FORUM DI AMMINISTRAZIONE IN CAMMINO

Rivista elettronica di diritto pubblico, diritto amministrativo, diritto dell'economia e scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"

Direttori Prof. Giuseppe Di Gaspare - Prof. Bernardo Giorgio Mattarella - Prof. Aristide Police

# La Direttiva NIS2 e le strutture sanitarie private: brevi note sui profili applicativi

di Marco Santangeli*

28 luglio 2026

Abstract: Le recenti evoluzioni normative hanno determinato una forte accelerazione verso il riconoscimento dell'importanza della tutela dei sistemi informatici da eventuali attacchi cibernetici. Fin dal d.lgs. 18 maggio 2018, n. 65, che ha attuato la Dir. UE 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS1), passando per i d.l. 21 settembre 2019, n. 105 e 14 giugno 2021, n. 82, che hanno istituito, rispettivamente, il Perimetro di sicurezza nazionale cibernetica e l'Agenzia per la cybersicurezza nazionale, il tema della *cybersecurity* ha acquisito enorme peso all'interno delle regole di *governance* di importanti realtà aziendali. Da ultimo, il d.lgs. 4 settembre 2024, n. 138, di recepimento della Dir. UE 2022/2555 (c.d. Direttiva NIS2), ha individuato un nuovo paradigma della materia "cybersicurezza", che ha, ad oggi, autonoma rilevanza rispetto ad altri settori di intervento aziendale. Il presente contributo mira, in particolare, a evidenziare alcuni profili applicativi della normativa richiamata, soprattutto avendo riguardo ad uno specifico settore, quello delle strutture sanitarie private, le quali intervengono in un ambito che la stessa Direttiva NIS2 qualifica come "ad alta criticità".

The on-going legislative development has significantly accelerated the importance of protecting IT systems against cyber threats. Since the entry into force of the Legislative Decree 18th May 2018, no. 65, which implemented Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS 1 Directive), and continuing with Decree-Law 21th September 2019, no. 105 and Decree-Law 14th June 2021, no. 82, which established the National Cybersecurity Perimeter and the National Cybersecurity Agency, cybersecurity has assumed an increasingly central role within the corporate governance frameworks. Most recently, Legislative Decree 4th September 2024, no. 138, implementing Directive (EU) 2022/2555 (the so-called NIS2 Directive), has introduced a new regulatory pattern for cybersecurity, which has now acquired autonomous relevance. This article aims to examine several practical issues regarding the aforementioned regulatory framework, especially for those concerning the private healthcare sector, which operates in an area expressly classified as one of "high criticality".



## 1. Premessa: la cybersicurezza nazionale e il settore sanitario

"*Nel periodo compreso tra il 2023 e il 2024, si è osservato un notevole incremento nella frequenza degli eventi cyber, documentati in un totale di 84 casi. L'analisi del numero*

* Avvocato, Dottore di ricerca in Law and Business. Articolo **non** sottoposto a *double-blind peer review* ai fini della pubblicazione quale articolo di Fascia A.

*di eventi cyber registrati nel 2024 rivela un aumento del 111% rispetto all'anno precedente* (…). *Nel periodo da gennaio a dicembre 2025 il numero complessivo degli eventi cyber è aumentato di circa il 47,4% rispetto al 2024* (…). *Il settore sanitario ha registrato principalmente minacce riconducibili a esposizione dati (divulgazione non autorizzata di dati personali), accessi non autorizzati tramite l'utilizzo di credenziali valide, compromissione da malware, con una significativa incidenza di attacchi ransomware. Quest'ultima tipologia si conferma tra le più rilevanti in termini di impatto, per la capacità di compromettere la disponibilità dei sistemi informativi e di incidere in maniera significativa sulla continuità operativa delle strutture sanitarie*".

Con queste parole, l'Agenzia per la cybersicurezza nazionale (ACN) ha riassunto, in una relazione dal titolo "*La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni gennaio 2023 – dicembre 2025*", l'impatto che gli eventi di compromissione dei sistemi informatici[1] hanno avuto sulle strutture sanitarie, evidenziando la necessità di implementazione di fondamentali pratiche di sicurezza cibernetica[2].

Come evidente, l'ACN ha inteso rimarcare, da un lato, l'esposizione delle strutture sanitarie a sempre più frequenti attacchi informatici, tenuto conto della sensibilità dell'attività svolta da tali soggetti; dall'altro, ha sottolineato come l'assenza di misure di sicurezza[3], al di là degli effetti strettamente giuridici che si vedranno nel paragrafo successivo, potrebbe determinare un blocco di alcuni (o di tutti) i servizi essenziali per il funzionamento delle strutture stesse[4].

