Gazzetta ufficiale dell'Unione europea

L 151

Edizione in lingua italiana

Legislazione

62° anno

7 giugno 2019

Sommario

[1] Testo rilevante ai fini del SEE.

IT

Gli atti i cui titoli sono stampati in caratteri chiari appartengono alla gestione corrente. Essi sono adottati nel quadro della politica agricola e hanno generalmente una durata di validità limitata.

I titoli degli altri atti sono stampati in grassetto e preceduti da un asterisco.

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2019/880 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019

relativo all'introduzione e all'importazione di beni culturali

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 207, paragrafo 2,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria [1],

considerando quanto segue:

(1) Alla luce delle conclusioni del Consiglio del 12 febbraio 2016 sulla lotta contro il finanziamento del terrorismo, della comunicazione della Commissione al Parlamento europeo e al Consiglio del 2 febbraio 2016 relativa a un piano d'azione per rafforzare la lotta contro il finanziamento del terrorismo e della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio [2], è opportuno prevedere l'adozione di norme comuni sul commercio con i paesi terzi per garantire la protezione efficace dal commercio illecito di beni culturali e contro la loro perdita o distruzione, la preservazione del patrimonio culturale dell'umanità e la prevenzione del finanziamento del terrorismo e del riciclaggio mediante la vendita ad acquirenti dell'Unione di beni culturali saccheggiati.

(2) Lo sfruttamento dei popoli e dei territori che può condurre al commercio illecito di beni culturali, in particolare se il commercio illecito ha origine in un contesto di conflitto armato. In questo senso, è opportuno che il presente regolamento tenga conto delle caratteristiche regionali e locali dei popoli e dei territori, piuttosto che del valore di mercato dei beni culturali.

(3) I beni culturali formano parte del patrimonio culturale e spesso rivestono una notevole importanza culturale, artistica, storica e scientifica. Il patrimonio culturale rappresenta uno degli elementi fondanti della civiltà, anche perché apporta un valore simbolico e costituisce la memoria culturale dell'umanità. Arricchisce la vita culturale di tutti i popoli e li accomuna attraverso la condivisione della memoria, della conoscenza e dello sviluppo della civiltà. Dovrebbe pertanto essere tutelato dall'appropriazione illecita e dal saccheggio. I saccheggi di siti archeologici si sono sempre verificati, ma ora tale fenomeno ha raggiunto proporzioni industriali e, insieme al commercio dei beni culturali riportati alla luce illegalmente, costituisce un grave reato che arreca considerevoli sofferenze a coloro che ne sono colpiti direttamente e indirettamente. Il commercio illecito di beni culturali contribuisce in molti casi all'omogeneizzazione culturale forzata o alla perdita forzata dell'identità culturale, mentre il saccheggio di beni culturali conducono, fra l'altro, alla disgregazione delle culture. Fino a quando sarà possibile dedicarsi a un proficuo commercio di beni culturali riportati alla luce illegalmente e ottenerne un profitto senza rischi significativi, gli scavi e i saccheggi continueranno. A causa del loro valore economico e artistico, i beni culturali hanno una forte domanda sul mercato internazionale. L'assenza di solide misure legislative internazionali e la loro relativa inefficace applicazione fa sì che i beni in questione finiscano nell'economia sommersa. Pertanto, è opportuno che l'Unione

[1] Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.

[2] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU L 88 del 31.3.2017, pag. 6).

vieti l'introduzione nel territorio doganale dell'Unione di beni culturali esportati illecitamente da paesi terzi, segnatamente di beni culturali provenienti da paesi terzi interessati da conflitti armati, in special modo se tali beni culturali sono stati commerciati in modo illecito da organizzazioni terroristiche o criminali di altro tipo. Se è vero che tale divieto generale non dovrebbe comportare controlli sistematici, gli Stati membri dovrebbero nondimeno essere autorizzati a intervenire quando ricevono informazioni relative a spedizioni sospette e adottare tutte le misure appropriate per intercettare i beni culturali esportati illecitamente.

(4) Alla luce della diversità delle norme applicate negli Stati membri riguardo all'importazione di beni culturali nel territorio doganale dell'Unione, è opportuno adottare misure volte in particolare a garantire che determinate importazioni di beni culturali siano soggette a controlli uniformi al momento della loro entrata nel territorio doganale dell'Unione, sulla base degli attuali processi, regimi e strumenti amministrativi volti a conseguire un'applicazione uniforme del regolamento (UE) n. 952/2013 del Parlamento europeo e del Consiglio ([3]).

(5) La protezione dei beni culturali considerati patrimonio nazionale degli Stati membri è già contemplata dal regolamento (CE) n. 116/2009 del Consiglio ([4]) e dalla direttiva 2014/60/UE del Parlamento europeo e del Consiglio ([5]). Il presente regolamento non dovrebbe pertanto applicarsi ai beni culturali creati o scoperti nel territorio doganale dell'Unione. È opportuno che le norme comuni introdotte dal presente regolamento disciplinino il trattamento doganale dei beni culturali non unionali che entrano nel territorio doganale dell'Unione. Ai fini del presente regolamento, il pertinente territorio doganale dovrebbe coincidere con il territorio doganale dell'Unione al momento dell'importazione.

(6) E opportuno che le misure di controllo da adottare in merito alle zone franche e ai cosiddetti «porti franchi» abbiano un ambito di applicazione quanto più ampio possibile in termini di regimi doganali interessati, al fine di evitare che il presente regolamento sia aggirato attraverso il ricorso a tali zone franche, che potrebbero potenzialmente essere utilizzate per la continua proliferazione del commercio di prodotti illegali nell'Unione. È opportuno pertanto che tali misure di controllo non si applichino solo ai beni culturali immessi in libera pratica ma anche ai beni culturali vincolati a un regime doganale speciale. L'ambito di applicazione non dovrebbe tuttavia andare oltre l'obiettivo di impedire ai beni culturali esportati illecitamente di entrare nel territorio doganale dell'Unione. Pertanto, pur applicandosi l'immissione in libera pratica e alcuni regimi doganali speciali a cui possono essere vincolati i beni che entrano nel territorio doganale dell'Unione, è opportuno che le misure di controllo sistematiche non si applichino al transito.

(7) Molti paesi terzi e la maggior parte degli Stati membri hanno familiarità con le definizioni utilizzate nella convenzione dell'Unesco concernente le misure da adottare per interdire e impedire l'illecita importazione, esportazione e trasferimento di proprietà dei beni culturali, firmata a Parigi il 14 novembre 1970 («convenzione Unesco del 1970») della quale sono parti numerosi Stati membri, e nella convenzione dell'Unidroit sui beni culturali rubati o illecitamente esportati, firmata a Roma il 24 giugno 1995. Per tale ragioni le definizioni utilizzate nel presente regolamento sono basate su tali definizioni.

(8) È opportuno che la legalità dell'esportazione di beni culturali sia esaminata in primo luogo sulla base delle disposizioni legislative e regolamentari del paese in cui tali beni culturali sono stati creati o scoperti. Tuttavia, per non ostacolare in maniera irragionevole il commercio legittimo, in taluni casi è opportuno che la persona che intende importare beni culturali nel territorio doganale dell'Unione sia eccezionalmente autorizzata a dimostrare piuttosto la lecita esportazione da un diverso paese terzo in cui i beni culturali erano localizzati prima di essere spediti nell'Unione. Tale eccezione dovrebbe applicarsi qualora il paese in cui i beni culturali sono stati creati o scoperti non possa essere determinato in modo attendibile o quando l'esportazione dei beni culturali in questione abbia avuto luogo prima che la convenzione Unesco del 1970 entrasse in vigore, ossia il 24 aprile 1972. Al fine di evitare che il presente regolamento sia aggirato semplicemente mediante la spedizione illegale di beni culturali in un altro paese terzo prima della loro importazione nell'Unione, tali eccezioni dovrebbero essere applicabili qualora i beni culturali si siano trovati in un paese terzo per un periodo superiore a cinque anni per scopi diversi dall'utilizzo temporaneo, dal transito, dalla riesportazione o dal trasbordo. Qualora tali condizioni siano soddisfatte per più di un paese, l'ultimo di questi paesi prima dell'introduzione dei beni culturali nel territorio doganale dell'Unione dovrebbe essere quello pertinente.

(9) L'articolo 5 della convenzione Unesco del 1970 esorta gli Stati parti ad istituire uno o più servizi nazionali per la protezione dei beni culturali contro l'importazione, l'esportazione e il trasferimento illeciti di proprietà. Tali servizi nazionali dovrebbero essere dotati di personale qualificato e in numero sufficiente al fine di garantire tale protezione in conformità di tale convenzione ed inoltre dovrebbero consentire la necessaria collaborazione attiva tra le autorità competenti degli Stati membri parte di tale convenzione nel settore della sicurezza e nella lotta contro l'importazione illegale di beni culturali, in particolare dalle aree colpite da conflitti armati.

([3]) Regolamento (UE) n. 952/2013 del Parlamento europeo e del Consiglio, del 9 ottobre 2013, che istituisce il codice doganale dell'Unione (GU L 269 del 10.10.2013, pag. 1).

([4]) Regolamento (CE) n. 116/2009 del Consiglio, del 18 dicembre 2008, relativo all'esportazione di beni culturali (GU L 39 del 10.2.2009, pag. 1).

([5]) Direttiva 2014/60/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa alla restituzione dei beni culturali usciti illecitamente dal territorio di uno Stato membro e che modifica il regolamento (UE) n. 1024/2012 (GU L 159 del 28.5.2014, pag. 1).

(10) Al fine di non ostacolare in misura sproporzionata il commercio di beni attraverso la frontiera esterna, è opportuno che il presente regolamento si applichi esclusivamente ai beni culturali che superino un certo limite d'età, che è stabilito dal presente regolamento. Sembra inoltre opportuno stabilire anche una soglia finanziaria per escludere i beni culturali di valore inferiore dall'applicazione delle condizioni e procedure per l'importazione nel territorio doganale dell'Unione. Tali soglie garantiranno che le misure introdotte dal presente regolamento si concentrino sui beni culturali più probabilmente appetiti dai saccheggiatori nelle zone di conflitto, senza escludere altri beni il cui controllo è necessario per assicurare la protezione del patrimonio culturale.

(11) Il commercio illecito di beni culturali saccheggiati è stato identificato come una possibile fonte di finanziamento del terrorismo e di attività di riciclaggio nel contesto della valutazione sovranazionale dei rischi legati al riciclaggio e al finanziamento del terrorismo che incidono sul mercato interno.

(12) Poiché talune categorie di beni culturali, segnatamente i reperti archeologici e gli elementi provenienti dai monumenti, sono particolarmente esposte al rischio di saccheggio e distruzione, sembra necessario prevedere un sistema di controllo rafforzato prima che a tali beni sia permesso di entrare nel territorio doganale dell'Unione. È opportuno che tale sistema preveda l'obbligo di presentazione di una licenza d'importazione rilasciata dall'autorità competente di uno Stato membro prima dell'immissione in libera pratica di tali beni culturali nell'Unione o del vincolo degli stessi a un regime doganale speciale diverso dal transito. Le persone che intendano ottenere tale licenza dovrebbero essere in grado di dimostrare l'esportazione lecita dal paese in cui i beni culturali sono stati creati o scoperti mediante gli adeguati documenti giustificativi e di prova, quali certificati di esportazione, titoli di proprietà, fatture, contratti di vendita, documenti assicurativi, documenti di trasporto e perizie. È opportuno che le autorità competenti degli Stati membri decidano, sulla base della completezza e dell'accuratezza delle domande, se rilasciare o no una licenza senza indebito ritardo. Tutte le licenze di importazione dovrebbero essere archiviate in un sistema elettronico.

