza dei sistemi, con fallimenti che possono avere conseguenze gravi. Sono spesso fondamentali per infrastrutture critiche e servizi essenziali.
    - Categorie di Prodotti: l'**Allegato IV** del CRA include esempi come **dispositivi hardware con box di sicurezza**, gateway di contatori intelligenti e smartcard, sottolineando la loro importanza per la sicurezza avanzata.

2. Valutazione della Conformità:
    - I prodotti critici sono soggetti a **procedure di valutazione della conformità più rigorose**, che possono includere la certificazione europea obbligatoria per la sicurezza informatica. Questa certificazione, basata su schemi come l'EUCC, può raggiungere il livello più alto per i prodotti destinati ad ambienti sensibili.

Il CRA prevede che la Commissione possa modificare le categorie di prodotti critici basandosi su criteri come la dipendenza critica dei soggetti essenziali e le potenziali perturbazioni delle catene di approvvigionamento critiche.

Prodotti con elementi critici:

1. Dispositivi hardware con cassette di sicurezza
2. Gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti, e altri dispositivi a fini di sicurezza avanzati, compreso il trattamento crittografico sicuro
3. Carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri

Fonte: CRA, Articolo 8 e Articolo 32

Ambito di applicazione ed esclusioni

2. Il presente regolamento non si applica ai prodotti con elementi digitali a cui si applicano i seguenti atti giuridici dell'Unione:

a) regolamento (UE) 2017/745; ⇨ Regolamento relativo ai **Dispositivi Medici**

b) regolamento (UE) 2017/746; ⇨ Regolamento relativo ai **Dispositivi Medico-Diagnostici in Vitro**

c) regolamento (UE) 2019/2144. ⇨ Regolamento relativo ai requisiti di omologazione dei **veicoli a motore** e dei loro rimorchi

3. Il presente regolamento non si applica ai prodotti con elementi digitali che sono stati certificati in conformità del regolamento (UE) 2018/1139. ⇨ Regolamento recante norme comuni nel settore dell'**aviazione civile**

4. Il presente regolamento non si applica all'equipaggiamento che rientra nell'ambito di applicazione della direttiva n. 2014/90/UE del Parlamento europeo e del Consiglio ([36]). ⇨ Direttiva che intende migliorare la **sicurezza in mare**; prevenire l'inquinamento marino; garantire che le norme di sicurezza internazionali per l'equipaggiamento a bordo delle navi dell'Unione Europea.

DIGITAL 360 ADVISORY

CRA vs GPSR

(50) Il presente regolamento affronta i rischi di cibersicurezza in modo mirato. I prodotti con elementi digitali possono tuttavia comportare altri rischi di ***safety*** che non sono sempre connessi alla cibersicurezza ma che possono essere la conseguenza di una violazione della ***security***. Tali rischi dovrebbero continuare a essere regolamentati da altre normative di armonizzazione dell'Unione pertinenti diverse dal presente regolamento. **Se non sono applicabili altre normative di armonizzazione dell'Unione diverse dal presente regolamento, essi dovrebbero essere soggetti al regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio (21).Pertanto, alla luce della natura mirata del presente regolamento, in deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento (UE) 2023/988, il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento (UE) 2023/988 dovrebbero applicarsi ai prodotti con elementi digitali per quanto riguarda i rischi di *safety* non contemplati dal presente regolamento**, qualora tali prodotti non siano soggetti a requisiti specifici stabiliti da altre normative di armonizzazione dell'Unione diverse dal presente regolamento ai sensi dell'articolo 3, punto 27), del regolamento (UE) 2023/988.

Articolo 11- Sicurezza generale dei prodotti

In deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento (UE) 2023/988, il capo III, sezione 1, i capi V e VII e i capi da IX a XI di tale regolamento si applicano ai prodotti con elementi digitali per quanto riguarda gli aspetti e i rischi o le categorie di rischio non contemplati dal presente regolamento qualora tali prodotti non siano soggetti a requisiti specifici di sicurezza imposti da altra «normativa di armonizzazione dell'Unione» ai sensi dell'articolo 3, punto 27), del regolamento (UE) 2023/988.