Si tratta, dunque, di un settore estremamente delicato, nel quale la necessaria *compliance* alle norme deve essere accompagnata da una rimodulazione reale ed effettiva delle esistenti procedure aziendali, tale da ricomprendere anche il rischio cibernetico.

---

[1] Sul punto si rimanda a N. MICHIELI, *Cybersecurity e gestione del rischio ICT: l'impatto sulla Corporate Governance*, in *BIS*, 2024, 2, p. 243 e ss.

[2] Già evidenziata, in generale, da altri studi in materia: dal Rapporto *Cyber index PMI* 2024, promosso da Generali e Confindustria, con il supporto scientifico degli Osservatori *Digital Innovation* della School of Management del Politecnico di Milano e in *partnership* istituzionale con l'ACN, emerge che (nel 2023) l'incremento degli incidenti cyber in Italia è aumentato in misura maggiore rispetto a quello globale (+65% rispetto al +12%). A conferma di ciò si possono confrontare i dati reperibili nel sito dell'Agenzia per la cybersicurezza nazionale (www.acn.gov.it) che espongono numeri, su base mensile, che, pur non tenendo conto di quelli non palesati o non rilevati, evidenziano l'assoluta rilevanza del fenomeno, come esposto nella Relazione annuale al Parlamento 2024 dell'ACN (p. 28 e ss.).

[3] O, come precisato dalla medesima ACN, l'"*adozione di cattive pratiche*" (Relazione "*La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni gennaio 2023 – dicembre 2025*" – anno 2025, p. 21).

[4] Sono stati mappati, nell'ordine: esfiltrazioni di dati (riservatezza), non sempre ai fini di riscatto; modifiche ai dati (e quindi perdita dell'integrità, con conseguente impossibilità per gli operatori sanitari di utilizzare alcuni macchinari); cancellazioni di file (disponibilità). In particolare, gli impatti rilevati sono stati: blocco temporaneo dell'erogazione di almeno un servizio, nella maggioranza dei casi; blocco di tutti i servizi IT; modifiche arbitrarie dei dati effettuate dagli attaccanti (violazione dell'integrità dei dati).

Tutto ciò, sulla scorta di quanto già da tempo avviene, ad esempio, in materia di responsabilità da reato degli enti *ex* d.lgs. n. 231/2001, sicurezza sul lavoro (d.lgs. 81/2008), trattamento dei dati personali (GDPR Regolamento UE 2016/679).
In particolare, in tale ultimo ambito, è espressamente codificato il principio del *by design*, che demanda agli amministratori delle società la predisposizione di un modello che persegua una specifica tutela dei dati personali - nel rispetto di determinati presidi - in qualsiasi sistema, servizio, prodotto o processo che comporti un trattamento dei dati personali.
Come recentemente osservato, «*per tutti i soggetti, e in particolare per le società, gli aspetti puramente tecnici-informatici (...) dovranno essere implementati anche in termini di governance, quindi di assetti organizzativi. Questo al fine di consentire la gestione del cyber risk a tutela dei dati personali, dei segreti industriali ma anche della continuità aziendale e quindi dell'operatività della società*»[5].

**2. Le norme sulla cybersicurezza e le strutture sanitarie private**

Nel corso degli ultimi anni il legislatore nazionale è intervenuto più volte sul tema della cybersicurezza[6], delineando un quadro uniforme di norme volto alla creazione e relativa stabilizzazione di un sistema nazionale di tutela dagli attacchi informatici o cibernetici.
Al di là delle singole discipline di settore[7], ciò che più interessa ai fini del presente contributo sono le disposizioni contenute nel decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (c.d. Direttiva NIS2)[8], nonché nella più recente legge 28 giugno 2024, n. 90, rubricata "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"[9].