(13) Un'icona è una qualsiasi rappresentazione di figure o di eventi religiosi. Essa può essere prodotta con vari materiali e in diverse dimensioni, e può essere sia monumentale che portatile. Nei casi in cui un tempo faceva parte, per esempio, dell'interno di una chiesa, di un monastero, di una cappella, come elemento a sé stante o parte di mobilia architetturale, ad esempio un'iconostasi o un porta icona, l'icona costituisce un elemento fondamentale e inseparabile della vita liturgica e del culto divino, e dovrebbe essere considerata parte integrante di un monumento religioso che sia stato smembrato. L'icona dovrebbe rientrare nella categoria «elementi provenienti dallo smembramento di monumenti artistici o storici o di siti archeologici» elencati nell'allegato, anche qualora il monumento specifico al quale essa apparteneva non sia noto ma sussistano prove che una volta l'icona era parte integrante di un monumento, specie quando presenti segni o elementi attestanti che un tempo faceva parte di un'iconostasi o di un porta icona.

(14) Tenuto conto della particolare natura dei beni culturali, il ruolo delle autorità doganali è estremamente importante ed esse dovrebbero essere in grado, ove necessario, di richiedere ulteriori informazioni al dichiarante e analizzare i beni culturali sottoponendoli a un esame fisico.

(15) È opportuno che la persona che intende importare nel territorio doganale dell'Unione categorie di beni culturali per l'importazione delle quali non è richiesta una licenza d'importazione certifichi, mediante una dichiarazione, la legalità dell'esportazione degli stessi dal paese terzo e se ne assuma la responsabilità, nonché fornisca informazioni sufficienti affinché tali beni culturali possano essere identificati dalle autorità doganali. Al fine di agevolare la procedura e per motivi di certezza del diritto è opportuno che le informazioni sui beni culturali siano fornite mediante l'uso di un documento standardizzato. Potrebbe essere utilizzato lo standard dell'Object ID, raccomandato dall'Unesco, per descrivere i beni culturali. Il titolare dei beni dovrebbe registrare tali informazioni in un sistema elettronico, al fine di agevolare l'identificazione da parte delle autorità doganali, consentire un'analisi dei rischi e controlli mirati e in modo da garantire la tracciabilità una volta che i beni culturali sono entrati nel mercato interno.

(16) Nel contesto dello sportello unico per le dogane, la Commissione dovrebbe essere responsabile dell'istituzione di un sistema elettronico centralizzato per la presentazione delle domande di licenze di importazione e di dichiarazioni dell'importatore, nonché per l'archiviazione e lo scambio di informazioni tra le autorità degli Stati membri, in particolare per quanto riguarda le dichiarazioni dell'importatore e le licenze di importazione.

(17) Il trattamento dei dati di cui al presente regolamento dovrebbe poter comprendere anche i dati personali e tale trattamento dovrebbe essere effettuato conformemente al diritto dell'Unione. È opportuno che gli Stati membri e la Commissione trattino i dati personali solo per le finalità del presente regolamento o, in circostanze debitamente giustificate, a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi o esecuzione di sanzioni penali, comprese la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. La raccolta, la

divulgazione, la trasmissione, la comunicazione e qualunque altro tipo di trattamento dei dati personali rientrante nell'ambito di applicazione del presente regolamento dovrebbero essere soggetti alle prescrizioni dei regolamenti (UE) 2016/679 ([6]) e (UE) 2018/1725 ([7]) del Parlamento europeo e del Consiglio. Il trattamento dei dati personali ai fini del presente regolamento dovrebbe tener conto anche del diritto al rispetto della vita privata e familiare riconosciuto all'articolo 8 della convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché del diritto al rispetto della vita privata e della vita familiare e del diritto alla protezione dei dati di carattere personale riconosciuti, rispettivamente, agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

(18) I beni culturali che non sono stati creati o scoperti nel territorio doganale dell'Unione ma che sono stati esportati in quanto beni dell'Unione non dovrebbero essere soggetti alla presentazione di una licenza di importazione o di una dichiarazione dell'importatore quando sono reintrodotti in tale territorio in quanto merci in reintroduzione ai sensi del regolamento (UE) n. 952/2013.

(19) Non dovrebbe essere soggetta alla presentazione di una licenza di importazione o di una dichiarazione dell'importatore nemmeno l'ammissione temporanea di beni culturali a fini formativi, scientifici, di conservazione, di restauro, di esposizione, di digitalizzazione, di spettacolo, di ricerca condotta da istituti accademici o a fini di collaborazione tra musei o enti analoghi.

(20) Dovrebbe inoltre essere consentito, senza la presentazione di una licenza di importazione. o di una dichiarazione dell'importatore, il deposito di beni culturali provenienti da paesi in cui è in corso un conflitto armato o una catastrofe naturale, con il fine esclusivo di trovare un rifugio sicuro per garantirne la custodia e la conservazione da parte di un'autorità pubblica, o sotto la sua supervisione.

(21) Al fine di agevolare la presentazione dei beni culturali nell'ambito di fiere d'arte commerciali, una licenza di importazione non dovrebbe essere necessaria qualora i beni culturali siano in regime di ammissione temporanea, ai sensi dell'articolo 250 del regolamento (UE) n. 952/2013, e sia stata fornita una dichiarazione dell'importatore anziché una licenza di importazione. Tuttavia, la presentazione di una licenza di importazione dovrebbe essere necessaria qualora tali beni culturali restino nell'Unione dopo la fiera d'arte.

(22) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione affinché adotti modalità dettagliate relative ai beni culturali che sono beni reintrodotti, o all'ammissione temporanea di beni culturali nel territorio doganale dell'Unione e alla loro custodia, ai modelli per le domande di licenza di importazione e ai moduli perle licenze di importazione, ai modelli per le dichiarazioni dell'importatore e i documenti di cui sono corredate, e alle ulteriori norme procedurali riguardanti la presentazione e il trattamento degli stessi. È opportuno inoltre attribuire alla Commissione competenze di esecuzione per l'istituzione di un sistema elettronico per la presentazione delle domande di licenze di importazione e di dichiarazioni dell'importatore e per l'archiviazione e lo scambio di informazioni tra gli Stati membri. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([8]).

(23) Al fine di garantire un coordinamento efficace ed evitare la duplicazione degli sforzi nell'organizzare attività di formazione e di sviluppo delle capacità e campagne di sensibilizzazione, nonché di commissionare attività di ricerca pertinenti e lo sviluppo di norme, ove opportuno, la Commissione e gli Stati membri dovrebbero cooperare con organizzazioni e organismi internazionali, quali l'Unesco, Interpol, Europol, l'Organizzazione mondiale delle dogane, l'Istituto internazionale per la conservazione e il restauro dei beni culturali e il Consiglio internazionale dei musei (ICOM).

(24) È opportuno che informazioni rilevanti sui flussi commerciali di beni culturali siano raccolte per via elettronica e condivise tra gli Stati membri e la Commissione, affinché siano di sostegno all'attuazione efficace del presente regolamento e fungano da base per la sua valutazione futura. Ai fini della trasparenza e del controllo pubblico, è opportuno rendere pubbliche quante più informazioni possibili. I flussi commerciali di beni culturali non possono essere monitorati in modo efficace solo in base al valore o al peso degli stessi. È essenziale raccogliere per via elettronica informazioni sul numero dei pezzi dichiarati. Dal momento che la nomenclatura combinata non specifica alcuna unità di misura supplementare per i beni culturali, è necessario richiedere la dichiarazione del numero di pezzi.

([6]) 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).

([7]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

([8]) 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).

(25) La strategia e il piano d'azione dell'UE per la gestione dei rischi doganali mirano, tra l'altro, a rafforzare le capacità delle autorità doganali al fine di migliorare la reattività ai rischi nel settore dei beni culturali. È opportuno che si utilizzi il quadro comune in materia di gestione del rischio previsto dal regolamento (UE) n. 952/2013 e che le autorità doganali si scambino le informazioni pertinenti sui rischi.

(26) Al fine di beneficiare delle competenze delle organizzazioni e degli organismi internazionali attivi nel settore culturale e della loro esperienza per quanto riguarda il commercio illecito di beni culturali, le raccomandazioni e gli orientamenti formulati da tali organizzazioni e organismi dovrebbero essere presi in considerazione nel quadro comune in materia di gestione del rischio al momento di identificare i rischi connessi ai beni culturali. In particolare, le liste rosse pubblicate dall'ICOM dovrebbero fungere da orientamento per individuare quei paesi terzi il cui patrimonio è particolarmente a rischio e gli oggetti esportati da tali paesi che sarebbero più spesso esposti a commercio illecito.

(27) È necessario istituire campagne di sensibilizzazione rivolte agli acquirenti di beni culturali per quanto riguarda il rischio del commercio illecito e assistere gli operatori del mercato nella loro comprensione e applicazione del presente regolamento. Nella diffusione di tali informazioni gli Stati membri dovrebbero coinvolgere i competenti punti di contatto nazionali e altri servizi di fornitura di tali informazioni.

(28) La Commissione dovrebbe assicurare che le microimprese e le piccole e medie imprese (PMI) beneficino di un'assistenza tecnica adeguata e dovrebbe agevolare l'informazione delle stesse ai fini dell'efficace attuazione del presente regolamento. Le PMI stabilite nell'Unione che importano beni culturali dovrebbero pertanto beneficiare dei programmi attuali e futuri dell'Unione a sostegno della competitività delle piccole e medie imprese.

(29) Al fine di incentivare la conformità e scoraggiare l'elusione, gli Stati membri dovrebbero introdurre sanzioni effettive, proporzionate e dissuasive in caso di violazione delle disposizioni del presente regolamento e comunicare tali sanzioni alla Commissione. Le sanzioni introdotte dagli Stati membri contro le violazioni del presente regolamento dovrebbero avere un effetto deterrente equivalente in tutta l'Unione.

(30) Gli Stati membri dovrebbero assicurare che le autorità doganali e le autorità competenti concordino misure ai sensi dell'articolo 198 del regolamento (UE) n. 952/2013. I dettagli relativi a tali misure dovrebbero essere soggetti al diritto nazionale.

(31) È opportuno che la Commissione adotti senza indugio norme per l'attuazione del presente regolamento, in particolare norme riguardanti i moduli elettronici standardizzati appropriati da utilizzare per richiedere una licenza di importazione o redigere una dichiarazione dell'importatore, e istituisca il sistema elettronico nel più breve tempo possibile. È opportuno posticipare di conseguenza l'applicazione delle disposizioni relative alle licenze di importazione e alle dichiarazioni dell'importatore.

