Consiglio
dell'Unione europea

Bruxelles, 26 novembre 2021
(OR. en)

14337/21

Fascicolo interistituzionale:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTA

Origine:	Segretariato generale del Consiglio
Destinatario:	Consiglio
n. doc. prec.:	9583/2/21, 11724/21
n. doc. Comm.:	14150/20
Oggetto:	Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 *- Orientamento generale*

I. INTRODUZIONE

1. Il 16 dicembre 2020 la Commissione ha adottato la proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS riveduta o "NIS 2")[1] con l'obiettivo di sostituire l'attuale direttiva sulla sicurezza delle reti e dei sistemi informativi ("direttiva NIS")[2].

[1] Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148.

[2] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

La proposta figurava tra le azioni previste nella strategia dell'UE in materia di cibersicurezza per il decennio digitale[3], che mira a garantire che tutti i cittadini e le imprese possano beneficiare di tecnologie digitali affidabili.

2. L'obiettivo della proposta, basata sull'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), è quello di migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso.

3. Al Parlamento europeo, la commissione competente per la proposta è la commissione per l'industria, la ricerca e l'energia (ITRE). La commissione ITRE ha adottato la relazione del relatore il 28 ottobre 2021.

4. Il Comitato economico e sociale europeo ha adottato il suo parere il 28 aprile 2021.

5. Il 3 febbraio 2021 il Comitato dei rappresentanti permanenti ha deciso di consultare il Comitato europeo delle regioni in merito alla proposta[4]. Il Comitato europeo delle regioni non si è ancora pronunciato.

6. Il Garante europeo della protezione dei dati ha adottato un parere l'11 marzo 2021[5].

7. Nelle conclusioni[6] del 22 marzo 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, il Consiglio ha preso atto della nuova proposta che si basa sulla direttiva NIS e ha ribadito il suo sostegno al rafforzamento e all'armonizzazione dei quadri nazionali di cibersicurezza e alla cooperazione continua tra gli Stati membri.

8. Nelle sue conclusioni del 21 e 22 ottobre 2021, il Consiglio europeo ha invitato a portare avanti i lavori sulla proposta di direttiva NIS riveduta.

---

[3] Doc. 14133/20.
[4] Doc. 5573/21.
[5] Parere 5/2021 sulla strategia in materia di cibersicurezza e sulla direttiva NIS 2.0.
[6] Doc. 6722/21.

II. LAVORI NELL'AMBITO DEGLI ORGANI PREPARATORI DEL CONSIGLIO

9. In sede di Consiglio, l'esame della proposta è stato affidato al gruppo orizzontale "Questioni riguardanti il ciberspazio" (di seguito il "gruppo orizzontale"). L'esame della proposta è iniziato il 19 gennaio, durante la presidenza portoghese, con un'attenta lettura della proposta, in cui gli Stati membri hanno avuto l'opportunità di sollevare interrogativi e di evidenziare le loro principali preoccupazioni, ricevendo dalla Commissione spiegazioni dettagliate sulle modifiche contenute nella direttiva riveduta.

10. Durante la presidenza portoghese, il gruppo orizzontale ha dedicato 17 riunioni alla presentazione e alla lettura della proposta. Una relazione sullo stato di avanzamento dell'esercizio di lettura è stata presentata al Consiglio TTE del 4 giugno 2021.

11. I lavori sono proseguiti e si sono intensificati durante la presidenza slovena, con l'obiettivo di raggiungere un orientamento generale nella sessione del Consiglio "Trasporti, telecomunicazioni e energia" del 3 dicembre 2021.La presidenza slovena ha dedicato alla revisione della proposta NIS 2 15 riunioni e numerose discussioni bilaterali a tutti i livelli.

12. I lavori del gruppo orizzontale si sono concentrati sulla riformulazione del testo della proposta, in un primo momento per quanto riguarda l'interazione tra la direttiva NIS 2 e la legislazione settoriale e l'ambito di applicazione, segnatamente in ordine alla pubblica amministrazione, ai server DNS radice e alla clausola di esclusione, e successivamente, tra l'altro, per quanto riguarda le revisioni tra pari, la giurisdizione e l'assistenza reciproca, la divulgazione coordinata delle vulnerabilità, le banche dati di nomi di dominio e dati di registrazione e la cooperazione internazionale.

13. Una prima proposta di compromesso sul testo della proposta di direttiva è stata pubblicata il 21 settembre 2021[7], sulla base delle osservazioni scritte e dei documenti informali trasmessi dagli Stati membri, nonché delle precedenti proposte di compromesso sull'interazione tra la direttiva NIS 2 e la legislazione settoriale e sull'ambito di applicazione della direttiva NIS 2.

[7] Doc. 12019/21.

14. L'ultima revisione[8] della proposta di compromesso della presidenza è stata discussa a livello di gruppo il 22 novembre 2021. Sebbene in linea generale le delegazioni abbiano accolto con favore il testo di compromesso, alcune hanno espresso riserve d'esame o formulato osservazioni su parti della proposta di compromesso. Sono state proposte ulteriori riformulazioni tecniche in alcuni punti del testo.

III. SUL MERITO

15. Sulla base delle discussioni a livello di gruppo, le principali questioni politiche individuate riguardano i seguenti punti:

a) Ambito di applicazione (articolo 2)

Dall'inizio delle discussioni sulla proposta NIS 2, la principale preoccupazione espressa dagli Stati membri è stata l'aumento significativo del numero di soggetti contemplati dalla direttiva e, in particolare, l'introduzione della regola della soglia di dimensione in base alla quale tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva NIS 2 rientrano nel suo ambito di applicazione. Pur mantenendo questa regola generale, la proposta di compromesso contiene disposizioni supplementari per garantire la necessaria proporzionalità, un livello più elevato di gestione dei rischi e criteri di criticità definiti in modo chiaro per determinare i soggetti che rientrano nell'ambito di applicazione della direttiva. Inoltre, la proposta di compromesso contiene disposizioni specifiche sull'ordine di priorità nel ricorso a misure di vigilanza, secondo un approccio basato sui rischi.

[8] Doc. 12019/5/21 REV 5.

b) Pubblica amministrazione (articolo 2, paragrafo 2 bis)

L'inclusione della pubblica amministrazione nell'ambito di applicazione della direttiva NIS 2 è stato un tema molto dibattuto, dato che il settore della pubblica amministrazione è più specifico rispetto ad altri settori contemplati dalla direttiva NIS 2. La presidenza ha cercato di conseguire un approccio equilibrato che tenga conto delle specificità dei quadri nazionali della pubblica amministrazione e garantisca agli Stati membri un certo grado di flessibilità per quanto riguarda la determinazione degli enti della pubblica amministrazione che rientrano nell'ambito di applicazione della NIS 2. Pertanto, nel testo di compromesso, la direttiva NIS 2 si applica agli enti della pubblica amministrazione delle amministrazioni centrali, mentre gli Stati membri possono stabilire che la direttiva si applichi anche agli enti della pubblica amministrazione a livello regionale e locale.

c) Clausola di esclusione (articolo 2, paragrafi 3 bis e 3 bis bis)

Gli Stati membri hanno voluto chiarire ulteriormente la clausola di esclusione riguardo al fatto che la direttiva non si applica ai soggetti operanti principalmente nei settori della difesa, della sicurezza nazionale, della pubblica sicurezza o dell'attività di contrasto né alle attività concernenti la sicurezza nazionale o la difesa. Sono esclusi anche il settore della giustizia, i parlamenti e le banche centrali.

d) Interazione con la legislazione settoriale

Gli Stati membri hanno sottolineato la necessità di un allineamento tra la direttiva NIS 2 e la legislazione settoriale, in particolare il regolamento relativo alla resilienza operativa digitale per il settore finanziario (DORA) e la direttiva sulla resilienza dei soggetti critici (direttiva CER). La direttiva NIS 2, che dovrebbe costituire lo scenario di riferimento per l'armonizzazione minima in materia di cibersicurezza, contiene un articolo dedicato agli atti settoriali dell'Unione (articolo 2 ter). Per quanto riguarda l'interazione con la direttiva CER, la proposta di compromesso offre maggiore chiarezza in merito all'approccio "multirischio". Altre importanti integrazioni riguardano le modalità di cooperazione tra le autorità competenti a norma dei rispettivi atti giuridici.

e) Apprendimento tra pari (articolo 16)

Salvo alcune eccezioni, gli Stati membri si sono opposti all'istituzione da parte della Commissione di revisioni tra pari obbligatorie. La proposta di compromesso garantisce che il nuovo meccanismo di apprendimento tra pari si basi sulla fiducia reciproca e sia un processo volontario guidato dagli Stati membri.

f) Giurisdizione e territorialità (articolo 24) e assistenza reciproca (articolo 34)

Gli Stati membri hanno espresso preoccupazione per le conseguenze di una giurisdizione differenziata per i soggetti del settore delle TIC, come proposto dalla Commissione. Il testo di compromesso ha chiarito la giurisdizione sulla base del tipo di soggetto e ha rafforzato la formulazione relativa all'assistenza reciproca.

g) Obblighi di segnalazione (articolo 20)

A seguito delle preoccupazioni espresse dagli Stati membri, secondo le quali ciò comporterebbe un onere eccessivo per i soggetti contemplati dalla direttiva NIS 2 e un eccesso di segnalazioni, nel testo di compromesso è stata esclusa la segnalazione obbligatoria delle minacce informatiche significative.

IV. CONCLUSIONE

16. Il 24 novembre 2021 il Comitato dei rappresentanti permanenti ha raggiunto un accordo sul testo di compromesso che figura nell'allegato e ha deciso di presentarlo al Consiglio "Trasporti, telecomunicazioni e energia" per l'adozione di un orientamento generale.

17. Si invita pertanto il Consiglio ad approvare il testo di compromesso presentato dalla presidenza e riportato nell'allegato e ad adottare un orientamento generale nella sua sessione del 3 dicembre 2021.

ALLEGATO

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[9],

visto il parere del Comitato delle regioni[10],

deliberando secondo la procedura legislativa ordinaria,

---

[9] GU C del , pag. .
[10] GU C del , pag. .

considerando quanto segue:

(1) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[11] mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, ad attenuare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti di cibersicurezza, contribuendo in tal modo al funzionamento efficace dell'economia e della società dell'Unione.

(2) Dall'entrata in vigore della direttiva (UE) 2016/1148 sono stati compiuti progressi significativi nell'aumentare il livello di resilienza dell'Unione in materia di cibersicurezza. La revisione di tale direttiva ha mostrato quanto quest'ultima sia servita da catalizzatore per l'approccio istituzionale e normativo alla cibersicurezza nell'Unione, aprendo la strada a un significativo cambiamento della mentalità. Tale direttiva ha garantito il completamento dei quadri nazionali definendo le strategie nazionali [...] **in materia di sicurezza dei sistemi informatici e di rete**, stabilendo capacità nazionali e attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. Ha inoltre contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione[12] e **della** [...] rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente ("rete di CSIRT")[13]. Nonostante tali risultati, la revisione della direttiva (UE) 2016/1148 ha rivelato carenze intrinseche che le impediscono di affrontare efficacemente le sfide attuali ed emergenti in materia di cibersicurezza.

---

[11] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

[12] Articolo 11 della direttiva (UE) 2016/1148.

[13] Articolo 12 della direttiva (UE) 2016/1148.

(3) I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce alla cibersicurezza, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti di cibersicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete. Tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno.

(4) La base giuridica della direttiva (UE) 2016/1148 era l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Gli obblighi di cibersicurezza imposti ai soggetti che forniscono servizi o attività economicamente rilevanti variano notevolmente da uno Stato membro all'altro in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza. Tali disparità comportano costi aggiuntivi e creano difficoltà per le imprese che offrono beni o servizi transfrontalieri. Gli obblighi imposti da uno Stato membro che sono diversi o addirittura in conflitto con quelli imposti da un altro Stato membro possono incidere in modo sostanziale su tali attività transfrontaliere.

Inoltre è probabile che una progettazione o attuazione non ottimale delle **misure** [...] di cibersicurezza in uno Stato membro abbia ripercussioni sul livello di cibersicurezza di altri Stati membri, in particolare in considerazione degli intensi scambi transfrontalieri. Il riesame della direttiva (UE) 2016/1148 ha evidenziato notevoli divergenze nella sua attuazione da parte degli Stati membri, anche per quanto riguarda il suo ambito di applicazione, la cui delimitazione è stata lasciata in larga misura alla discrezione degli Stati membri. La direttiva (UE) 2016/1148 ha inoltre conferito agli Stati membri un ampio potere discrezionale per quanto riguarda l'attuazione degli obblighi in materia di sicurezza e segnalazione degli incidenti ivi stabiliti. Tali obblighi sono stati pertanto attuati in modi significativamente diversi a livello nazionale. Analoghe divergenze nell'attuazione si sono verificate in relazione alle disposizioni di tale direttiva in materia di vigilanza e esecuzione.

(5) Tutte queste divergenze comportano una frammentazione del mercato interno e possono avere un effetto pregiudizievole sul suo funzionamento, con ripercussioni in particolare sulla fornitura transfrontaliera di servizi e sul livello di resilienza della cibersicurezza dovute all'applicazione di [...] **misure** diverse. La presente direttiva mira a eliminare tali ampie divergenze tra gli Stati membri, in particolare stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili in ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e prevedendo mezzi di ricorso e sanzioni effettivi che siano funzionali all'efficace esecuzione di tali obblighi. La direttiva (UE) 2016/1148 dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(6) [...] Gli Stati membri [...] **dovrebbero essere in grado** di adottare le misure necessarie a garantire la tutela degli interessi essenziali della loro sicurezza, a salvaguardare l'ordine pubblico e la pubblica sicurezza e a consentire l'indagine, l'accertamento e il perseguimento dei reati [...]. [...] **La direttiva non dovrebbe applicarsi a taluni soggetti pubblici o privati che svolgono attività in tali settori. Non dovrebbe applicarsi neppure alle attività di soggetti svolte in tali settori. Inoltre**, nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza. [...] **S**ono pertinenti le norme nazionali **o** [...] dell'Unione per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP[14].

(6 bis) A qualsiasi trattamento di dati personali ai sensi della presente direttiva si applica il diritto dell'Unione in materia di protezione dei dati personali e della vita privata. In particolare, la presente direttiva lascia impregiudicati il regolamento (UE) 2016/679 e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio e pertanto, in particolare, non dovrebbe pregiudicare i compiti e i poteri delle autorità di controllo indipendenti con competenza a monitorare la conformità al diritto dell'Unione applicabile in materia di protezione dei dati.

[14] Il protocollo TLP (Traffic Light Protocol) è uno strumento che consente a chi condivide informazioni di informare il proprio pubblico in merito a eventuali limitazioni dell'ulteriore diffusione di tali informazioni. È utilizzato in quasi tutte le comunità di CSIRT e in alcuni centri di condivisione e di analisi delle informazioni (ISAC).

(7) Con l'abrogazione della direttiva (UE) 2016/1148, l'ambito di applicazione per settore dovrebbe essere esteso a una parte più ampia dell'economia alla luce delle considerazioni di cui ai considerando da 4 a 6. I settori contemplati dalla direttiva (UE) 2016/1148 dovrebbero pertanto essere ampliati per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche nel mercato interno. Le norme non dovrebbero essere diverse a seconda che i soggetti siano operatori di servizi essenziali o fornitori di servizi digitali. Tale differenziazione si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.

(8) Conformemente alla direttiva (UE) 2016/1148, gli Stati membri erano responsabili di determinare quali soggetti soddisfacevano i criteri per essere considerati operatori di servizi essenziali ("processo di identificazione"). Al fine di eliminare le ampie divergenze tra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda gli obblighi di gestione e segnalazione dei rischi per tutti i soggetti pertinenti, è opportuno stabilire un criterio uniforme che determini quali soggetti rientrano nell'ambito di applicazione della presente direttiva. Tale criterio dovrebbe consistere nell'applicazione della regola della soglia di dimensione, in base alla quale rientrano nell'ambito di applicazione della direttiva tutte le medie e le grandi imprese, quali definite nella raccomandazione 2003/361/CE della Commissione[15], che operano nei settori o forniscono il tipo di servizi contemplati dalla presente direttiva. [...]

[15] Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

(8 bis) Al fine di garantire una panoramica chiara dei soggetti che rientrano nell'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero poter istituire meccanismi nazionali di autonotifica che impongano ai soggetti che rientrano nell'ambito di applicazione della presente direttiva di comunicare alle autorità competenti ai sensi della presente direttiva o agli organismi designati a tal fine dagli Stati membri almeno il loro nome, il loro indirizzo, i loro dati di contatto, nonché il settore in cui operano o il tipo di servizio che forniscono e, se del caso, un elenco degli Stati membri in cui prestano servizi. Gli Stati membri possono adottare decisioni in merito ai meccanismi appropriati laddove esistano registri a livello nazionale che consentono l'individuazione dei soggetti che rientrano nell'ambito di applicazione della presente direttiva.

(9) La presente direttiva dovrebbe tuttavia applicarsi anche ai [...] **micro o** piccoli [...] soggetti che soddisfano determinati criteri che indicano un ruolo chiave per le economie o le società degli Stati membri o per particolari settori o tipi di servizi. Gli Stati membri dovrebbero essere responsabili di [...] presentar**e** [...] alla Commissione **almeno le informazioni pertinenti circa il numero di soggetti individuati, il settore cui appartengono o il tipo di servizio che forniscono, nonché i criteri specifici sulla cui base sono stati individuati**. **Gli Stati membri possono altresì decidere, ove ciò sia conforme alle norme nazionali di sicurezza, di trasmettere alla Commissione i nomi di tali soggetti.**

(9 bis) Gli enti della pubblica amministrazione operanti nei settori della sicurezza nazionale, della difesa, della pubblica sicurezza, dell'attività di contrasto, nonché il settore della giustizia, i parlamenti e le banche centrali sono esclusi dall'ambito di applicazione della presente direttiva. Ai fini della presente direttiva, non si considera che i soggetti con competenza normativa operino nel settore dell'attività di contrasto; pertanto non sono esclusi per tali motivi dall'ambito di applicazione della presente direttiva. Inoltre, gli enti della pubblica amministrazione delle amministrazioni centrali istituiti congiuntamente con un paese terzo in conformità di un accordo internazionale non rientrano nell'ambito di applicazione della presente direttiva.

(9 bis bis) Gli Stati membri dovrebbero poter stabilire che i soggetti definiti, prima dell'entrata in vigore della presente direttiva, come operatori di servizi essenziali ai sensi della direttiva (UE) 2016/1148 debbano essere considerati soggetti essenziali.

(9 bis bis bis) La presente direttiva non si applica alle missioni diplomatiche e consolari degli Stati membri all'estero né alle infrastrutture TIC da esse utilizzate, nella misura in cui tali infrastrutture si trovano all'estero o sono utilizzate per utenti all'estero.

(10) La Commissione, in collaborazione con il gruppo di cooperazione, può emanare orientamenti relativi all'attuazione dei criteri applicabili alle microimprese e alle piccole imprese.

(11) [...] **I soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero essere classificati in due categorie: essenziali e importanti, tenendo conto del livello di criticità del settore o del tipo di servizio che forniscono, nonché delle loro dimensioni. A tale riguardo, si dovrebbe tenere debitamente conto, se del caso, anche di tutte le valutazioni settoriali dei rischi o di tutti gli orientamenti pertinenti elaborati dalle autorità competenti.** Sia ai soggetti essenziali sia a quelli importanti dovrebbero applicarsi gli [...] obblighi di gestione e segnalazione dei rischi. I regimi sanzionatori e di vigilanza tra queste due categorie di soggetti dovrebbero essere differenziati per garantire un giusto equilibrio tra i requisiti e gli obblighi **basati sui rischi**, da un lato, e gli oneri amministrativi derivanti dalla vigilanza della conformità, dall'altro.

(12) **La direttiva stabilisce lo scenario di riferimento per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione in tutti i settori che rientrano nel suo ambito di applicazione. Al fine di evitare la frammentazione delle disposizioni in materia di cibersicurezza contenute negli atti giuridici dell'Unione, allorché ulteriori disposizioni settoriali relative alle** misure di gestione dei rischi di cibersicurezza **e agli obblighi di segnalazione siano ritenuti necessari per garantire un elevato livello di cibersicurezza, la Commissione dovrebbe valutare se tali disposizioni possano essere stabilite in un atto di esecuzione nell'ambito del conferimento di potere previsto dalla presente direttiva. Qualora tali atti non siano adeguati a detto scopo,** la legislazione **settoriale potrebbe** contribuire a garantire **un livello elevato**[...] di cibersicurezza, tenendo pienamente conto delle specificità e delle complessità [...]**dei** settori **interessati**. **Il ragionamento in base al quale un atto di esecuzione in virtù del conferimento di potere previsto dalla presente direttiva non è stato ritenuto adeguato dovrebbe essere illustrato nella legislazione settoriale. Nel contempo, tali disposizioni settoriali di atti giuridici dell'Unione dovrebbero tenere debitamente conto della necessità di un quadro di cibersicurezza globale e armonizzato.** [...] **Ciò** lascia impregiudicate le competenze di esecuzione esistenti conferite alla Commissione in una serie di settori, tra cui i trasporti e l'energia.