---

[5] I. DEMURO, *La Governance della Cybersecurity secondo la Direttiva NIS*, in *Le Società*, 8-9, 2025, p. 883.
[6] L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 2022, p. 65 e ss.
[7] Sulle quali è opportuno richiamare, per un approfondimento: A. CONTALDO - D. MULA (a cura di), *Cybersecurity Law*, Pacini giuridica, Pisa, 2020; E.C. RAFFIOTTA, *Cybersecurity regulation in the European Union and the issues of Constitutional Law*, in *Rivista AIC*, 4, 2022, p. 1 e ss.; S. ROSSA, *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica, Napoli, 2023, p. 65 e ss.; R. URSI (a cura di), *La sicurezza nel cyberspazio*, Franco Angeli, Milano, 2023; E. BUOSO, *Potere amministrativo e sicurezza nazionale cibernetica*, Giappichelli, Torino, 2023, p. 87 e ss.; M. MATASSA, *Una strategia nazionale a difesa del cyberspazio*, in *P.A. Persona e amministrazione*, 2, 2022, p. 625 e ss.; E. LONGO, *La disciplina della cybersecurity nell'Unione europea e in Italia*, in F. PIZZETTI - S. CALZOLAIO - A. IANNUZZI - E. LONGO - M. OROFINO (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 203 e ss.
[8] Sulla quale si rimanda a I. MACRÌ, *Cybersicurezza: le novità per il 2024*, in *Azienditalia*, 1, 2024, p. 17 e ss.
[9] Per un approfondimento, si veda L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giornale di diritto amministrativo*, 1, 2025.

FORUM DI AMMINISTRAZIONE IN CAMMINO

Rivista elettronica di diritto pubblico, diritto amministrativo, diritto dell'economia e scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"

Direttori Prof. Giuseppe Di Gaspare - Prof. Bernardo Giorgio Mattarella - Prof. Aristide Police

**2.1 L'ambito di applicazione**

Il tema posto dalla normativa richiamata è stato, *prima facie*, quello di capire se e in che misura le disposizioni in tema di cybersicurezza possano applicarsi alle strutture sanitarie private.

In tal senso, sovviene quanto previsto dal d.lgs. 138/2024, in particolare l'articolo 3, comma 1, il quale espressamente dispone che "*nell'ambito di applicazione del presente decreto rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV* (…) *che sono sottoposti alla giurisdizione nazionale*"; poi, ulteriormente precisa, al comma 2 del medesimo articolo, che l'applicazione del decreto è riservata ai soli "*soggetti delle tipologie di cui all'allegato I e II, che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE*".

L'analisi delle due disposizioni richiamate determina, dunque, l'ambito di applicazione del decreto in esame, dal quale si può ricavare, in via interpretativa, l'effettiva applicabilità alle strutture sanitarie private.

Da un lato, infatti, si dispone l'applicazione ai soggetti "*di cui agli allegati I, II, III e IV*" sottoposti alla "*giurisdizione nazionale*" e, nell'allegato I, rientrano pacificamente i "*prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio*"[10], ossia "*qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro*".

L'assistenza sanitaria, a sua volta, ricomprende "*i servizi prestati da professionisti sanitari a pazienti, al fine di valutare, mantenere o ristabilire il loro stato di salute, ivi compresa la prescrizione, la somministrazione e la fornitura di medicinali e dispositivi medici*" (articolo 3, lettera a), della direttiva 2011/24/UE.

[10] Oltre a: laboratori di riferimento dell'UE ai sensi dell'articolo 15 del regolamento 2022/2371/UE del Parlamento europeo e del Consiglio relativo alle gravi minacce per la salute a carattere transfrontaliero ("*la Commissione può, mediante atti di esecuzione, designare laboratori di riferimento dell'UE per fornire supporto ai laboratori di riferimento nazionali al fine di promuovere le buone pratiche e l'allineamento da parte degli Stati membri su base volontaria in materia di diagnosi, metodi di analisi, utilizzo di determinati test per la sorveglianza uniforme, la notifica e la segnalazione delle malattie da parte degli Stati membri*"); soggetti che svolgono attività di ricerca e sviluppo relative a medicinali, quali definiti dall' articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ("*qualsiasi sostanza o combinazione di sostanze presentata allo scopo di curare o prevenire le malattie negli esseri umani; è considerato medicinale anche qualsiasi sostanza o associazione di sostanze che può essere somministrata all'uomo allo scopo di stabilire una diagnosi medica o di ripristinare, correggere o modificare funzioni fisiologiche dell'uomo*"); soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21 della NACE; soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica di cui all'"*elenco dei dispositivi critici per l'emergenza di sanità pubblica*" *ex* articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio sul rafforzamento del ruolo dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici.