(32) Secondo il principio di proporzionalità, è necessario ed appropriato, ai fini del raggiungimento dell'obiettivo fondamentale del presente regolamento, stabilire una disciplina sull'introduzione, le condizioni e le procedure per l'importazione di beni culturali nel territorio doganale dell'Unione. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo, in ottemperanza all'articolo 5, paragrafo 4, del trattato sull'Unione europea.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento definisce le condizioni per l'introduzione di beni culturali e le condizioni e procedure per la loro importazione al fine di salvaguardare il patrimonio culturale dell'umanità e di impedire il commercio illecito di beni culturali, in particolare qualora tale commercio illecito possa contribuire al finanziamento del terrorismo.

2. Il presente regolamento non si applica ai beni culturali creati o scoperti nel territorio doganale dell'Unione.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) «beni culturali»: qualsiasi articolo di importanza archeologica, preistorica, storica, letteraria, artistica o scientifica, elencato nell'allegato;

2) «introduzione di beni culturali»: l'entrata nel territorio doganale dell'Unione di beni culturali che sono soggetti a vigilanza doganale o a controlli doganali nel territorio doganale dell'Unione conformemente al regolamento (UE) n. 952/2013;

3) «importazione di beni culturali»:

a) l'immissione di beni culturali in libera pratica di cui all'articolo 201 del regolamento (UE) n. 952/2013; o

b) il vincolo di beni culturali a una delle seguenti categorie di regimi speciali di cui all'articolo 210 del regolamento (UE) n. 952/2013:

i) deposito, che comprende il deposito doganale e le zone franche,

ii) uso particolare, che comprende l'ammissione temporanea e l'uso finale,

iii) perfezionamento attivo;

4) «titolare dei beni»: il titolare delle merci definito all'articolo 5, punto 34, del regolamento (UE) n. 952/2013;

5) «autorità competenti»: le autorità pubbliche designate dagli Stati membri per il rilascio delle licenze di importazione.

Articolo 3

Introduzione e importazione di beni culturali

1. È vietata l'introduzione dei beni culturali di cui alla parte A dell'allegato, rimossi dal territorio del paese in cui sono stati creati o scoperti in violazione delle disposizioni legislative e regolamentari di tale paese.

Le autorità doganali e le autorità competenti adottano tutte le misure opportune qualora si tenti di introdurre i beni culturali di cui al primo comma.

2. L'importazione dei beni culturali elencati nelle parti B e C dell'allegato è consentita solo previa presentazione di:

a) una licenza di importazione rilasciata in conformità dell'articolo 4; o

b) di una dichiarazione dell'importatore presentata in conformità dell'articolo 5.

3. La licenza di importazione o la dichiarazione dell'importatore di cui al paragrafo 2 del presente articolo è fornita alle autorità doganali in conformità dell'articolo 163 del regolamento (UE) n. 952/2013. Nel caso di vincolo dei beni culturali al regime di zona franca, il titolare dei beni fornisce la licenza di importazione o la dichiarazione dell'importatore dietro presentazione dei beni in conformità dell'articolo 245, paragrafo 1, lettere a) e b), del regolamento (UE) n. 952/2013.

4. Il paragrafo 2 del presente articolo non si applica:

a) ai beni culturali che sono beni reintrodotti ai sensi dell'articolo 203 del regolamento (UE) n. 952/2013;

b) all'importazione di beni culturali al fine esclusivo di garantirne la custodia da parte di un'autorità pubblica o sotto la sua supervisione, con l'intento di restituire tali beni culturali, quando la situazione lo consenta;

c) all'ammissione temporanea di beni culturali, ai sensi dell'articolo 250 del regolamento (UE) n. 952/2013, nel territorio doganale dell'Unione a fini formativi, scientifici, di conservazione, di restauro, di esposizione, di digitalizzazione, di spettacolo, di ricerca condotta da istituzioni accademiche o di collaborazione tra musei o enti analoghi.

5. Non è richiesta la presentazione di una licenza di importazione per i beni culturali che sono stati vincolati in regime di ammissione temporanea, ai sensi dell'articolo 250 del regolamento (UE) n. 952/2013, qualora tali beni debbano essere esposti nell'ambito di fiere d'arte commerciali. In tali casi deve essere fornita una dichiarazione dell'importatore in conformità del procedimento di cui all'articolo 5 del presente regolamento.

Qualora tali beni culturali siano successivamente vincolati a un altro regime doganale di cui all'articolo 2, punto 3, del presente regolamento è richiesta una licenza di importazione rilasciata in conformità dell'articolo 4 del presente regolamento.

6. La Commissione stabilisce, mediante atti di esecuzione, le modalità dettagliate per i beni culturali che sono beni reintrodotti, per l'importazione di beni culturali a fini di custodia, e per l'ammissione temporanea di beni culturali di cui ai paragrafi 4 e 5 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 13, paragrafo 2.

7. Il paragrafo 2 del presente articolo lascia impregiudicate le altre misure adottate dall'Unione in conformità dell'articolo 215 del trattato sul funzionamento dell'Unione europea.

8. Al momento della presentazione di una dichiarazione in dogana per l'importazione dei beni culturali elencati nelle parti B e C dell'allegato, il numero dei pezzi è espresso mediante l'unità supplementare, come indicato in tale allegato. Nel caso in cui i beni culturali siano vincolati al regime di zona franca, il possessore dei beni indica il numero dei pezzi dietro presentazione dei beni in conformità dell'articolo 245, paragrafo 1, lettere a) e b), del regolamento (UE) n. 952/2013.

Articolo 4

Licenza di importazione

1. L'importazione dei beni culturali elencati alla parte B dell'allegato, diversi da quelli di cui all'articolo 3, paragrafi 4 e 5, richiede una licenza di importazione. Tale licenza di importazione è rilasciata dall'autorità competente dello Stato membro in cui i beni culturali sono vincolati a uno dei regimi doganali di cui all'articolo 2, punto 3, per la prima volta.

2. Le licenze di importazione rilasciate dalle autorità competenti di uno Stato membro in conformità del presente articolo sono valide in tutta l'Unione.

3. Una licenza di importazione rilasciata in conformità del presente articolo non è considerata prova di legittima provenienza o proprietà dei beni culturali in questione.

4. Il titolare dei beni presenta una domanda di licenza di importazione all'autorità competente dello Stato membro di cui al paragrafo 1 del presente articolo tramite il sistema elettronico di cui all'articolo 8. La domanda è accompagnata da qualsiasi documento giustificativo e informazione atti a comprovare che i beni culturali in questione sono stati esportati dal paese in cui sono stati creati o scoperti in conformità delle disposizioni legislative e regolamentari di tale paese o comprovanti l'assenza di tali disposizioni legislative e regolamentari al momento in cui detti beni sono stati portati fuori dal suo territorio.

In deroga al primo comma, la domanda può essere accompagnata invece da qualsiasi documento giustificativo e informazione atti a comprovare che i beni culturali in questione sono stati esportati in conformità delle disposizioni legislative e regolamentari dell'ultimo paese in cui si sono trovati per un periodo superiore a cinque anni e per scopi diversi dall'utilizzo temporaneo, dal transito, dalla riesportazione o dal trasbordo, nei seguenti casi:

a) il paese in cui i beni culturali sono stati creati o scoperti non può essere determinato in modo attendibile; o

b) i beni culturali sono stati rimossi dal paese in cui sono stati creati o scoperti prima del 24 aprile 1972.

5. La prova che i beni culturali in questione sono stati esportati ai sensi del paragrafo 4 deve essere fornita nella forma di certificati di esportazione o le licenze di esportazione, ove il paese in questione abbia stabilito tali documenti per l'esportazione di beni culturali al momento dell'esportazione.

6. L'autorità competente controlla la completezza della domanda. Essa chiede al richiedente di fornire qualsiasi informazione o documento mancante o aggiuntivo entro ventuno giorni dalla ricezione della domanda.

7. L'autorità competente, entro 90 giorni dalla ricezione della domanda completa, esamina la domanda e decide se rilasciare la licenza di importazione o respingere la domanda.

L'autorità competente respinge la domanda se:

a) dispone di informazioni o ragionevoli motivazioni per credere che i beni culturali siano stati rimossi dal territorio del paese in cui tali beni sono stati creati o scoperti in violazione delle disposizioni legislative e regolamentari di tale paese;

b) non è stata fornita la prova richiesta al paragrafo 4;

c) dispone di informazioni o ragionevoli motivazioni per credere che il titolare dei beni non li abbia acquisiti legalmente; o

d) è a conoscenza di richieste di restituzione pendenti dei beni culturali da parte delle autorità del paese in cui tali beni sono stati creati o scoperti.

8. Qualora la domanda sia respinta, la decisione amministrativa di cui al paragrafo 7, accompagnata da una motivazione che comprende informazioni sulla procedura di ricorso, è comunicata senza indugio al richiedente.

9. All'atto della presentazione di una domanda di licenza di importazione relativa a beni culturali per i quali una precedente domanda sia stata respinta, il richiedente informa di tale rigetto l'autorità competente cui presenta la domanda.

10. Se uno Stato membro respinge una domanda, tale rigetto e le motivazioni che ne erano alla base sono comunicati agli altri Stati membri e alla Commissione tramite il sistema elettronico di cui all'articolo 8.

11. Gli Stati membri designano senza indugio le autorità competenti per il rilascio delle licenze di importazione in conformità del presente articolo. Gli Stati membri comunicano alla Commissione i dati relativi alle autorità competenti, nonché qualsiasi cambiamento a tale riguardo.

La Commissione pubblica i dati delle autorità competenti e qualsiasi cambiamento a tale riguardo nella *Gazzetta ufficiale dell'Unione europea*, serie «C».

12. La Commissione stabilisce, mediante atti di esecuzione, il modello e il formato della domanda della licenza di importazione ed individua gli eventuali documenti giustificativi atti a comprovare la provenienza lecita dei beni culturali in questione, nonché le norme procedurali per la presentazione e il trattamento di tale domanda. Nello stabilire tali elementi, la Commissione si adopera per conseguire un'applicazione uniforme da parte delle autorità competenti delle procedure in materia di licenze di importazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 13, paragrafo 2.

Articolo 5

Dichiarazione dell'importatore

1. L'importazione dei beni culturali elencati alla parte C dell'allegato richiede una dichiarazione dell'importatore presentata dal titolare dei beni tramite il sistema elettronico di cui all'articolo 8.

2. La dichiarazione dell'importatore comprende:

a) una dichiarazione firmata dal titolare dei beni in cui egli afferma che i beni culturali sono stati esportati dal paese in cui sono stati creati o scoperti in conformità delle disposizioni legislative e regolamentari di tale paese al momento in cui essi sono stati portati fuori dal suo territorio; e

b) un documento standardizzato in cui i beni culturali in questione sono descritti in modo sufficientemente dettagliato da permetterne l'identificazione da parte delle autorità e consentire un'analisi dei rischi e controlli mirati.

In deroga alla lettera a) del primo comma, la dichiarazione può invece indicare che i beni culturali in questione sono stati esportati in conformità delle disposizioni legislative e regolamentari dell'ultimo paese in cui vi si sono trovati per un periodo superiore a cinque anni e per scopi diversi dall'utilizzo temporaneo, dal transito, dalla riesportazione o dal trasbordo, nei seguenti casi:

a) il paese in cui i beni culturali sono stati creati o scoperti non può essere determinato in modo attendibile; o

b) i beni culturali sono stati rimossi dal paese in cui sono stati creati o scoperti prima del 24 aprile 1972.