Il considerando (53) affronta il tema del coordinamento con il Regolamento Macchine

Milestones

20 novembre 2024
Pubblicazione in Gazzetta Ufficiale della Unione Europea

3 febbraio 2025
Mandato di normazione
La Commissione Europea invita organismi di normazione CEN, CNELEC ed ETSI a elaborare le norme armonizzate

Entro 11 dicembre 2025
La Commissione Europea era tenuta a definire specifiche tecniche dettagliate per le categorie di prodotti degli allegati III e IV (prodotti importanti e critici)

3 marzo 2026
Bozza di linee guida
La Commissione Europea pubblica la bozza di linee guida per le aziende e la apre ai contributi degli stakeholder fino al 31 marzo 2026

11 Giugno 2026
(*) 18 mesi dopo pubblicazione
- Scadenza degli stati membri per definire i **processi di notifica** alle autorità. (CAPO IV, articoli 35 – 51)

11 settembre 2026
(*) 21 mesi dopo pubblicazione
- Scadenza **per fabbricanti (**)** di obblighi di segnalazione di vulnerabilità sfruttabili e degli incidenti di sicurezza. (Articolo 14)

11 dicembre 2027
(*) 36 mesi dopo pubblicazione
- Applicazione totale del regolamento

(*) Scadenze: Le deadline/scadenze inizieranno ad essere applicate **20 giorni dopo la pubblicazione** del CRA **nella Gazzetta Ufficiale** dell'UE.

(**) Fabbricante: Una persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o che fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, di monetizzazione o gratuito

DIGITAL 360 ADVISORY

Chi sono gli operatori economici?

Il Cyber Resilience Act è un **regolamento** che si applica allo stesso modo a tutti i membri dell'UE. Tuttavia ci sono delle distinzioni negli obblighi per gli operatori economici, che vengono suddivisi in tre soggetti diversi: **fabbricanti, importatori** e **distributori**.

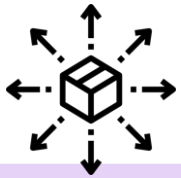
FABBRICANTE

Una persona fisica o giuridica che **sviluppa o fabbrica prodotti** con elementi digitali o che **fa progettare, sviluppare o fabbricare prodotti** con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, di monetizzazione o gratuito;

- Hanno la maggior parte degli obblighi e responsabilità ai sensi del CRA

IMPORTATORE

Una persona fisica o giuridica stabilita nell'Unione che **immette sul mercato un prodotto con elementi digitali** recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione;



DISTRIBUTORE

Una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che **mette a disposizione un prodotto con elementi digitali sul mercato** dell'Unione senza modificarne le proprietà;

DIGITAL 360 ADVISORY

Obblighi più importanti per la conformità

Soggetti	Obblighi (più importanti)	Numero totale di obblighi
Fabbricanti	• **Cybersecurity by Design** e by Default (13 controlli indicati nel **Allegato I, Parte I)** • Analisi del **Rischio Cybersecurity** • Realizzare una **distinta base** / Software Bill of Materials **(SBOM)** • **Gestione delle Vulnerabilità (Allegato I, Parte II)** • **Documentazione Tecnica** e **Valutazione di Conformità** • Apporre **marcatura CE** • Obblighi di **segnalazione**	• **Articolo 13:** 25 punti • **Articolo 14:** 10 punti
Importatori	• Verifica della documentazione dei fabbricanti • Dettagli di contatto chiari sui prodotti. • Verifica della presenza marcatura CE • Obblighi di segnalazione • Cooperazione con le autorità	• **Articolo 19:** 8 punti
Distributori	• Confermare la conformità CRA della supply chain • Verifica della presenza marcatura CE • Obblighi di segnalazione • Cooperazione con le autorità	• **Articolo 20**: 6 punti

D'accordo con l'articolo 21 gli **importatori** e i **distributori** possono essere considerati fabbricanti se:

- Commercializzano un prodotto con elementi digitali sotto il proprio nome o marchio
- Modificano un prodotto esistente in modo che influisca sulla sua conformità al regolamento.