Ovviamente, la norma deve essere interpretata nel senso di ricomprendere, fra i prestatori di assistenza sanitaria, i soggetti (imprese) che prestino tali servizi di assistenza per il tramite di professionisti sanitari, quale che sia il rapporto giuridico (di lavoro dipendente, di lavoro autonomo o di collaborazione) intercorrente.
Sotto altro aspetto, l'inclusione nell'allegato I dei prestatori di assistenza sanitaria non è sufficiente a determinare l'automatica applicazione del d.lgs. 138/2024 a tali soggetti, dovendosi, altresì, verificare che essi siano comunque sottoposti alla giurisdizione nazionale e se superino i massimali per le piccole imprese, ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.
Tale ultima disposizione prevede che, nella categoria delle PMI, si possa definire piccola impresa "*un'impresa che occup*[i] *meno di 50 persone e realizz*[i] *un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di Euro*".
Ne consegue che l'applicazione del decreto cybersicurezza alle strutture sanitarie private dipende, sostanzialmente, dalla dimensione organizzativa delle stesse: solo le strutture che abbiano più di 50 dipendenti e realizzino un fatturato annuo di più di dieci milioni di euro sono soggette alle disposizioni del decreto *de qua*.
Inoltre, la stessa normativa in esame sottolinea (articolo 3, comma 4) che "*per determinare se un soggetto è da considerarsi una media o grande impresa* (…) *si applica l'articolo 6, paragrafo 2, del medesimo allegato* [allegato della raccomandazione 2003/361/CE]*, salvo che ciò non sia proporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce*",
In altre parole, il calcolo dei parametri per stabilire la riconducibilità di una organizzazione alla categoria delle medie e grandi imprese nel contesto dei gruppi di imprese (imprese collegate e/o associate) prevede, di norma, una forma di consolidamento. La clausola di salvaguardia inserita nel predetto articolo consente, proprio, di disapplicare questa forma di consolidamento, causando un potenziale declassamento dell'organizzazione, con conseguenti potenziali impatti sull'applicabilità del d.lgs. 138/2024.
Per quanto concerne, invece, il parallelo criterio della sottoposizione alla "*giurisdizione nazionale*", il decreto cybersicurezza prevede, in generale, che sia sufficiente l'essere "*stabiliti*" sul territorio nazionale (articolo 5, comma 1). Pertanto, rientrano nell'ambito di applicazione del decreto anche le organizzazioni di diritto di altri Stati membri che sono stabilite in Italia. Inoltre, qualora una organizzazione sia stabilita in più Stati membri, è possibile che sia soggetta alla giurisdizione di più Stati membri.
Come precisato dall'ACN[11], con riferimento ai gruppi di imprese multi-nazionali stabiliti anche in Italia (ovvero gruppi europei con filiali in Italia o gruppi italiani con

[11] Determinazione ACN 19 dicembre 2025, n. 379887.

filiali all'estero), salvo specifiche eccezioni, il decreto cybersicurezza si applica solo alle persone giuridiche del gruppo (*legal entities*/filiali) stabilite in Italia: anzi, alle singole filiali, senza che sia possibile ottemperare alle disposizioni del d.lgs. 138/2024 mediante il gruppo (anche solo quello stabilito sul territorio italiano).
Peraltro, è interessante evidenziare che sempre il d.lgs. 138/2024 ha individuato una ulteriore distinzione interna in merito ai soggetti rientranti nel campo di applicazione: quella tra soggetti essenziali e soggetti importanti[12], con lo scopo di graduare, secondo il principio di proporzionalità, gli obblighi applicabili.
In tal senso, l'articolo 6, comma 1, dispone che "*i soggetti di cui all'allegato I che superano i massimali per le medie imprese*[13] *di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE*" siano considerati soggetti "*essenziali*", restando ovviamente qualificati come "*soggetti importanti*" quelli che, pur rientrando nell'allegato I, non abbiano caratteristiche organizzative tali da farli rientrare nella nozione di grande impresa.
In conclusione, l'applicazione delle disposizioni del decreto è riservata alle strutture sanitarie private che siano almeno medie imprese (dipendenti tra 50 e 249 unità; fatturato tra 10 e 50 milioni di euro) e, nel caso in cui si superino tali criteri, le strutture - ferma l'ovvia applicabilità del decreto - vengono qualificate ulteriormente come "soggetti importanti", con aggravio degli obblighi normativi in materia di cybersicurezza.
È interessante notare che l'applicazione delle norme sulla cybersicurezza, come visto, non è stata ancorata ad una distinzione tra strutture sanitarie private autorizzate o autorizzate e accreditate, come avvenuto per altre normative di settore.
Basti pensare, a tal proposito, a quanto avvenuto in tema di responsabilità da reato degli enti *ex* d.lgs. n. 231/2001.
In questa chiave di analisi, giova ricordare che, sin dal 2004[14], la regione Lombardia ha mutuato i contenuti del d.lgs. n. 231/2001, prevedendone inizialmente l'applicazione in via sperimentale per una serie di ASL e Aziende ospedaliere pubbliche, estendendola successivamente a tutte le altre aziende operanti sul territorio regionale, anche private accreditate.
Simili iniziative sono state adottate anche da altre regioni quali, ad esempio, la Calabria con l'art. 54, co. 1, legge n. 15/2008, che ha comportato l'adozione del Modello 231 da