(12 bis) Qualora un atto giuridico settoriale dell'Unione **contenga disposizioni che impongono** ai soggetti essenziali o importanti obblighi relativi all'adozione di misure di **effetto almeno equivalente agli obblighi stabiliti nella presente direttiva in relazione alla** gestione dei rischi di cibersicurezza [...] **e agli obblighi** di notifica di incidenti **significativi** o minacce informatiche significative [...], dovrebbero applicarsi tali disposizioni settoriali**, anche in materia di vigilanza ed esecuzione**. **Nel determinare l'effetto equivalente degli obblighi stabiliti nelle disposizioni settoriali di un atto giuridico dell'Unione, è opportuno considerare i seguenti aspetti: i) le misure di gestione dei rischi di cibersicurezza dovrebbero consistere in misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che i soggetti pertinenti utilizzano nella fornitura dei loro servizi e dovrebbero comprendere almeno tutti gli elementi stabiliti nella presente direttiva; ii) l'obbligo di notificare gli incidenti e le minacce informatiche significativi dovrebbe essere almeno equivalente agli obblighi stabiliti nella presente direttiva per quanto riguarda il contenuto, il formato e i tempi delle notifiche; iii) le modalità di segnalazione da parte dei soggetti e delle autorità competenti di cui agli atti giuridici settoriali dell'Unione dovrebbero essere almeno equivalenti ai requisiti stabiliti nella presente direttiva per quanto riguarda il contenuto, il formato e i tempi e dovrebbero tenere conto del ruolo dei CSIRT; iv) i requisiti in materia di cooperazione transfrontaliera per le autorità competenti dovrebbero essere almeno equivalenti a quelli stabiliti nella presente direttiva. Qualora le disposizioni settoriali di un atto giuridico dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva dovrebbero continuare ad applicarsi ai soggetti non contemplati da tali disposizioni settoriali.**

(12 bis bis) La Commissione **dovrebbe riesaminare periodicamente l'applicazione del requisito dell'effetto equivalente in relazione alle disposizioni settoriali di atti giuridici dell'Unione** [...]. **La Commissione dovrebbe consultare il gruppo di cooperazione in sede di preparazione del riesame periodico.**

(12 bis bis bis) I futuri atti giuridici settoriali dell'Unione dovrebbero tenere debitamente conto delle definizioni di cui all'articolo 4 e del quadro di vigilanza ed esecuzione di cui al capo VI della presente direttiva.

(12 bis ter) Qualora le disposizioni settoriali di atti giuridici dell'Unione impongano ai soggetti essenziali o importanti di adottare misure di effetto almeno equivalente agli obblighi di segnalazione stabiliti dalla presente direttiva, dovrebbe essere evitata la sovrapposizione degli obblighi di segnalazione e dovrebbero essere garantite la coerenza e l'efficacia della gestione delle notifiche di minacce informatiche o incidenti. A questo scopo, tali disposizioni settoriali possono consentire agli Stati membri di istituire un meccanismo di segnalazione comune, automatico e diretto per la notifica di incidenti e minacce informatiche significativi sia alle autorità i cui compiti sono stabiliti nelle rispettive disposizioni settoriali sia alle autorità competenti, compresi, se del caso, il punto di contatto unico e i CSIRT, responsabili dei compiti di cibersicurezza previsti dalla presente direttiva, o un meccanismo che garantisca la condivisione sistematica e immediata delle informazioni e la cooperazione tra le autorità competenti e i CSIRT in merito alla gestione di tali notifiche. Ai fini della semplificazione della segnalazione e dell'attuazione del meccanismo di segnalazione comune, automatico e diretto, gli Stati membri possono, conformemente alle legislazioni settoriali, utilizzare il punto di ingresso unico da essi stabilito a norma dell'articolo 11, paragrafo 5 bis, della presente direttiva. Per assicurare l'armonizzazione, gli obblighi di segnalazione degli atti giuridici settoriali dell'Unione dovrebbero essere allineati a quelli previsti dalla presente direttiva. Gli Stati membri possono stabilire che le autorità competenti ai sensi della presente direttiva o i CSIRT nazionali siano i destinatari della segnalazione, conformemente alle legislazioni settoriali.

(13) Il regolamento XXXX/XXXX del Parlamento europeo e del Consiglio dovrebbe essere considerato un atto giuridico settoriale dell'Unione in relazione alla presente direttiva per quanto riguarda i soggetti del settore finanziario. Invece delle disposizioni stabilite dalla presente direttiva dovrebbero applicarsi quelle del regolamento XXXX/XXXX relative alle misure di gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (TIC), alla gestione degli incidenti connessi alle TIC e, in particolare, alla segnalazione degli incidenti, nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e al rischio di terze parti relativo alle TIC. Gli Stati membri non dovrebbero pertanto applicare le disposizioni della presente direttiva riguardanti gli obblighi di gestione [...] e segnalazione dei rischi di cibersicurezza, [...] la vigilanza e l'esecuzione ai soggetti finanziari contemplati dal regolamento XXXX/XXXX. Al tempo stesso è importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario a norma della presente direttiva. A tal fine il regolamento XXXX/XXXX consente [...] alle autorità europee di vigilanza (AEV) per il settore finanziario e alle autorità nazionali competenti a norma del regolamento XXXX/XXXX di partecipare [...] ai lavori [...] del gruppo di cooperazione, nonché di scambiare informazioni e cooperare con i punti di contatto unici designati a norma della presente direttiva e con i CSIRT nazionali. Le autorità competenti a norma del regolamento XXXX/XXXX dovrebbero trasmettere i dettagli degli incidenti più gravi connessi alle TIC **e delle minacce informatiche significative** anche ai punti di contatto unici**, alle autorità competenti o ai CSIRT nazionali** designati a norma della presente direttiva. **Ciò può essere realizzato mediante la trasmissione automatica e diretta delle notifiche di incidenti o attraverso una piattaforma comune di segnalazione.** Gli Stati membri dovrebbero inoltre continuare a includere il settore finanziario nelle loro strategie di cibersicurezza e i CSIRT nazionali possono contemplare il settore finanziario nelle loro attività.

(13 bis) Al fine di evitare lacune e duplicazioni per quanto riguarda gli obblighi di cibersicurezza imposti ai soggetti del settore dell'aviazione di cui al punto 2, lettera a), dell'allegato I, le autorità nazionali designate a norma dei regolamenti (CE) n. 300/2008[16] e (UE) 2018/1139[17] del Parlamento europeo e del Consiglio e le autorità competenti a norma della presente direttiva dovrebbero cooperare in relazione all'attuazione delle misure di gestione dei rischi di cibersicurezza e alla vigilanza su tali misure a livello nazionale. Il rispetto, da parte di un soggetto, delle misure di gestione dei rischi di cibersicurezza di cui alla presente direttiva [...] può essere considerato dalle autorità nazionali designate ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139 equivalente al rispetto dei requisiti di cui a tali regolamenti e ai pertinenti atti delegati e di esecuzione adottati ai sensi degli stessi.

---

16 **Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).**

17 **Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).**

(14) In considerazione delle interconnessioni tra la cibersicurezza e la sicurezza fisica dei soggetti, dovrebbe essere garantito un approccio coerente tra la direttiva (UE) XXX/XXX del Parlamento europeo e del Consiglio e la presente direttiva. A tal fine, gli Stati membri dovrebbero garantire che i soggetti critici **[**e i soggetti equivalenti**]** a norma della direttiva (UE) XXX/XXX siano considerati soggetti essenziali a norma della presente direttiva. Gli Stati membri dovrebbero inoltre garantire che le loro strategie di cibersicurezza prevedano un quadro strategico per un coordinamento rafforzato tra l'autorità competente a norma della presente direttiva e quella prevista dalla direttiva (UE) XXX/XXX nel contesto della condivisione di informazioni su incidenti e minacce informatiche e dell'esercizio dei compiti di vigilanza. Le autorità **competenti** a norma di entrambe le direttive dovrebbero cooperare e scambiarsi informazioni, in particolare per quanto riguarda l'individuazione dei soggetti critici, le minacce informatiche, i rischi di cibersicurezza, gli incidenti **e i rischi, le minacce e gli incidenti non informatici** che interessano i soggetti critici **[o soggetti equivalenti ai soggetti critici]**, [...] **tra cui** le misure di cibersicurezza **e fisiche** adottate dai soggetti critici **e i risultati delle attività di vigilanza svolte riguardo a tali soggetti**. **Inoltre, al fine di razionalizzare le attività di vigilanza tra le autorità competenti designate a norma delle due direttive e di ridurre al minimo gli oneri amministrativi per i soggetti interessati, le autorità competenti dovrebbero adoperarsi per armonizzare i modelli di notifica degli incidenti e le procedure di vigilanza.** [...] **Ove opportuno, le** autorità competenti a norma della direttiva (UE) XXX/XXX [...] **possono chiedere** alle autorità competenti a norma della presente direttiva [...] di esercitare i propri poteri di vigilanza e di esecuzione [...] **in relazione a** un soggetto essenziale individuato come critico. [...]

(14 bis) I soggetti appartenenti al settore delle infrastrutture digitali sono essenzialmente basati su sistemi informatici e di rete e pertanto gli obblighi loro imposti dalla presente direttiva dovrebbero riguardare in modo globale la sicurezza fisica di tali sistemi nell'ambito dei loro obblighi di gestione e segnalazione dei rischi di cibersicurezza. Poiché tali materie sono disciplinate dalla presente direttiva, gli obblighi di cui ai capi da III a VI della direttiva (UE) XXX/XXX [CER] non si applicano a detti soggetti.

(15) Sostenere e preservare un sistema dei nomi di dominio affidabile, resiliente e sicuro è un fattore chiave per mantenere l'integrità di Internet ed è essenziale per il suo funzionamento costante e stabile, da cui dipendono l'economia e la società digitali. La presente direttiva dovrebbe applicarsi [...] **ai** fornitori di servizi DNS lungo la catena di **fornitura e** risoluzione DNS **che rivestono importanza per il mercato interno**, compresi [...] **i registri** dei nomi di dominio di primo livello (top level domain, TLD), **i soggetti che forniscono servizi di registrazione dei nomi di dominio, gli operatori** dei server autorevoli dei nomi per i nomi di dominio e **gli operatori** dei risolutori ricorsivi. **Il termine "fornitore di servizi DNS" non dovrebbe applicarsi ai servizi DNS gestiti per fini propri dal soggetto interessato e dai suoi soggetti affiliati. Gli obblighi di cibersicurezza derivanti dalla presente direttiva per questa categoria di fornitori sono strettamente limitati alle misure di gestione dei rischi di cibersicurezza e alla segnalazione e pertanto lasciano impregiudicata la governance del DNS globale da parte della comunità multipartecipativa.**

(16) I servizi di cloud computing dovrebbero comprendere i servizi che consentono, su richiesta, un ampio accesso remoto a un pool scalabile ed elastico di risorse di calcolo condivisibili e distribuite. Tali risorse di calcolo comprendono risorse quali reti, server o altre infrastrutture, sistemi operativi, software, archiviazione, applicazioni e servizi. **I modelli di servizio del cloud computing comprendono, tra gli altri, il servizio a livello di infrastruttura (IaaS), il servizio a livello di piattaforma (PaaS), il servizio a livello di software (SaaS) e il servizio a livello di rete (NaaS).** I modelli di distribuzione del cloud computing dovrebbero comprendere il cloud privato, di comunità, pubblico e ibrido. I suddetti modelli di servizio e di distribuzione hanno lo stesso significato dei termini di servizio e dei modelli di distribuzione di cui alla norma ISO/IEC 17788:2014. La capacità dell'utente di cloud computing di provvedere unilateralmente all'autofornitura di capacità di calcolo, come il tempo di utilizzo di un server o lo spazio di archiviazione in rete, senza alcuna interazione umana da parte del fornitore di servizi di cloud computing potrebbe essere descritta come "amministrazione su richiesta". L'espressione "ampio accesso remoto" (broad network access) è utilizzata per descrivere il fatto che le capacità cloud sono fornite sulla rete e accessibili attraverso meccanismi che promuovono l'uso di piattaforme client eterogenee leggere o pesanti (compresi telefoni cellulari, tablet, computer portatili e workstation).

Il termine "scalabile" si riferisce alle risorse di calcolo che sono assegnate in modo flessibile dal fornitore di servizi cloud, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione "pool elastico" è usata per descrivere quelle risorse di calcolo che sono fornite e rilasciate in base alla domanda, al fine di aumentare e diminuire rapidamente le risorse disponibili in base al carico di lavoro. Il termine "condivisibile" è usato per descrivere le risorse di calcolo che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre l'elaborazione è effettuata separatamente per ciascun utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica. Il termine "distribuito" è usato per descrivere quelle risorse di calcolo che si trovano su diversi computer o dispositivi collegati in rete e che comunicano e si coordinano tra di loro mediante il passaggio di messaggi.

(17) Dato l'emergere di tecnologie innovative e di nuovi modelli di business, si prevede che compariranno sul mercato nuovi modelli di servizio e di distribuzione del cloud computing in risposta all'evoluzione delle esigenze dei clienti. In tale contesto, i servizi di cloud computing possono essere forniti in una forma altamente distribuita, anche più vicina al luogo in cui i dati vengono generati o raccolti, passando così dal modello tradizionale a un modello altamente distribuito (edge computing).

(18) È possibile che i servizi offerti dai fornitori di servizi di data center non siano sempre forniti sotto forma di servizi di cloud computing. È pertanto possibile che i data center non facciano sempre parte dell'infrastruttura di cloud computing. Al fine di gestire tutti i rischi posti alla sicurezza dei sistemi informatici e di rete, la presente direttiva dovrebbe applicarsi anche ai fornitori di tali servizi di data center che non sono servizi di cloud computing. Ai fini della presente direttiva, il termine "servizio di data center" dovrebbe applicarsi alla fornitura di un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale. Il termine "servizio di data center" non si applica ai data center interni e aziendali posseduti e gestiti per fini propri dal soggetto interessato.

(19) I fornitori di servizi postali ai sensi della direttiva 97/67/CE del Parlamento europeo e del Consiglio[18], [...] **compresi** i fornitori di servizi di corriere [...], dovrebbero essere soggetti alla presente direttiva se provvedono ad almeno una delle fasi della catena di consegna postale, in particolare la raccolta, lo smistamento o la distribuzione, compresi i servizi di ritiro. I servizi di trasporto che non sono forniti nell'ambito di una di tali fasi dovrebbero essere esclusi dall'ambito di applicazione dei servizi postali.

---

[18] Direttiva 97/67/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e il miglioramento della qualità del servizio (GU L 15 del 21.1.1998, pag. 14).

(20) Queste crescenti interdipendenze sono il risultato di una rete di fornitura di servizi sempre più transfrontaliera e interdipendente che utilizza infrastrutture chiave in tutta l'Unione nei settori dell'energia, dei trasporti, delle infrastrutture digitali, delle acque potabili e reflue, della sanità, di determinati aspetti della pubblica amministrazione, nonché dello spazio, per quanto riguarda la fornitura di determinati servizi che dipendono da infrastrutture di terra possedute, gestite e utilizzate dagli Stati membri o da soggetti privati, ad esclusione, pertanto, delle infrastrutture possedute, gestite o utilizzate dall'Unione o per suo conto nell'ambito dei suoi programmi spaziali. Tali interdipendenze implicano che qualsiasi perturbazione, anche se inizialmente limitata a un soggetto o a un settore, possa avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata sulla fornitura di servizi in tutto il mercato interno. La pandemia di COVID-19 ha mostrato la vulnerabilità delle nostre società sempre più interdipendenti di fronte a rischi di bassa probabilità.

(20 bis) Al fine di conseguire e mantenere un livello elevato di cibersicurezza, le strategie nazionali per la cibersicurezza richieste dalla presente direttiva dovrebbero consistere in quadri coerenti che prevedano una governance nel settore della cibersicurezza. Tali strategie possono essere composte da uno o più documenti di natura legislativa o non legislativa.

(21) In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali già esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione, è opportuno che gli Stati membri abbiano la facoltà di designare più di un'autorità nazionale competente responsabile di svolgere i compiti connessi alla sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti a norma della presente direttiva. Gli Stati membri dovrebbero avere facoltà di assegnare questo ruolo a un'autorità esistente.

(22) Al fine di agevolare la cooperazione e la comunicazione transfrontaliere tra autorità e permettere che la presente direttiva sia attuata efficacemente, è necessario che ogni Stato membro designi un punto di contatto unico nazionale incaricato di coordinare le questioni relative alla sicurezza dei sistemi informatici e di rete e la cooperazione transfrontaliera a livello dell'Unione.

(23) Le autorità competenti o i CSIRT dovrebbero ricevere le notifiche di incidenti dai soggetti in modo efficace ed efficiente**, anche per agevolare, se del caso, una risposta tempestiva agli incidenti e fornire una risposta al soggetto notificante**. I punti di contatto unici dovrebbero essere incaricati di trasmettere le notifiche degli incidenti ai punti di contatto unici di altri Stati membri interessati. [...]

(23 bis) Gli atti giuridici settoriali dell'Unione che richiedono misure di gestione dei rischi di cibersicurezza o obblighi di segnalazione di effetto almeno equivalente a quelli stabiliti nella presente direttiva potrebbero prevedere che le rispettive autorità competenti designate esercitino i loro poteri di vigilanza ed esecuzione in relazione a tali misure o obblighi con l'assistenza delle autorità competenti designate ai sensi della presente direttiva. Le autorità competenti interessate potrebbero stabilire modalità di cooperazione a tale scopo. Tali modalità di cooperazione potrebbero precisare, tra l'altro, le procedure relative al coordinamento delle attività di vigilanza, tra cui le procedure di indagine e di ispezione in loco conformemente al diritto nazionale e un meccanismo per lo scambio di informazioni pertinenti tra autorità competenti in materia di vigilanza ed esecuzione, compreso l'accesso alle informazioni relative alla cibersicurezza richieste dalle autorità competenti designate ai sensi della presente direttiva.

(24) Gli Stati membri dovrebbero essere adeguatamente dotati delle capacità tecniche e organizzative necessarie a prevenire, rilevare e attenuare i rischi e gli incidenti a carico dei sistemi informatici e di rete, nonché a rispondervi. Gli Stati membri dovrebbero pertanto assicurare la disponibilità di CSIRT, anche noti come squadre di pronto intervento informatico ("CERT"), ben funzionanti e rispondenti a determinati requisiti essenziali, al fine di garantire l'esistenza di capacità efficaci e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello dell'Unione. Al fine di rafforzare il rapporto di fiducia tra i soggetti e i CSIRT, nei casi in cui un CSIRT faccia parte dell'autorità competente, gli Stati membri [...] **possono** prendere in considerazione la separazione funzionale tra i compiti operativi svolti dai CSIRT, in particolare per quanto riguarda la condivisione delle informazioni e il sostegno ai soggetti, e le attività di vigilanza delle autorità competenti.

(25) Per quanto riguarda i dati personali, i CSIRT dovrebbero essere in grado di fornire, in conformità del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[19] per quanto riguarda i dati personali, per conto e su richiesta di un soggetto a norma della presente direttiva, una scansione proattiva dei sistemi informatici e di rete utilizzati per la fornitura dei loro servizi. **Se del caso,** gli Stati membri dovrebbero mirare a garantire un pari livello di capacità tecniche per tutti i CSIRT settoriali. Gli Stati membri possono chiedere l'assistenza dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) nello sviluppo di CSIRT nazionali.

(26) Data l'importanza della cooperazione internazionale in materia di cibersicurezza, i CSIRT dovrebbero poter partecipare a reti di cooperazione internazionale, oltre alla rete di CSIRT istituita dalla presente direttiva. **Pertanto, i CSIRT e le autorità competenti potrebbero scambiare informazioni, compresi dati personali, con i CSIRT di paesi terzi o con le loro autorità al fine di assolvere i loro compiti ai sensi del regolamento (UE) 2016/679. In assenza di una decisione di adeguatezza adottata a norma dell'articolo 45 del regolamento (UE) 2016/679 o di garanzie adeguate a norma dell'articolo 46 del medesimo regolamento, lo scambio di dati personali ritenuto necessario al fine di attenuare minacce informatiche significative e rispondere a un incidente significativo in corso potrebbe essere considerato un importante motivo di interesse pubblico a norma dell'articolo 49, paragrafo 1, lettera d), del regolamento (UE) 2016/679.**

[19] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(27) Conformemente all'allegato della raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala ("programma")[20], per incidente su vasta scala si dovrebbe intendere un incidente che ha un impatto significativo su almeno due Stati membri o che causa perturbazioni che superano la capacità di risposta di uno Stato membro. A seconda della loro causa e del loro impatto, gli incidenti su vasta scala possono aggravarsi e trasformarsi in vere e proprie crisi che non consentono il corretto funzionamento del mercato interno. Data l'ampia portata e, nella maggior parte dei casi, la natura transfrontaliera di tali incidenti, gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'Unione dovrebbero cooperare a livello tecnico, operativo e politico per coordinare adeguatamente la risposta in tutta l'Unione.

(28) Poiché lo sfruttamento delle vulnerabilità nei sistemi informatici e di rete può causare perturbazioni e danni significativi, la rapida individuazione e correzione di tali vulnerabilità è un fattore importante per la riduzione dei rischi di cibersicurezza. I soggetti che sviluppano **o amministrano** tali sistemi dovrebbero pertanto stabilire procedure adeguate per gestire le vulnerabilità nel momento in cui vengono scoperte. Poiché le vulnerabilità sono spesso rilevate e segnalate (divulgate) da terzi (soggetti segnalanti), il fabbricante o fornitore di prodotti o servizi TIC dovrebbe anche mettere in atto le procedure necessarie per ricevere informazioni sulla vulnerabilità da terzi. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC [...] **29147** forniscono rispettivamente orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. Per quanto riguarda la divulgazione delle vulnerabilità, è particolarmente importante il coordinamento tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate alle organizzazioni in modo tale da consentire a queste ultime di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. La divulgazione coordinata delle vulnerabilità dovrebbe comprendere anche il coordinamento tra il soggetto segnalante e l'organizzazione per quanto riguarda i tempi per la risoluzione e la pubblicazione delle vulnerabilità.

---

[20] Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

(29) Gli Stati membri dovrebbero pertanto adottare misure volte a facilitare la divulgazione coordinata delle vulnerabilità stabilendo una politica nazionale pertinente. **Nell'ambito di tale politica nazionale, gli Stati membri dovrebbero mirare ad affrontare, nella misura del possibile, le sfide incontrate dagli esperti che cercano di individuare le vulnerabilità, compresa la loro potenziale esposizione alla responsabilità penale, conformemente al proprio ordinamento giuridico nazionale.** [...] Gli Stati membri dovrebbero designare un CSIRT che assuma il ruolo di "coordinatore", fungendo da intermediario tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC ove necessario. I compiti del CSIRT coordinatore dovrebbero comprendere in particolare l'individuazione e il contatto dei soggetti interessati, il sostegno ai soggetti segnalanti, la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più organizzazioni (divulgazione multilaterale **coordinata** di vulnerabilità). Qualora l[...]**a** vulnerabilità **segnalata possa potenzialmente avere un impatto significativo su soggetti** in più di uno Stato membro, i CSIRT designati [...] dovrebbero cooperare nell'ambito della rete di CSIRT**, se del caso**.

