Cyber Security, Intelligenza Artificiale, Privacy e il relativo quadro sanzionatorio

Sin dall'anno 2022 e sino al 2028 è nota l'entrata in vigore e l'applicazione di diverse legislazioni, europee e nazionali, ovvero la Direttiva (UE) 2022/2555, sui requisiti comuni per un livello elevato di cibersicurezza, c.d. *NIS 2* (Network and Information Security 2), il Regolamento (UE) 2024/2847 sui requisiti orizzontali di cibersicurezza, c.d. *Cyber Resilience Act*, il Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario, c.d. *DORA* (Digital Operational Resilience Act), il Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale, c.d. *AI Act*, il Regolamento (UE) 2016/679 sulla protezione dei dati personali, c.d. *GDPR*, il Regolamento (UE) 2023/1230 sui requisiti di salute e sicurezza per la progettazione e costruzione delle macchine, e il Regolamento (UE) 2023/2854 sull'accesso equo, condivisione e utilizzo dei dati, c.d. *Data Act*, in forza delle quali le aziende italiane ed europee dovrebbero operare attraverso diversi interventi normativi, per una compliance integrata, completa ed univoca negli ambiti di interesse, anche al fine di una semplificazione interna delle policies aziendali.

Il nuovo quadro normativo europeo e nazionale digitale mira a rafforzare la sicurezza e la solidità del modello digitale aziendale, con l'introduzione di nuovi obblighi, governance, responsabilità, al fine di poter dimostrare, come i sistemi, i servizi e i prodotti digitali sono valutati, gestiti e monitorati.

L'anno in corso rappresenta un periodo rilevante nell'attuazione del Regolamento (UE) 2024/2847 riguardante i requisiti orizzontali di cibersicurezza, (di seguito, "CRA") con l'avvio dei primi adempimenti per i fabbricanti, importatori e distributori. In particolare, essi riguardano la gestione delle vulnerabilità, la notifica degli incidenti, la conformità dei prodotti digitali, con i relativi obblighi, responsabilità, ruoli e scadenze, rilevanti per gli adeguamenti normativi delle imprese.

Il Regolamento (UE) 2024/2847, in vigore dal 10.12.2024, introduce norme comuni di cibersicurezza per i produttori e gli sviluppatori di prodotti con elementi digitali, obblighi già oggetto di sanzioni, oltre alle scadenze per i fabbricanti, importatori e distributori.

In particolare, il CRA stabilisce i requisiti obbligatori di cibersicurezza per i fabbricanti, afferenti alla pianificazione, progettazione, sviluppo e manutenzione dei prodotti, in ogni loro fase.

Il CRA si applica dall'11.12.2027, ma gli obblighi di segnalazione delle vulnerabilità da parte dei fabbricanti di cui all'art. 14 (Obblighi di segnalazione dei fabbricanti), si applica dall'11.09.2026. Mentre, il Capo IV riguardante la notifica degli organismi di valutazione della conformità (artt. da 35 a 51), che intendono operare come valutatori di conformità, si applica dall'11.06.2026.