[12] La stessa direttiva NIS2 effettua una prima distinzione fra soggetti essenziali e soggetti importanti, introducendo una gradazione che non compariva nella precedente direttiva. In particolare, si stabilisce che le Pubbliche Amministrazioni centrali sono soggetti essenziali (art. 3, par. 1, lett. d, Dir. 2022/2555). I soggetti importanti sono definiti per esclusione. La direttiva, infatti, stabilisce che sono soggetti importanti quelli elencati negli allegati I e II, che non sono considerati soggetti essenziali (art. 3, par. 2).
[13] Imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di Euro oppure il cui totale di bilancio annuo non supera i 43 milioni di Euro.
[14] DGR n. VII/17864 del 11 giugno 2004.

parte di numerose aziende operanti nel settore sanitario e che agiscono, per l'appunto, in regime di accreditamento.

L'Abruzzo, con la Legge regionale del 27 maggio 2011 n. 15, in tema di "*Adozione dei modelli di organizzazione e di gestione ai sensi dell'articolo 6 del Decreto legislativo 8 giugno 2001 n. 231*", ha imposto l'obbligo di adozione di Modelli 231 da parte delle strutture private accreditate e di tutti gli enti "*dipendenti e strumentali della Regione, con o senza personalità giuridica, ai consorzi, alle agenzie ed alle aziende regionali, nonché alle società controllate e partecipate dalla Regione ad esclusione degli enti pubblici non economici, nel rispetto dell'autonomia statutaria di cui alla disciplina civilistica in materia*".

Successivamente, si sono mosse in tale direzione la Sicilia con il Decreto assessorato sanità n. 1179/2011 ed il Lazio con decreto del Commissario *ad acta* n. U00183/2013 (poi confermato dai successivi decreti e, da ultimo, dalla deliberazione della Giunta regionale 12 giugno 2025, n. 440).

Quest'ultimo, concernente l'"*approvazione schema tipo di contratto/accordo per la definizione dei rapporti giuridici ed economici tra le Aziende Sanitarie Locali e i soggetti erogatori di prestazioni sanitarie a carico del Servizio Sanitario Regionale*" - nell'indicare i requisiti minimi per la stipula dell'accordo contrattuale con la Regione - prescrive che la ASL è tenuta ad acquisire "*dichiarazione attestante l'avvenuta adozione del Modello Organizzativo di cui al D.lgs. n. 231/2001 in materia di prevenzione dei reati*".

Come evidente, l'applicazione della normativa 231 è stata riservata alle sole strutture private accreditate, ossia a quelle strutture che possono erogare prestazioni per conto (e a carico, una volta sottoscritto l'accordo contrattuale) del Servizio sanitario nazionale.

Parimenti è avvenuto in materia di anticorruzione e trasparenza, settore nel quale, ad esempio, le norme in materia di obblighi di pubblicazione di cui al decreto legislativo 14 marzo 2013, n. 33, si applicano alle sole strutture private "*che erogano prestazioni per conto del servizio sanitario*" (articolo 41) e, comunque, limitatamente alle "*attività di pubblico interesse*" (*rectius*, le attività accreditate).

Il d.lgs. 138/2024, invece, adottando un approccio basato sulla dimensione organizzativa dei soggetti coinvolti nella normativa c.d. NIS2, ha inteso correttamente includere anche le strutture sanitarie private autorizzate, le quali, in ogni caso, pongono in essere attività assistenziale che comporta l'utilizzo di sistemi informatici, con il rischio che l'eventuale violazione di tali sistemi si riverberi sia sulla funzionalità aziendale, sia sui fondamentali diritti vantati da terzi (soprattutto in materia di trattamento dei dati personali).

Ciò, tuttavia, porrà un problema di *governance* per tutte le strutture sanitarie autorizzate (soprattutto se appartenenti a gruppi societari che posseggono anche strutture accreditate) che, non avendo avuto necessità di tracciare *ex lege* autonome procedure organizzative, si troveranno a dover implementare una specifica procedura di gestione

del rischio informatico, senza poter far ricorso, in via analogica, all'applicazione di *compliance rules* di gruppo (come avviene, ad esempio, in materia GDPR, con la possibilità di nomina di un unico responsabile della protezione dei dati - DPO).