(30) L'accesso a informazioni corrette e tempestive sulle vulnerabilità che interessano i prodotti e i servizi TIC contribuisce a una migliore gestione dei rischi di cibersicurezza. A tale riguardo le fonti di informazioni pubblicamente disponibili sulle vulnerabilità sono uno strumento importante per i soggetti e i loro utenti, ma anche per le autorità nazionali competenti e i CSIRT. Per questo motivo l'ENISA dovrebbe istituire un registro delle vulnerabilità in cui i soggetti essenziali e importanti e i loro fornitori, nonché i soggetti che non rientrano nell'ambito di applicazione della presente direttiva **o i CSIRT designati**, possano, su base volontaria, divulgare le vulnerabilità e fornire informazioni su di esse che consentano agli utenti di adottare adeguate misure di attenuazione.

(31) Sebbene simili registri o banche dati delle vulnerabilità esistano già, questi sono ospitati e mantenuti da soggetti non stabiliti nell'Unione. Un registro europeo delle vulnerabilità mantenuto dall'ENISA garantirebbe una maggiore trasparenza, per quanto riguarda la procedura di pubblicazione prima della divulgazione ufficiale della vulnerabilità, e resilienza in caso di perturbazioni o interruzioni nella fornitura di servizi analoghi. Per evitare la duplicazione degli sforzi e perseguire, nella misura del possibile, la complementarità, l'ENISA dovrebbe valutare la possibilità di concludere accordi di cooperazione strutturata con registri simili nelle giurisdizioni di paesi terzi. **In particolare, l'ENISA dovrebbe valutare la possibilità di cooperare strettamente con gli operatori del sistema delle vulnerabilità e delle esposizioni comuni, ivi compresa la possibilità di diventare un'autorità di base competente per l'assegnazione di numeri identificativi alle vulnerabilità e alle esposizioni comuni ("root CVE Numbering Authority").**

(32) **Il gruppo di cooperazione dovrebbe continuare a sostenere e agevolare la cooperazione strategica e lo scambio di informazioni, come anche a rafforzare la fiducia tra gli Stati membri.** Il gruppo di cooperazione dovrebbe stabilire ogni due anni un programma di lavoro comprendente le azioni che il gruppo deve intraprendere per attuare i suoi obiettivi e compiti. Il calendario del primo programma adottato a norma della presente direttiva dovrebbe essere allineato a quello dell'ultimo programma adottato a norma della direttiva (UE) 2016/1148, al fine di evitare eventuali perturbazioni nel lavoro del gruppo.

(33) Nell'elaborare i documenti di orientamento, il gruppo di cooperazione dovrebbe sistematicamente: mappare le soluzioni e le esperienze nazionali, valutare l'impatto dei risultati del gruppo di cooperazione per quanto riguarda gli approcci nazionali, discutere le sfide in materia di attuazione e formulare raccomandazioni specifiche da realizzare attraverso una migliore attuazione delle norme esistenti.

(34) Il gruppo di cooperazione dovrebbe rimanere un forum flessibile ed essere in grado di reagire alle nuove e mutevoli priorità strategiche e alle sfide, tenendo conto nel contempo della disponibilità di risorse. Esso dovrebbe organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo e raccogliere contributi sulle sfide strategiche emergenti. Al fine di rafforzare la cooperazione a livello dell'Unione, il gruppo dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali il Centro europeo per la lotta alla criminalità informatica (EC3), l'Agenzia dell'Unione europea per la sicurezza aerea (AESA) e l'Agenzia dell'Unione europea per il programma spaziale (EUSPA).

(35) Le autorità competenti e i CSIRT dovrebbero avere la facoltà di partecipare a programmi di scambio per funzionari di altri Stati membri al fine di migliorare la cooperazione. Le autorità competenti dovrebbero adottare le misure necessarie per consentire a funzionari di altri Stati membri di svolgere un ruolo efficace nelle attività dell'autorità competente ospitante.

(35 bis) La rete di CSIRT dovrebbe continuare a contribuire al rafforzamento della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri. Al fine di rafforzare la cooperazione operativa a livello dell'Unione, la rete di CSIRT dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali Europol.

(36) [...]

(36 bis) Al fine di facilitare l'effettiva attuazione delle disposizioni della presente direttiva, quali la gestione delle vulnerabilità, la gestione dei rischi di cibersicurezza, le misure in materia di segnalazione e gli accordi di condivisione delle informazioni, gli Stati membri possono cooperare con i paesi terzi e intraprendere attività ritenute appropriate a tal fine, tra cui scambi di informazioni relative a minacce, incidenti, vulnerabilità, strumenti e metodi, tattiche, tecniche e procedure, preparazione e esercitazioni in materia di gestione delle crisi informatiche, formazioni, instaurazione di un clima di fiducia e accordi strutturati di condivisione delle informazioni. Tali accordi di cooperazione dovrebbero essere conformi al diritto dell'Unione in materia di protezione dei dati.

(37) Gli Stati membri dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE, di cui alla raccomandazione (UE) 2017/1584, attraverso le reti di cooperazione esistenti, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), la rete di CSIRT e il gruppo di cooperazione. EU-CyCLONe e la rete di CSIRT dovrebbero cooperare sulla base di disposizioni procedurali che definiscano le modalità di tale cooperazione **ed evitare duplicazioni dei compiti**. Il regolamento interno di EU-CyCLONe dovrebbe specificare ulteriormente le modalità di funzionamento della rete, compresi, ma non solo, i ruoli, le modalità di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione. Per la gestione delle crisi a livello **politico** dell'Unione, le parti pertinenti dovrebbero affidarsi alle disposizioni dei dispositivi integrati per la risposta politica alle crisi (IPCR). A tal fine la Commissione dovrebbe far ricorso al processo di coordinamento intersettoriale delle crisi ad alto livello del sistema ARGUS. Se la crisi implica un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) dovrebbe essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna (SEAE).

(37 bis) EU-CyCLONe dovrebbe fungere da rete intermediaria tra il livello tecnico e quello politico in caso di incidenti e crisi di cibersicurezza su vasta scala. Dovrebbe rafforzare la cooperazione a livello operativo, sulla base delle conclusioni della rete di CSIRT e utilizzando le proprie capacità per creare analisi dell'impatto degli incidenti e delle crisi su vasta scala nonché sostenendo il processo decisionale a livello politico. Le istituzioni, gli organismi e le agenzie dell'UE dovrebbero designare un'autorità competente responsabile della gestione degli incidenti e delle crisi di sicurezza su vasta scala affinché diventi membro di EU-CyCLONe.

(38) [...]

(39) [...]

(39 bis) La responsabilità di garantire la sicurezza dei sistemi informatici e di rete incombe in larga misura ai soggetti essenziali e importanti. È opportuno promuovere e sviluppare una cultura della gestione dei rischi, che comprenda la valutazione dei rischi e l'attuazione di misure di sicurezza commisurate al rischio corso.

(40) Le misure di gestione dei rischi dovrebbero **tenere conto del grado di dipendenza dei soggetti dai sistemi informatici e di rete e** comprendere misure per individuare eventuali rischi di incidenti, per prevenire, rilevare e gestire incidenti, nonché per attenuarne l'impatto. La sicurezza dei sistemi informatici e di rete dovrebbe comprendere la sicurezza dei dati conservati, trasmessi e elaborati.

(40 bis) Poiché le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, la presente direttiva applica un approccio "multirischio" che comprende la protezione dei sistemi informatici e di rete e del loro ambiente fisico da qualsiasi evento (ad esempio furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente) o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi. Le misure di gestione dei rischi dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente includendo misure volte a proteggere i sistemi informatici e di rete dei soggetti da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme riconosciute a livello europeo o internazionale, come quelle di cui alla serie ISO 27000. A tale riguardo, i soggetti dovrebbero altresì, nell'ambito delle loro misure di gestione dei rischi, affrontare la questione della sicurezza delle risorse umane e disporre di strategie adeguate di controllo dell'accesso. Tali misure dovrebbero essere coerenti con la direttiva XXXX [direttiva CER].

(40 ter) In mancanza di adeguati sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881, gli Stati membri potrebbero imporre ai soggetti di utilizzare prodotti, servizi o processi TIC certificati oppure di ottenere un certificato nell'ambito dei sistemi nazionali di cibersicurezza disponibili ai fini del rispetto degli obblighi di gestione dei rischi di cibersicurezza di cui alla presente direttiva.

(41) Per evitare di imporre un onere finanziario e amministrativo sproporzionato ai soggetti essenziali e importanti, gli obblighi di gestione dei rischi di cibersicurezza dovrebbero essere proporzionati al rischio corso dal sistema informatico e di rete interessato, tenendo conto dello stato dell'arte di tali misure **e dei relativi costi di attuazione**. **Si dovrebbe inoltre tenere debitamente conto delle dimensioni del soggetto nonché della probabilità che si verifichino incidenti e della loro gravità.**

(41 bis) Al fine di ridurre gli oneri normativi, gli obblighi relativi all'attuazione delle misure di gestione dei rischi di cibersicurezza per soggetti di medie dimensioni o per micro o piccoli soggetti dovrebbero, in linea di principio, essere meno rigidi, a meno che i criteri di criticità o le valutazioni nazionali del rischio non giustifichino l'esistenza di obblighi più rigorosi, in particolare per quanto riguarda i soggetti che soddisfano i criteri connessi alla criticità di cui alla presente direttiva.

(42) I soggetti essenziali e importanti dovrebbero garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività. Si tratta in particolare di sistemi informatici e di rete privati gestiti dal loro personale informatico interno oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di gestione e segnalazione dei rischi di cibersicurezza a norma della presente direttiva dovrebbero applicarsi ai pertinenti soggetti essenziali e importanti indipendentemente dal fatto che questi effettuino internamente la manutenzione dei loro sistemi informatici e di rete o che la esternalizzino.

(42 bis bis) Vista la loro natura transfrontaliera, i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti dovrebbero essere soggetti a un livello di armonizzazione più elevato su scala UE. L'attuazione delle misure di cibersicurezza dovrebbe pertanto essere agevolata da un atto di esecuzione.

(43) Affrontare i rischi di cibersicurezza derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono rimasti vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti dovrebbero pertanto valutare e tenere in considerazione la qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

(44) Tra i fornitori di servizi, i fornitori di servizi di sicurezza gestiti (managed security services providers, MSSP) in settori quali la risposta agli incidenti, i test di penetrazione, gli audit sulla sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per il rilevamento degli incidenti e la risposta agli stessi. Tali MSSP sono stati tuttavia essi stessi bersaglio di attacchi informatici e, a causa della loro stretta integrazione nelle attività degli operatori, presentano un particolare rischio di cibersicurezza. I soggetti dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un MSSP.

(44 bis) Nell'ambito dei loro compiti di vigilanza, le autorità nazionali competenti possono inoltre beneficiare di servizi di cibersicurezza quali gli audit sulla sicurezza e i test di penetrazione o la risposta agli incidenti. Per aiutare i soggetti, come pure le autorità nazionali competenti, nella selezione di fornitori di servizi di cibersicurezza qualificati e affidabili, la Commissione, con l'assistenza del gruppo di cooperazione e dell'ENISA, dovrebbe valutare la possibilità di richiedere sistemi europei di certificazione della cibersicurezza in conformità dell'articolo 48 del regolamento (UE) 2019/881.

(45) I soggetti dovrebbero inoltre affrontare i rischi di cibersicurezza derivanti dalle loro interazioni e relazioni con altri portatori di interessi nell'ambito di un ecosistema più ampio. In particolare, i soggetti dovrebbero adottare misure adeguate per garantire che la loro cooperazione con gli istituti accademici e di ricerca avvenga in linea con le loro politiche in materia di cibersicurezza e segua le buone pratiche per quanto riguarda l'accesso sicuro e la diffusione delle informazioni in generale e la tutela della proprietà intellettuale in particolare. Analogamente, data l'importanza e il valore dei dati per le attività dei soggetti, questi ultimi dovrebbero adottare tutte le opportune misure di cibersicurezza quando si affidano ai servizi di trasformazione e analisi dei dati forniti da terzi.

(46) Per affrontare ulteriormente i principali rischi relativi alla catena di approvvigionamento e aiutare i soggetti che operano nei settori disciplinati dalla presente direttiva a gestire adeguatamente i rischi di cibersicurezza connessi alla catena di approvvigionamento e ai fornitori, il gruppo di cooperazione, coinvolgendo le autorità nazionali competenti, in cooperazione con la Commissione e l'ENISA, dovrebbe effettuare valutazioni settoriali e coordinate dei rischi relativi alla catena di approvvigionamento, come già fatto per le reti 5G in seguito alla raccomandazione (UE) 2019/534 sulla cibersicurezza delle reti 5G[21], al fine di individuare, per settore, quali sono i servizi, i sistemi o i prodotti TIC critici e le minacce e le vulnerabilità pertinenti.

[21] Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, dal titolo "Cibersicurezza delle reti 5G" (GU L 88 del 29.3.2019, pag. 42).

(47) Le valutazioni dei rischi relativi alla catena di approvvigionamento, alla luce delle caratteristiche del settore interessato, dovrebbero tenere conto dei fattori tecnici e, se opportuno, non tecnici, compresi quelli definiti nella raccomandazione (UE) 2019/534, nella valutazione dei rischi coordinata a livello dell'UE della sicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione. Per individuare le catene di approvvigionamento che dovrebbero essere soggette a una valutazione coordinata dei rischi, dovrebbero essere presi in considerazione i seguenti criteri: i) la misura in cui i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi, sistemi o prodotti TIC critici; ii) la pertinenza di specifici servizi, sistemi o prodotti TIC critici per lo svolgimento di funzioni critiche o sensibili, compreso il trattamento dei dati personali; iii) la disponibilità di servizi, sistemi o prodotti TIC alternativi; iv) la resilienza dell'intera catena di approvvigionamento di servizi, sistemi o prodotti TIC contro eventi perturbatori e v) per i servizi, sistemi o prodotti TIC emergenti, la loro potenziale importanza futura per le attività dei soggetti.

(48) Al fine di semplificare gli obblighi giuridici imposti ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico e ai prestatori di servizi fiduciari relativi alla sicurezza dei loro sistemi informatici e di rete, nonché di consentire a tali soggetti e alle rispettive autorità competenti di beneficiare del quadro giuridico istituito dalla presente direttiva (compresa la designazione del CSIRT responsabile della gestione dei rischi e degli incidenti e la partecipazione delle autorità e degli organismi competenti ai lavori del gruppo di cooperazione e della rete di CSIRT), essi dovrebbero essere inclusi nell'ambito di applicazione della presente direttiva. Le corrispondenti disposizioni stabilite nel regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio[22] e nella direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio[23] relative all'imposizione di obblighi di sicurezza e notifica a **tali** tipi di soggetti dovrebbero pertanto essere abrogate.

---

22 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

23 Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

(48 bis) Gli obblighi in materia di sicurezza stabiliti nella presente direttiva dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n. 910/2014 (regolamento eIDAS). È opportuno chiedere ai prestatori di servizi fiduciari di adottare tutte le misure adeguate e proporzionate per gestire i rischi posti ai loro servizi, anche in relazione ai clienti e ai terzi che vi fanno affidamento, nonché di segnalare gli incidenti di sicurezza a norma della presente direttiva. Tali obblighi in materia di sicurezza e segnalazione dovrebbero riguardare anche la protezione fisica del servizio fornito. L'articolo 24 del regolamento (UE) n. 910/2014 continua ad applicarsi.

(48 bis bis) Gli Stati membri possono conferire il ruolo di autorità competenti per i servizi fiduciari agli organismi di vigilanza eIDAS al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite nell'applicazione del regolamento eIDAS. Qualora tale ruolo sia conferito a un organismo diverso, le autorità nazionali competenti a norma della presente direttiva dovrebbero cooperare strettamente, e in modo tempestivo, scambiando le informazioni pertinenti al fine di assicurare l'efficace vigilanza dei prestatori di servizi fiduciari nonché l'effettivo rispetto, da parte di questi ultimi, delle prescrizioni stabilite nella presente direttiva e nel regolamento [XXXX/XXXX].

Se del caso, le autorità nazionali competenti a norma della presente direttiva dovrebbero informare immediatamente l'organismo di vigilanza eIDAS di qualunque minaccia informatica o incidente significativi notificati aventi un impatto sui servizi fiduciari nonché di qualunque inosservanza, da parte di un prestatore di servizi fiduciari, degli obblighi di cui alla presente direttiva. Ai fini della segnalazione, gli Stati membri possono utilizzare, se del caso, il punto di ingresso unico stabilito per effettuare segnalazioni comuni e automatiche di incidenti destinate sia all'organismo di vigilanza eIDAS sia all'autorità competente a norma della presente direttiva. Le norme relative agli obblighi di segnalazione dovrebbero lasciare impregiudicati il regolamento (UE) 2016/679 e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio[24].

---

[24] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

(49) Se opportuno e per evitare inutili perturbazioni, gli orientamenti nazionali esistenti [...] adottat**i** per il recepimento delle norme relative alle misure di sicurezza di cui a**gli** articol**i** 40[...] e 41 della direttiva (UE) 2018/1972[...] **dovrebbero essere presi in considerazione nelle disposizioni di recepimento attuate dagli Stati membri in relazione alla presente direttiva, basandosi quindi sulle conoscenze e competenze già acquisite nell'ambito della direttiva (UE) 2018/1972 per quanto concerne le misure di gestione dei rischi di sicurezza e le notifiche degli incidenti. L'ENISA può inoltre elaborare orientamenti sui requisiti di sicurezza e segnalazione per i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico al fine di facilitare l'armonizzazione e la transizione e di ridurre al minimo le perturbazioni. Gli Stati membri possono conferire il ruolo di autorità competenti per le comunicazioni elettroniche alle autorità nazionali di regolamentazione al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite nell'ambito della direttiva (UE) 2018/1972.**

(50) Vista la crescente importanza dei servizi di comunicazione interpersonale indipendenti dal numero, è necessario assicurare che anche tali servizi siano soggetti ad adeguati requisiti di sicurezza in considerazione della loro specificità e della loro rilevanza economica. I fornitori di tali servizi dovrebbero pertanto garantire un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio esistente. Dato che i fornitori di servizi di comunicazione interpersonale indipendenti dal numero solitamente non esercitano un controllo effettivo sulla trasmissione dei segnali sulle reti, il grado di rischio di tali servizi può essere considerato, per certi aspetti, inferiore a quello dei servizi di comunicazione elettronica tradizionali. Lo stesso vale per i servizi di comunicazione interpersonale che utilizzano numeri e che non esercitano un controllo effettivo sulla trasmissione dei segnali.

(51) Il mercato interno dipende più che mai dal funzionamento di Internet. I servizi di quasi tutti i soggetti essenziali e importanti dipendono dai servizi forniti via Internet. Al fine di garantire l'erogazione senza intoppi dei servizi forniti dai soggetti essenziali e importanti, è fondamentale che le reti pubbliche di comunicazione elettronica, quali ad esempio le dorsali Internet o i cavi di comunicazione sottomarini, dispongano di adeguate misure di cibersicurezza e segnalino gli incidenti connessi.

(52) **Se del caso** [...], i soggetti dovrebbero informare i destinatari dei loro servizi di [...] particolari [...] misure che possono adottare per attenuare i rischi che [...] derivano **da una minaccia informatica significativa**. **Se del caso, e in particolare nei casi in cui la minaccia informatica significativa può concretizzarsi, i soggetti dovrebbero notificare della minaccia stessa anche i destinatari dei loro servizi, parallelamente alle autorità competenti o ai CSIRT.** L'obbligo di informare tali destinatari in merito alle minacce non dovrebbe esonerare i soggetti dall'obbligo di adottare, a proprie spese, provvedimenti adeguati e immediati per prevenire eventuali minacce informatiche o porvi rimedio e ristabilire il normale livello di sicurezza del servizio. La fornitura ai destinatari di tali informazioni riguardanti le minacce **informatiche** [...] dovrebbe essere gratuita.

(53) In particolare, i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico dovrebbero informare i destinatari dei servizi di minacce informatiche particolari e significative e delle misure che questi ultimi possono adottare per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecnologie di cifratura.

(54) Al fine di salvaguardare la sicurezza delle reti e dei servizi di comunicazione elettronica, l'uso della cifratura, in particolare la cifratura end-to-end, dovrebbe essere promosso e, ove necessario, dovrebbe essere reso obbligatorio per i fornitori di tali servizi e reti conformemente ai principi di sicurezza e tutela della vita privata per impostazione predefinita e fin dalla progettazione ai fini dell'articolo 18. L'uso della cifratura end-to-end dovrebbe essere conciliato con i poteri degli Stati membri di garantire la tutela della sicurezza pubblica e dei loro interessi essenziali in materia di sicurezza, nonché di consentire l'indagine, l'accertamento e il perseguimento di reati nel rispetto del diritto dell'Unione. Le soluzioni per l'accesso legittimo alle informazioni nelle comunicazioni che utilizzano la cifratura end-to-end dovrebbero mantenere l'efficacia della cifratura nella protezione della privacy e della sicurezza delle comunicazioni, fornendo nel contempo una risposta efficace alla criminalità.

(55) La presente direttiva stabilisce un approccio in due fasi alla segnalazione degli incidenti al fine di trovare il giusto equilibrio tra, da un lato, una segnalazione rapida che contribuisca ad attenuare la potenziale diffusione di incidenti e consenta ai soggetti di chiedere sostegno e, dall'altro, una segnalazione approfondita che tragga insegnamenti preziosi dai singoli incidenti e migliori nel tempo la resilienza alle minacce informatiche delle singole imprese e di interi settori. Qualora vengano a conoscenza di un incidente, i soggetti dovrebbero essere tenuti a presentare una notifica iniziale entro 24 ore, seguita da una relazione finale entro un mese. La notifica iniziale dovrebbe contenere solo le informazioni strettamente necessarie per informare le autorità competenti dell'incidente e consentire al soggetto di chiedere assistenza, se necessario. Tale notifica, ove applicabile, dovrebbe indicare se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola. Gli Stati membri dovrebbero garantire che l'obbligo di presentare tale notifica iniziale non sottragga le risorse del soggetto segnalante alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie. Per evitare ulteriormente che gli obblighi di segnalazione degli incidenti sottraggano risorse alla gestione della risposta agli incidenti o possano altrimenti compromettere gli sforzi dei soggetti a tale riguardo, gli Stati membri dovrebbero altresì prevedere che, in casi debitamente giustificati e d'intesa con le autorità competenti o con il CSIRT, il soggetto interessato possa derogare dai termini di 24 ore per la notifica iniziale e di un mese per la relazione finale.