3. La Commissione stabilisce, mediante atti di esecuzione, il modello standardizzato e il formato della dichiarazione dell'importatore, nonché le norme procedurali per la sua presentazione, ed individua gli eventuali documenti giustificativi atti a comprovare la provenienza lecita dei beni culturali in questione che dovrebbero essere in possesso del titolare dei beni e le norme per il trattamento di tale dichiarazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 13, paragrafo 2.

Articolo 6

Uffici doganali competenti

Gli Stati membri possono limitare il numero degli uffici doganali competenti per la gestione dell'importazione dei beni culturali soggetti al presente regolamento. Qualora applichino detta limitazione, gli Stati membri comunicano alla Commissione i dati relativi a tali uffici doganali, nonché qualsiasi cambiamento a tale riguardo.

La Commissione pubblica i dati degli uffici doganali competenti, e qualsiasi cambiamento a tale riguardo, nella *Gazzetta ufficiale dell'Unione europea*, serie «C».

Articolo 7

Cooperazione amministrativa

Ai fini dell'attuazione del presente regolamento, gli Stati membri garantiscono la cooperazione tra le rispettive autorità doganali e le autorità competenti di cui all'articolo 4.

Articolo 8

Uso di un sistema elettronico

1. L'archiviazione e lo scambio di informazioni tra le autorità degli Stati membri, in particolare per quanto riguarda le licenze di importazione e le dichiarazioni dell'importatore, sono effettuati per mezzo di un sistema elettronico centralizzato.

Altri mezzi per l'archiviazione e lo scambio di informazioni possono essere usati su base temporanea, in caso di guasto temporaneo del sistema elettronico.

2. La Commissione stabilisce, mediante atti di esecuzione:

a) le modalità per la messa a disposizione, il funzionamento e la manutenzione del sistema elettronico di cui al paragrafo 1;

b) le norme dettagliate riguardanti la presentazione, il trattamento, l'archiviazione e lo scambio di informazioni tra le autorità degli Stati membri mediante il sistema elettronico o altri mezzi di cui al paragrafo 1.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 13, paragrafo 2, entro il 28 giugno 2021.

Articolo 9

Istituzione di un sistema elettronico

La Commissione istituisce il sistema elettronico di cui all'articolo 8. Il sistema elettronico diviene operativo al più tardi quattro anni dopo l'entrata in vigore del primo degli atti di esecuzione di cui all'articolo 8, paragrafo 2.

Articolo 10

Protezione dei dati personali e periodi di conservazione dei dati

1. Le autorità doganali e le autorità competenti degli Stati membri agiscono in qualità di titolari del trattamento dei dati personali ottenuti ai sensi degli articoli 4, 5 e 8.

2. Il trattamento dei dati personali sulla base del presente regolamento avviene solo ai fini definiti all'articolo 1, paragrafo 1.

3. I dati personali ottenuti ai sensi degli articoli 4, 5 e 8 sono accessibili solo al personale debitamente autorizzato delle autorità e sono adeguatamente protetti contro l'accesso o la comunicazione non autorizzati. I dati non possono essere divulgati o comunicati senza l'esplicita autorizzazione scritta dell'autorità che ha ottenuto per prima l'informazione. Tale autorizzazione non è tuttavia necessaria qualora le autorità siano tenute a divulgare o comunicare tale informazione conformemente alle norme in vigore nello Stato membro interessato, in particolare in caso di procedimenti giudiziari.

4. Le autorità conservano i dati personali ottenuti in forza degli articoli 4, 5 e 8 per un periodo di venti anni dalla data in cui sono stati ottenuti. Allo scadere di tale termine, tali dati personali sono cancellati.

Articolo 11

Sanzioni

Gli Stati membri stabiliscono le norme in materia di sanzioni applicabili alle violazioni del presente regolamento, e adottano tutte le misure necessarie a garantire l'applicazione di tali norme. Le sanzioni previste sono effettive, proporzionate e dissuasive.

Gli Stati membri comunicano alla Commissione le norme e mire relative alle sanzioni applicabili all'introduzione di beni culturali in violazione dell'articolo 3, paragrafo 1, entro il 28 dicembre 2020.

Gli Stati membri comunicano alla Commissione le norme e mire relative alle sanzioni applicabili alle altre violazione del presente regolamento, in particolare alla resa di false dichiarazioni e alla presentazione di informazioni false, entro il 28 giugno 2025.

Gli Stati membri comunicano senza indugio alla Commissione qualsiasi modifica successiva di tali norme e misure.

Articolo 12

Cooperazione con i paesi terzi

Per quanto attiene alle sue attività e nella misura necessaria per l'espletamento dei suoi compiti a norma del presente regolamento, la Commissione può organizzare attività di formazione e di sviluppo delle capacità a favore dei paesi terzi in cooperazione con gli Stati membri.

Articolo 13

Procedura di comitato

1. La Commissione è assistita dal comitato istituito dall'articolo 8 del regolamento (CE) n. 116/2009 del Consiglio. 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.

Articolo 14

Comunicazione e valutazione

1. Gli Stati membri forniscono informazioni alla Commissione in merito all'attuazione del presente regolamento.

A tal fine la Commissione propone questionari pertinenti agli Stati membri. Gli Stati membri dispongono di sei mesi dalla ricezione del questionario per comunicare alla Commissione le informazioni richieste.

2. Entro tre anni dalla data di applicazione del presente regolamento nella sua interezza e, successivamente ogni cinque anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'attuazione del presente regolamento. Detta relazione è resa pubblica e include informazioni statistiche pertinenti a livello sia di Unione sia nazionale, quali il numero di licenze di importazione rilasciate, di domande respinte e di dichiarazioni dell'importatore presentate. Essa tiene conto dell'attuazione pratica, compreso l'impatto sugli operatori economici dell'Unione, in particolare sulle PMI.

3. Entro il 28 giugno 2020 e successivamente ogni dodici mesi fintanto che il sistema elettronico di cui all'articolo 9 non sia stato istituito, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sui progressi relativi all'adozione degli atti di esecuzione di cui all'articolo 8, paragrafo 2, e all'istituzione del sistema elettronico di cui all'articolo 9.

Articolo 15

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 16

Applicazione

1. Il presente regolamento si applica a decorrere dalla data di entrata in vigore.

2. In deroga al paragrafo 1:

a) l'articolo 3, paragrafo 1, si applica dal 28 dicembre 2020;

b) l'articolo 3, paragrafi da 2 a 5, 7 ed 8, l'articolo 4, paragrafi da 1 a 10, l'articolo 5, paragrafi 1 e 2, e l'articolo 8, paragrafo 1, si applicano dalla data in cui il sistema elettronico di cui all'articolo 8 diviene operativo o al più tardi dal 28 giugno 2025. La Commissione pubblica la data in cui le condizioni del presente paragrafo sono state soddisfatte nella *Gazzetta ufficiale dell'Unione europea*, serie «C».

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO

Parte A. Beni culturali di cui all'articolo 3, paragrafo 1

a) collezioni ed esemplari rari di fauna, flora, mineralogia e anatomia, e oggetti aventi interesse paleontologico;

b) beni riguardanti la storia, comprese la storia della scienza e della tecnica e la storia militare e sociale, nonché la vita dei leader, dei pensatori, degli scienziati e degli artisti nazionali e gli avvenimenti di importanza nazionale;

c) prodotti di scavi archeologici (inclusi regolari e clandestini) e di scoperte archeologiche terrestri o subacquee;

d) elementi provenienti dallo smembramento di monumenti artistici o storici o di siti archeologici [1];

e) oggetti di antichità, aventi più di cento anni, quali iscrizioni, monete e sigilli incisi;

f) oggetti aventi interesse etnologico;

g) oggetti aventi interesse artistico, quali:

  i) quadri, pitture e disegni eseguiti interamente a mano su qualsiasi supporto e di qualsiasi materia (esclusi i disegni industriali e gli oggetti manufatti decorati a mano);

  ii) opere originali dell'arte statuaria e dell'arte scultoria, di qualsiasi materia;

  iii) incisioni, stampe e litografie originali;

  iv) assemblaggi e montaggi artistici originali di qualsiasi materia;

h) manoscritti rari e incunaboli;

i) libri, documenti e pubblicazioni antichi d'interesse particolare (storico, artistico, scientifico, letterario ecc.), isolati o in collezioni;

j) francobolli, marche da bollo e simili, isolati o in collezioni;

k) archivi, compresi gli archivi fonografici, fotografici e cinematografici;

[1] oggetti di mobilia, aventi più di cento anni, e strumenti musicali antichi.

Parte B. Beni culturali di cui all'articolo 4

Categorie di beni culturali conformemente alla parte A	Capitolo, voce o sottovoce della nomenclatura combinata (NC)	Soglia di età minima	Soglia finanziaria minima (valore doganale)	Unità supplementari
c) prodotti di scavi archeologici (regolari o clandestini) e di scoperte archeologiche terrestri o subacquee;	ex 9705; ex 9706	oltre 250 anni	qualunque ne sia il valore	numero di pezzi (p/st)
d) elementi provenienti dallo smembramento di monumenti artistici o storici o di siti archeologici [1];	ex 9705; ex 9706	oltre 250 anni	qualunque ne sia il valore	numero di pezzi (p/st)

[1] Le icone liturgiche e le statue, anche a sé stanti, sono da considerarsi beni culturali appartenenti a questa categoria.

Parte C. Beni culturali di cui all'articolo 5

Categorie di beni culturali conformemente alla parte A	Capitolo, voce o sottovoce della nomenclatura combinata (NC)	Soglia di età minima	Soglia finanziaria minima (valore doganale)	Unità supplementari
a) collezioni ed esemplari rari di fauna, flora, mineralogia e anatomia, e oggetti aventi interesse paleontologico;	ex 9705	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
b) beni riguardanti la storia, comprese la storia della scienza e della tecnica e la storia militare e sociale, nonché la vita dei leader, dei pensatori, degli scienziati e degli artisti nazionali e gli avvenimenti di importanza nazionale;	ex 9705	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
e) oggetti di antichità, quali iscrizioni, monete e sigilli incisi;	ex 9706	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
f) oggetti aventi interesse etnologico;	ex 9705	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
g) oggetti aventi interesse artistico, quali:				
i) quadri, pitture e disegni eseguiti interamente a mano su qualsiasi supporto e di qualsiasi materia (esclusi i disegni industriali e gli oggetti manufatti decorati a mano);	ex 9701	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)

Categorie di beni culturali conformemente alla parte A	Capitolo, voce o sottovoce della nomenclatura combinata (NC)	Soglia di età minima	Soglia finanziaria minima (valore doganale)	Unità supplementari
ii) opere originali dell'arte statuaria e dell'arte scultoria, di qualsiasi materia;	ex 9703	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
iii) incisioni, stampe e litografie originali;	ex 9702	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
iv) assemblaggi e montaggi artistici originali di qualsiasi materia;	ex 9701	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
h) manoscritti rari e incunaboli;	ex 9702; ex 9706	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)
i) libri, documenti e pubblicazioni antichi d'interesse particolare (storico, artistico, scientifico, letterario ecc.) isolati o in collezioni;	ex 9705; ex 9706	oltre 200 anni	18 000 EUR o più al pezzo	numero di pezzi (p/st)

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»)

(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 ([1]),

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di comunicazione elettronica svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione (TIC) sono alla base dei sistemi complessi su cui poggiano le attività quotidiane della società, fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, organizzazioni e imprese di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'Internet degli oggetti (*Internet of Things* — IoT) nel prossimo decennio dovrebbero essere disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi sia connesso a Internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti individuali, nelle organizzazioni e nelle aziende dispongano di informazioni insufficienti sulle caratteristiche dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. La rete e i sistemi informativi sono in grado di aiutarci in tutti gli aspetti della vita e danno impulso alla crescita economica dell'Unione. Sono fondamentali per il raggiungimento del mercato unico digitale.

