In data 27 febbraio 2023, è stata pubblicata nella Gazzetta ufficiale dell'UE la direttiva 14 dicembre 2022, n. 2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2). Detta direttiva, entrata in vigore il 16 gennaio 2023, individua la data del 17 ottobre 2024 quale termine per il recepimento delle disposizioni nel diritto nazionale da parte degli Stati membri.

La direttiva NIS 2 sostituisce la direttiva NIS del 2016 con l'introduzione di nuovi obblighi in materia di cibersicurezza al fine di garantire un elevato livello comune di protezione contro gli attacchi informatici stante la centralità che i sistemi informatici e di rete hanno assunto nella vita odierna a seguito della rapida trasformazione digitale e dell'interconnessione della società, da cui deriva un ampliamento delle potenziali minacce informatiche.

Al riguardo è pertanto utile ricordare che la prima direttiva NIS, recepita dall'Italia con il D.lgs. 65/2018, è stata approvata con la finalità di definire le misure necessarie al conseguimento di un elevato livello di sicurezza delle reti e dei sistemi informativi attraverso la designazione di autorità competenti, la creazione di gruppi di intervento per la sicurezza informatica in caso di incidente, l'adozione di strategie nazionali per la sicurezza della rete e dei sistemi informativi, nonché la gestione degli incidenti di sicurezza informatica in coordinamento tra gli Stati dell'Unione Europea. In particolare, detta direttiva si rivolgeva agli "operatori di servizi essenziali", quali i soggetti pubblici e privati che fornivano i servizi essenziali per la società e l'economia dei settori dell'acqua potabile, dell'energia, delle infrastrutture digitali, del mercato bancario e finanziario, nonché quello sanitario e dei trasporti, e ai "fornitori di servizi digitali", ovverosia le persone giuridiche che fornivano servizi di e-commerce, cloud computing o motori di ricerca digitali.

Con la nuova NIS 2 la citata distinzione è stata superata, in quanto ritenuta obsoleta, con l'introduzione di nuove categorie, quella dei soggetti essenziali e quella dei soggetti importanti, ex articolo 3. In particolare, il paragrafo 3 precisa che, entro il 17 aprile 2025, gli Stati membri dovranno definire un elenco dei soggetti essenziali ed importanti, nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, da aggiornare periodicamente, almeno ogni due anni, o quando ritenuto opportuno, al fine di garantire uniformità di applicazione della direttiva.

Ai sensi dell'articolo 21, paragrafo 1, a detti soggetti spetta l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi legati alla sicurezza dei sistemi informatici e di rete che i medesimi utilizzano nelle loro attività o nella fornitura di servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei servizi. Nella valutazione della proporzionalità delle citate misure, è necessario considerare il grado di esposizione del soggetto ai rischi, le dimensioni del soggetto, la probabilità che si verifichino incidenti nonché la gravità e, infine, l'impatto sociale ed economico.

Il successivo paragrafo 2 individua le misure minime da adottare nell'approccio multirischio finalizzato a proteggere i sistemi informatici di rete e il loro ambiente fisico da incidenti.

Quanto agli obblighi di segnalazione di cui all'articolo 23, gli eventuali incidenti significativi dovranno essere notificati senza indebito ritardo al Team di risposta agli incidenti di sicurezza informatica (CSIRT), istituito ai sensi dell'articolo 10 della nuova direttiva NIS 2. Al riguardo si sottolinea che un incidente è considerato significativo se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziariarie per il soggetto interessato; nonché se si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Si sottolinea, inoltre, che le differenze tra i soggetti essenziali e i soggetti importanti si rivelano con riferimento alle misure di vigilanza e delle sanzioni, che per i soggetti importanti sono più lievi.

Tra le principali novità, si evidenzia che la NIS 2, all'articolo 2, paragrafo 2, lettera f), dispone l'applicazione della direttiva anche alle pubbliche amministrazioni:

- dell'amministrazione centrale, quale definito da uno Stato membro conformemente al diritto nazionale;

- a livello regionale, quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche.

Inoltre, ai sensi dell'articolo 2, paragrafo 5, lettera a), gli Stati membri possono prevedere l'applicazione della direttiva agli enti della pubblica amministrazione a livello locale.

Sono esclusi dall'applicazione della direttiva gli enti della pubblica amministrazione che, invece, svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.