(55 bis) Un approccio proattivo alle minacce informatiche è una componente essenziale della gestione dei rischi di cibersicurezza che dovrebbe consentire alle autorità competenti di impedire efficacemente che le minacce informatiche si trasformino in incidenti concreti che possono causare perdite materiali o immateriali considerevoli. A tal fine, la notifica di minacce informatiche significative riveste un'importanza fondamentale.

(56) I soggetti essenziali e importanti si trovano spesso in una situazione in cui un particolare incidente, a causa delle sue caratteristiche, deve essere segnalato a varie autorità in conseguenza degli obblighi di notifica previsti da vari strumenti giuridici. Tali casi creano ulteriori oneri e possono anche generare incertezze in merito al formato e alle procedure di tali notifiche. In considerazione di ciò e al fine di semplificare la segnalazione degli incidenti di sicurezza, gli Stati membri [...] **potrebbero** istituire un punto di ingresso unico per tutte le notifiche richieste a norma della presente direttiva e anche a norma di altri atti dell'Unione quali il regolamento (UE) 2016/679 e la direttiva 2002/58/CE. L'ENISA, in collaborazione con il gruppo di cooperazione, dovrebbe elaborare modelli comuni di notifica mediante orientamenti che semplifichino e razionalizzino le informazioni di segnalazione richieste dal diritto dell'Unione e riducano gli oneri per le imprese.

(57) Se si sospetta che un incidente sia connesso ad attività criminali gravi a norma del diritto dell'Unione o nazionale, gli Stati membri dovrebbero incoraggiare i soggetti essenziali e importanti, in base alle norme applicabili ai procedimenti penali in conformità al diritto dell'Unione, a segnalare alle autorità di contrasto pertinenti gli incidenti di cui si sospetta la natura criminale grave. Ove opportuno, e fatte salve le norme in materia di protezione dei dati personali applicabili a Europol, è auspicabile che l'EC3 e l'ENISA agevolino il coordinamento tra le autorità competenti e le autorità di contrasto dei diversi Stati membri.

(58) In molti casi gli incidenti compromettono i dati personali. In tale contesto, le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di protezione dei dati e con le autorità di vigilanza a norma della direttiva 2002/58/CE.

(59) Il mantenimento di banche dati precise e complete dei nomi di dominio e dei dati di registrazione (i cosiddetti "dati WHOIS") e la fornitura di un accesso legittimo a tali dati sono essenziali per garantire la sicurezza, la stabilità e la resilienza del DNS, che a sua volta contribuisce a un elevato livello comune di cibersicurezza all'interno dell'Unione. Se l'elaborazione dei dati comprende il trattamento dei dati personali, quest'ultimo deve essere conforme al diritto dell'Unione in materia di protezione dei dati.

(60) La disponibilità e la tempestiva accessibilità di tali dati per le autorità pubbliche, comprese le autorità competenti a norma del diritto dell'Unione o nazionale in materia di prevenzione, indagine o perseguimento di reati, ai CERT, ai CSIRT e, per quanto riguarda i dati dei loro clienti, ai fornitori di reti e servizi di comunicazione elettronica e ai fornitori di tecnologie e servizi di cibersicurezza che agiscono per conto di tali clienti, sono essenziali per prevenire e combattere l'abuso del sistema dei nomi di dominio, in particolare per la prevenzione e il rilevamento degli incidenti di cibersicurezza e la risposta agli stessi. Tale accesso dovrebbe essere conforme al diritto dell'Unione in materia di protezione dei dati nella misura in cui è relativo ai dati personali.

(61) Al fine di garantire la disponibilità di dati di registrazione dei nomi di dominio accurati e completi, i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD (i cosiddetti registrar) dovrebbero raccogliere i dati di registrazione dei nomi di dominio e garantirne l'integrità e la disponibilità. **Per quanto concerne i dati di registrazione, i soggetti dovrebbero in particolare verificare il nome e l'indirizzo di posta elettronica del registrante.** I[...] registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD dovrebbero stabilire politiche e procedure per raccogliere e mantenere i dati di registrazione accurati e completi, nonché per prevenire e rettificare dati di registrazione inesatti in conformità delle norme dell'Unione in materia di protezione dei dati.

(62) I registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio dovrebbero rendere pubblicamente disponibili i dati di registrazione dei nomi di dominio che non rientrano nell'ambito di applicazione delle norme dell'Unione in materia di protezione dei dati, come i dati riguardanti le persone giuridiche[25]. I registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD dovrebbero inoltre consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio riguardanti le persone fisiche ai legittimi richiedenti l'accesso, in conformità del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri dovrebbero garantire che i registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo alle richieste di divulgazione dei dati di registrazione dei nomi di dominio presentate dai legittimi richiedenti l'accesso**, come le autorità competenti nel settore della sicurezza nazionale e della giustizia penale a norma del diritto dell'Unione o nazionale, o i CSIRT**. I registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per la pubblicazione e la divulgazione dei dati di registrazione, compresi gli accordi sul livello dei servizi, ai fini del trattamento delle richieste di accesso dei legittimi richiedenti l'accesso. La procedura di accesso può comprendere anche l'uso di un'interfaccia, di un portale o di un altro strumento tecnico per fornire un sistema efficiente per la richiesta dei dati di registrazione e l'accesso agli stessi. **Gli Stati membri dovrebbero garantire che tutte le modalità di accesso ai dati di registrazione del dominio (dati personali e non personali) siano gratuite.** Al fine di promuovere pratiche armonizzate in tutto il mercato interno, la Commissione può adottare orientamenti su tali procedure, fatte salve le competenze del comitato europeo per la protezione dei dati**, in linea con le norme internazionali sviluppate dalla comunità multipartecipativa e in maniera ad esse complementare**.

[25] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, considerando 14: "Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto."

(63) [...]**I** soggetti essenziali e importanti a norma della presente direttiva dovrebbero rientrare nella giurisdizione dello Stato membro in cui forniscono i loro servizi. **I soggetti di cui ai punti da 1 a 7 e al punto 10 dell'allegato I, i prestatori di servizi fiduciari e i fornitori di punti di interscambio Internet di cui al punto 8 dell'allegato I e i soggetti di cui ai punti da 1 a 5 dell'allegato II della presente direttiva dovrebbero rientrare nella giurisdizione dello Stato membro in cui sono stabiliti.** Se fornisce servizi **o ha lo stabilimento** in più di uno Stato membro, il soggetto dovrebbe rientrare nella giurisdizione separata e concorrente di ciascuno di tali Stati membri. Le autorità competenti di tali Stati membri dovrebbero cooperare, prestarsi assistenza reciproca e, ove opportuno, condurre azioni comuni di vigilanza. **Qualora decidano di esercitare la giurisdizione, gli Stati membri dovrebbero evitare che la stessa condotta sia sanzionata più di una volta per la violazione degli obblighi stabiliti dalla presente direttiva.**

(64) Per tener conto della natura transfrontaliera dei servizi e delle attività dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, **dei soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD,** dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center e dei fornitori di servizi digitali, tali soggetti dovrebbero essere posti sotto la giurisdizione di un solo Stato membro. La giurisdizione dovrebbe essere attribuita allo Stato membro in cui il rispettivo soggetto ha lo stabilimento principale nell'Unione. Il criterio dello stabilimento ai fini della presente direttiva implica l'esercizio effettivo dell'attività nel quadro di un'organizzazione stabile. A tale riguardo non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.

Il rispetto di tale criterio non dovrebbe dipendere dal fatto che i sistemi informatici e di rete siano situati fisicamente in un determinato luogo; la presenza e l'utilizzo dei sistemi in questione non costituiscono di per sé lo stabilimento principale e non sono pertanto criteri decisivi per la sua determinazione. Lo stabilimento principale dovrebbe essere il luogo in cui sono **prevalentemente** adottate nell'Unione le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Ciò corrisponderà di norma alla sede dell'amministrazione centrale delle società nell'Unione. Se **il luogo in cui tali decisioni sono prevalentemente adottate non può essere determinato o se** tali decisioni non sono adottate nell'Unione, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui il soggetto ha lo stabilimento con il maggior numero di dipendenti nell'Unione. Qualora i servizi siano forniti da un gruppo di imprese, si dovrebbe considerare lo stabilimento principale dell'impresa controllante come lo stabilimento principale del gruppo di imprese.

(64 bis) Quando un servizio DNS ricorsivo è fornito da un fornitore di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico solo come parte del servizio di accesso a internet, il soggetto dovrebbe essere considerato sotto la giurisdizione di tutti gli Stati membri in cui i suoi servizi sono forniti.

(64 bis bis) Al fine di garantire una panoramica chiara dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center e dei fornitori di servizi digitali che forniscono servizi in tutta l'Unione nell'ambito di applicazione della presente direttiva, l'ENISA dovrebbe creare e mantenere un registro per tali soggetti, sulla base delle notifiche ricevute dagli Stati membri, se del caso attraverso i meccanismi nazionali di autonotifica. Al fine di garantire l'accuratezza e la completezza delle informazioni che dovrebbero essere incluse in tale registro, gli Stati membri dovrebbero trasmettere all'ENISA le informazioni su tali soggetti disponibili nei rispettivi registri nazionali. L'ENISA e gli Stati membri dovrebbero adottare misure per agevolare l'interoperabilità di tali registri, garantendo nel contempo la protezione delle informazioni riservate o classificate.

(65) Qualora un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi di cloud computing, un fornitore di servizi di data center e un fornitore di servizi digitali non stabilito nell'Unione offra servizi all'interno dell'Unione, esso dovrebbe designare un rappresentante. Per determinare se tale soggetto stia offrendo servizi nell'Unione, è opportuno verificare se risulta che il soggetto stia progettando di fornire servizi a persone in uno o più Stati membri. La semplice accessibilità nell'Unione del sito web del soggetto o di un intermediario, o di un indirizzo di posta elettronica e di altri dati di contatto, o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il soggetto è stabilito sono di per sé insufficienti per accertare tale intenzione. Tuttavia fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione, possono evidenziare che il soggetto sta progettando di offrire servizi all'interno dell'Unione. Il rappresentante dovrebbe agire a nome del soggetto e le autorità competenti o i CSIRT dovrebbero poterlo contattare. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del soggetto affinché agisca a suo nome con riguardo agli obblighi che a quest'ultimo derivano dalla presente direttiva, compresa la segnalazione di incidenti.

(66) Qualora informazioni considerate classificate in conformità al diritto nazionale o dell'Unione siano scambiate, comunicate o altrimenti condivise a norma delle disposizioni della presente direttiva, dovrebbero essere applicate le corrispondenti norme specifiche sulla gestione delle informazioni classificate.

(67) Di fronte a minacce informatiche che si fanno sempre più complesse e sofisticate, la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche che, a sua volta, accresce la capacità dei soggetti di impedire che le minacce si trasformino in incidenti concreti e consente ai soggetti di arginare in maniera più efficace gli effetti degli incidenti e di riprendersi in modo più efficiente. In assenza di orientamenti a livello dell'Unione, numerosi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di concorrenza e responsabilità, sembrano aver ostacolato tale condivisione delle informazioni di intelligence.

(68) È quindi opportuno incoraggiare i soggetti a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le loro capacità di valutare e monitorare adeguatamente le minacce informatiche, difendersi da esse e rispondervi. È pertanto necessario consentire la creazione a livello dell'Unione di meccanismi per accordi volontari di condivisione delle informazioni. A tal fine gli Stati membri dovrebbero sostenere e incoraggiare attivamente anche i soggetti pertinenti che non rientrano nell'ambito di applicazione della presente direttiva a partecipare a tali meccanismi di condivisione delle informazioni. Tali meccanismi dovrebbero essere attuati nel pieno rispetto delle norme dell'Unione in materia di concorrenza e di protezione dei dati.

(69) [...] **N**ella misura strettamente necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete**, il trattamento dei dati personali** da parte di soggetti **essenziali e importanti** [...] e fornitori di tecnologie e servizi di sicurezza **potrebbe essere considerato necessario per adempiere un obbligo legale o** [...] costituire un interesse legittimo del titolare del trattamento in questione di cui al regolamento (UE) 2016/679. Ciò **potrebbe** [...] includere misure relative alla prevenzione, al rilevamento e all'analisi degli incidenti e alla risposta agli stessi, misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, nonché lo scambio volontario di informazioni su tali incidenti, sulle minacce informatiche e sulle vulnerabilità, sugli indicatori di compromissione, sulle tattiche, sulle tecniche e le procedure, sugli allarmi di cibersicurezza e sugli strumenti di configurazione. Tali misure possono richiedere il trattamento [...] **di vari** tipi di dati personali**, quali**: indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio e indirizzi di posta elettronica. **Il trattamento dei dati personali da parte delle autorità competenti, degli SPOC e dei CSIRT dovrebbe essere previsto dal diritto nazionale ed essere considerato necessario per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, a norma dell'articolo 6, paragrafo 1, lettere c) o e), del regolamento (UE) 2016/679.**

(69 bis) Nella misura strettamente necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete di soggetti essenziali e importanti, la legislazione degli Stati membri può stabilire norme che consentono alle autorità competenti, agli SPOC e ai CSIRT di trattare categorie particolari di dati personali conformemente all'articolo 9 del regolamento (UE) 2016/679, in particolare prevedendo misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi delle persone fisiche, tra cui limitazioni tecniche al riutilizzo di tali dati e l'utilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

(70) Al fine di rafforzare i poteri e le azioni di vigilanza che contribuiscono a garantire l'effettiva conformità, la presente direttiva dovrebbe prevedere un elenco minimo di azioni e mezzi di vigilanza attraverso i quali le autorità competenti possono vigilare sui soggetti essenziali e importanti. La presente direttiva dovrebbe inoltre stabilire una differenziazione del regime di vigilanza tra i soggetti essenziali e i soggetti importanti al fine di garantire un giusto equilibrio degli obblighi sia per i soggetti che per le autorità competenti. Pertanto i soggetti essenziali dovrebbero essere sottoposti a un regime di vigilanza completo (ex ante ed ex post), mentre i soggetti importanti dovrebbero essere sottoposti a un regime di vigilanza leggero, solo ex post. In base a quest'ultimo i soggetti importanti non dovrebbero **essere tenuti a** documentare sistematicamente il rispetto degli obblighi di gestione dei rischi di cibersicurezza, mentre le autorità competenti dovrebbero attuare un approccio ex post reattivo alla vigilanza e, di conseguenza, non dovrebbero avere un obbligo generale di vigilanza su tali soggetti. **Per i soggetti importanti, la vigilanza ex post può essere innescata da elementi di prova o da eventuali indicazioni o informazioni portati all'attenzione delle autorità competenti che tali autorità ritengono suggerire una possibile inosservanza degli obblighi stabiliti dalla presente direttiva. Ad esempio, tali elementi di prova, indicazioni o informazioni potrebbero essere del tipo fornito alle autorità competenti da altre autorità, soggetti, cittadini, media o altre fonti, informazioni pubblicamente disponibili, o emergere nel corso di altre attività svolte dalle autorità competenti nell'adempimento dei loro compiti.**

(70 bis) Nell'esercizio della vigilanza ex ante, le autorità competenti dovrebbero poter decidere in modo proporzionato l'ordine di priorità nel ricorso alle azioni e ai mezzi di vigilanza a loro disposizione. Ciò implica che le autorità competenti possano decidere l'ordine di priorità sulla base di metodologie di vigilanza che dovrebbero seguire un approccio basato sui rischi. Più specificamente, tali metodologie potrebbero includere criteri o parametri di riferimento per la classificazione dei soggetti essenziali in categorie di rischio e corrispondenti azioni e mezzi di vigilanza raccomandati per categoria di rischio, quali l'uso, la frequenza o il tipo di ispezioni in loco, audit sulla sicurezza mirati o scansioni di sicurezza, il tipo di informazioni da richiedere e il livello di dettaglio di tali informazioni. Tali metodologie di vigilanza possono inoltre essere corredate da programmi di lavoro ed essere valutate e riesaminate periodicamente, anche per quanto riguarda aspetti quali l'assegnazione e il fabbisogno di risorse.

(70 bis bis) In relazione agli enti della pubblica amministrazione, i poteri di vigilanza dovrebbero essere esercitati in linea con l'ordinamento giuridico e i quadri nazionali. Gli Stati membri dovrebbero avere facoltà di decidere in merito all'imposizione di misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti.

(70 bis bis bis) Al fine di dimostrare il rispetto di determinate misure di gestione dei rischi di cibersicurezza, gli Stati membri potrebbero imporre ai soggetti essenziali e importanti di utilizzare servizi fiduciari qualificati o regimi di identificazione elettronica notificati a norma del regolamento (UE) n. 910/2014.

(71) Al fine di rendere efficace l'esecuzione, è opportuno stabilire un elenco minimo di sanzioni amministrative in caso di violazione degli obblighi di gestione e segnalazione dei rischi di cibersicurezza previsti dalla presente direttiva, istituendo un quadro chiaro e coerente per tali sanzioni in tutta l'Unione. Occorre tenere debitamente conto della natura, della gravità e della durata dell'infrazione, del danno effettivamente causato o delle perdite effettivamente subite o del danno o delle perdite potenziali che si sarebbero potuti verificare, del carattere doloso o colposo della violazione, delle azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite, del grado di responsabilità o di eventuali violazioni precedenti pertinenti, del grado di cooperazione con l'autorità competente e di qualsiasi altro fattore aggravante o attenuante. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie, dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

(71 bis) Le disposizioni relative alla responsabilità delle persone fisiche che detengono determinati incarichi all'interno di un ente in caso di inadempimento del loro dovere di garantire il rispetto degli obblighi stabiliti dalla presente direttiva non impongono agli Stati membri di assicurare l'azione penale o la responsabilità civile per i danni causati a terzi da tale inadempimento.

(72) Al fine di garantire l'efficace esecuzione degli obblighi stabiliti nella presente direttiva, ciascuna autorità competente dovrebbe avere il potere di imporre o chiedere l'imposizione di sanzioni amministrative pecuniarie.

(73) Qualora le sanzioni amministrative pecuniarie siano imposte a imprese, queste ultime dovrebbero essere intese quali imprese conformemente agli articoli 101 e 102 TFUE a tali fini. Qualora le sanzioni amministrative pecuniarie siano imposte a persone che non sono imprese, l'autorità di vigilanza dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. L'imposizione di una sanzione amministrativa pecuniaria non pregiudica l'applicazione di altri poteri da parte delle autorità competenti o di altre sanzioni previste dalle norme nazionali di recepimento della presente direttiva.

(74) Gli Stati membri [...] **possono** stabilire le norme relative alle sanzioni penali in caso di violazione delle norme nazionali di recepimento della presente direttiva. Tuttavia l'imposizione di sanzioni penali per le violazioni di tali norme nazionali e delle relative sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia.

(75) Qualora la presente direttiva non armonizzi le sanzioni amministrative o ove necessario in altri casi, ad esempio in caso di violazioni gravi degli obblighi stabiliti nella presente direttiva, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri.

(76) Al fine di rafforzare ulteriormente l'efficacia e il carattere dissuasivo delle sanzioni applicabili alle violazioni degli obblighi stabiliti a norma della presente direttiva, le autorità competenti dovrebbero avere la facoltà di applicare sanzioni consistenti nella sospensione di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi forniti da un soggetto essenziale e nell'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di una persona fisica. Data la loro gravità e l'impatto sulle attività dei soggetti e, in ultima analisi, sui consumatori, tali sanzioni dovrebbero essere applicate solo in proporzione alla gravità della violazione e tenere conto delle circostanze specifiche di ciascun caso, tra cui il carattere doloso o colposo della violazione e le azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite. Tali sanzioni dovrebbero essere applicate solo come ultima ratio, vale a dire solo una volta esaurite le altre pertinenti misure di esecuzione previste dalla presente direttiva, e solo fino a quando i soggetti ai quali si applicano non adottano le misure necessarie per rimediare alle carenze o per conformarsi alle prescrizioni dell'autorità competente per cui tali sanzioni sono state applicate. L'imposizione di tali sanzioni dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale, il giusto processo, la presunzione di innocenza e i diritti della difesa.

(76 bis) Al fine di garantire una vigilanza e un'esecuzione efficaci, in particolare nei casi a dimensione transfrontaliera, gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca dovrebbero, nella misura in cui è richiesto, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che dispone di sistemi informatici e di rete sul territorio di tali Stati membri.

(77) La presente direttiva dovrebbe stabilire norme di cooperazione tra le autorità competenti e le autorità di controllo conformemente al regolamento (UE) 2016/679 per far fronte alle violazioni relative ai dati personali.

(78) La presente direttiva dovrebbe mirare a garantire un elevato livello di responsabilità per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a livello delle organizzazioni. Pertanto gli organismi di gestione dei soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero approvare le misure relative ai rischi di cibersicurezza e vigilare sulla loro attuazione.

(79) Dovrebbe essere introdotto un [...] **sistema di apprendimento** tra pari **per contribuire a rafforzare la fiducia reciproca e trarre insegnamenti dalle buone pratiche e dalle esperienze,** che consenta agli esperti designati dagli Stati membri **di effettuare scambi tra pari**[...] **sul**l'attuazione delle politiche in materia di cibersicurezza [...]. **Nell'attuare il sistema di apprendimento tra pari si dovrebbe prestare particolare attenzione a garantire che esso non comporti oneri inutili o sproporzionati per le autorità competenti degli Stati membri. La Commissione dovrebbe esplorare tutte le alternative possibili per garantire la copertura finanziaria dei costi che potrebbero insorgere dall'organizzazione di missioni di apprendimento tra pari. Inoltre, il sistema di apprendimento tra pari dovrebbe tenere conto dei risultati di meccanismi analoghi, come il sistema di revisione tra pari della rete di CSIRT, apportare un valore aggiunto ed evitare duplicazioni. L'attuazione del sistema di apprendimento tra pari dovrebbe lasciare impregiudicate le normative nazionali o dell'Unione in materia di protezione delle informazioni riservate e classificate. Prima dell'inizio dei cicli di apprendimento tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti pertinenti. Su richiesta del gruppo di cooperazione, l'ENISA può fornire, se necessario, orientamenti sull'autovalutazione e i modelli pertinenti. Gli Stati membri potrebbero decidere di rendere pubbliche le rispettive relazioni.**

(80) [...]