(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi connessi alla cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di comunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, organizzazioni e imprese, a partire dalle piccole e medie imprese (PMI), quali definite nella raccomandazione della Commissione 2003/361/CE ([4]), fino ai gestori delle infrastrutture critiche.

([1]) GU C 227 del 28.6.2018, pag. 86.
([2]) GU C 176 del 23.5.2018, pag. 29.
([3]) Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.
([4]) Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

(4) Mettendo a disposizione del pubblico le informazioni pertinenti, l'Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security* — ENISA), istituita dal regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio ([5]), contribuisce allo sviluppo del settore della cibersicurezza nell'Unione, in particolare le PMI e le start-up. L'ENISA dovrebbe puntare a una cooperazione più stretta con le università e gli istituti di ricerca al fine di contribuire alla riduzione della dipendenza da prodotti e servizi della cibersicurezza provenienti dall'esterno dell'Unione e a rinforzare le filiere all'interno dell'Unione.

(5) Gli attacchi informatici sono in aumento e la maggiore vulnerabilità alle minacce e agli attacchi informatici di un'economia e di una società connesse impone un rafforzamento delle difese. Tuttavia, mentre gli attacchi informatici avvengono spesso attraverso le frontiere, le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali. Gli incidenti su vasta scala possono ostacolare la prestazione di servizi essenziali in tutto il territorio dell'Unione. Ciò richiede capacità effettive e coordinate di risposta e di gestione delle crisi a livello di Unione, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca. Inoltre, una valutazione periodica dello stato della cibersicurezza e della resilienza nell'Unione, che sia basata su dati affidabili a livello di Unione, e previsioni sistematiche degli sviluppi, delle sfide e delle minacce futuri, a livello di Unione e a livello mondiale, sono importanti per i responsabili delle politiche, il settore e gli utenti.

(6) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura il rafforzamento ulteriore delle capacità e della preparazione degli Stati membri e delle imprese e il miglioramento della cooperazione, la condivisione di informazioni e il coordinamento tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare nei casi di crisi e incidenti transfrontalieri su vasta scala, pur tenendo conto dell'importanza di mantenere e rafforzare ulteriormente le capacità nazionali di risposta alle minacce informatiche di qualsiasi dimensione.

(7) Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la cibersicurezza. In aggiunta, dato che gli incidenti minano la fiducia nei fornitori di servizi digitali e nel mercato unico digitale stesso, soprattutto fra i consumatori, essa dovrebbe essere ulteriormente rafforzata fornendo informazioni in maniera trasparente in merito al livello di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC che evidenzi che persino un livello elevato di certificazione della cibersicurezza non può garantire che un prodotto TIC, un servizio TIC o un processo TIC sia completamente sicuro. Un aumento di fiducia può essere agevolato da una certificazione a livello di Unione che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

(8) La cibersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'«igiene informatica», vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche.

(9) Al fine di rafforzare le strutture della cibersicurezza dell'Unione, è importante mantenere e sviluppare le capacità degli Stati membri di rispondere in modo globale alle minacce informatiche, compresi gli incidenti transfrontalieri.

(10) Le imprese e i singoli consumatori dovrebbero disporre di informazioni precise sul livello di affidabilità con cui è stata certificata la sicurezza dei loro prodotti TIC, servizi TIC e processi TIC. Allo stesso tempo, nessun prodotto TIC o servizio TIC garantisce completamente la cibersicurezza e bisogna promuovere regole basilari sull'igiene informatica, dando loro la priorità. Alla luce della crescente disponibilità di dispositivi IoT, vi è una serie di misure volontarie che il settore privato può adottare per rafforzare la fiducia nella sicurezza dei prodotti TIC, servizi TIC e processi TIC.

(11) I moderni prodotti e sistemi TIC spesso integrano e utilizzano una o più tecnologie e componenti terzi quali moduli software, biblioteche o interfacce per programmi applicativi. Tale utilizzo, detto «dipendenza», potrebbe presentare rischi supplementari connessi alla cibersicurezza in quanto le vulnerabilità riscontrate in componenti terzi potrebbero pregiudicare anche la sicurezza dei prodotti TIC, servizi TIC e processi TIC. In molti casi, l'individuazione e la documentazione di tali dipendenze consentono agli utenti finali dei prodotti TIC, servizi TIC e processi TIC di migliorare le loro attività di gestione dei rischi in materia di cibersicurezza ottimizzando, ad esempio, le procedure messe in atto per individuare le vulnerabilità e porvi rimedio.

([5]) Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).

(12) Le organizzazioni, i fabbricanti o i fornitori coinvolti nella progettazione e nello sviluppo di prodotti TIC, servizi TIC e processi TIC dovrebbero essere incoraggiati ad attuare misure nelle prime fasi di progettazione e sviluppo per tutelare il più possibile sin dall'inizio la sicurezza di tali prodotti, servizi e processi, in modo che si presuma il verificarsi di attacchi informatici e se ne anticipi e riduca al minimo l'impatto («sicurezza fin dalla progettazione»). La sicurezza dovrebbe essere assicurata in tutto il ciclo di vita del prodotto TIC, servizio TIC o processo TIC, con un'evoluzione costante dei processi di progettazione e sviluppo al fine di ridurre il rischio di danni derivanti da un utilizzo doloso.

(13) Le imprese, le organizzazioni e il settore pubblico dovrebbero configurare i prodotti TIC, servizi TIC o processi TIC da loro progettati in modo da garantire un livello di sicurezza superiore che dovrebbe consentire al primo utente di ricevere una configurazione predefinita con le impostazioni più sicure possibili («sicurezza predefinita»), riducendo al contempo l'onere in capo agli utenti di dover configurare un prodotto TIC, servizio TIC o processo TIC in modo adeguato. La sicurezza predefinita non dovrebbe necessitare di configurazioni dettagliate né di conoscenze tecniche specifiche o di un comportamento non intuitivo da parte dell'utente, e dovrebbe funzionare in modo semplice e affidabile quando attuata. Qualora, su base puntuale, un'analisi del rischio e dell'usabilità porti a concludere che tali impostazioni predefinite non sono attuabili, gli utenti dovrebbero essere sollecitati a optare per l'impostazione più sicura.

(14) Il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio ([6]) ha istituito l'ENISA al fine di contribuire ad assicurare un livello di sicurezza elevato ed efficace delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni pubbliche. Il regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio ([7]) ha prorogato il mandato dell'ENISA fino a marzo 2012. Il regolamento (EU) n. 580/2011 del Parlamento europeo e del Consiglio ([8]) ha prorogato ulteriormente il mandato dell'ENISA fino al 13 settembre 2013. Il regolamento (UE) n. 526/2013 ha prorogato il mandato dell'ENISA fino al 19 giugno 2020.

(15) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la Strategia dell'Unione europea per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi informatici. Nell'intento di proteggere maggiormente i cittadini online, nel 2016 è stato adottato il primo atto giuridico nel campo della cibersicurezza, vale a dire la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([9]). La direttiva (UE) 2016/1148 ha stabilito obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, fornitura e distribuzione di acqua potabile, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di *cloud computing* e mercati online).

All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza. Altri atti giuridici, quali il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([10]) e le direttive 2002/58/CE ([11]) e (UE) 2018/1972 ([12]) del Parlamento europeo e del Consiglio, contribuiscono inoltre a un elevato livello di cibersicurezza nel mercato unico digitale.

([6]) Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1).

([7]) Regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008, pag. 1).

([8]) Regolamento (UE) n. 580/2011 del Parlamento europeo e del Consiglio, dell'8 giugno 2011, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 165 del 24.6.2011, pag. 3).

([9]) 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).

([10]) 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).

([11]) 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).

([12]) 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).

(16) Dall'adozione della Strategia dell'Unione europea per la cibersicurezza nel 2013 e dall'ultima revisione del mandato dell'ENISA, il contesto politico generale è cambiato in modo significativo, in quanto il contesto globale è diventato più incerto e meno sicuro. Data la situazione e considerato lo sviluppo positivo del ruolo dell'ENISA quale punto di riferimento per pareri e competenze e facilitatore della cooperazione e dello sviluppo delle capacità, nonché nel quadro della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama della minaccia informatica, a fronte del quale l'attuale mandato non è sufficiente, come riconosciuto in fase di valutazione dell'ENISA.

(17) L'ENISA istituita dal presente regolamento dovrebbe succedere all'ENISA istituita con il regolamento (UE) n. 526/2013. L'ENISA dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli altri atti giuridici dell'Unione nel campo della cibersicurezza, anche fornendo pareri e competenze e fungendo da centro di informazioni e conoscenze dell'Unione. Dovrebbe promuovere lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornire suggerimenti strategici alla Commissione e agli Stati membri, fungere da punto di riferimento per iniziative politiche settoriali dell'Unione sulle questioni di cibersicurezza e promuovere la cooperazione operativa, sia tra gli Stati membri sia tra questi ultimi e le istituzioni, gli organi e gli organismi dell'Unione.

(18) Nel quadro della decisione 2004/97/CE, Euratom adottata di comune accordo dai rappresentanti dei governi degli Stati membri, riuniti a livello di capi di Stato o di governo ([13]), i rappresentanti degli Stati membri hanno deciso che la sede dell'ENISA sarebbe stata in Grecia, in una città designata dal governo greco. Lo Stato membro ospitante dovrebbe garantire le migliori condizioni possibili per il corretto ed efficace funzionamento dell'ENISA. Per uno svolgimento adeguato ed efficiente dei suoi compiti, per l'assunzione e il trattenimento del personale e per aumentare l'efficacia delle attività di rete, è imprescindibile che l'ENISA sia ubicata in una sede adeguata che garantisca, tra l'altro, collegamenti e infrastrutture di trasporto appropriati per i coniugi e i figli del personale. Le disposizioni necessarie dovrebbero essere fissate in un accordo concluso tra l'ENISA e lo Stato membro ospitante, previa approvazione del consiglio di amministrazione dell'ENISA.

(19) Tenuto conto dei rischi e delle sfide crescenti in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'ENISA dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale dell'Unione, consentendo all'ENISA di svolgere efficacemente i compiti che le sono conferiti dal presente regolamento.

(20) È opportuno che l'ENISA sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'ENISA dovrebbe sostenere attivamente gli sforzi nazionali e contribuire in modo proattivo agli sforzi dell'Unione, collaborando pienamente con le istituzioni, gli organi e gli organismi dell'Unione e con gli Stati membri, evitando la duplicazione delle attività e promuovendo le sinergie. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione del settore privato e di altri portatori d'interessi. È opportuno stabilire una serie di compiti che definiscano in che modo l'ENISA debba raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione.