A tal fine, le aziende produttrici delle categorie critiche, ai fini dell'accesso al mercato UE, dovrebbero preliminarmente verificare se l'organismo di certificazione prescelto abbia già avviato o completato il processo di notifica nel proprio Stato membro.
Dal punto di vista operativo, ai sensi dell'art. 14 i fabbricanti devono presentare una notifica di preallarme entro 24 ore dalla conoscenza della vulnerabilità, e in mancanza di informazioni pertinenti, una notifica delle vulnerabilità entro 72 ore dalla conoscenza della vulnerabilità, e, sempre in mancanza di informazioni pertinenti, una relazione finale entro 14 giorni dalla disponibilità di una misura correttiva o di attenuazione per le vulnerabilità attivamente sfruttate, ed entro un mese per gli incidenti gravi che abbiano un impatto sulla sicurezza del prodotto con elementi digitali di cui viene a conoscenza.
In sostanza, i fabbricanti comunicano attraverso la piattaforma unica di comunicazione del CRA, e la notifica viene trasmessa al CSIRT (Computer Security Incident Response Team) dello Stato membro in cui i fabbricanti hanno il proprio stabilimento principale e, salvo circostanze particolarmente eccezionali, le informazioni sono messe a disposizione dell'ENISA (Agenzia dell'Unione europea per la cibersicurezza).
Le autorità di vigilanza del mercato collaborano, all'occorrenza, con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati. Queste ultime hanno il potere di richiedere qualsiasi documentazione creata o conservata a norma del CRA e di accedervi, qualora l'accesso a tale documentazione sia necessario per lo svolgimento dei loro compiti. Esse informano le autorità di vigilanza del mercato designate dello Stato membro interessato di tale richiesta.
La compliance agli obblighi di segnalazione predetti è strettamente collegata a quanto già stabilito dalla Direttiva (UE) 2022/2555, (di seguito, NIS 2), recepita in Italia con il D.Lgs. n. 138/2024, che impone regimi analoghi di notifica degli incidenti agli operatori di settori critici. A tal fine, le aziende soggette al CRA e alla NIS 2 dovranno coordinare i propri processi interni per evitare duplicazioni, e garantire la coerenza delle segnalazioni verso i diversi destinatari istituzionali.
Il CRA stabilisce gli obblighi fondamentali per i produttori, i quali devono integrare la sicurezza informatica nei loro prodotti sin dalla fase di sviluppo, e ne sono responsabili sino a tutto il ciclo di vita del prodotto, con o senza terze parti coinvolte, e le best practices per gli utenti finali.
Per quanto concerne la gestione delle vulnerabilità, il CRA richiede ai fabbricanti una gestione strutturata delle vulnerabilità per l'intero periodo di assistenza del prodotto, pari ad almeno cinque anni o ad una durata di utilizzo, se inferiore.
Si precisa al riguardo, che il 21.12.2025 è entrato in vigore il Regolamento di esecuzione (UE) n. 2025/2392 relativo alla descrizione tecnica delle categorie di prodotti con elementi digitali importanti e critici (Allegato III e IV) a norma del Regolamento UE 2024/2847 del Parlamento europeo e del Consiglio (CRA). I prodotti con elementi digitali importanti sono suddivisi in Classe I, che contiene i sistemi di gestione delle password, i sistemi di gestione della rete, i sistemi di gestione delle informazioni e degli eventi di sicurezza, le infrastrutture a chiave pubblica e software per il rilascio di