(81) Al fine di garantire condizioni uniformi di attuazione delle pertinenti disposizioni della presente direttiva riguardanti le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione, gli elementi tecnici relativi alle misure di gestione dei rischi o al tipo di informazioni**,** [...] il formato e la procedura per le notifiche degli incidenti**, e le categorie di soggetti cui deve essere imposto di utilizzare determinati prodotti, servizi e processi TIC certificati**, dovrebbero essere attribuite alla Commissione competenze di esecuzione. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[26].

(82) È opportuno che la Commissione riesamini la presente direttiva a scadenze regolari, in consultazione con le parti interessate, in particolare al fine valutare la necessità di modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato.

---

[26] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

(83) Poiché l'obiettivo della presente direttiva, vale a dire conseguire un elevato livello comune di cibersicurezza nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione, può essere conseguito meglio a livello dell'Unione, quest'ultima può adottare misure in conformità al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(84) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo dinanzi a un giudice e il diritto al contraddittorio. La presente direttiva dovrebbe essere attuata in conformità a tali diritti e principi,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione **in modo da migliorare il funzionamento del mercato interno**.

2. A tal fine la presente direttiva:

   a) fa obbligo agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e designare autorità nazionali competenti, punti di contatto unici e team di risposta agli incidenti di sicurezza informatica (computer security incident response team, CSIRT);

   b) stabilisce obblighi in materia di gestione e segnalazione dei rischi di cibersicurezza per i tipi di soggetti definiti [...] **negli allegati I e II** [...];

   c) stabilisce **norme e** obblighi in materia di condivisione delle informazioni sulla cibersicurezza.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai tipi di soggetti pubblici e privati [...] [...] **elencati negli allegati I e II** [...] **che raggiungono o superano le soglie relative alle medie imprese** ai sensi della raccomandazione 2003/361/CE della Commissione[27]. **L'articolo 3, paragrafo 4, e l'articolo 6, paragrafo 2, secondo e terzo comma, dell'allegato di tale raccomandazione non si applicano ai fini della presente direttiva.**

2. [...]**I**ndipendentemente dalle [...] dimensioni **dei soggetti di cui al paragrafo 1**, la presente direttiva si applica anche qualora: [...]

   a) i servizi siano forniti da uno dei soggetti seguenti:

      (i) **fornitori di** reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico di cui all'allegato I, punto 8;

      (ii) **prestatori di servizi fiduciari qualificati di cui all'allegato I, punto XX;**

      iii) **prestatori di servizi fiduciari non qualificati di cui all'allegato I, punto XX;**

      iv) registri di nomi di dominio di primo livello [...] di cui all'allegato I, punto 8;

   b) [...]

[27] Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

c) il soggetto sia l'unico fornitore **in uno Stato membro** di un servizio [...] **che è essenziale per il mantenimento di attività sociali o economiche fondamentali**;

d) una possibile perturbazione del servizio fornito dal soggetto potrebbe avere un impatto **significativo** sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

e) una possibile perturbazione del servizio fornito dal soggetto potrebbe comportare rischi sistemici **significativi**, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

f) [...];

g) il soggetto sia identificato come soggetto critico a norma della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio[28] [direttiva sulla resilienza dei soggetti critici] **[**o come soggetto equivalente a un soggetto critico a norma dell'articolo 7 di tale direttiva**]**.

2 bis. Indipendentemente dalle loro dimensioni, la presente direttiva si applica anche agli enti della pubblica amministrazione delle amministrazioni centrali riconosciuti come tali in uno Stato membro conformemente al diritto nazionale e di cui all'allegato I, punto 9. Gli Stati membri possono stabilire che la presente direttiva si applichi anche agli enti della pubblica amministrazione ai livelli regionale e locale.

[28] [Inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti]

3. [...]

La presente direttiva lascia impregiudicate le responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

3 bis. 1) La presente direttiva non si applica:

a) ai soggetti che non rientrano nell'ambito di applicazione del diritto dell'Unione e in ogni caso a tutti i soggetti operanti principalmente nei settori della difesa, della sicurezza nazionale, della pubblica sicurezza o dell'attività di contrasto, indipendentemente dal soggetto che svolge tali attività e dal fatto che si tratti di un soggetto pubblico o privato, fatto salvo il punto 2);

b) ai soggetti che operano nel settore della giustizia, ai parlamenti o alle banche centrali.[...]

2) Qualora svolgano attività in tali settori soltanto come parte delle loro attività globali, gli enti della pubblica amministrazione sono esclusi nella loro integralità dall'ambito di applicazione della presente direttiva.

3 bis bis. La presente direttiva non si applica:

i) alle attività di soggetti che non rientrano nell'ambito di applicazione del diritto dell'Unione e in ogni caso a tutte le attività concernenti la sicurezza nazionale o la difesa, indipendentemente dal soggetto che svolge tali attività e dal fatto che si tratti di un soggetto pubblico o privato;

ii) alle attività di soggetti nel settore della giustizia, dei parlamenti, delle banche centrali e nel settore della pubblica sicurezza, compresi gli enti della pubblica amministrazione che svolgono attività di contrasto a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

3 bis bis bis. Gli obblighi definiti nella presente direttiva non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

3 bis bis bis bis. La presente direttiva non pregiudica il diritto dell'Unione in materia di protezione dei dati personali, in particolare le disposizioni del regolamento (UE) 2016/679 e della direttiva 2002/58/CE.

3 ter. La presente direttiva non si applica ai soggetti che sono esentati dal regolamento (UE) XXXX/XXXX del Parlamento europeo e del Consiglio [regolamento DORA] a norma dell'articolo 2, paragrafo 4, del regolamento DORA.

4. La presente direttiva si applica fatte salve [...][29] le direttive 2011/93/UE[30] e 2013/40/UE[31] del Parlamento europeo e del Consiglio.

5. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione e nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti **conformemente alla presente direttiva** solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali dei soggetti essenziali o importanti.

---

29 [...]

30 Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

31 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

Articolo 2 bis

Soggetti essenziali e importanti

1. Dei soggetti ai quali si applica la presente direttiva, sono considerati essenziali:

i) i tipi di soggetti di cui ai punti da 1 a 8 bis e al punto 10 dell'allegato I della presente direttiva che superano le soglie relative alle medie imprese quali definite nella raccomandazione 2003/361/CE della Commissione;

ii) i soggetti di medie dimensioni di cui all'articolo 2, paragrafo 2, lettera a), punto i);

iii) i soggetti di cui all'articolo 2, paragrafo 2, lettera a), punti ii) e iv), della presente direttiva, indipendentemente dalle dimensioni;

iv) i soggetti di cui all'articolo 2, paragrafo 2, lettera g), e all'articolo 2, paragrafo 2 bis, della presente direttiva, indipendentemente dalle dimensioni;

v) ove stabilito dagli Stati membri, i soggetti che gli Stati membri hanno definito, prima dell'entrata in vigore della presente direttiva, come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale;

vi) i soggetti che superano le soglie relative alle medie imprese quali definite nella raccomandazione 2003/361/CE della Commissione del tipo previsto nell'allegato II che gli Stati membri definiscono essenziali sulla base dei criteri di cui all'articolo 2, paragrafo 2, lettere da c) a e);

vii) i soggetti di medie dimensioni ai sensi della raccomandazione 2003/361/CE della Commissione che gli Stati membri definiscono essenziali sulla base dei criteri di cui all'articolo 2, paragrafo 2, lettere da c) a e);

viii) i micro o piccoli soggetti ai sensi della raccomandazione 2003/361/CE della Commissione di cui al paragrafo 2, lettera a), punto i), o individuati a norma del paragrafo 2, lettere da c) a e), del presente articolo che gli Stati membri definiscono come essenziali sulla base di valutazioni nazionali del rischio.

2. Dei soggetti ai quali si applica la presente direttiva, sono considerati soggetti importanti:

i) i tipi di soggetti di cui all'allegato I della presente direttiva che si qualificano come medie imprese ai sensi della raccomandazione 2003/361/CE della Commissione e i tipi di soggetti di cui all'allegato II che soddisfano o superano le soglie relative alle medie imprese ai sensi della raccomandazione 2003/361/CE della Commissione[32];

ii) i soggetti di cui all'articolo 2, paragrafo 2, lettera a), punto iii), della presente direttiva, indipendentemente dalle dimensioni;

iii) i piccoli e micro soggetti di cui all'articolo 2), paragrafo 2, lettera a), punto i);

iv) i piccoli e micro soggetti che gli Stati membri definiscono come soggetti importanti sulla base dell'articolo 2, paragrafo 2, lettere da c) a e).

---

[32] **Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).**

Articolo 2a

Meccanismi di notifica

1. **Gli Stati membri possono istituire un meccanismo nazionale di autonotifica che imponga a tutti i soggetti che rientrano nell'ambito di applicazione della presente direttiva di comunicare alle autorità competenti a norma della presente direttiva o agli organismi designati a tal fine dagli Stati membri almeno il loro nome, il loro indirizzo, i loro dati di contatto, il settore in cui operano o il tipo di servizio che forniscono e, se del caso, l'elenco degli Stati membri in cui prestano servizi soggetti alla presente direttiva.**

2. Gli Stati membri [...] trasmettono alla Commissione, **in relazione ai soggetti che hanno individuato a norma dell'articolo 2, paragrafo 2, lettere da b) a e), almeno le informazioni pertinenti circa il numero di soggetti individuati, il settore cui appartengono o il tipo di servizio che forniscono conformemente agli allegati, nonché la disposizione o le disposizioni specifiche dell'articolo 2, paragrafo 2, sulla cui base sono stati individuati, entro [12 mesi dopo il termine di recepimento della presente direttiva].** Gli Stati membri riesaminano [...] **tali informazioni** [...] periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

Articolo 2b

Atti settoriali dell'Unione

1. Qualora gli [...] **atti giuridici** settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti o le minacce informatiche **significativi**, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, **a tali soggetti** non si applicano le pertinenti disposizioni della presente direttiva, **comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VI**. **Qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva continuano ad applicarsi ai soggetti non contemplati da tali disposizioni settoriali.**

2. Gli effetti degli obblighi di cui al paragrafo 1 sono considerati equivalenti a quelli degli obblighi stabiliti nella presente direttiva se il rispettivo atto settoriale dell'Unione prevede l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte delle autorità competenti a norma della presente direttiva o dei CSIRT designati e se:

a) gli effetti delle misure di gestione dei rischi di cibersicurezza sono almeno equivalenti a quelli delle misure di cui all'articolo 18, paragrafi 1 e 2, della presente direttiva; o

b) gli effetti degli obblighi di notifica degli incidenti significativi sono almeno equivalenti a quelli degli obblighi di cui all'articolo 20, paragrafi da 1 a 6.

3. La Commissione riesamina periodicamente l'applicazione dei requisiti dell'effetto equivalente di cui ai paragrafi 1 e 2 in relazione alle disposizioni settoriali di atti giuridici dell'Unione. La Commissione consulta il gruppo di cooperazione e l'ENISA in sede di preparazione di tali riesami periodici.

Articolo 3

Armonizzazione minima

Fatti salvi i loro obblighi derivanti dal diritto dell'Unione, gli Stati membri [...] possono adottare o mantenere disposizioni che garantiscono un livello più elevato di cibersicurezza **nei settori contemplati dalla presente direttiva**.

Articolo 4

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) "sistema informatico e di rete":

   a) una rete di comunicazione elettronica ai sensi dell'articolo 2, punto 1, della direttiva (UE) 2018/1972;

   b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali;

   c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

2) "sicurezza dei sistemi informatici e di rete": la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli **eventi** che **potrebbero** compromettere **[...]** la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o **dei** servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi;

2 bis) "servizi di comunicazione elettronica": [...] i servizi di comunicazione elettronica ai sensi dell'articolo 2, punto 4, della direttiva (UE) 2018/1972;

3) "cibersicurezza": la cibersicurezza ai sensi dell'articolo 2, punto 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[33];

4) "strategia nazionale per la **cibersicurezza**": un quadro coerente di uno Stato membro che definisce la governance per conseguire priorità e obiettivi strategici in materia di [...] **cibersicurezza** [...] in tale Stato membro;

5) "incidente": un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei [...] servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;

5 bis) "incidente di cibersicurezza su vasta scala": un incidente che ha un impatto significativo su almeno due Stati membri o che causa perturbazioni che superano la capacità di risposta di uno Stato membro;

---

33 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

6) "gestione degli incidenti": tutte le azioni e le procedure volte a rilevare, analizzare e contenere un incidente e a rispondervi;

6 bis) "rischio": la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi detto incidente;

7) "minaccia informatica": una minaccia informatica ai sensi dell'articolo 2, punto 8, del regolamento (UE) 2019/881;

7 **bis) "minaccia informatica significativa": una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o dei suoi utenti causando perdite materiali o immateriali considerevoli;**

8) "vulnerabilità": un punto debole, una suscettibilità o un difetto di una risorsa TIC o di un sistema [...] che possono essere sfruttati da una minaccia informatica;

8 bis) "quasi incidente": un evento che avrebbe potenzialmente potuto causare un danno ai sistemi informatici e di rete di un soggetto o dei suoi utenti, ma che è stato efficacemente evitato prima che si verificasse;

9) "rappresentante": qualsiasi persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di i) un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello (top-level domain, TLD), un fornitore di servizi di cloud computing, un fornitore di servizi di data center o un fornitore di reti di distribuzione dei contenuti (content delivery network) di cui all'allegato I, punto 8, o ii) soggetti di cui all'allegato II, [...] punto **6**, che non sono stabiliti nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva;

10) "norma": una norma ai sensi dell'articolo 2, punto 1, del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[34];

11) "specifica tecnica": una specifica tecnica ai sensi dell'articolo 2, punto 4, del regolamento (UE) n. 1025/2012;

12) "punto di interscambio Internet (IXP)": un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico Internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico Internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;

13) "sistema dei nomi di dominio (DNS)": un sistema di nomi gerarchico e distribuito che consente agli utenti finali di accedere a servizi e risorse su Internet;

14) "fornitore di servizi DNS": un soggetto che fornisce un servizio di risoluzione dei nomi di dominio autorevole o ricorsivo [...] **per uso da parte di terzi, fatta eccezione per i server dei nomi radice** [...];

---

[34] Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

15) "registro dei nomi di dominio di primo livello": un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compreso il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD tra i server dei nomi, **escludendo le situazioni in cui i nomi di dominio di primo livello sono utilizzati da un registro esclusivamente per uso proprio**;

15 bis) "soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD": i registri dei nomi di dominio di primo livello, i registrar per i TLD e gli agenti dei registrar quali i rivenditori e i fornitori di servizi proxy;

16) "servizio digitale": un servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio[35];

16 bis) "servizi fiduciari": i servizi fiduciari ai sensi dell'articolo 3, punto 16, del regolamento (UE) n. 910/2014;

[35] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

16 ter) "prestatore di servizi fiduciari qualificato": un prestatore di servizi fiduciari qualificato ai sensi dell'articolo 3, punto 20, del regolamento (UE) n. 910/2014;

17) "mercato online": un servizio digitale ai sensi dell'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio[36];

18) "motore di ricerca online": un servizio digitale ai sensi dell'articolo 2, punto 5, del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio[37];

19) "servizio di cloud computing": un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili [...] e l'ampio accesso remoto a quest'ultimo, **anche quando tali risorse sono distribuite in varie ubicazioni**;

20) "servizio di data center": un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

---

36 Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio ("direttiva sulle pratiche commerciali sleali") (GU L 149 dell'11.6.2005, pag. 22).

37 Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (GU L 186 dell'11.7.2019, pag. 57).

21) "rete di distribuzione dei contenuti (content delivery network)": una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di Internet per conto di fornitori di contenuti e servizi;

22) "piattaforma di servizi di social network": una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi e, in particolare, attraverso chat, post, video e raccomandazioni [...];

23) "ente della pubblica amministrazione": un soggetto **riconosciuto come tale in uno Stato membro conformemente al diritto nazionale,** [...] che soddisfa i criteri seguenti:

a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

b) è dotato di personalità giuridica **o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica;**

c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico; oppure la sua gestione è soggetta alla vigilanza di tali autorità o organismi; oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;

d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali.

24) "soggetto": una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

25) "soggetto essenziale": un tipo di soggetto che figura [...] **nell'allegato I e designato come "essenziale" a norma dell'articolo 2 bis, paragrafo 1**;

26) "soggetto importante": un tipo di soggetto che figura [...] **negli allegati I e II e designato come "importante" a norma dell'articolo 2 bis, paragrafo 2**;

26 bis) "prodotto TIC": un prodotto TIC ai sensi dell'articolo 2, punto 12, del regolamento (UE) 2019/881;

26 bis bis) "servizio TIC": un servizio TIC ai sensi dell'articolo 2, punto 13, del regolamento (UE) 2019/881;

26 bis ter) "processo TIC": un processo TIC ai sensi dell'articolo 2, punto 14, del regolamento (UE) 2019/881;

26 bis quater) "fornitore di servizi gestiti": qualsiasi soggetto che fornisce servizi, quali reti, applicazioni, infrastrutture e sicurezza, attraverso una gestione continua e regolare, un sostegno e un'amministrazione attiva nei locali dei clienti, nel data center del fornitore di servizi gestiti (hosting) o in un data center di terzi;

26 bis quinquies) "fornitore di servizi di sicurezza gestiti": qualsiasi soggetto che fornisce il monitoraggio e la gestione esternalizzati dei dispositivi e dei sistemi di sicurezza. Tra i servizi comuni figurano la gestione dei firewall, il rilevamento delle intrusioni, le reti private virtuali, la scansione delle vulnerabilità e servizi antivirus.

È altresì incluso l'uso di centri operativi di sicurezza ad alta disponibilità (a partire dai propri locali o dai data center di altri fornitori) per fornire servizi 24 ore 24, 7 giorni su 7, concepiti per ridurre il numero di addetti alla sicurezza operativa che un'impresa deve assumere, formare e trattenere per mantenere una posizione di sicurezza accettabile.

CAPO II

Quadri normativi coordinati in materia di cibersicurezza

Articolo 5

Strategia nazionale per la cibersicurezza

1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che definisce obiettivi strategici e adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza. La strategia nazionale per la cibersicurezza comprende, in particolare, gli elementi seguenti:

   a) [...] gli obiettivi e le priorità della strategia per la cibersicurezza dello Stato membro;

   b) un quadro di governance per la realizzazione di tali obiettivi e priorità, comprendente le misure strategiche di cui al paragrafo 2 e i ruoli e le responsabilità delle diverse autorità e dei diversi attori coinvolti nell'attuazione della strategia [...];

   c) [...] **orientamenti per** individuare le risorse e **valutare i** rischi di cibersicurezza pertinenti nello Stato membro;

   d) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;

   e) [...]

f) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio[38] [direttiva sulla resilienza dei soggetti critici] ai fini della condivisione delle informazioni [...] **sui rischi di cibersicurezza,** [...] sulle minacce [...] **e gli incidenti informatici, nonché sui rischi, le minacce e gli incidenti non informatici**, come pure dello svolgimento di compiti di vigilanza**, se del caso**;

f bis) un quadro strategico per il coordinamento e la cooperazione tra le autorità competenti a norma della presente direttiva e le autorità competenti designate a norma della legislazione settoriale.

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare le misure strategiche seguenti:

a) misure relative alla cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione (TIC) utilizzati da soggetti [...] per la fornitura dei loro servizi;

b) [...] **misure** relativ**e** all'inclusione e alla definizione di requisiti relativi alla cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici**, compresa la certificazione della cibersicurezza**;

c) misure **relative alla gestione delle vulnerabilità, che comprendano la promozione e l'agevolazione della** [...] divulgazione coordinata **volontaria** delle vulnerabilità ai sensi dell'articolo 6**, paragrafo 1**;

d) misure relative al sostegno della disponibilità generale**,** [...] dell'integrità **e della riservatezza** del carattere fondamentale pubblico di una rete Internet aperta;

e) misure volte a promuovere e sviluppare **attività di istruzione e formazione,** competenze, attività di sensibilizzazione e iniziative di ricerca e sviluppo in materia di cibersicurezza;

---

38 *[Inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti].*

f) misure per sostenere gli istituti accademici e di ricerca nello sviluppo di strumenti di cibersicurezza e di infrastrutture di rete sicure;

g) misure, procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra imprese, nel rispetto del diritto dell'Unione;

h) misure volte a rispondere alle esigenze specifiche delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, relativamente a orientamenti e sostegno per rafforzare la loro resilienza alle minacce [...] **informatiche**.

3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. **In tale contesto** gli Stati membri possono escludere **elementi della strategia riguardanti** [...] la sicurezza nazionale.

4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni [....] **cinque** anni sulla base di indicatori chiave di prestazione e, se necessario, le modificano. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) assiste gli Stati membri, su richiesta **di questi ultimi**, nell'elaborazione di una strategia nazionale e di indicatori chiave di prestazione per la relativa valutazione.

Articolo 6

Divulgazione coordinata delle vulnerabilità e registro europeo delle vulnerabilità

1. Ogni Stato membro designa uno dei propri CSIRT di cui all'articolo 9 come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra il soggetto che effettua la segnalazione**, il titolare della potenziale vulnerabilità** e il fabbricante o fornitore di servizi TIC o prodotti TIC. **Qualsiasi persona fisica o giuridica può segnalare, eventualmente in forma anonima, una vulnerabilità ai sensi dell'articolo 4, punto 8, al CSIRT designato. Il CSIRT designato assicura un seguito diligente della segnalazione e la riservatezza dell'identità della persona che segnala la vulnerabilità.** Se la vulnerabilità segnalata [...] **può potenzialmente avere un impatto significativo su soggetti in più di uno Stato membro**, il CSIRT designato di ciascuno Stato membro interessato coopera**, se del caso,** con **altri CSIRT designati nell'ambito del**la rete di CSIRT.