(21) Per poter fornire adeguato sostegno alla cooperazione operativa tra gli Stati membri, l'ENISA dovrebbe rafforzare ulteriormente le proprie capacità e abilità tecniche e umane. L'ENISA dovrebbe incrementare il proprio know-how e le proprie capacità. L'ENISA e gli Stati membri, su base volontaria, potrebbero sviluppare programmi per il distacco di esperti nazionali presso l'ENISA, la creazione di pool di esperti e lo scambio di personale.

(22) L'ENISA dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione, l'aggiornamento e la revisione di politiche e normative nel campo della cibersicurezza, nonché i relativi aspetti settoriali al fine di rafforzare la pertinenza delle politiche e normative dell'Unione aventi una dimensione di cibersicurezza e assicurarne la coerenza dell'attuazione a livello nazionale. L'ENISA dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative settoriali dell'Unione che presentano aspetti correlati alla cibersicurezza. L'ENISA dovrebbe informare periodicamente il Parlamento europeo in merito alle sue attività.

([13]) Decisione 2004/97/CE, Euratom adottata di comune accordo dai rappresentanti dei governi degli Stati membri, riuniti a livello di capi di Stato o di governo, del 13 dicembre 2003, relativa alla fissazione delle sedi di taluni uffici ed agenzie dell'Unione europea (GU L 29 del 3.2.2004, pag. 15).

(23) Il nucleo pubblico dell'Internet aperta, vale a dire i suoi protocolli e le sue infrastrutture principali, che costituiscono un bene pubblico globale, consente la funzionalità essenziale di Internet nel suo complesso e ne supporta il normale funzionamento. L'ENISA dovrebbe sostenere la sicurezza del nucleo pubblico dell'Internet aperta e la stabilità del suo funzionamento, compresi, solo a titolo di esempio, i protocolli chiave (in particolare DNS, BGP e IPv6), il funzionamento del sistema dei nomi di dominio (come il funzionamento di tutti i domini di primo livello) e il funzionamento della zona root.

(24) Il compito di base dell'ENISA è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva (UE) 2016/1148 e degli altri strumenti giuridici pertinenti che presentano aspetti relativi alla cibersicurezza, che è essenziale per rafforzare la ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.

(25) L'ENISA dovrebbe assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare le minacce e gli incidenti e relativi alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — «CSIRT») nazionali e dell'Unione previsti dalla direttiva (UE) 2016/1148 perché raggiungano un livello comune elevato di maturità nell'Unione. Le attività svolte dall'ENISA in relazione alle capacità operative degli Stati membri dovrebbero sostenere attivamente le azioni intraprese dagli Stati membri per adempiere agli obblighi derivanti dalla direttiva (UE) 2016/1148 e non dovrebbero pertanto sostituirsi a esse.

(26) L'ENISA dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie in materia di sicurezza delle reti e dei sistemi informativi a livello di Unione e, su richiesta, a livello di Stati membri, in particolare per quanto riguarda la cibersicurezza, e dovrebbe promuovere la diffusione di tali strategie e seguirne il progresso della loro attuazione. Dovrebbe inoltre contribuire a soddisfare la necessità di formazione e materiale formativo, comprese le necessità degli enti pubblici e, se del caso, in larga misura «formare i formatori», basandosi sul quadro delle competenze digitali per i cittadini al fine di assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nello sviluppo di capacità di formazione autonome.

(27) L'ENISA dovrebbe sostenere gli Stati membri nel campo della sensibilizzazione e dell'istruzione in materia di cibersicurezza facilitando un coordinamento più stretto e lo scambio delle migliori pratiche tra Stati membri. Tale sostegno potrebbe consistere nello sviluppo di una rete di punti di contatto nazionali in materia di istruzione e di una piattaforma di formazione sulla cibersicurezza. La rete di punti di contatto nazionali in materia di istruzione potrebbe operare nel quadro della rete dei funzionari nazionali di collegamento e costituire un punto di partenza per il coordinamento futuro all'interno degli Stati membri.

(28) L'ENISA dovrebbe assistere il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 nell'esecuzione dei suoi compiti, in particolare mettendo a disposizione competenze, fornendo consulenze e agevolando lo scambio di migliori pratiche, tra l'altro per quanto riguarda l'individuazione degli operatori di servizi essenziali da parte degli Stati membri, nonché in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

(29) Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, in particolare per sostenere la protezione delle infrastrutture critiche, l'ENISA dovrebbe sostenere la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili e sulle procedure, nonché fornendo orientamenti su come affrontare le questioni normative relative alla condivisione delle informazioni, ad esempio agevolando la creazione di centri settoriali di condivisione e di analisi delle informazioni.

(30) Considerando il potenziale impatto negativo delle vulnerabilità nei prodotti TIC, servizi TIC e processi TIC è in costante aumento, nella riduzione del rischio totale connesso alla cibersicurezza è di considerevole importanza individuare ed eliminare tali vulnerabilità. È comprovato che la cooperazione tra le organizzazioni, i fabbricanti o i fornitori di prodotti TIC, servizi TIC e processi TIC vulnerabili, i membri della comunità di ricerca in materia di cibersicurezza e le autorità che individuano tali vulnerabilità accresce considerevolmente il tasso di individuazione e di eliminazione delle vulnerabilità nei prodotti TIC, servizi TIC e processi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato di cooperazione in cui le vulnerabilità sono segnalate al proprietario del sistema informativo, offrendo in tal modo all'organizzazione la possibilità di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano comunicate a terze parti o al pubblico. Il processo prevede anche il coordinamento tra la parte che ha individuato le vulnerabilità e l'organizzazione per quanto riguarda la pubblicazione di dette vulnerabilità. Le politiche di gestione della divulgazione coordinata delle vulnerabilità potrebbero svolgere un ruolo importante negli sforzi degli Stati membri tesi a migliorare la cibersicurezza.

(31) L'ENISA dovrebbe aggregare e analizzare le relazioni nazionali volontariamente condivise dei CSIRT e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione istituita dall'accordo tra il Parlamento europeo, il Consiglio europeo, il Consiglio dell'Unione europea, la Commissione europea, la Corte di giustizia dell'Unione europea, la Banca centrale europea, la Corte dei conti europea, il Servizio europeo per l'azione esterna, il Comitato economico e sociale europeo, il Comitato europeo delle regioni e la Banca europea per gli investimenti sull'organizzazione e il funzionamento della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (*Computer Emergency Response Team* — «CERT-UE») ([14]) allo scopo di contribuire alla definizione di procedure, lingua e terminologia comuni per lo scambio delle informazioni. In tale contesto l'ENISA dovrebbe coinvolgere il settore privato nell'ambito della direttiva (UE) 2016/1148, che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo, nella rete di gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Teams* — «rete CSIRT») istituita da tale direttiva.

(32) L'ENISA dovrebbe contribuire a una risposta a livello di Unione in caso di crisi e incidenti transfrontalieri su vasta scala relativi alla cibersicurezza. Tale compito dovrebbe essere espletato questa funzione conformemente al mandato assegnatole ai sensi del presente regolamento e a un approccio da concordarsi tra gli Stati membri nel contesto della raccomandazione (UE) 2017/1584 della Commissione ([15]) e delle conclusioni del Consiglio del 26 giugno 2018 relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala. Tale compito potrebbe comprendere la raccolta delle informazioni pertinenti e il ruolo di facilitatore tra la rete di CSIRT e la comunità tecnica nonché tra i responsabili decisionali nella gestione delle crisi. Inoltre, l'ENISA dovrebbe sostenere la cooperazione operativa tra gli Stati membri, se richiesto da uno o più Stati membri, nella gestione degli incidenti dal punto di vista tecnico, agevolando gli scambi di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'ENISA dovrebbe sostenere la cooperazione operativa sottoponendo a prova le modalità di tale cooperazione attraverso esercitazioni periodiche di cibersicurezza.

(33) Nel sostenere la cooperazione operativa, l'ENISA dovrebbe avvalersi delle competenze tecniche e operative disponibili della CERT-UE attraverso una cooperazione strutturata. Tale cooperazione strutturata potrebbe fondarsi sulle competenze dell'ENISA. Se del caso, dovrebbero essere conclusi appositi accordi tra i due soggetti per definire l'attuazione pratica di tale cooperazione ed evitare la duplicazione delle attività.

(34) Nello svolgere il suo compito di sostegno della cooperazione operativa nell'ambito della rete di CSIRT, l'ENISA dovrebbe essere in grado di assistere gli Stati membri su loro richiesta, ad esempio fornendo consulenza su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi, agevolando la gestione tecnica di incidenti aventi un impatto rilevante o sostanziale, o assicurando che minacce e incidenti informatici siano analizzati. L'ENISA dovrebbe agevolare la gestione tecnica di incidenti aventi un impatto rilevante o sostanziale, in particolare sostenendo la condivisione volontaria di soluzioni tecniche tra gli Stati membri o producendo informazioni tecniche combinate, quali soluzioni tecniche volontariamente condivise dagli Stati membri. Nella raccomandazione (UE) 2017/1584, la Commissione raccomanda agli Stati membri di cooperare in buona fede e di condividere tra loro e con l'ENISA, senza indebiti ritardi, le informazioni sugli incidenti e le crisi su vasta scala relativi alla cibersicurezza. Tali informazioni aiuterebbero ulteriormente l'ENISA nello svolgimento dei suoi compiti di sostegno alla cooperazione operativa.

(35) Nell'ambito della costante cooperazione a livello tecnico per sostenere la consapevolezza della situazione dell'Unione, l'ENISA dovrebbe elaborare periodicamente, in stretta cooperazione con gli Stati membri, una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatici, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise dai CSIRT degli Stati membri o dai punti di contatto unici in materia di sicurezza delle reti e dei sistemi informativi («punti di contatto unici») previsti dalla direttiva (UE) 2016/1148, in entrambi i casi su base volontaria, dal Centro europeo per la lotta alla criminalità informatica (*European Cybercrime Centre* — EC3) presso Europol, dalla CERT-UE e, ove necessario, dal Centro UE di situazione e di intelligence (*European Union Intelligence and Situation Centre* — EU INTCEN) presso il Servizio europeo per l'azione esterna. Tale relazione dovrebbe essere messa a disposizione del Consiglio, della Commissione, dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e della rete di CSIRT.

(36) Il sostegno dell'ENISA alle indagini tecniche ex post effettuate, su richiesta degli Stati membri interessati, sugli incidenti aventi un impatto rilevante o sostanziale dovrebbe essere incentrato sulla prevenzione degli incidenti futuri. Gli Stati membri interessati dovrebbero fornire le informazioni e l'assistenza necessarie per consentire all'ENISA di sostenere efficacemente l'indagine tecnica ex post.

([14]) GU C 12 del 13.1.2018, pag. 1.
([15]) 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).

(37) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'ENISA, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale e le informazioni pertinenti alla pubblica sicurezza.

(38) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni, agli organi e agli organismi dell'Unione, l'ENISA ha bisogno di analizzare i rischi attuali ed emergenti connessi alla cibersicurezza. A tal fine, in cooperazione con gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'ENISA dovrebbe raccogliere le informazioni pertinenti pubblicamente disponibili o volontariamente condivise, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'ENISA dovrebbe inoltre assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nell'individuazione dei rischi emergenti connessi alla cibersicurezza e nella prevenzione degli incidenti attraverso l'analisi di minacce informatiche, vulnerabilità e incidenti.