**2.2 L'obbligo di registrazione e il punto di contatto**

Il decreto cybersicurezza prevede, in un'ottica proattiva, che l'eventuale inclusione tra i soggetti sottoposti alla normativa NIS2 sia demandata ad un'attività posta in essere dai soggetti stessi.

Nel caso in cui si rientri nell'ambito di applicazione appena esaminato, l'impresa sanitaria privata deve, a norma dell'articolo 7 del d.lgs. 138/2024[15], dal 1° gennaio al 28 febbraio di ogni anno successivo alla data di entrata in vigore del medesimo decreto, registrare o aggiornare la propria registrazione sulla piattaforma digitale resa disponibile dall'ACN, al fine di consentire alla stessa Autorità di redigere l'"*elenco dei soggetti essenziali e dei soggetti importanti*".

Da un punto di vista "pratico", l'impresa sanitaria privata (al pari di quelle di altri settori), prima di procedere alla registrazione, deve svolgere una autovalutazione circa la riconducibilità all'ambito di applicazione del decreto cybersicurezza, secondo un processo delineato dall'ACN[16].

Inoltre, è opportuno ribadire che gli adempimenti previsti dal d.lgs. 138/2024 sono relativi alle singole persone giuridiche. Pertanto, l'obbligo di registrazione deve essere assolto da ogni persona giuridica distintamente, anche se parte di un medesimo gruppo societario.

Il medesimo articolo 7 del d.lgs. 138/2024 prevede, poi, "*la designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono*".

Ai sensi dell'articolo 4, comma 2, della determinazione ACN 19 dicembre 2025, n. 379887, le funzioni di punto di contatto possono essere svolte dal rappresentante legale o da un suo procuratore generale (censito sul registro delle imprese) oppure da un dipendente delegato del soggetto. Come precisato - di recente - dalla determinazione ACN 13 aprile 2026, n. 127437, il punto di contatto è una "*persona fisica designata dal*

[15] Le disposizioni in esame sono state ulteriormente disciplinate dalle seguenti determinazioni ACN: 26 novembre 2024, n. 38565, 10 aprile 2025, n. 136117, 22 luglio 2025, n. 283727, 19 settembre 2025, n. 333017, 19 dicembre 2025, n. 379887 e 13 aprile 2026, n. 127437.

[16] Anzitutto, l'organizzazione deve procedere alla determinazione dell'applicabilità della giurisdizione nazionale. In secondo luogo, il processo prevede la determinazione della riconducibilità dell'organizzazione alle categorie delle medie e grandi imprese (ai sensi della Raccomandazione 2003/361/CE), che rientrano nell'ambito di applicazione qualora svolgano attività o eroghino servizi riconducibili alle tipologie di soggetto di cui agli allegati I e II. In caso affermativo, anche per una sola tipologia di soggetto, anche qualora l'attività o il servizio siano svolti in forma residuale (fatta eccezione per i settori "Acqua potabile", "Acque reflue" e "Gestione rifiuti"), è necessario procedere alla registrazione.

*soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso*".

Il punto di contatto, dunque, non ha la responsabilità degli adempimenti di cui al decreto in esame, ma ne cura l'attuazione , tenuto conto che la responsabilità delle violazioni è posta in capo ai vertici aziendali (organi di amministrazione e direttivi), ovvero i componenti del Consiglio di amministrazione (CDA e/o assimilabili), richiamati, poi, all'articolo 38 relativo alle sanzioni.

In ogni caso, i soggetti che fanno parte di un gruppo di imprese possono designare quale punto di contatto il dipendente di un'altra impresa che rientra nell'ambito di applicazione del decreto cybersicurezza e che fa parte del medesimo gruppo di imprese.

Sotto tale aspetto - tenendo presente che le norme sulle cybersicurezza si applicano alle singole *legal entities* - va però precisato che qualora il punto di contatto abbia l'esigenza di associarsi a più organizzazioni, dovrà ripetere la procedura di associazione per ciascuna delle organizzazioni per le quali svolgerà le funzioni di punto di contatto. Dal punto di vista operativo, come evidenziato dall'ACN[17], è, quindi, necessario completare una prima volta la procedura ordinaria di censimento dell'utente e associazione alla prima organizzazione (generalmente, quella della quale si è dipendenti).

### 2.3 Gli organi di amministrazione e direttivi

Il d.lgs. 138/2024 pone grande enfasi sul ruolo svolto dagli organi di amministrazione e direttivi[18], tenuto conto della rilevanza della normativa cybersicurezza che, come visto, riguarda tutte le strutture sanitarie private, non esclusivamente quelle accreditate.