2. L'ENISA elabora e mantiene un registro europeo delle vulnerabilità**, in consultazione con il gruppo di cooperazione**. A tal fine l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati, volti in particolare a consentire ai soggetti essenziali e importanti e ai relativi fornitori di sistemi informatici e di rete di divulgare e registrare**, su base volontaria,** le vulnerabilità **pubblicamente note** presenti nei prodotti TIC o nei servizi TIC, nonché a fornire a tutte le parti interessate l'accesso alle informazioni sulle vulnerabilità contenute nel registro. Il registro contiene, in particolare, informazioni che illustrano la vulnerabilità, i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata, la disponibilità di relative patch e, qualora queste non fossero disponibili, orientamenti **elaborati dalle autorità nazionali competenti o dai CSIRT** rivolti agli utenti dei prodotti e dei servizi vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate. **L'ENISA provvede affinché il registro europeo delle vulnerabilità utilizzi un'infrastruttura di informazione e comunicazione sicura e resiliente.**

Articolo 7

Quadri nazionali di gestione delle crisi di cibersicurezza

1. Ogni Stato membro designa una o più autorità competenti responsabili della gestione delle crisi e degli incidenti **di cibersicurezza** su vasta scala. Gli Stati membri provvedono affinché le autorità competenti dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente. **Gli Stati membri assicurano la coerenza con i quadri esistenti di gestione generale delle crisi.**

2. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva.

3. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza in cui sono stabiliti gli obiettivi e le modalità della gestione delle crisi e degli incidenti di cibersicurezza su vasta scala. Nel piano sono definiti, in particolare, i seguenti elementi:

   a) gli obiettivi delle misure e delle attività nazionali di preparazione;

   b) i compiti e le responsabilità delle autorità nazionali competenti;

   c) le procedure di gestione delle crisi di cibersicurezza**, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi** e i canali di scambio di informazioni;

   d) le misure di preparazione, comprese periodiche esercitazioni e attività di formazione;

   e) le parti pertinenti [...] del settore pubblico e privato e le infrastrutture coinvolte;

   f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno efficace dello Stato membro alla gestione coordinata delle crisi e degli incidenti di cibersicurezza su vasta scala a livello dell'Unione e la sua effettiva partecipazione a tale gestione.

4. Gli Stati membri [...] **informano** [...]la Commissione **della designazione del**le **rispettive** autorità competenti di cui al paragrafo 1 e trasmettono **le pertinenti informazioni relative alle prescrizioni di cui al paragrafo 3 in merito a**i propri piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza [...] entro tre mesi da tali designazioni e dall'adozione di tali piani. Gli Stati membri possono omettere [...] informazioni specifiche se e nella misura in cui ciò sia [...] necessario ai fini della loro sicurezza nazionale **o pubblica oppure a fini di difesa.**

Articolo 8

Autorità nazionali competenti e punti di contatto unici

1. Ogni Stato membro designa una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VI della presente direttiva. Gli Stati membri possono designare a questo scopo una o più autorità esistenti.

2. Le autorità competenti di cui al paragrafo 1 controllano l'applicazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa un punto di contatto unico nazionale in materia di cibersicurezza ("punto di contatto unico"). Se uno Stato membro designa soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico per tale Stato membro.

4. Ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, nonché per garantire la cooperazione intersettoriale con altre autorità nazionali competenti dello stesso Stato membro.

5. Gli Stati membri provvedono affinché le autorità competenti di cui al paragrafo 1 e i punti di contatto unici dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente e conseguire in questo modo gli obiettivi della presente direttiva. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei rappresentanti designati nel gruppo di cooperazione di cui all'articolo 12.

6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'autorità competente designata di cui al paragrafo 1 e il punto di contatto unico designato di cui al paragrafo 3, i rispettivi compiti e qualsiasi ulteriore modifica dei medesimi. Ogni Stato membro rende pubbliche le designazioni. La Commissione pubblica l'elenco dei punti di contatto unici designati.

Articolo 9

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

1. Ogni Stato membro designa uno o più CSIRT conformi ai requisiti di cui all'articolo 10, paragrafo 1, che si occupano almeno dei settori, dei sottosettori o dei soggetti di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita. È possibile istituire un CSIRT all'interno di un'autorità competente di cui all'articolo 8.

2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 10, paragrafo 2. **Nello svolgimento di tali compiti i CSIRT possono dare priorità alla fornitura di determinati servizi a soggetti sulla base di un approccio basato sui rischi.**

3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente per scambiare informazioni con i soggetti essenziali e importanti e con le altre parti interessate pertinenti. A tal fine gli Stati membri provvedono affinché i CSIRT contribuiscano allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 26 con comunità settoriali o intersettoriali fidate di soggetti essenziali e importanti.

5. I CSIRT partecipano [...]**alle attività di apprendimento** tra pari organizzate conformemente all'articolo 16.

6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT di cui all'articolo 13.

7. Gli Stati membri comunicano alla Commissione senza indebiti ritardi i CSIRT designati conformemente al paragrafo 1 e il CSIRT coordinatore designato conformemente all'articolo 6, paragrafo 1, nonché i relativi compiti previsti in relazione ai soggetti di cui agli allegati I e II.

8. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo di CSIRT nazionali.

Articolo 10

Requisiti e compiti dei CSIRT

1. I CSIRT soddisfano i seguenti requisiti:

   a) i CSIRT garantiscono un alto livello di disponibilità dei propri [...] **canali** di comunicazione evitando singoli punti di vulnerabilità (single points of failure) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento. I CSIRT indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;

   b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;

c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

d) i CSIRT dispongono di personale sufficiente a garantirne l'operatività in qualsiasi momento;

e) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi;

f) i CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.

2. I CSIRT svolgono i seguenti compiti:

a) monitorano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale;

b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti, nonché **alle autorità competenti e** alle altre pertinenti parti interessate, in merito a minacce informatiche, vulnerabilità e incidenti;

c) forniscono una risposta agli incidenti;

d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;

e) effettuano **[...]** una scansione proattiva dei sistemi informatici e di rete [...] **per rilevare vulnerabilità con potenziale impatto significativo, a condizione che, in assenza del consenso del soggetto, non avvenga un'intrusione in detti sistemi informatici e di rete né vi siano ripercussioni negative sul loro funzionamento;**

f) partecipano alla rete di CSIRT e, su richiesta, forniscono assistenza reciproca**, secondo le loro capacità e competenze,** agli altri membri della rete.

f bis) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità a norma dell'articolo 6, paragrafo 1, il che prevede, in particolare: facilitare l'interazione tra i soggetti segnalanti, il titolare della potenziale vulnerabilità e il fabbricante o fornitore di prodotti o servizi TIC nei casi in cui ciò sia necessario; individuare e contattare i soggetti interessati; fornire sostegno ai soggetti segnalanti; negoziare i tempi di divulgazione e gestire le vulnerabilità che interessano più organizzazioni (divulgazione coordinata multilaterale di vulnerabilità).

3. I CSIRT instaurano rapporti di cooperazione con i pertinenti attori del settore privato al fine di perseguire meglio gli obiettivi della presente direttiva.

3 bis. I CSIRT possono instaurare rapporti di cooperazione con i CSIRT nazionali di paesi terzi. Nel quadro di tale cooperazione possono scambiarsi informazioni pertinenti, compresi dati personali, in conformità del diritto dell'Unione in materia di protezione dei dati.

4. Al fine di agevolare la cooperazione, i CSIRT promuovono l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la gestione delle crisi di cibersicurezza;

c) la divulgazione coordinata delle vulnerabilità.

Articolo 11

Cooperazione a livello nazionale

1. Se sono separati, le autorità competenti di cui all'articolo 8, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva.

2. Gli Stati membri provvedono affinché le loro autorità competenti o i loro CSIRT ricevano le notifiche in merito agli incidenti, alle minacce informatiche significative e ai quasi incidenti (near miss) trasmesse a norma della presente direttiva. Qualora uno Stato membro decida che i suoi CSIRT non debbano ricevere tali notifiche, a questi ultimi viene dato accesso, nella misura necessaria per lo svolgimento dei loro compiti, ai dati sugli incidenti notificati dai soggetti essenziali o importanti, a norma dell'articolo 20.

3. Ogni Stato membro provvede affinché le sue autorità competenti o i suoi CSIRT informino il suo punto di contatto unico in merito alle notifiche relative agli incidenti, alle minacce informatiche significative e ai quasi incidenti trasmesse a norma della presente direttiva.

4. Nella misura necessaria per l'efficace adempimento dei compiti e degli obblighi stabiliti nella presente direttiva, gli Stati membri provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra le autorità competenti, **i CSIRT,** i punti di contatto unici e le autorità di contrasto, le autorità di protezione dei dati, le autorità [...] **competenti designate** a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] [...] **, le autorità competenti a norma del regolamento di esecuzione (UE) 2019/1583 della Commissione, le autorità nazionali di regolamentazione designate in conformità della direttiva (UE) 2018/1972, le autorità nazionali designate a norma dell'articolo 17 del regolamento (UE) n. 910/2014,** [...] le autorità finanziarie nazionali designate conformemente al regolamento (UE) XXXX/XXXX del Parlamento europeo e del Consiglio [il regolamento DORA], **nonché le autorità competenti designate da altri atti giuridici settoriali dell'Unione**.

5. Gli Stati membri provvedono affinché le loro autorità competenti **a norma della presente direttiva e le autorità competenti designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici]** [...] **si scambino** periodicamente informazioni per quanto riguarda **l'individuazione dei soggetti critici,** [...]i rischi di cibersicurezza, [...] **le minacce e gli incidenti informatici come pure i rischi, le minacce e gli incidenti non informatici** [...] che interessano i soggetti essenziali identificati come critici, **[**o come soggetti equivalenti ai soggetti critici,**]** a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici], nonché [...]le misure adottate [...] in risposta a tali rischi e incidenti. **Gli Stati membri provvedono affinché le autorità competenti a norma della presente direttiva** [...] **e le autorità competenti a norma del regolamento XXXX/XXXX [regolamento DORA], della direttiva (UE) 2018/1972 e del regolamento (UE) n. 910/2014 si scambino periodicamente informazioni pertinenti.**

Per quanto riguarda i prestatori di servizi fiduciari e [...] in particolare [...] nei casi in cui il ruolo di vigilanza sia conferito a un organismo diverso dagli organismi di vigilanza designati a norma del regolamento (UE) n. 910/2014, le autorità nazionali competenti a norma della presente direttiva cooperano strettamente, e in modo tempestivo, scambiando le informazioni pertinenti al fine di assicurare l'efficace vigilanza dei prestatori di servizi fiduciari nonché l'effettivo rispetto, da parte di questi ultimi, delle prescrizioni stabilite nella presente direttiva e nel regolamento [XXXX/XXXX], **e, se del caso, le autorità nazionali competenti a norma della presente direttiva informano senza indebito ritardo l'organismo di vigilanza eIDAS di qualunque minaccia informatica o incidente significativi notificati aventi un impatto sui servizi fiduciari**.

5 bis. [...] Al fine di semplificare la segnalazione degli incidenti, gli Stati membri possono istituire un punto di ingresso unico per tutte le notifiche richieste a norma della presente direttiva nonché del regolamento (UE) 2016/679 e della direttiva 2002/58/CE, se del caso. Gli Stati membri possono utilizzare il punto di ingresso unico per le notifiche richieste a norma di altri atti giuridici settoriali dell'Unione. Tale punto di ingresso unico non pregiudica l'applicazione delle disposizioni del regolamento (UE) 2016/679 e della direttiva 2002/58/CE, in particolare quelle relative alle autorità di controllo indipendenti.

CAPO III

*Cooperazione **dell'UE***

Articolo 12

Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri **nonché** [...] **rafforzare la fiducia** [...], è istituito un gruppo di cooperazione.

2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 6.

3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) **e le autorità competenti designate a norma del regolamento (UE) XXXX/XXXX [il regolamento DORA]** [...] possono partecipare alle attività del gruppo di cooperazione **ai sensi dell'articolo 42, paragrafo 1, del regolamento (UE) XXXX/XXXX [il regolamento DORA].**

   Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori i rappresentanti dei pertinenti portatori di interessi.

   La Commissione ne assicura il segretariato.

4. Il gruppo di cooperazione svolge i seguenti compiti:

   a) fornisce orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva;

   a bis) fornisce orientamenti in relazione allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 5, paragrafo 2, lettera c), e all'articolo 6, paragrafo 1;

b) scambia migliori pratiche e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche;

c) effettua scambi di consulenza e coopera con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza;

d) effettua scambi di consulenza e coopera con la Commissione per quanto riguarda i progetti di atti di esecuzione [...] della Commissione adottati a norma della presente direttiva;

e) scambia migliori pratiche e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione;

e bis) scambia opinioni sull'attuazione della legislazione settoriale che presenta aspetti relativi alla cibersicurezza;

f) discute le relazioni sulle [...]**attività di apprendimento** tra pari di cui all'articolo 16, paragrafo 7;

g) discute **le esperienze** [...] delle attività di vigilanza comuni nei casi transfrontalieri di cui all'articolo 34;

h) fornisce orientamenti strategici alla rete di CSIRT **ed EU–CyCLONe** su specifiche questioni emergenti;

h bis)scambia opinioni sul seguito strategico dato agli incidenti di cibersicurezza su vasta scala sulla base degli insegnamenti tratti dalla rete di CSIRT e da EU-CyCLONe;

i) contribuisce alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolge il personale delle autorità competenti o dei CSIRT degli Stati membri;

j) organizza riunioni congiunte periodiche con le pertinenti parti interessate del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo e raccogliere contributi sulle sfide strategiche emergenti;

k) discute le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA**;**

k bis)istituisce il meccanismo di apprendimento tra pari a norma dell'articolo 16 della presente direttiva.

5. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.

6. Entro il …[24 mesi dopo la data di entrata in vigore della presente direttiva] e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti. Il calendario del primo programma adottato a norma della presente direttiva è allineato a quello dell'ultimo programma adottato a norma della direttiva (UE) 2016/1148.

7. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2.

8. Il gruppo di cooperazione si riunisce periodicamente, almeno una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] al fine di promuovere la cooperazione strategica e **facilitare** lo scambio di informazioni.

Articolo 13

Rete di CSIRT

1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

2. La rete di CSIRT è composta da rappresentanti dei CSIRT degli Stati membri **designati a norma dell'articolo 9** e del CERT-UE. La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e sostiene attivamente la cooperazione fra i CSIRT.

3. La rete di CSIRT svolge i seguenti compiti:

   a) scambia informazioni sulle capacità dei CSIRT;

   b) scambia informazioni pertinenti sugli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità;

b bis)scambia informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza;

b ter)condivide soluzioni tecniche che facilitino la gestione tecnica degli incidenti;

b quater) scambia migliori pratiche, strumenti e processi per quanto riguarda i compiti dei CSIRT;

c) su richiesta di un [...] **membro** della rete di CSIRT potenzialmente interessato da un incidente, scambia e discute informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati;

d) su richiesta di un [...] **membro** della rete di CSIRT, discute e, ove possibile, attua una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

e) fornisce sostegno agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;

f) fornisce assistenza ai CSIRT designati di cui all'articolo 6**,** [...] coopera e **scambia** con essi **le migliori pratiche** per quanto riguarda la gestione della divulgazione coordinata [...] di vulnerabilità che riguardano molteplici fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC stabiliti in Stati membri differenti;

g) discute e individua ulteriori forme di cooperazione operativa, anche in relazione a:

i) categorie di minacce informatiche e incidenti;

ii) preallarmi;

iii) assistenza reciproca;

iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza di cui all'articolo 7, paragrafo 3, **su richiesta di uno Stato membro**;

h) informa il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera g) e, se necessario, chiede orientamenti in merito;

i) fa il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA;

j) su richiesta di un singolo CSIRT, discute le capacità e lo stato di preparazione di tale CSIRT;

k) coopera e scambia informazioni, con i centri operativi di sicurezza regionali e a livello dell'UE, al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce in tutta l'Unione;

l) discute le relazioni sulle [...] **sessioni di apprendimento** tra pari di cui all'articolo 16, paragrafo 7;

m) formula orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

4. Ai fini del riesame di cui all'articolo 35 ed entro il [24 mesi dopo la data di entrata in vigore della presente direttiva], e successivamente ogni due anni, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni sui risultati dell[...]**'apprendimento** tra pari di cui all'articolo 16 effettuate in relazione ai CSIRT nazionali e perseguite nell'ambito di tale articolo, comprese conclusioni e raccomandazioni. Tale relazione è trasmessa anche al gruppo di cooperazione.

5. La rete di CSIRT adotta il proprio regolamento interno.

6. La rete di CSIRT coopera con EU-CyCLONe sulla base di modalità procedurali concordate.

Articolo 14

Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)

1. Al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE, è istituita la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).

2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi **informatiche** degli Stati membri designate conformemente all'articolo 7 [...]. **La Commissione partecipa alle attività della rete in qualità di osservatore.** L'ENISA assicura il segretariato della rete e sostiene lo scambio sicuro di informazioni **, oltre a fornire gli strumenti necessari per sostenere la cooperazione tra gli Stati membri garantendo uno scambio sicuro di informazioni**.

   Ove opportuno, EU-CyCLONe può invitare a partecipare ai suoi lavori i rappresentanti dei pertinenti portatori di interessi.

3. EU-CyCLONe svolge i seguenti compiti:

a) aumenta il livello di preparazione per la gestione di crisi e incidenti **di cibersicurezza** su vasta scala;

b) sviluppa una consapevolezza situazionale [...] in merito a crisi e incidenti **di cibersicurezza** su vasta scala;

b bis)valuta le conseguenze e l'impatto dei pertinenti incidenti di cibersicurezza su vasta scala e propone possibili misure di attenuazione;

c) coordina la gestione degli incidenti e delle crisi **di cibersicurezza** su vasta scala e sostiene il processo decisionale a livello politico in merito a tali incidenti e crisi;

d) **su richiesta di uno Stato membro,** discute i **suoi** piani nazionali di risposta agli incidenti **e alle crisi** di cibersicurezza di cui all'articolo 7, paragrafo [...] **3;**[...]

4. EU-CyCLONe adotta il proprio regolamento interno.

5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito **alla gestione degli incidenti e delle crisi di cibersicurezza su vasta scala** [...], concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti.

6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate.

7. EU CyCLONe presenta al Parlamento europeo e al Consiglio una relazione di valutazione dei suoi lavori entro [24 mesi dalla data di entrata in vigore della presente direttiva].

Articolo 14 bis

Cooperazione internazionale

Ove opportuno l'Unione può concludere accordi internazionali, in conformità all'articolo 218 TFUE, con paesi terzi od organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad alcune delle attività del gruppo di cooperazione, della rete di CSIRT e di EU CyCLONe, conformemente alla normativa dell'Unione in materia di protezione dei dati.

Articolo 15

Relazione sullo stato della cibersicurezza nell'Unione

1. L'ENISA, in collaborazione con la Commissione **e con il gruppo di cooperazione**, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione. **In particolare,** [...]la relazione comprende [...] i seguenti aspetti:

   aa) una valutazione del rischio di cibersicurezza a livello dell'Unione, che tenga conto del panorama delle minacce;

   a) [...] **una valutazione del**lo sviluppo delle capacità di cibersicurezza nei settori pubblico e privato in tutta l'Unione;

   b) [...]

   c) **una valutazione aggregata basata su indicatori quantitativi e qualitativi** in materia [...] di cibersicurezza, che fornisca una **panoramica** [...] del livello di maturità delle capacità di cibersicurezza**, incluse le capacità specifiche per settore**.

2. La relazione contiene raccomandazioni strategiche specifiche per aumentare il livello di cibersicurezza nell'Unione e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881.

Articolo 16

Attività di apprendimento tra pari

1. **Al fine di rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e rafforzare le capacità e le politiche degli Stati membri in materia di cibersicurezza necessarie per un'efficace attuazione della presente direttiva, il gruppo di cooperazione**, **con il sostegno della Commissione e**, previa consultazione [...] dell'ENISA **e, se opportuno, della rete di CSIRT,** ed entro **24 [...]** mesi dall'entrata in vigore della presente direttiva, stabilisce la metodologia [...] **per** un sistema di **apprendimento** [...] tra pari **obiettivo, non discriminatorio ed equo** [...] **concernente l'attuazione della presente direttiva** [...] da parte degli Stati membri. **La partecipazione all'apprendimento tra pari è volontaria.** Il **sistema consiste in cicli di valutazione** [...] condott**i** da esperti [...] di cibersicurezza provenienti da**gli** Stati membri [...] e riguarda [...] **uno o più de**gli aspetti seguenti:

   i) [...]l'attuazione delle prescrizioni in materia di gestione e segnalazione dei rischi di cibersicurezza di cui agli articoli 18 e 20;

   ii) [...]le capacità, comprese le risorse [...] disponibili, e [...]lo svolgimento dei compiti delle autorità nazionali competenti **di cui all'articolo 8, e dei CSIRT di cui all'articolo 9**;

[...]

i**ii**[...]) l'[...]**attuazione** dell'assistenza reciproca di cui all'articolo 34;

iv) l'[...]**attuazione** del quadro di condivisione delle informazioni di cui all'articolo 26 [...].

2. **I criteri sulla base dei quali gli Stati membri designano gli esperti idonei a partecipare ai cicli di apprendimento tra pari sono** [...] obiettivi, non discriminatori ed equi [...] **e sono inclusi nella metodologia di cui al paragrafo 1**. L'ENISA e la Commissione [...] **possono** designare esperti che partecipano [...] **ai cicli di apprendimento tra pari** in qualità di osservatori. [...]

3. [...] .

3 bis. Prima dell'inizio dei cicli di apprendimento tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti contemplati da quel particolare ciclo di apprendimento tra pari e fornire tale autovalutazione agli esperti designati di cui al paragrafo 2.