certificati digitali, i sistemi operativi, e vari altri, e Classe II, quali ad esempio i firewall, i sistemi di rilevamento e prevenzione delle intrusioni, per i quali, come già precisato, risulta necessaria la valutazione di conformità certificata da un organismo terzo notificato entro la scadenza dell'11.06.2026.
Uno degli aspetti principali e rilevanti riguarda le sanzioni di cui all'art. 64 del CRA, secondo il quale:
- la non conformità ai requisiti essenziali di cibersicurezza di cui all'Allegato I e agli obblighi di cui agli artt. 13 (Obblighi dei fabbricanti) e 14 è soggetta a sanzioni amministrative pecuniarie fino ad euro 15 MLN o, se l'autore del reato è un'impresa, fino al 2,5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- la non conformità agli obblighi relativi a rappresentanti autorizzati, importatori, distributori, dichiarazione di conformità UE, marcatura CE, documentazione tecnica e valutazione di conformità per prodotti con elementi digitali è soggetta a sanzioni fino ad euro 10 MLN o, se l'autore del reato è un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- ed infine, per informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato, si applicano le sanzioni fino ad euro 5 MLN o, se l'autore del reato è un'impresa, fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Gli Stati membri fissano le norme sulle sanzioni applicabili in caso di violazione, e prendono tutti i provvedimenti necessari per assicurarne l'applicazione. Esse devono essere effettive, proporzionate e dissuasive, e gli Stati membri notificano tali norme e misure alla Commissione, senza indugio, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.
Il CRA si colloca all'interno di un quadro normativo europeo in continuo sviluppo e collegato anche al Regolamento UE 2019/881, c.d. *Cybersecurity Act*, che definisce il sistema europeo di certificazione della sicurezza informatica, e con la nota NIS 2, che impone obblighi di gestione dei rischi e notifiche di incidenti a numerosi settori strategici.
Come già precedentemente descritto, le priorità operative da affrontare riguardano:
- la catalogazione dei prodotti rispetto alle categorie dei prodotti con elementi digitali importanti e critici,
- la verifica dello stato di notifica degli organismi di valutazione della conformità nel proprio Stato membro entro la data dell'11.06.2026 e,
- la predisposizione di processi interni per la rilevazione e la notifica delle vulnerabilità entro le tempistiche predette di cui all'art. 14 del CRA.
Per quanto concerne invece gli adempimenti di cui alla NIS 2, le organizzazioni soggette alla Direttiva dovranno completare l'elencazione, la caratterizzazione e la categorizzazione delle proprie attività e dei propri servizi attraverso la piattaforma dell'Agenzia per la Cybersicurezza Nazionale (di seguito, ACN) entro il 30.06.2026.
In particolare, la compliance per i soggetti NIS è quella di identificare le attività essenziali svolte dall'organizzazione, individuare i servizi erogati al proprio interno o

verso terzi, e attribuire le categorie di rilevanza secondo i criteri definiti dall'ACN.
L'Autorità fornisce riscontro ai soggetti essenziali e ai soggetti importanti circa la conformità di quanto comunicatole rispetto alle modalità e ai criteri per l'elencazione, la caratterizzazione e categorizzazione delle attività e dei servizi.
Tali adempimenti sono rilevanti per le organizzazioni, per conoscere meglio quali sono i processi e servizi strategici, che costituiscono la base per l'applicazione delle misure di sicurezza previste dalla normativa.
Le informazioni raccolte rappresentano inoltre un elemento essenziale per la governance della sicurezza e per la pianificazione degli investimenti in ambito cyber, per avviare le attività di analisi e categorizzazione in tempi brevi, quali sono le attività rilevanti e servizi critici, ai fini della trasmissione delle informazioni all'ACN e al rispetto degli obblighi previsti dalla NIS 2.
In sostanza, gli adempimenti richiesti prevedono che ogni azienda soggetta alla NIS 2 trasmetta sulla piattaforma ACN l'elenco completo delle proprie attività e dei propri servizi, classificati per categoria di rilevanza, utilizzando l'apposito modulo scaricabile dalla stessa piattaforma. Per ogni attività o servizio censito dovranno essere indicati la denominazione, una breve descrizione, la macro-area ACN di appartenenza e, soprattutto, la categoria di rilevanza. Il modello prevede quattro categorie di rilevanza, con livello di impatto crescente da "minimo" ad "alto", per attività come la sicurezza informatica e fisica.
Il file a disposizione sulla piattaforma (modello di categorizzazione) attribuisce automaticamente un livello predefinito a ogni macro-area, ma può essere modificato e adeguato alla situazione specifica, motivandone la scelta.
Le aziende già iscritte in elenco devono completare l'adeguamento completo entro il mese di ottobre 2026, mentre per la prima registrazione nel corso del 2026, le aziende, entro il 31.12.2026 dovranno provvedere alla designazione del referente CSIRT e avvio dei piani di adeguamento, ed entro il 01.01.2027 adempiere all' obbligo di notifica degli incidenti significativi. Ed infine, entro il mese di luglio 2027 dovranno essere adottate le misure di sicurezza di base.
La NIS 2 si applica direttamente a soggetti essenziali e soggetti importanti, identificati principalmente in base al settore di attività e alle dimensioni aziendali. I settori ad alta criticità sono:
- energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio (Allegato I).
I settori a criticità elevata sono invece:
- servizi postali, gestione dei rifiuti, produzione e distribuzione di prodotti chimici, produzione di dispositivi medici, fabbricazione di computer e prodotti elettronici, e altri (Allegato II).
In linea generale, rientrano nell'obbligo di registrazione le medie e grandi imprese operanti nei settori predetti, e con più di 50 dipendenti e un fatturato o bilancio annuo superiore a euro 10 MLN.
Le microimprese e le piccole imprese sono esonerate, salvo eccezioni specifiche legate