Gli organi di amministrazione e gli organi direttivi delle strutture sanitarie private che siano soggetti NIS devono, infatti, approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, essendo, altresì, responsabili delle violazioni delle disposizioni del suddetto d.lgs. 138/2024.

Tuttavia, l'ACN[19] ha, in parte, mitigato gli effetti di tale disposizione, prevedendo che sia possibile conferire una delega per lo svolgimento delle attività finalizzate all'attuazione dei predetti obblighi (v. paragrafo precedente in merito al punto di contatto), ferma restando in capo agli organi di amministrazione e agli organi direttivi la responsabilità, in quanto trattasi di obblighi di indirizzo e pianificazione strategica che, in quanto tali, non potrebbero essere delegabili.

Inoltre, sempre l'ACN, nella *faq* pubblicate sul proprio sito istituzionale, ha ulteriormente sottolineato che "*nelle organizzazioni in cui è previsto un Consiglio di*

[17] Si vedano le *faq* NIS pubblicate sul sito www.acn.gov.it.

[18] Con la locuzione "*organi di amministrazione*" e "*organi direttivi*" ci si riferisce a quegli organi che detengono il potere di direzione dell'Organizzazione, incluso, ove presente, il Consiglio di amministrazione dell'organizzazione (*cfr*. articolo 1, comma 1, lettera e) della Determinazione ACN 19 dicembre 2025, n. 379887).

[19] Determinazione ACN 19 dicembre 2025, n. 379887.

*amministrazione è necessario elencare tutti i membri quali componenti degli organi di amministrazione e direttivi. Nelle organizzazioni in cui il CDA è monocratico, è necessario indicare la persona fisica che ricopre tale ruolo. Nelle organizzazioni in cui non è previsto un CDA, è necessario individuare l'organo che svolge le analoghe funzioni ed elencarne i membri quali componenti degli organi di amministrazione e direttivi*".

**2.4 Gli obblighi di cybersicurezza e le sanzioni**

L'impianto normativo individuato dal decreto cybersicurezza impone ai soggetti cui tale decreto si applica l'adozione di misure tecniche, operative e organizzative, adeguate e proporzionate, finalizzate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi.

È questo il nucleo essenziale della normativa sulla cybersicurezza che, come precisato dall'articolo 24 del citato d.lgs. 138/2024, è basato su un approccio multi-rischio, volto a "*proteggere i sistemi informativi e di rete, nonché il loro ambiente fisico da incidenti*".

Si prevede che i soggetti importanti siano tenuti ad adottare le misure di sicurezza di base riportate nell'allegato 1[20] della determinazione ACN 19 dicembre 2025, n. 379907, mentre i soggetti essenziali siano tenuti ad adottare le misure di sicurezza riportate nell'allegato 2 della medesima determina.

Inoltre, nella *faq* dell'ACN, si precisa che il termine per l'adozione delle misure di sicurezza di base si configura differentemente a seconda che il soggetto sia stato inserito nell'elenco dei soggetti NIS per la prima volta nel corso dell'anno solare 2025 o dell'anno solare 2026. In dettaglio: per i soggetti inseriti nell'elenco dei soggetti NIS nel corso dell'anno solare 2025, il termine è fissato in diciotto mesi dalla ricezione da

[20] A titolo meramente esemplificativo: i ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati. È definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità. È mantenuto un elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS. All'interno dell'organizzazione per la sicurezza informatica sono inclusi il punto di contatto e il suo sostituto, il referente CSIRT e gli eventuali suoi sostituti. I ruoli e le responsabilità di cui sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti: a) gestione del rischio; b) ruoli e responsabilità; c) affidabilità delle risorse umane; d) conformità e audit di sicurezza; e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento; f) gestione degli asset; g) gestione delle vulnerabilità; h) continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche; i) gestione dell'autenticazione, delle identità digitali e del controllo accessi; j) sicurezza fisica; k) formazione del personale e consapevolezza; l) sicurezza dei dati; m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete; n) protezione delle reti e delle comunicazioni; o) monitoraggio degli eventi di sicurezza; p) risposta agli incidenti e ripristino.

parte del soggetto della comunicazione di inserimento nell'elenco; per i soggetti inseriti nell'elenco dei soggetti NIS per la prima volta nel corso dell'anno solare 2026, il termine scade il 31 luglio 2027.
Il d.lgs. 138/2024 pone, infine, il tema dell'inosservanza delle disposizioni ivi contenute, prevedendo un sistema sanzionatorio, in particolare mediante sanzioni amministrative pecuniarie, per mancata osservanza degli obblighi imposti dall'articolo 23 agli organi di amministrazione e agli organi direttivi, nonché degli obblighi relativi alla gestione del rischio per la sicurezza informatica.
Si tratta, come disposto dall'articolo 38, comma 9, di sanzioni che raggiungono - per i soggetti essenziali - fino a un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto; e per i soggetti importanti fino a un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo.