4. [...] **Le attività di apprendimento** tra pari **possono**comporta[...]**re** visite in loco [...] **in presenza** o virtuali e scambi a distanza. In virtù del principio di buona collaborazione, gli Stati membri [...] **che partecipano all'apprendimento tra pari** forniscono agli esperti designati le informazioni [...] necessarie per la valutazione [...]**, fatte salve le legislazioni nazionali o dell'Unione in materia di protezione di informazioni riservate o classificate o di salvaguardia delle funzioni essenziali dello Stato, quali la sicurezza nazionale**. Le informazioni ottenute mediante il processo di [...] **apprendimento** tra pari sono utilizzate unicamente a tal fine. Gli esperti che partecipano all[...]**'apprendimento** tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute [...] **in** tale [...] **contesto**. **Lo Stato membro che partecipa all'apprendimento tra pari può opporsi alla designazione di particolari esperti per motivi debitamente giustificati comunicati al gruppo di cooperazione.**

5. Una volta che sono stati **oggetto di un ciclo di apprendimento tra pari** [...], i medesimi aspetti non sono più soggetti a ulteriori [...] **cicli di apprendimento**tra pari [...] **per gli** Stat**i** membr**i partecipanti** nei [...] **quattro** anni successivi alla conclusione di tale [...] **ciclo di apprendimento tra pari**, a meno che **lo Stato membro interessato non lo richieda o non concordi con la proposta** [...] del gruppo di cooperazione [...].

6. [...]

7. Gli esperti che partecipano a[...]**i cicli di apprendimento** tra pari elaborano relazioni sui risultati e sulle conclusioni delle [...] **valutazioni**. **Gli Stati membri sono autorizzati a formulare osservazioni sui rispettivi progetti di relazione, che sono allegati alla relazione.** Le relazioni **finali** sono trasmesse [...] al gruppo di cooperazione. **Gli Stati membri possono decidere di rendere pubbliche le rispettive relazioni**.

CAPO IV

Obblighi di gestione e segnalazione dei rischi di cibersicurezza

SEZIONE I

Gestione e segnalazione dei rischi di cibersicurezza

Articolo 17

Governance

1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti al fine di conformarsi all'articolo 18, [...] **sovraintendano alla sua** attuazione e [...] **possano essere** ritenuti responsabili in caso di mancato rispetto, da parte dei soggetti, degli obblighi di cui al presente articolo.

   L'applicazione del presente paragrafo lascia impregiudicate le legislazioni nazionali degli Stati membri per quanto riguarda le norme in materia di responsabilità nelle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti e nominati.

2. Gli Stati membri provvedono affinché i **membri dell'organo di gestione siano tenuti a** segu**ire**[...] periodicamente attività di formazione [...] al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi di cibersicurezza e le relative pratiche di gestione e il loro impatto sulle attività del soggetto.

Articolo 18

Misure di gestione dei rischi di cibersicurezza

1 **bis. La presente direttiva applica un approccio "multirischio" che comprende la protezione dei sistemi informatici e di rete e del loro ambiente fisico da qualsiasi evento che possa compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.**

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nella fornitura dei loro servizi. Tenuto conto delle conoscenze più aggiornate in materia **e del costo di attuazione**, tali misure assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio esistente. **Nel valutare la proporzionalità di tali misure si tiene debitamente conto del grado di esposizione del soggetto ai rischi, delle sue dimensioni, della probabilità che si verifichino incidenti e della loro gravità. Tenuto conto del livello e del tipo di rischio per la società in caso di incidenti che interessano soggetti essenziali o importanti, le misure di gestione dei rischi di cibersicurezza imposte ai soggetti importanti possono essere meno rigorose di quelle imposte ai soggetti essenziali.**

2. Le misure di cui al paragrafo 1 comprendono almeno i seguenti elementi:

a) analisi dei rischi e politiche di sicurezza dei sistemi informatici;

b) gestione degli incidenti (prevenzione e rilevamento degli incidenti, [...] risposta agli **incidenti e recupero dagli incidenti**);

c) continuità operativa e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi **diretti** fornitori o fornitori di servizi, quali i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure [...] per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) **strategie relative all'** uso della crittografia e della cifratura;

g bis) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi.

3. Gli Stati membri provvedono affinché, nel prendere in considerazione le misure adeguate di cui al paragrafo 2, lettera d), i soggetti [...] **siano tenuti a tenere** conto delle vulnerabilità specifiche per ogni **diretto** fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. **Gli Stati membri provvedono inoltre affinché, nel prendere in considerazione le misure adeguate di cui al paragrafo 2, lettera d), i soggetti siano tenuti a tenere conto dei risultati delle valutazioni dei rischi coordinate effettuate conformemente all'articolo 19, paragrafo 1.**

4. Gli Stati membri provvedono affinché, qualora un soggetto rilevi che i suoi servizi o i suoi compiti non rispettano le prescrizioni di cui al paragrafo 2, tale soggetto adotti, senza indebito ritardo, tutte le misure correttive necessarie a rendere conforme il servizio interessato.

5. La Commissione può adottare atti di esecuzione al fine di stabilire le specifiche tecniche e metodologiche**, nonché le specifiche settoriali, ove necessario,** relative agli elementi di cui al paragrafo 2. **Entro [18 mesi dall'entrata in vigore della presente direttiva] la Commissione adotta atti di esecuzione al fine di stabilire le specifiche tecniche e metodologiche per i soggetti di cui all'articolo 24, paragrafo 1, e per i prestatori di servizi fiduciari di cui all'allegato I, punto 8. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2.** Nell'elaborare tali atti **di esecuzione** la Commissione [...] segue, nella maggior misura possibile, le norme internazionali ed europee, nonché le pertinenti specifiche tecniche **e procede a consultare il gruppo di cooperazione e l'ENISA in merito ai progetti di atti di esecuzione conformemente all'articolo 12, paragrafo 4, lettera d).**

6. [...]

Articolo 19

Valutazioni dei rischi coordinate a livello dell'UE delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi, sistemi o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, identifica i servizi, i sistemi o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata dei rischi di cui al paragrafo 1.

Articolo 20

Obblighi di segnalazione

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT, conformemente ai paragrafi 3 e 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi. Se opportuno, tali soggetti notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti che possono ripercuotersi negativamente sulla fornitura di tali servizi. Gli Stati membri provvedono affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta alle autorità competenti o al CSIRT di determinare l'eventuale impatto transfrontaliero dell'incidente. **L'atto della notifica non espone di per sé il soggetto che la effettua a una maggiore responsabilità.**

2. [...]

   Se opportuno, [...] **i soggetti essenziali e importanti** notificano senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia. Se opportuno, i soggetti notificano a tali destinatari anche la minaccia stessa. **L'atto del**la notifica non espone **di per sé** il soggetto che la effettua a una maggiore responsabilità.

3. Un incidente è considerato significativo se:

a) ha causato o può causare una perturbazione operativa **del servizio** o perdite finanziarie **di grave entità** per il soggetto interessato;

b) si è ripercosso o può ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano alle autorità competenti o al CSIRT:

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, una notifica iniziale **di preallarme** che, se opportuno, indichi se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola;

b) su richiesta di un'autorità competente o di un CSIRT, una relazione intermedia sui pertinenti aggiornamenti della situazione;

c) una relazione **finale** entro un mese dalla trasmissione della notifica **iniziale** di cui alla lettera a), che comprenda almeno:

i) una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

iii) le misure di attenuazione adottate e in corso.

Gli Stati membri dispongono che, in casi debitamente giustificati e con l'accordo delle autorità competenti o del CSIRT, il soggetto interessato possa derogare alle scadenze di cui alle lettere a) e c). **In particolare, una deroga alla scadenza di cui alla lettera c) può essere giustificata nei casi in cui l'incidente sia ancora in corso.**

5. [...] **Senza indebito ritardo** dal ricevimento della notifica iniziale di cui al paragrafo 4, lettera a), le autorità nazionali competenti o il CSIRT forniscono una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente e, su richiesta del soggetto, orientamenti sull'attuazione di possibili misure di attenuazione. Se il CSIRT non ha ricevuto la notifica di cui al paragrafo 1, gli orientamenti sono forniti dall'autorità competente in collaborazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente abbia carattere criminale, le autorità nazionali competenti o il CSIRT forniscono anche orientamenti sulla segnalazione dell'incidente alle autorità di contrasto.

6. Se opportuno, e in particolare se l'incidente di cui al paragrafo 1 interessa due o più Stati membri, l'autorità competente**,** [...]il CSIRT **o il punto di contatto unico** ne informa gli altri Stati membri interessati e l'ENISA. **Tali informazioni comprendono almeno gli elementi di cui al paragrafo 4.** Nel farlo le autorità competenti, i CSIRT e i punti di contatto unici tutelano, in conformità al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite.

7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente o affrontare un incidente in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato l'autorità competente o il CSIRT e, se opportuno, le autorità o i CSIRT degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente o imporre al soggetto di farlo.

8. Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico inoltra le notifiche ricevute a norma de**l** paragraf**o** 1 [...] ai punti di contatto unici degli altri Stati membri interessati.

9. **Ogni sei mesi i**l punto di contatto unico trasmette [...] all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti, sulle minacce informatiche significative e sui quasi incidenti notificati conformemente a**l** paragraf**o** 1 e all'articolo 27. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può pubblicare orientamenti tecnici sui parametri delle informazioni incluse nella relazione di sintesi. **Ogni sei mesi l'ENISA informa il gruppo di cooperazione e la rete di CSIRT delle sue constatazioni in merito alle notifiche ricevute.**

10. Le autorità competenti forniscono alle autorità competenti designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] le informazioni sugli incidenti e sulle minacce informatiche notificati conformemente ai paragrafi 1 e 2 dai soggetti essenziali identificati come soggetti critici **[**o come soggetti equivalenti ai soggetti critici**]** a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici].

11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma dei paragrafi 1 e 2. La Commissione può anche adottare atti di esecuzione al fine di specificare ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2.

Articolo 21

Uso dei sistemi europei di certificazione della cibersicurezza

1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 18, **gli Stati membri possono imporre ai soggetti di utilizzare particolari prodotti** [...], **servizi** [...] **e processi TIC certificati** nell'ambito di specifici sistemi europei di certificazione della cibersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. I prodotti, i servizi e i processi **TIC** soggetti a certificazione possono essere sviluppati da un soggetto essenziale o importante o acquistati da terze parti.

2. La Commissione [...] **può** adottare atti [...] **di esecuzione** che specifichino quali categorie di soggetti essenziali **o importanti** sono tenute **a utilizzare determinati prodotti, servizi o processi TIC oppure a** ottenere un certificato [...] nell'ambito [...] **dei** sistemi europei di certificazione della cibersicurezza **adottati a norma dell'articolo 49 del regolamento (UE) 2019/881**. [...] **Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2. Conformemente all'articolo 56 del regolamento (UE) 2019/881, nell'elaborare tali atti di esecuzione la Commissione:**

   i) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti, servizi o processi TIC e sugli utenti in termini di costi di tali misure nonché i benefici sociali o economici derivanti dal previsto aumento del livello di sicurezza per i prodotti, i servizi o i processi TIC in questione, nonché la disponibilità di alternative agli stessi sul mercato;

   ii) procede a un processo di consultazione aperto, trasparente e inclusivo con tutti i pertinenti portatori di interessi e gli Stati membri;

(iii) **prende in considerazione le scadenze di attuazione, le misure transitorie e i periodi di transizione, in particolare con riferimento al possibile impatto delle misure sui fornitori o fabbricanti di prodotti, servizi o processi TIC, in particolare le PMI;**

(iv) **tiene conto dell'esistenza e dell'attuazione della normativa degli Stati membri e dei paesi terzi in materia.**

3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2, la Commissione può chiedere all'ENISA di preparare una proposta di sistema **o di rivedere un sistema europeo di certificazione della cibersicurezza esistente** a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.

Articolo 22

Normazione

1. Per promuovere l'attuazione convergente dell'articolo 18, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza dei sistemi informatici e di rete.

2. L'ENISA, in collaborazione con gli Stati membri, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali degli Stati membri, che potrebbero essere applicate a tali settori.

Articolo 23

Banche dati di nomi di dominio e dati di registrazione

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri provvedono affinché i registri dei **nomi di dominio di primo livello (**TLD**)** e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD raccolgano e mantengano dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati [...] **con la dovuta diligenza conformemente** al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali.

2. Gli Stati membri provvedono affinché le banche dati dei dati di registrazione dei nomi di dominio di cui al paragrafo 1 contengano le informazioni pertinenti per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD**, tra cui almeno i dati seguenti:**

   a) nome di dominio;

   b) data di registrazione;

   c) dati del registrante, compresi:

      i) per le persone fisiche – nome, cognome e indirizzo e-mail;

      ii) per le persone giuridiche – nome e indirizzo e-mail.

3. Gli Stati membri provvedono affinché i registri dei **nomi di dominio di primo livello (**TLD**)** e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD predispongano politiche e procedure per garantire che le banche dati comprendano informazioni accurate e complete. Gli Stati membri provvedono affinché tali politiche e procedure siano rese pubbliche.

4. Gli Stati membri provvedono affinché i registri dei **nomi di dominio di primo livello (**TLD**)** e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD pubblichino, senza indebito ritardo dopo la registrazione di un nome di dominio, i dati di registrazione del dominio che non sono dati personali.

5. Gli Stati membri provvedono affinché i registri dei **nomi di dominio di primo livello (**TLD**)** e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD, su richiesta legittima e debitamente giustificata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri provvedono affinché i registri dei **nomi di dominio di primo livello (**TLD**)** e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rispondano senza indebito ritardo **e in ogni caso entro 72 ore** a tutte le richieste di accesso. Gli Stati membri provvedono affinché le politiche e le procedure di divulgazione di tali dati siano rese pubbliche.

Sezione II

Giurisdizione e registrazione

Articolo 24

Giurisdizione e territorialità

1 bis. I soggetti a norma della presente direttiva sono considerati sotto la giurisdizione dello Stato membro in cui prestano i propri servizi. I soggetti di cui ai punti da 1 a 7 e al punto 10 dell'allegato I, i prestatori di servizi fiduciari e i fornitori di punti di interscambio Internet di cui al punto 8 dell'allegato I e i soggetti di cui ai punti da 1 a 5 dell'allegato II sono considerati sotto la giurisdizione dello Stato membro nel cui territorio sono stabiliti.

1. I fornitori di servizi DNS, i registri dei nomi di dominio di primo livello (TLD) **e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD,** i fornitori di servizi di cloud computing, i fornitori di servizi di data center**,** [...] i fornitori di reti di distribuzione dei contenuti **i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti**di cui all'allegato I, punt**i** 8 **e 8 bis**, nonché i fornitori di servizi digitali di cui all'allegato II, punto 6, sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione.

2. Ai fini della presente direttiva, i soggetti di cui al paragrafo 1 sono considerati avere il loro stabilimento principale nell'Unione nello Stato membro in cui sono **prevalentemente** adottate le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Se **il luogo in cui tali decisioni sono prevalentemente adottate non può essere determinato o se** tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui i soggetti hanno lo stabilimento con il maggior numero di dipendenti nell'Unione. **Qualora i servizi siano forniti da un gruppo di imprese, lo stabilimento principale è considerato essere lo stabilimento principale del gruppo di imprese.**

3. Se un soggetto di cui al paragrafo 1 non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante designato nell'Unione a norma del presente articolo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per mancato rispetto degli obblighi di cui alla presente direttiva.

4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1 fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.

4 bis. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione ai soggetti di cui al paragrafo 1 possono, entro i limiti della richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che ha il sistema informatico e di rete nel loro territorio.

Articolo 25

Registro di determinati soggetti di infrastrutture digitali e fornitori di servizi digitali

1. [...] **Gli Stati membri provvedono affinché i** [...] soggetti **di cui all'articolo 24, paragrafo 1, che hanno lo stabilimento principale nel loro territorio o, qualora non siano stabiliti nell'Unione, il cui rappresentante designato nell'Unione è stabilito nel loro territorio siano tenuti a trasmettere** [...] le informazioni seguenti [...] **alle autorità competenti** entro il [12 mesi dopo l'entrata in vigore della presente direttiva]:

a) il proprio nome;

a bis) il tipo di soggetto conformemente agli allegati I e II della presente direttiva;

b) l'indirizzo del proprio stabilimento principale e degli altri stabilimenti legali nell'Unione o, se non sono stabiliti nell'Unione, del proprio rappresentante a norma dell'articolo 24, paragrafo 3;

c) i propri dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono**, nonché dei loro rappresentanti;**

d) gli Stati membri in cui il soggetto fornisce il servizio.

Se del caso, tali informazioni sono trasmesse tramite il meccanismo nazionale [...] di autonotifica di cui all'articolo 2 bis.

2. **Gli Stati membri provvedono affinché i** [...] soggetti di cui al paragrafo 1 **notifichino anche** [...] qualsiasi modifica delle informazioni trasmesse a norma del paragrafo 1 tempestivamente, e in ogni caso entro tre mesi dalla data in cui è avvenuta la modifica.

3. [...] **I punti di contatto unici degli Stati membri inoltrano le informazioni di cui ai paragrafi 1 e 2 all'ENISA.** [...]

3 bis. Sulla base delle informazioni ricevute in conformità del paragrafo 3, l'ENISA crea e mantiene un registro dei soggetti di cui al paragrafo 1. Su richiesta degli Stati membri, l'ENISA consente alle pertinenti autorità competenti di accedere al registro, provvedendo nel contempo alle garanzie necessarie per tutelare la riservatezza delle informazioni, se del caso.

4. [...]

CAPO V

Condivisione delle informazioni

Articolo 26

Accordi di condivisione delle informazioni sulla cibersicurezza

1. [...] Gli Stati membri provvedono affinché i soggetti essenziali e importanti possano scambiarsi**, su base volontaria,** pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, **quasi incidenti,** vulnerabilità, indicatori di compromissione, tattiche, tecniche e procedure, allarmi di cibersicurezza e strumenti di configurazione, se tale condivisione di informazioni:

   a) mira a prevenire, rilevare o attenuare gli incidenti o a rispondervi;

b) aumenta il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento delle minacce, strategie di attenuazione o fasi di risposta e recupero.

2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità [...] di soggetti essenziali e importanti. Tale scambio è attuato mediante accordi di condivisione delle informazioni che tengono conto della natura potenzialmente sensibile delle informazioni condivise [...].

3. Gli Stati membri [...] **possono stabilire** norme che specificano la procedura, gli elementi operativi (compreso l'uso di piattaforme TIC dedicate), i contenuti e le condizioni degli accordi di condivisione delle informazioni di cui al paragrafo 2. Tali norme [...] **possono stabilire** anche i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, nonché agli elementi operativi, compreso l'uso di piattaforme informatiche dedicate. Gli Stati membri offrono sostegno all'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 5, paragrafo 2, lettera g).

4. I soggetti essenziali e importanti notificano alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. [...] **L**'ENISA sostiene la conclusione di accordi per la condivisione delle informazioni di cibersicurezza di cui al paragrafo 2 fornendo orientamenti e migliori pratiche.

Articolo 27

Notifica volontaria di informazioni pertinenti

1. Fatto salvo l'articolo 20, gli Stati membri provvedono affinché i soggetti essenziali e importanti possano notificare, su base volontaria, alle autorità competenti o ai CSIRT eventuali incidenti, minacce informatiche o quasi incidenti rilevanti.

2. Gli Stati membri provvedono affinché, fatto salvo l'articolo 3, i soggetti che non rientrano nell'ambito di applicazione della presente direttiva possano trasmettere, su base volontaria, notifiche di incidenti significativi, minacce informatiche o quasi incidenti. Nel trattamento delle notifiche gli Stati membri agiscono secondo la procedura di cui all'articolo 20. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie. **Fatti salvi l'indagine, l'accertamento e il perseguimento dei reati,** [...] **l**a segnalazione volontaria non ha l'effetto di imporre al soggetto che la effettua alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

3. Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo per lo Stato membro interessato.

CAPO VI

Vigilanza ed esecuzione

Articolo 28

Aspetti generali relativi alla vigilanza e all'esecuzione

1. Gli Stati membri provvedono affinché le autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva, in particolare degli obblighi di cui agli articoli 18**,** [...] 20 **e 23**. **Gli Stati membri possono consentire alle autorità competenti di dare priorità alla vigilanza, che si basa su un approccio basato sui rischi.**

2. Nei casi di incidenti di cibersicurezza le autorità competenti operano in stretta cooperazione con le autorità di protezione dei dati**, con le autorità competenti designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici], con gli organismi di vigilanza designati a norma del regolamento (UE) n. 910/2014 e con le altre autorità competenti designate a norma di atti giuridici settoriali dell'Unione**. [...]

3. Fatti salvi i quadri istituzionali e legislativi nazionali, gli Stati membri provvedono affinché nel vigilare sul rispetto, da parte degli enti della pubblica amministrazione, della presente direttiva e nell'applicare potenziali sanzioni in caso di inosservanza, le autorità competenti dispongano dei poteri adeguati per svolgere tali compiti con indipendenza operativa rispetto agli enti sottoposti a vigilanza. Gli Stati membri possono decidere di imporre misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti conformemente all'ordinamento giuridico e ai quadri nazionali.

Articolo 29

Vigilanza ed esecuzione per i soggetti essenziali

1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, **seguano un approccio basato sui rischi e** abbiano il potere di sottoporre tali soggetti **come minimo** a:

   a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali;

   b) audit **sulla sicurezza** periodici;

   c) audit sulla sicurezza mirati, basati su valutazioni dei rischi o sulle informazioni disponibili relative ai rischi;

   d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti**, se necessario per motivi tecnici, con la cooperazione del soggetto interessato**;

   e) richieste di informazioni necessarie a valutare le misure di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate[...];

   f) richieste di accesso a dati, documenti o altre informazioni necessari allo svolgimento dei compiti di vigilanza;

   g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

2 bis. Nell'esercizio dei rispettivi compiti di vigilanza di cui al paragrafo 2 del presente articolo, le autorità competenti possono stabilire metodologie di vigilanza che consentono di conferire priorità a tali compiti secondo un approccio basato sui rischi.