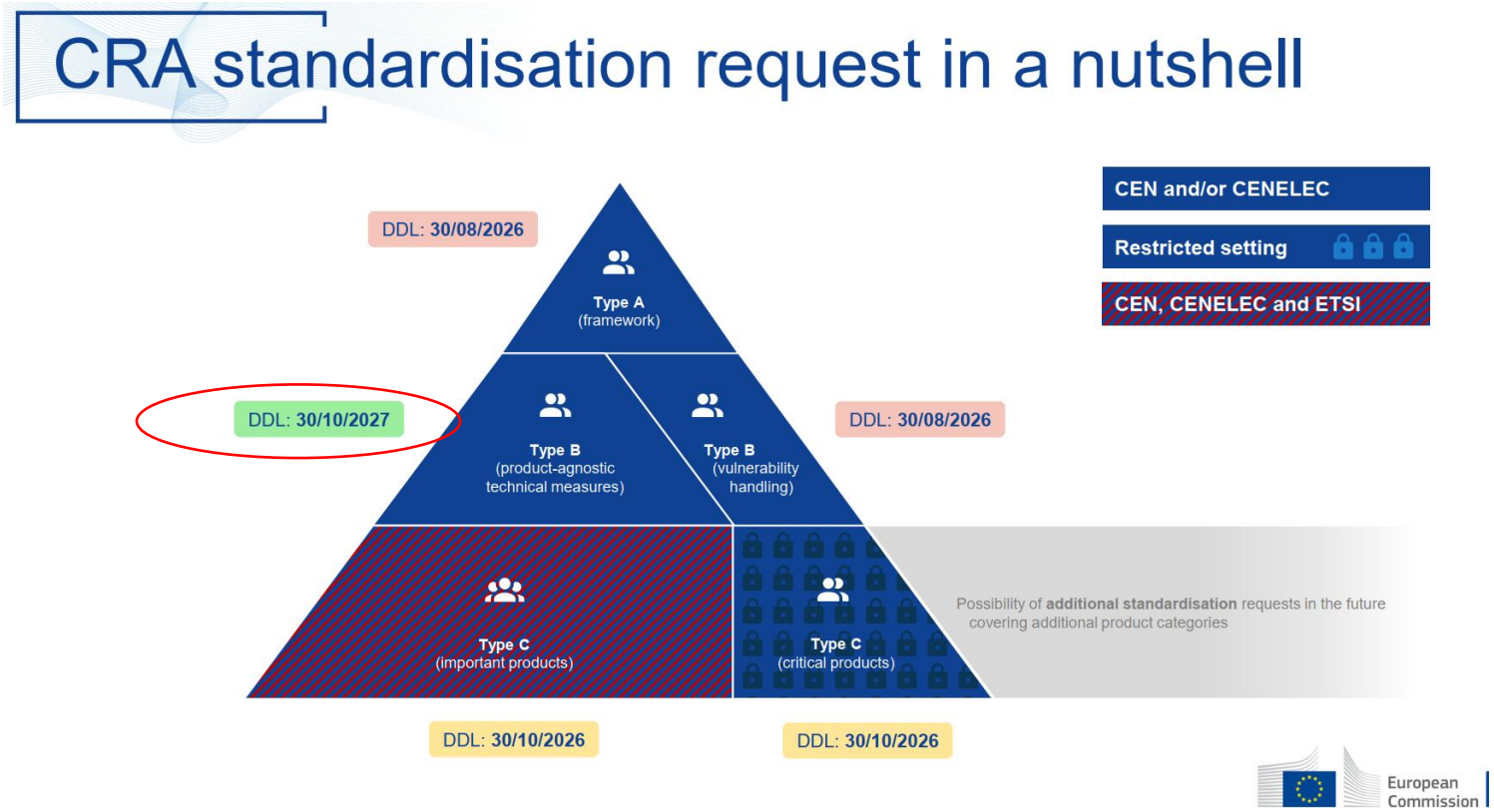
Norme armonizzate per la conformità

È attualmente in corso un'attività di standardizzazione che coinvolge CEN, CENELEC e ETSI per la definizione delle norme armonizzate relative ai requisiti CRA a supporto della marcatura CE.

La serie EN 40000 è una famiglia di **norme orizzontali** sviluppata nel contesto del CRA:

- EN 40000-1-1: Vocabulary.
- EN 40000-1-2: Principles for cyber resilience.
- EN 40000-1-3: Vulnerability handling requirements.
- EN 40000-1-4: Generic security requirements.

Vi sono poi **norme verticali** con requisiti specifici per determinati prodotti



DIGITAL 360 ADVISORY

DIGITAL 360
ADVISORY

GRAZIE

Viale L. Bodio, 37 - 20158 Milano

https://www.digital360.it/advisory-servizi