a settori critici. Tuttavia, esse devono osservare la supply chain security, in quanto le aziende soggette alla NIS 2 sono obbligate a valutare e gestire i rischi dei loro fornitori, trasmettendo parte degli obblighi lungo tutta la catena.
Il trattamento dei dati personali a norma della NIS 2 da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di comunicazioni elettroniche accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione in materia di protezione dei dati e della legislazione dell'Unione in materia di riservatezza, segnatamente la direttiva 2002/58/CE.
Merita particolare attenzione l'adozione delle misure di sicurezza previste dall'art. 24 (Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica) del D.Lgs. n. 138/2024, che richiedono alcune procedure aziendali rilevanti da redigere e aggiornare, per la politica di analisi dei rischi e sicurezza, la gestione degli incidenti, la continuità operativa, la sicurezza della catena di approvvigionamento, gestione delle vulnerabilità e la formazione del personale in materia di cybersicurezza.
Fra le procedure, la gestione del rischio rappresenta un aspetto rilevante della NIS 2, di cui all'art. 21 (Misure di gestione dei rischi di cibersicurezza), che richiede ai soggetti obbligati di identificare, valutare e gestire i rischi derivanti dai loro fornitori di servizi ICT, con particolare attenzione ai fornitori che hanno accesso a sistemi critici o trattano dati sensibili.
La categorizzazione dei fornitori dovrebbe seguire un criterio di rischio che tenga conto della criticità del servizio erogato, del livello di accesso ai sistemi e della sicurezza del fornitore. In tal senso, sarebbe di utilità per le imprese effettuare una catalogazione dei fornitori e dei loro servizi, una valutazione del rischio, la conoscenza delle misure di sicurezza, e monitorare i fornitori nel corso delle attività aziendali.
L'ACN ha il compito di monitorare e valutare il rispetto degli obblighi NIS 2 da parte delle aziende, e attraverso ispezioni o verifiche della documentazione necessaria, in caso di violazioni, l'ACN può applicare (art. 38 - Sanzioni amministrative-):
- per i soggetti essenziali (escluse le P.A.), sanzioni fino ad un massimo di euro 10 MLN o del 2% del totale del fatturato annuo,
- per i soggetti importanti (escluse le P.A.) sanzioni fino ad un massimo di euro 7 MLN o dell'1,4% del totale del fatturato annuo,
- per le P.A. che rientrano tra i soggetti essenziali, sanzioni da euro 25.000 a euro 125.000,
- per le P.A. che rientrano tra i soggetti importanti, le sanzioni sono ridotte di un terzo.
Anche il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (di seguito, IA Act), in vigore dall' 01.08.2025, disciplina le scadenze e sanzioni sino al 2028, ciascuna con obblighi specifici per sviluppatori, fornitori, utilizzatori e distributori di strumenti IA, in base al livello di rischio dei sistemi utilizzati.
L'IA Act (art. 2) si applica:
a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese

terzo,
b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione,
c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione,
d) agli importatori e ai distributori di sistemi di IA,
e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio,
f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione,
g) alle persone interessate che si trovano nell'Unione.
L'art. 113 dell'IA Act prevede scadenze cadenzate annualmente, che introducono nuovi obblighi per fornitori, sviluppatori e utilizzatori di IA, ovvero, la disciplina sulle autorità di notifica e sugli organismi notificati incaricati della valutazione dei sistemi di intelligenza artificiale ad alto rischio, gli obblighi specifici per i fornitori di modelli di IA per finalità generali, la governance a livello dell'Unione e il sistema sanzionatorio sono entrati in vigore il 02.08.2025.
I fornitori di modelli di IA per finalità generali che sono stati immessi sul mercato prima del 02.08.2025 adottano le misure necessarie per conformarsi agli obblighi di cui al Regolamento entro il 02.08.2027. Per gli operatori dei sistemi di IA ad alto rischio, gli obblighi decorrono dal 02.08.2026.
Inoltre, dal 02.08.2027 entra in vigore l'art. 6 par. 1 dell'IA Act, riguardante le regole di classificazione per i sistemi di IA ad alto rischio, che consente alla Commissione Europea di monitorare costantemente la realtà dell'intelligenza artificiale al fine di modificare o integrare l'elenco dei sistemi di IA ad alto rischio in base a dei criteri predisposti per la loro identificazione; ed infine, entro il 02.08.2028 la Commissione Europea dovrà pubblicare una valutazione complessiva sull'efficacia e sull'impatto del Regolamento (art. 112 Valutazione e Riesame).
Per quanto concerne il regime sanzionatorio, ai sensi dell'art. 99 (Sanzioni), sono previste sanzioni amministrative pecuniarie, tenendo conto degli interessi delle PMI, comprese le start-up, e della loro sostenibilità economica, sino a:
- euro 35 MLN o, se l'autore del reato è un'impresa, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazioni delle pratiche vietate di IA di cui all'art. 5 del Regolamento,
- euro 15 MLN o, se l'autore del reato è un'impresa, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazioni degli obblighi previsti dal Regolamento diversi da quelle di cui all'art. 5 (Pratiche di IA vietate),
- euro 7,5 MLN o, se l'autore del reato è un'impresa, fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di comunicazioni di informazioni inesatte, incomplete o fuorvianti o agli organismi notificati o alle autorità nazionali competenti.
Nel caso delle PMI, comprese le start-up, ciascuna sanzione pecuniaria di cui all'art. 99,

è pari al massimo alle percentuali o all'importo di cui ai punti precedenti, se inferiore.
La Commissione può infliggere ai fornitori di modelli di IA per finalità generali sanzioni pecuniarie non superiori al 3 % del fatturato mondiale annuo totale dell'esercizio precedente o a euro 15 MLN, se superiore, ove essa rilevi che il fornitore, intenzionalmente o per negligenza:
a) ha violato le pertinenti disposizioni del Regolamento,
b) non ha ottemperato a una richiesta di documento o di informazioni a norma dell'art. 91 (Potere di richiedere documentazione e informazioni) o ha fornito informazioni inesatte, incomplete o fuorvianti,
c) non ha ottemperato a una misura richiesta a norma dell'art. 93 (Potere di richiedere misure),
d) non ha messo a disposizione della Commissione l'accesso al modello di IA per finalità generali o al modello di IA per finalità generali con rischio sistemico al fine di effettuare una valutazione a norma dell'art. (Potere di effettuare valutazioni).
Il quadro normativo digitale entra in una fase concreta e operativa per le imprese, per le quali esso rappresenta l'opportunità per migliorare la governance, completa e integrata delle tecnologie, compliance, sicurezza, responsabilità e garanzie, evitando rischi tecnici ed operativi nei confronti delle autorità, e che offra un vantaggio competitivo in termini di affidabilità, trasparenza e solidità del modello digitale. E ciò anche in ragione delle normative descritte nel presente articolo, e dell'utilizzo dell'Intelligenza Artificiale e dei suoi sviluppi normativi nazionali, protezioni dei dati, ruoli e responsabilità del management, fornitori, personale e l'adozione di misure preventive e correttive aziendali.