3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettere da e) a g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere **come minimo** di:

   a) emanare avvertimenti relativi al mancato rispetto, da parte dei soggetti, degli obblighi stabiliti dalla presente direttiva;

   b) emanare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi stabiliti dalla presente direttiva;

   c) imporre a tali soggetti di porre termine al comportamento che non è conforme agli obblighi stabiliti dalla presente direttiva e di astenersi dal ripeterlo;

   d) imporre a tali soggetti di rendere le loro misure di gestione dei rischi e/o i loro obblighi di segnalazione conformi alle prescrizioni di cui agli articoli 18 e 20 in una maniera ed entro un termine specificati;

   e) imporre a tali soggetti di informare le persone fisiche o giuridiche cui forniscono servizi o attività potenzialmente interessati da una minaccia informatica significativa in merito **alla natura della minaccia e** alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

   f) imporre a tali soggetti di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

   g) [...]

h) imporre a tali soggetti di rendere pubblici gli aspetti di mancato rispetto degli obblighi stabiliti dalla presente direttiva in una maniera specificata**, quando tale divulgazione pubblica non comporta un'esposizione pericolosa del rispettivo soggetto**;

i) [...]

j) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di una sanzione amministrativa pecuniaria a norma dell'articolo 31, in aggiunta alle misure di cui al presente paragrafo, lettere da a) a i), o in luogo di tali misure, a seconda delle circostanze di ciascun singolo caso.

5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le autorità competenti abbiano il potere di:

a) sospendere o chiedere a un organismo di certificazione o autorizzazione, **o agli organi giurisdizionali secondo le legislazioni nazionali,** di sospendere un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività forniti da un soggetto essenziale;

b) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di un divieto temporaneo nei confronti di qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale, e di qualsiasi altra persona fisica ritenuta responsabile della violazione, di svolgere funzioni dirigenziali in tale soggetto.

Tali sanzioni sono applicate solo finché il soggetto non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le sanzioni sono state applicate.

Le sanzioni di cui al presente paragrafo non si applicano agli enti della pubblica amministrazione soggetti alla presente direttiva.

6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia i poteri per garantirne il rispetto degli obblighi stabiliti dalla presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto degli obblighi stabiliti dalla presente direttiva. **Per quanto riguarda gli enti della pubblica amministrazione, la presente disposizione lascia impregiudicate le legislazioni degli Stati membri in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti e nominati.**

7. Nell'adottare qualsiasi misura di esecuzione o nell'applicare qualsiasi sanzione a norma dei paragrafi 4 e 5, le autorità competenti rispettano i diritti di difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

   a) la gravità della violazione e l'importanza delle disposizioni non rispettate. Tra le violazioni che dovrebbero essere considerate gravi rientrano: le violazioni ripetute, la mancata notifica di incidenti con un effetto negativo rilevante o il mancato rimedio a tali incidenti, il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti, l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione e la fornitura di informazioni false o gravemente inesatte relative agli obblighi di gestione o segnalazione dei rischi di cui agli articoli 18 e 20;

b) la durata della violazione, compreso l'aspetto relativo alla reiterazione delle violazioni;

c) il danno effettivamente causato o le perdite effettivamente subite, oppure il danno o le perdite potenziali che si sarebbero potuti verificare, nella misura in cui possono essere determinati. Nel valutare tale aspetto si tiene conto, tra l'altro, delle perdite finanziarie o economiche effettive o potenziali, degli effetti sugli altri servizi e del numero di utenti interessati o potenzialmente interessati;

d) il carattere doloso o colposo della violazione;

e) le misure adottate dal soggetto per prevenire o attenuare il danno e/o le perdite;

f) il rispetto dei codici di condotta o dei meccanismi di certificazione approvati;

g) il livello di cooperazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti.

8. Le autorità competenti espongono nei particolari la motivazione delle loro decisioni di esecuzione. Prima di adottare tali decisioni le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari e concedono a tali soggetti un tempo ragionevole per presentare osservazioni**, salvo in caso di pericolo imminente**.

9. Gli Stati membri provvedono affinché le loro autorità competenti **a norma della presente direttiva** informino le autorità competenti pertinenti **nello stesso** [...] Stato membro [...] designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto essenziale identificato come critico **[**o come soggetto equivalente a un soggetto critico**]** a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici]. **Ove opportuno,** [...] le autorità competenti a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] [...] **possono chiedere alle** autorità competenti **a norma della presente direttiva** [...] **di** esercitare i propri **poteri** di vigilanza ed esecuzione **nei confronti di** un soggetto essenziale rientrante nell'ambito di applicazione della presente direttiva anch'esso identificato come critico **[**o equivalente**]** **a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici].**

10. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza a norma dell'articolo 29, paragrafo 1, del regolamento (UE) XXXX/XXXX [DORA] quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto essenziale designato come un fornitore terzo di servizi di TIC critico a norma dell'articolo 28 del regolamento (UE) XXXX/XXXX [DORA].

10 bis. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino le autorità competenti pertinenti designate a norma del regolamento (UE) n. 910/2014 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto designato come prestatori di servizi fiduciari a norma del regolamento (UE) n. 910/2014.

Articolo 30

Vigilanza ed esecuzione per i soggetti importanti

1. Se ricevono elementi di prova**,** indicazioni **o informazioni** secondo cui un soggetto importante non rispetta **presumibilmente** gli obblighi stabiliti dalla presente direttiva, in particolare dagli articoli 18 e 20, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, **seguano un approccio basato sui rischi e** abbiano il potere di sottoporre tali soggetti **come minimo** a:

   a) ispezioni in loco e vigilanza ex post a distanza;

   b) audit sulla sicurezza mirati, basati su valutazioni dei rischi o sulle informazioni disponibili relative ai rischi;

   c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, **non discriminatori,** equi e trasparenti**, se necessario per motivi tecnici, con la cooperazione del soggetto interessato**;

   d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di cibersicurezza[...];

   e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei compiti di vigilanza;

   e bis) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

2 bis. Nell'esercizio dei rispettivi compiti di vigilanza di cui al paragrafo 2 del presente articolo, le autorità competenti possono stabilire metodologie di vigilanza che consentono di conferire priorità a tali compiti secondo un approccio basato sui rischi.

3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere **da** d) **a e bis)**, le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere **come minimo** di:

   a) emanare avvertimenti relativi al mancato rispetto, da parte dei soggetti, degli obblighi stabiliti dalla presente direttiva;

   b) emanare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alla violazione degli obblighi stabiliti dalla presente direttiva;

   c) imporre a tali soggetti di porre termine al comportamento che non rispetta gli obblighi stabiliti dalla presente direttiva e di astenersi dal ripeterlo;

   d) imporre a tali soggetti di rendere le loro misure di gestione dei rischi o i loro obblighi di segnalazione conformi alle prescrizioni di cui agli articoli 18 e 20 in una maniera ed entro un termine specificati;

   e) imporre a tali soggetti di informare le persone fisiche o giuridiche cui forniscono servizi o attività potenzialmente interessati da una minaccia informatica significativa in merito **alla natura della minaccia e** alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

   f) imporre a tali soggetti di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) imporre a tali soggetti di rendere pubblici gli aspetti di mancato rispetto degli obblighi stabiliti dalla presente direttiva in una maniera specificata**, quando tale divulgazione pubblica non comporta un'esposizione pericolosa del rispettivo soggetto**;

h) [...]

i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di una sanzione amministrativa pecuniaria a norma dell'articolo 31, in aggiunta alle misure di cui al presente paragrafo, lettere da a) a h), o in luogo di tali misure, a seconda delle circostanze di ciascun singolo caso.

5. L'articolo 29, paragrafi da 6 a 8, si applica anche alle misure di vigilanza ed esecuzione di cui al presente articolo per i soggetti importanti [...].

Articolo 31

Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni degli obblighi stabiliti dalla presente direttiva siano, in ciascun singolo caso, effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono imposte, a seconda delle circostanze di ciascun singolo caso, in aggiunta alle misure di cui all'articolo 29, paragrafo 4, lettere da a) a i), all'articolo 29, paragrafo 5, e all'articolo 30, paragrafo 4, lettere da a) a h), o in luogo di tali misure.

3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 29, paragrafo 7.

4. Gli Stati membri provvedono affinché le violazioni degli obblighi di cui all'articolo 18 o all'articolo 20 **da parte di soggetti essenziali** siano soggette, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni amministrative pecuniarie pari a un massimo di almeno **4**[...] 000 000 EUR o**, nel caso di una persona giuridica,** [...] al 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale [...] appartiene, se tale importo è superiore.

4 bis. Gli Stati membri provvedono affinché le violazioni degli obblighi di cui all'articolo 18 o all'articolo 20 da parte di soggetti importanti siano soggette, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni amministrative pecuniarie pari a un massimo di almeno 2 000 000 EUR o, nel caso di una persona giuridica, all'1 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

5. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione conformemente a una precedente decisione dell'autorità competente.

6. Fatti salvi i poteri delle autorità competenti a norma degli articoli 29 e 30, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione di cui all'articolo 4, punto 23, soggetti agli obblighi previsti dalla presente direttiva.

6 bis. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, gli Stati membri provvedono affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il [...] e comunicano sollecitamente ogni successiva modifica.

Articolo 32

Violazioni che comportano una violazione dei dati personali

1. Qualora le autorità competenti**, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto** che la violazione degli obblighi di cui agli articoli 18 e 20 **della presente direttiva** da parte di un soggetto essenziale o importante **possa** comporta**re** una violazione dei dati personali, quale definita all'articolo 4, punto 12, del regolamento (UE) 2016/679, che deve essere notificata a norma dell'articolo 33 del medesimo regolamento, ne informano**, senza indebito ritardo,** le autorità di controllo competenti a norma degli articoli 55 e 56 di tale regolamento [...].

2. Qualora le autorità di controllo competenti conformemente agli articoli 55 e 56 del regolamento (UE) 2016/679 decidano di esercitare i propri poteri a norma dell'articolo 58**, paragrafo 2**, lettera i), del medesimo regolamento e di imporre una sanzione amministrativa pecuniaria, le autorità competenti **di cui all'articolo 8 della presente direttiva** non impongono una sanzione amministrativa pecuniaria per **una** [...] violazione **mediante lo stesso atto** [...] **dell'**articolo 31 della presente direttiva. Le autorità competenti possono tuttavia applicare le misure di esecuzione o esercitare i poteri sanzionatori di cui all'articolo 29, paragrafo 4, lettere da a) a i), all'articolo 29, paragrafo 5, e all'articolo 30, paragrafo 4, lettere da a) ad h), della presente direttiva.

3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto all'autorità competente, l'autorità competente può informare l'autorità di controllo stabilita nello stesso Stato membro.

Articolo 33

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni nazionali adottate a norma della presente direttiva e adottano tutte le misure necessarie per assicurarne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive.

2. Gli Stati membri notificano tali norme e misure alla Commissione, entro [due] anni dall'entrata in vigore della presente direttiva, e provvedono poi a dare notifica, senza indebito ritardo, delle eventuali modifiche successive.

Articolo 34

Assistenza reciproca

1. Se un soggetto essenziale o importante fornisce servizi in più di uno Stato membro o [...] **fornisce servizi** in **uno o più** Stat**i** membr**i**, ma i suoi sistemi informatici e di rete sono ubicati in uno o più altri Stati membri, l**e** autorità competent**i** de**gli** Stat**i** membr**i** **interessati** [...] cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti:

a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate [...];

b) un'autorità competente può chiedere a un'altra autorità competente di adottare le misure di vigilanza o esecuzione [...];

c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente **un'**assistenza **proporzionata alle risorse a sua disposizione** affinché le misure di vigilanza o esecuzione [...] possano essere attuate in maniera efficace, efficiente e coerente. Tale assistenza reciproca può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che, a seguito di uno scambio con le altre autorità interessate, [...] non sia stabilito che l'autorità non è competente per fornire l'assistenza richiesta **o non dispone delle risorse necessarie,** o che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente [...] **, o che la richiesta riguarda informazioni o comporta attività che sono in contrasto con la sicurezza nazionale, la sicurezza pubblica o la difesa di detto Stato membro**.

2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza comuni [...].

CAPO VII

Disposizioni transitorie e finali

Articolo 35

Riesame

La Commissione riesamina periodicamente il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza dei settori, dei sottosettori, delle dimensioni e dei tipi di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. **Ai** fin**i** [...] **del riesame**, [...] la Commissione tiene conto delle relazioni [...] della rete di CSIRT sull'esperienza acquisita a livello [...] operativo. La prima relazione è presentata entro il … [54 mesi dopo la data di entrata in vigore della presente direttiva].

Articolo 36

[...]

[...]

[...]

Articolo 37

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

Articolo 38

Recepimento

1. **Entro** ... [[...] **24** mesi dalla data di entrata in vigore della presente direttiva**],** gli Stati membri adottano e pubblicano [...] le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione. Essi applicano tali disposizioni a decorrere dal … [un giorno dopo la data di cui al primo comma].

2. Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 39

Modifica del regolamento (UE) n. 910/2014

Nel regolamento (UE) n. 910/2014, l'articolo 19 [...] è soppresso **a decorrere dal ... [termine per il recepimento della presente direttiva].**

Articolo 40

Modifica della direttiva (UE) 2018/1972

Nella direttiva (UE) 2018/1972, gli articoli 40 e 41 [...] sono soppressi **a decorrere dal ... [termine per il recepimento della presente direttiva].**

Articolo 41

Abrogazione

La direttiva (UE) 2016/1148 è abrogata a decorrere dal ... [termine per il recepimento della direttiva].

I riferimenti alla direttiva (UE) 2016/1148 si intendono fatti alla presente direttiva e si leggono secondo la tavola di concordanza di cui all'allegato II[...].

Articolo 42

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

Articolo 43

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

ALLEGATO I

SETTORI, SOTTOSETTORI E TIPI DI SOGGETTI

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Imprese elettriche di cui all'articolo 2, punto 57, della direttiva (UE) 2019/944 che svolgono l'attività di "fornitura" di cui all'articolo 2, punto 12, di tale direttiva ([39])
		— Gestori del sistema di distribuzione di cui all'articolo 2, punto 29, della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione di cui all'articolo 2, punto 35, della direttiva (UE) 2019/944
		— Produttori di cui all'articolo 2, punto 38, della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato di cui all'articolo 2, punto 8, del regolamento (UE) 2019/943 ([40])
		— Partecipanti al mercato dell'energia elettrica di cui all'articolo 2, punto 25, del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia di cui all'articolo 2, punti 18, 20 e 59

[39] Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).

[40] Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).

		della direttiva (UE) 2019/944
	b) Teleriscaldamento e teleraffrescamento	— Teleriscaldamento o teleraffrescamento di cui all'articolo 2, punto 19, della direttiva (UE) 2018/2001 ([41]) sulla promozione dell'uso dell'energia da fonti rinnovabili
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio di cui all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio ([42])
	d) Gas	— Imprese fornitrici di cui all'articolo 2, punto 8, della direttiva 2009/73/CE ([43])
		— Gestori del sistema di distribuzione di cui all'articolo 2, punto 6, della direttiva 2009/73/CE
		— Gestori del sistema di trasporto di cui all'articolo 2, punto 4, della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio di cui all'articolo 2, punto 10, della

41 Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).

42 Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).

43 Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).

		direttiva 2009/73/CE
		— Gestori del sistema GNL di cui all'articolo 2, punto 12, della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1, della direttiva 2009/73/CE
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno
2. Trasporti	a) Trasporto aereo	— Vettori aerei di cui all'articolo 3, punto 4, del regolamento (CE) n. 300/2008 ([44]) **utilizzati a fini commerciali**
		— Gestori aeroportuali di cui all'articolo 2, punto 2, della direttiva 2009/12/CE ([45]), aeroporti di cui all'articolo 2, punto 1, di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 ([46]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo

[44] Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

[45] Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).

[46] Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).

		di cui all'articolo 2, punto 1, del regolamento (CE) n. 549/2004 ([47])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura di cui all'articolo 3, punto 2, della direttiva 2012/34/UE ([48])
		— Imprese ferroviarie di cui all'articolo 3, punto 1, della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio di cui all'articolo 3, punto 12, della direttiva 2012/34/UE
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci di cui all'allegato I del regolamento (CE) n. 725/2004 ([49]), escluse le singole navi gestite da tali compagnie
		— Organi di gestione dei porti di cui all'articolo 3, punto 1, della direttiva 2005/65/CE ([50]), compresi i relativi impianti portuali di cui all'articolo 2, punto 11, del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti

[47] Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo ("regolamento quadro") (GU L 96 del 31.3.2004, pag. 1).

[48] Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).

[49] Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).

[50] Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).

		— Gestori di servizi di assistenza al traffico marittimo di cui all'articolo 3, lettera o), della direttiva 2002/59/CE ([51])
	d) Trasporto su strada	— Autorità stradali di cui all'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione ([52]) responsabili del controllo della gestione del traffico**, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono solo una parte non essenziale della loro attività generale**
		— Gestori di sistemi di trasporto intelligenti di cui all'articolo 4, punto 1, della direttiva 2010/40/UE ([53])
3. Settore bancario		— Enti creditizi di cui all'articolo 4, punto 1, del regolamento (UE) n. 575/2013 ([54])**, esclusi quelli di cui all'articolo 2, paragrafo 5, punto 8), della direttiva 2013/36/UE che sono esentati conformemente all'articolo 2, paragrafo 4, del regolamento XX [DORA]]**

[51] Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10).

[52] Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).

[53] Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).

[54] Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).

4. Infrastrutture dei mercati finanziari		— Gestori di sedi di negoziazione di cui all'articolo 4, punto 24, della direttiva 2014/65/UE ([55])
		— Controparti centrali (CCP) di cui all'articolo 2, punto 1, del regolamento (UE) n. 648/2012 ([56])
5. Salute		— Prestatori di assistenza sanitaria di cui all'articolo 3, lettera g), della direttiva 2011/24/UE ([57])
		— Laboratori di riferimento dell'UE di cui all'articolo 15 del regolamento (UE) XXXX/XXXX relativo alle gravi minacce per la salute a carattere transfrontaliero [58]
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali di cui all'articolo 1, punto 2, della direttiva 2001/83/CE ([59]) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante

[55] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

[56] Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).

[57] Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

[58] [Regolamento del Parlamento europeo e del Consiglio relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE, riferimento da aggiornare dopo l'adozione della proposta COM(2020) 727 final].

[59] Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).

		un'emergenza di sanità pubblica ("elenco dei dispositivi critici per l'emergenza di sanità pubblica") di cui all'articolo 20 del regolamento (UE) XXXX/XXXX[60]
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, di cui all'articolo 2, punto 1, lettera a), della direttiva 98/83/CE del Consiglio ([61]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è solo una parte **non essenziale** dell'attività generale di distribuzione di altri prodotti e beni [...]
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche e industriali di cui all'articolo 2, punti da 1 a 3, della direttiva 91/271/CEE del Consiglio ([62]) **ma escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche e industriali è solo una parte non essenziale della loro attività generale.** [...]
8. Infrastrutture digitali		— Fornitori di punti di interscambio Internet
		— Fornitori di servizi DNS**, esclusi gli operatori dei server dei nomi radice**
		— Registri dei nomi di dominio di primo livello (TLD)
		— Fornitori di servizi di cloud

[60] [Regolamento del Parlamento europeo e del Consiglio relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici, riferimento da aggiornare dopo l'adozione della proposta COM(2020) 725 final].

[61] Direttiva 98/83/CE del Consiglio, del 3 novembre 1998, concernente la qualità delle acque destinate al consumo umano (GU L 330 del 5.12.1998, pag. 32).

[62] Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).

		computing
		— Fornitori di servizi di data center
		— Fornitori di reti di distribuzione dei contenuti (*content delivery network*)
		— Prestatori di servizi fiduciari di cui all'articolo 3, punto 19, del regolamento (UE) n. 910/2014 ([63])
		— Fornitori di reti pubbliche di comunicazione elettronica di cui all'articolo 2, punto 8, della direttiva (UE) 2018/1972([64]) o fornitori di servizi di comunicazione elettronica di cui all'articolo 2, punto 4, della direttiva (UE) 2018/1972 se tali servizi sono accessibili al pubblico
8 bis. Gestione dei servizi informatici (TIC) **(B2B)**		**— Fornitori di servizi gestiti** **— Fornitori di servizi di sicurezza gestiti**

[63] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

[64] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

9. **Enti** della pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali **come definiti da uno Stato membro conformemente al diritto nazionale** — [...][65][...] — [...]
10. Spazio		— Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica di cui all'articolo 2, punto 8, della direttiva (UE) 2018/1972

[65] [...]

ALLEGATO II

SETTORI, SOTTOSETTORI E TIPI DI SOGGETTI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali di cui all'articolo 2, punto 1, della direttiva 97/67/CE ([66]), **inclusi** [...] i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti di cui all'articolo 3, punto 9, della direttiva 2008/98/CE ([67]), escluse quelle per cui la gestione dei rifiuti non è la principale attività economica

[66] Direttiva 97/67/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e il miglioramento della qualità del servizio (GU L 15 del 21.1.1998, pag. 14), **come modificata dalla direttiva 2008/6/CE del Parlamento europeo e del Consiglio, del 20 febbraio 2008, che modifica la direttiva 97/67/CE per quanto riguarda il pieno completamento del mercato interno dei servizi postali comunitari (GU L 52 del 27.2.2008, pag. 3)**.

[67] Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).

3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione [...] e della distribuzione di sostanze e [...] **miscele** di cui all'articolo 3, punti [...], 9 e 14, del regolamento (CE) n. 1907/2006 ([68]) **e imprese che si occupano della produzione di articoli di cui all'articolo 3, punto 3 di detto regolamento a partire da sostanze e miscele.**
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari di cui all'articolo 3, punto 2, del regolamento (CE) n. 178/2002 ([69]) **che sono impegnate nella distribuzione all'ingrosso e nella produzione e trasformazione industriale**
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici di cui all'articolo 2, punto 1, del regolamento (UE) 2017/745 ([70]) e soggetti che fabbricano dispositivi medico-diagnostici in vitro di cui all'articolo 2, punto 2, del regolamento (UE) 2017/746 ([71]) ad eccezione dei

68 Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE (GU L 396 del 30.12.2006, pag. 1).

69 Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 dell'1.2.2002, pag. 1).

70 Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

71 Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

		soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5.
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network