(39) Al fine di aumentare la resilienza dell'Unione, l'ENISA dovrebbe sviluppare le competenze nel campo della cibersicurezza delle infrastrutture, in particolare per sostenere i settori di cui all'allegato II della direttiva (UE) 2016/1148 e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva, fornendo consulenza, emanando orientamenti e scambiando migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'ENISA dovrebbe sviluppare e mantenere il «polo d'informazione» dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dagli organi e dagli organismi dell'Unione e nazionali. Facilitare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili misure correttive potrebbe anche aiutare gli Stati membri a rafforzare le loro capacità, ad allineare le loro pratiche migliorando così la loro resilienza generale agli attacchi informatici.

(40) L'ENISA dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza, anche per mezzo di una campagna di sensibilizzazione in tutta l'UE promuovendo l'istruzione, e a fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini, organizzazioni e imprese. L'ENISA dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni, igiene informatica e alfabetizzazione informatica comprese, a livello di cittadini, organizzazioni e imprese mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione e la pubblicazione di relazioni e orientamenti per cittadini, organizzazioni e imprese, e a migliorare il livello complessivo di preparazione e resilienza di questi. L'ENISA dovrebbe impegnarsi, inoltre, a comunicare ai consumatori le informazioni pertinenti relative ai sistemi di certificazione applicabili, ad esempio fornendo orientamenti e raccomandazioni. L'ENISA dovrebbe inoltre organizzare regolarmente, in linea con il piano d'azione per l'istruzione digitale stabilito nella comunicazione della Commissione del 17 gennaio 2018 e in cooperazione con gli Stati membri e con le istituzioni, gli organi e gli organismi dell'Unione, campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali per promuovere comportamenti online più sicuri da parte degli individui e l'alfabetizzazione digitale, di accrescere la consapevolezza circa le potenziali minacce informatiche, compresa l'attività informatica online, ad esempio *phishing*, *botnet*, frodi finanziarie e bancarie, casi di frode di dati, nonché di promuovere consigli di base in materia di autenticazione multifattoriale, *patching*, cifratura, anonimizzazione e protezione dei dati.

(41) L'ENISA dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi e sull'uso sicuro dei servizi, e dovrebbe promuovere sicurezza e privacy fin dalla progettazione a livello di Unione. Nel perseguire tale obiettivo, l'ENISA dovrebbe utilizzare le migliori pratiche ed esperienze disponibili, in particolare quelle delle istituzioni universitarie e dei ricercatori che si occupano di sicurezza informatica.

(42) Al fine di sostenere le imprese operanti nel campo della cibersicurezza, come pure gli utilizzatori delle soluzioni di cibersicurezza, l'ENISA dovrebbe sviluppare e mantenere un «osservatorio del mercato» mediante l'esecuzione di analisi periodiche e la diffusione di informazioni sulle principali tendenze del mercato della cibersicurezza, sul versante sia della domanda che dell'offerta.

(43) L'ENISA dovrebbe contribuire agli sforzi di cooperazione dell'Unione con organizzazioni internazionali come anche nell'ambito dei pertinenti quadri di cooperazione internazionale nel campo della cibersicurezza. In particolare dovrebbe contribuire, se del caso, alla cooperazione con organizzazioni quali l'OCSE, l'OSCE e la NATO. Tale cooperazione potrebbe comprendere, tra l'altro, esercitazioni congiunte di cibersicurezza e il coordinamento congiunto della risposta agli incidenti. Occorre che tali attività si svolgano nel pieno rispetto dei principi di inclusività, reciprocità e autonomia decisionale dell'Unione, fatto salvo il carattere specifico della politica di sicurezza e di difesa di ciascuno Stato membro.

(44) Per conseguire appieno i propri obiettivi, l'ENISA dovrebbe instaurare rapporti con le autorità di vigilanza dell'Unione e con altre autorità competenti nell'Unione, le istituzioni, gli organi e gli organismi pertinenti dell'Unione, compresi la CERT-UE, l'EC3, l'Agenzia europea per la difesa (AED), l'Agenzia del sistema globale di navigazione via satellite europeo (Agenzia del GNSS europeo), l'organismo dei regolatori europei delle comunicazioni elettroniche (*Body of European Regulators for Electronic Communications* — BEREC), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE), il comitato europeo per la protezione dei dati (*European Data Protection Board* — EDPB), l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (*Agency for the Cooperation of Energy Regulators* — ACER), l'Agenzia europea per la sicurezza aerea (*European Union Aviation Safety Agency* — EASA) e tutte le agenzie dell'Unione coinvolte nella cibersicurezza. L'ENISA dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo di consulenza dell'ENISA. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'ENISA dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

(45) Si potrebbero istituire partenariati con le istituzioni universitarie che hanno avviato iniziative di ricerca nei settori interessati e vi dovrebbero essere opportuni canali per il contributo delle organizzazioni dei consumatori e di altre organizzazioni, che dovrebbe essere preso in considerazione.

(46) L'ENISA, nel suo ruolo di segretariato della rete di CSIRT, dovrebbe sostenere i CSIRT degli Stati membri e la CERT-UE nella cooperazione operativa in relazione a tutte le pertinenti funzioni della rete di CSIRT di cui alla direttiva (UE) 2016/1148. Inoltre, l'ENISA dovrebbe promuovere e sostenere la cooperazione tra i CSIRT interessati in caso di incidenti, attacchi o perturbazioni delle reti o delle infrastrutture della cui gestione o protezione sono responsabili i CSIRT e nei quali siano o possano essere coinvolti almeno due CSIRT, tenendo debitamente conto delle procedure operative standard della rete di CSIRT.

(47) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti, l'ENISA dovrebbe organizzare periodicamente esercitazioni di cibersicurezza a livello di Unione e, su loro richiesta, assistere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione e nell'organizzazione delle esercitazioni. Ogni due anni dovrebbero essere organizzate esercitazioni globali su vasta scala che comprendano elementi tecnici, operativi o strategici. L'ENISA dovrebbe poter inoltre organizzare periodicamente esercitazioni meno estese con lo stesso obiettivo di rafforzare la preparazione dell'Unione nel rispondere agli incidenti.

(48) L'ENISA dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'Unione in tale campo. L'ENISA dovrebbe basarsi sulle migliori pratiche esistenti e promuovere la diffusione della certificazione della cibersicurezza nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione (quadro europeo di certificazione della cibersicurezza) al fine di aumentare la trasparenza dell'affidabilità dei prodotti TIC, servizi TIC e processi TIC in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.

(49) Strategie efficaci in materia di cibersicurezza dovrebbero essere basate su buoni metodi di valutazione dei rischi, sia nel settore pubblico che in quello privato. I metodi di valutazione dei rischi sono utilizzati a diversi livelli, e non esiste una prassi comune per quanto riguarda le modalità per una loro applicazione efficiente. La promozione e lo sviluppo di migliori pratiche per la valutazione dei rischi e per soluzioni interoperabili per la loro gestione nelle organizzazioni del settore pubblico e del settore privato aumenteranno il livello di cibersicurezza nell'Unione. A tal fine, l'ENISA dovrebbe sostenere la cooperazione tra i portatori di interessi a livello di Unione e facilitare il loro impegno nella definizione e nella diffusione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza misurabile di prodotti, sistemi, reti e servizi elettronici che, insieme ai software, costituiscono le reti e i sistemi informativi.

(50) L'ENISA dovrebbe incoraggiare gli Stati membri, i fabbricanti o i fornitori prodotti TIC, servizi TIC o processi TIC a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di Internet possano adottare le misure necessarie a garantire la propria cibersicurezza e incentivarli a farlo. In particolare, i fabbricanti e i fornitori di servizi di prodotti TIC, servizi TIC o processi TIC dovrebbero fornire tutti i necessari aggiornamenti e richiamare, ritirare o riciclare i prodotti TIC, i servizi TIC o i processi TIC non conformi alle norme in materia di cibersicurezza, mentre gli importatori e i distributori dovrebbero garantire che i prodotti TIC, servizi TIC e processi TIC che immettono sul mercato dell'Unione siano conformi ai requisiti applicabili e non presentino rischi per i consumatori dell'Unione.

(51) In collaborazione con le autorità competenti, l'ENISA dovrebbe poter diffondere informazioni sul livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC offerti nel mercato interno e dovrebbe rivolgere avvertimenti ai fabbricanti e ai fornitori di prodotti TIC, servizi TIC o processi TIC imponendo loro di migliorare la sicurezza dei loro prodotti TIC, servizi TIC o processi TIC, ivi inclusa la cibersicurezza.

(52) L'ENISA dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, agli organi e agli organismi dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca e le priorità nel campo della cibersicurezza. Per individuare le esigenze e priorità in materia di ricerca, l'ENISA dovrebbe inoltre consultare i pertinenti gruppi di utenti. Più nello specifico si potrebbe istituire una cooperazione con il Consiglio europeo della ricerca, con l'Istituto europeo di innovazione e tecnologia e con l'Istituto dell'Unione europea per gli studi sulla sicurezza.

(53) L'ENISA dovrebbe consultare regolarmente le organizzazioni di normazione, in particolare quelle europee, nell'elaborare i sistemi europei di certificazione della cibersicurezza.

(54) Le minacce informatiche sono un problema globale. È necessaria una più stretta cooperazione internazionale per migliorare le norme di cibersicurezza, anche definendo norme di comportamento, ed è necessaria l'adozione di codici di condotta comuni, l'utilizzo di norme internazionali e la condivisione di informazioni, promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'ENISA dovrebbe sostenere una partecipazione e una cooperazione maggiori dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo le competenze e le analisi necessarie alle istituzioni, agli organi e agli organismi dell'Unione competenti, se del caso.

(55) L'ENISA dovrebbe essere in grado di rispondere alle richieste specifiche di consulenza e di assistenza inoltrate dagli Stati membri e dalle istituzioni, dagli organi e dagli organismi dell'Unione su materie che rientrano nei suoi obiettivi.

(56) È ragionevole e raccomandabile applicare taluni principi per la gestione dell'ENISA al fine di conformarsi alla dichiarazione congiunta e nell'approccio comune concordati nel luglio 2012 dal gruppo di lavoro interistituzionale sulle agenzie decentrate dell'Unione, il cui obiettivo è di razionalizzare le attività delle agenzie decentrate e di migliorarne l'efficacia. Le raccomandazioni contenute nella dichiarazione congiunta e nell'approccio comune dovrebbero riflettersi, se del caso, nei programmi di lavoro dell'ENISA, nelle sue valutazioni e nelle sue prassi di informazione e amministrazione.

(57) Il consiglio di amministrazione, composto dai rappresentanti degli Stati membri e della Commissione, dovrebbe stabilire l'orientamento generale delle operazioni dell'ENISA e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificare l'esecuzione del bilancio, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'ENISA, adottare il documento unico di programmazione dell'ENISA, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione e alla conclusione del suo mandato.

(58) Per garantire il funzionamento corretto ed efficace dell'ENISA, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze professionali e di esperienza adeguate. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori.

