

- (6) I soggetti che intervengono nella fornitura di servizi essenziali devono sempre più spesso rispettare requisiti divergenti imposti dal diritto nazionale. Il fatto che alcuni Stati membri prevedano per tali soggetti requisiti di sicurezza meno rigorosi non solo determina diversi livelli di resilienza, ma rischia anche di incidere negativamente sul mantenimento di funzioni vitali della società o di attività economiche nell'Unione e crea altresì ostacoli al corretto funzionamento del mercato interno. Gli investitori e le imprese possono fare affidamento su soggetti critici che sono resilienti e confidare in essi, in quanto l'affidabilità e la fiducia sono pietre angolari di un mercato interno ben funzionante. Tipi di soggetti simili sono considerati critici da alcuni Stati membri ma non da altri, e quelli individuati come critici devono soddisfare requisiti divergenti nei vari Stati membri. Ciò crea oneri amministrativi supplementari e non necessari per le imprese che operano a livello transfrontaliero, in particolare per quelle attive negli Stati membri con requisiti più rigorosi. Un quadro a livello di Unione determinerebbe quindi anche la creazione di condizioni di parità per i soggetti critici in tutta l'Unione.
- (7) È necessario stabilire norme minime armonizzate per garantire la fornitura di servizi essenziali nel mercato interno, aumentare la resilienza dei soggetti critici e migliorare la cooperazione transfrontaliera tra le autorità competenti. È importante che tali norme siano adeguate alle esigenze future in termini di concezione e attuazione, consentendo al contempo la necessaria flessibilità. È altresì fondamentale migliorare la capacità dei soggetti critici di fornire servizi essenziali di fronte a una serie diversificata di rischi.
- (8) Per conseguire un livello elevato di resilienza, gli Stati membri dovrebbero individuare i soggetti critici che saranno tenuti a soddisfare specifici requisiti, che saranno oggetto di vigilanza e che riceveranno anche particolare sostegno e orientamento rispetto a tutti i rischi rilevanti.
- (9) Data l'importanza della cibersicurezza per la resilienza dei soggetti critici e a fini di congruenza, dovrebbe essere assicurato, ogniqualvolta possibile, un approccio coerente fra la presente direttiva e la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio<sup>(9)</sup>. Alla luce della maggiore frequenza e delle particolari caratteristiche dei rischi informatici, la direttiva (UE) 2022/2555 impone a un'ampia gamma di soggetti requisiti dettagliati per garantire la propria cibersicurezza. Dato che l'aspetto della cibersicurezza è trattato in modo sufficiente da tale direttiva (UE) 2022/2555, le materie da essa disciplinate dovrebbero essere escluse dall'ambito di applicazione della presente direttiva, fermo restando il particolare regime per i soggetti del settore delle infrastrutture digitali.
- (10) Qualora le disposizioni di atti giuridici settoriali dell'Unione impongano ai soggetti critici di adottare misure per rafforzare la propria resilienza o di notificare gli incidenti, e qualora tali requisiti siano riconosciuti dagli Stati membri come almeno equivalenti ai corrispondenti obblighi stabiliti dalla presente direttiva, le pertinenti disposizioni della presente direttiva non dovrebbero applicarsi, in modo da evitare duplicazioni e oneri non necessari. In tal caso dovrebbero applicarsi le pertinenti disposizioni di tali atti giuridici dell'Unione. Qualora non si applichino le pertinenti disposizioni della presente direttiva, non dovrebbero applicarsi nemmeno le disposizioni di cui alla presente direttiva in materia di vigilanza ed esecuzione.
- (11) La presente direttiva non incide sulle competenze degli Stati membri e delle loro autorità in termini di autonomia amministrativa né sulla loro responsabilità di salvaguardare la sicurezza nazionale e la difesa o il loro potere di salvaguardare altre funzioni essenziali dello Stato, in particolare per quanto riguarda la pubblica sicurezza, l'integrità territoriale e il mantenimento dell'ordine pubblico. L'esclusione degli enti della pubblica amministrazione dall'ambito di applicazione della presente direttiva dovrebbe applicarsi a enti le cui attività sono svolte principalmente nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati. Tuttavia gli enti della pubblica amministrazione le cui attività sono connesse solo marginalmente a tali settori dovrebbero continuare a rientrare nell'ambito di applicazione della presente direttiva. Ai fini della presente direttiva, i soggetti con competenze normative non sono considerati quali operanti nel settore dell'attività di contrasto e non sono pertanto esclusi per tali motivi dall'ambito di applicazione della presente direttiva. Gli enti della pubblica amministrazione istituiti congiuntamente con un paese terzo in virtù di un accordo internazionale sono esclusi dall'ambito di applicazione della presente direttiva. La presente direttiva non si applica alle missioni diplomatiche e consolari degli Stati membri nei paesi terzi.

<sup>(9)</sup> 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, che modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (cfr. pagina 80 della presente Gazzetta ufficiale).