## 3. Rilievi conclusivi

La normativa NIS2, tradotta nel nostro ordinamento con il d.lgs. 138/2024, ha avuto l'obiettivo di garantire un aumento del livello di sicurezza cibernetica comune, grazie all'armonizzazione delle norme applicabili ai diversi operatori nei diversi Stati membri e al rafforzamento dei livelli standard di sicurezza rispetto a quelli previsti dalla disciplina vigente.
Come si è avuto già modo di sottolineare, la tematica riveste particolare rilevanza in tutti quei settori che la normativa stessa individua come estremamente critici, tra i quali rientra - a pieno titolo - il settore sanitario.
Ciò si traduce in una nuova *governance* delle aziende sanitarie private, le quali devono, necessariamente, affrontare il rischio cibernetico e predisporre un sistema di gestione corretto e *compliant* con le norme analizzate.
Il tema che si pone per le strutture sanitarie private (ovviamente, per quelle di medie o grandi dimensioni) è di individuare, anche all'interno di un unico gruppo e ognuna per sé, un complesso sistema di gestione del predetto rischio cibernetico, che vada a regolare le attività di registrazione sulla piattaforma ACN; l'istituzione del punto di contatto; l'implementazione delle misure di gestione dei rischi per la sicurezza informatica; l'adempimento degli obblighi di base in materia di notifica di incidente e di sicurezza informatica.
Potrebbe essere utile, in tal senso, adottare il medesimo approccio già sviluppato con riferimento alla responsabilità da reato degli enti *ex* d.lgs. n. 231/2001, secondo il paradigma del c.d. *compliance program*, nel quale l'eventuale responsabilità dell'ente si

fonda, essenzialmente, su un *deficit* organizzativo[21] che, per quanto possibile, deve essere evitato a tutti i livelli decisionali relativi alla singola organizzazione.

Quello che la normativa sulla cybersicurezza impone, a ben vedere, è proprio una marcata differenziazione del rischio cibernetico rispetto ad altre categorie di *compliance program*, capace di riflettere la varietà degli obblighi imposti *in subiecta materia* e di innestare, *con juicio*, buone pratiche organizzative, tali da garantire la sicurezza dei sistemi informatici e, in definitiva, la piena funzionalità e tutela delle attività assistenziali svolte dalle strutture sanitarie private.

[21] Con particolare riferimento all'ampia letteratura formatasi sul tema, si vedano: A.F. TRIPODI, *''Situazione organizzativa'' e ''colpa in organizzazione'': alcune riflessioni sulle nuove specificità del diritto penale dell'economia*, in *Riv. Trim. Dir. Pen. Eco.*, 2004, p. 483 e ss.; C.E. PALIERO, C. PIERGALLINI, *La colpa di organizzazione*, in *Resp. Amm. Soc. Enti*, 2006, 3, p. 167 e ss.; D. PIVA, *Contributo all'analisi della responsabilità per la ''organizzazione difettosa'' nel diritto penale dell'impresa*, Aracne editrice, Roma, 2007; C. PIERGALLINI, *Colpa di organizzazione e impresa*, in M. DONINI - R. ORLANDI (a cura di), *Reato colposo e modelli di responsabilità*, Il Mulino, Bologna, 2013; E. VILLANI, *Alle radici del concetto di 'colpa di organizzazione' nell'illecito dell'ente da reato*, Editoriale scientifica, Napoli, 2016; C.E. PALIERO, *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale*, in *Riv. Trim. Dir. Pen. Eco.*, 2018, p. 175 e ss.; ID., voce *Colpa di organizzazione e persone giuridiche*, in *Enc. dir.*, *I tematici, Reato colposo*, diretto da M. DONINI, II, Giuffrè, Milano, 2021, p. 64 e ss.; A. SERENI, *La colpa di organizzazione nella responsabilità dell'ente da reato. Profili generali*, in D. PIVA (a cura di), *La responsabilità degli enti ex d.lgs. n. 231/2001 tra diritto e processo*, Giappichelli, Torino, 2021, p. 58 e ss.; V. MONGILLO, *La colpa di organizzazione: enigma ed essenza della responsabilità ''da reato'' dell'ente collettivo*, in *Cass. Pen.*, 2023, p. 704 e ss.