(59) Il corretto funzionamento dell'ENISA esige che il direttore esecutivo sia nominato in base ai meriti e alle comprovate abilità amministrative e manageriali, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza. Le funzioni del direttore esecutivo dovrebbero essere svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'ENISA e adottare tutte le misure necessarie a garantirne l'adeguata attuazione. Il direttore esecutivo dovrebbe redigere una relazione annuale da trasmettere al consiglio di amministrazione che includa l'attuazione del programma di lavoro annuale dell'ENISA, fornire un progetto di stato di previsione delle entrate e delle spese dell'ENISA e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura scientifica, tecnica, giuridica o socio-economica. Si considera necessaria l'istituzione di un gruppo ad hoc soprattutto per quanto riguarda la preparazione di una specifica proposta di sistema europeo di certificazione della cibersicurezza («proposta di sistema»). Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti

secondo i più elevati standard di competenza, con l'intento di garantire un equilibrio di genere e un equilibrio adeguato, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e il settore privato, tra cui le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

(60) Il comitato esecutivo dovrebbe contribuire al funzionamento efficace del consiglio di amministrazione. Nel quadro dei lavori preparatori relativi alle decisioni del consiglio di amministrazione, il comitato esecutivo dovrebbe esaminare dettagliatamente le informazioni pertinenti, valutare le opzioni disponibili e fornire consulenza e soluzioni per la preparazione delle decisioni del consiglio di amministrazione.

(61) È opportuno che l'ENISA disponga di un gruppo consultivo ENISA come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo consultivo ENISA, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'ENISA. Il gruppo consultivo ENISA dovrebbe essere consultato in particolare in merito al progetto di programma di lavoro annuale dell'ENISA. La composizione del gruppo consultivo ENISA e i compiti assegnatigli dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'ENISA.

(62) È opportuno istituire il gruppo dei portatori di interessi per la certificazione della cibersicurezza al fine di aiutare l'ENISA e la Commissione ad agevolare la consultazione con i pertinenti portatori di interessi. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza dovrebbe essere costituito da membri che rappresentino il settore in proporzione equilibrata, sul versante sia della domanda che dell'offerta di prodotti TIC e servizi TIC, fra cui in particolare le PMI, i fornitori di servizi digitali, gli organismi europei e internazionali di normazione, gli organismi nazionali di accreditamento, le autorità di controllo preposte alla protezione dei dati e gli organismi di valutazione della conformità a norma del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([16]), e le università, nonché le organizzazioni dei consumatori.

(63) L'ENISA dovrebbe disporre di regole relative alla prevenzione e alla gestione dei conflitti di interessi. L'ENISA dovrebbe inoltre applicare le disposizioni pertinenti dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([17]). Il trattamento dei dati personali da parte dell'ENISA dovrebbe avvenire in conformità del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([18]). È opportuno che l'ENISA si conformi alle disposizioni applicabili alle istituzioni, gli organi e gli organismi dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate UE (ICUE).

(64) Per garantire all'ENISA piena autonomia e indipendenza e consentirle di svolgere compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'ENISA. Un idoneo bilancio è essenziale per garantire che l'ENISA disponga di capacità sufficienti ad adempiere i suoi crescenti compiti e conseguire i suoi obiettivi nella loro totalità. La maggior parte del personale dell'ENISA dovrebbe essere impiegata nell'attuazione operativa del suo mandato. Allo Stato membro ospitante, e a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente al bilancio dell'ENISA. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della rendicontabilità, la revisione contabile dell'ENISA dovrebbe essere svolta dalla Corte dei conti.

(65) La certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti TIC, servizi TIC e processi TIC e nell'accrescere la fiducia negli stessi. Il mercato unico digitale, in particolare l'economia dei dati e l'Internet degli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti, servizi e processi offrono un determinato livello di cibersicurezza. Le automobili connesse e automatizzate, i dispositivi medici elettronici, i sistemi di controllo per l'automazione industriale e le reti elettriche intelligenti sono solo alcuni esempi di settori in cui la certificazione è già ampiamente utilizzata o sarà probabilmente utilizzata in un prossimo futuro. La certificazione della cibersicurezza riveste un'importanza fondamentale anche nei settori disciplinati dalla direttiva (UE) 2016/1148.

([16]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

([17]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

([18]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

(66) Nella comunicazione del 2016 dal titolo «Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza» la Commissione ha sottolineato la necessità di prodotti e soluzioni di alta qualità, a costi contenuti e interoperabili. L'offerta di prodotti, servizi TIC e processi TIC nel mercato unico resta molto frammentata dal punto di vista geografico. La causa di tale frammentazione va ravvisata nel fatto che il settore della cibersicurezza in Europa si è sviluppato soprattutto in risposta alla domanda pubblica nazionale. Inoltre, l'assenza di soluzioni interoperabili (norme tecniche), di pratiche e di meccanismi di certificazione nell'Unione è un'altra delle lacune che influisce sul mercato unico nel campo della cibersicurezza. Ciò incide negativamente sulla competitività delle imprese europee a livello nazionale, dell'Unione e mondiale. Allo stesso tempo limita la gamma di tecnologie di cibersicurezza valide e utilizzabili a cui cittadini e imprese hanno accesso. Anche nella comunicazione del 2017 sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale — Un mercato unico digitale connesso per tutti, la Commissione ha evidenziato la necessità di prodotti e sistemi connessi sicuri e ha dichiarato che la creazione di un quadro europeo di sicurezza delle TIC che definisca regole su come organizzare la certificazione della sicurezza delle TIC nell'Unione potrebbe sia preservare la fiducia nei confronti di Internet sia permettere di affrontare l'attuale frammentazione del mercato interno.

(67) Attualmente la certificazione della cibersicurezza di prodotti TIC, servizi TIC e processi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dal settore. In tale contesto, un certificato rilasciato da un'autorità nazionale di certificazione della cibersicurezza non è, in linea di principio, riconosciuto negli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti TIC, servizi TIC e processi TIC nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti, il che aumenta i relativi costi. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'Internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo, impedendo meccanismi di riconoscimento reciproco nell'Unione.

(68) Sono stati compiuti sforzi finalizzati a garantire il reciproco riconoscimento dei certificati all'interno dell'Unione. Il loro successo tuttavia è stato solo parziale. L'esempio più importante in tal senso è l'accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (*Senior Officials Group — Information Systems Security* — SOG-IS). Sebbene rappresenti il più importante modello di cooperazione e di riconoscimento reciproco nel campo della certificazione della sicurezza, il SOG-IS comprende solo alcuni Stati membri. Ciò ha limitato l'efficacia dell'ARR del SOG-IS dal punto di vista del mercato interno.

(69) È pertanto necessario adottare un approccio comune e definire un quadro europeo di certificazione della cibersicurezza che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e che consenta di riconoscere e utilizzare i certificati europei di cibersicurezza e le dichiarazioni UE di conformità per i prodotti TIC, i servizi TIC o i processi TIC in tutti gli Stati membri. In questo senso, è essenziale basarsi sui sistemi nazionali e internazionali esistenti, nonché sui sistemi di riconoscimento reciproco, in particolare il SOG-IS, e consentire un'agevole transizione dai sistemi esistenti funzionanti nel loro ambito verso sistemi basati sul nuovo quadro europeo di certificazione della cibersicurezza. Il quadro europeo di certificazione della cibersicurezza dovrebbe avere un duplice obiettivo. In primo luogo dovrebbe contribuire ad aumentare la fiducia nei prodotti TIC, servizi TIC e processi TIC che sono stati certificati in base a detti sistemi europei di certificazione della cibersicurezza. In secondo luogo, dovrebbe evitare il proliferare di sistemi di certificazione nazionali della cibersicurezza confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi europei di certificazione della cibersicurezza dovrebbero essere non discriminatori e basati su norme europee o internazionali, a meno che tali norme non siano inefficaci o inadeguate ai fini del conseguimento dei legittimi obiettivi dell'Unione in tale ambito.

(70) Il quadro europeo di certificazione della cibersicurezza dovrebbe essere istituito in modo uniforme in tutti gli Stati membri, in modo da evitare la scelta della certificazione più vantaggiosa in base ai diversi livelli di rigore nei vari Stati membri.

(71) I sistemi europei di certificazione della cibersicurezza dovrebbero essere basati sui sistemi già esistenti a livello nazionale e internazionale e, se necessario, sulle specifiche tecniche di forum e consorzi, partendo dai loro punti di forza attuali e analizzando e correggendo i punti deboli.

(72) Occorrono soluzioni flessibili di cibersicurezza affinché il settore resti un passo avanti rispetto alle minacce, per cui qualsiasi sistema di certificazione dovrebbe essere ideato in modo tale da evitare il rischio di una rapida obsolescenza.

(73) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti, servizi TIC e processi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di certificazione della cibersicurezza e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dal settore o da altre organizzazioni private non dovrebbero rientrare nell'ambito di applicazione del presente regolamento. Tuttavia, gli organismi che li gestiscono dovrebbero poter proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo di certificazione della cibersicurezza.

(74) Le disposizioni del presente regolamento dovrebbero lasciare impregiudicato il diritto dell'Unione che prevede regole specifiche sulla certificazione di prodotti TIC, servizi TIC e processi TIC. In particolare, il regolamento (UE) 2016/679 stabilisce disposizioni per l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali meccanismi di certificazione e sigilli e marchi di protezione dei dati dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati dei prodotti e dei servizi. Il presente regolamento lascia impregiudicata la certificazione delle operazioni di trattamento dei dati nel quadro del regolamento (UE) 2016/679, anche nel caso in cui tali operazioni siano integrate nei TIC, servizi TIC e processi TIC.

(75) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti TIC, servizi TIC e processi TIC certificati nel loro ambito siano conformi a determinati requisiti volti a proteggere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o delle funzioni di o dei servizi offerti da o accessibili tramite tali prodotti, servizi e processi per tutto il loro ciclo di vita. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti TIC, servizi TIC e processi TIC nel presente regolamento. I prodotti TIC, servizi TIC e processi TIC e le esigenze di cibersicurezza ad essi relative sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, che dovrebbe essere integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento della progettazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui conseguire tali obiettivi nei prodotti TIC, servizi TIC e processi TIC specifici dovrebbero quindi essere ulteriormente specificate in modo dettagliato per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche in assenza di norme appropriate.

(76) Le specifiche tecniche da usare nei sistemi europei di certificazione della cibersicurezza dovrebbero rispettare i requisiti principi enunciati nell'allegato II del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([19]). In casi debitamente giustificati, tuttavia, si potrebbe ritenere necessario discostarsi da detti requisiti qualora le specifiche tecniche siano da usare in un sistema europeo di certificazione della cibersicurezza che fa riferimento a un livello di affidabilità elevato. Le motivazioni di tali scostamenti dovrebbero essere rese pubbliche.

(77) La valutazione della conformità è la procedura volta a valutare se siano stati rispettati i requisiti specifici connessi a un prodotto TIC, servizio TIC o processo TIC. Tale procedura è effettuata da un soggetto terzo indipendente, diverso dal fabbricante o dal fornitore del prodotto TIC, servizio TIC o processo TIC oggetto di valutazione. Il rilascio di un certificato europeo di cibersicurezza è in linea con la procedura di valutazione di un prodotto TIC, servizio TIC o processo TIC. Un certificato europeo di cibersicurezza dovrebbe essere rilasciato qualora la valutazione di un prodotto TIC, servizio TIC o processo TIC dia esito positivo. In funzione del livello di affidabilità, il sistema europeo di certificazione della cibersicurezza dovrebbe specificare se il certificato europeo di cibersicurezza deve essere rilasciato da un organismo pubblico o privato. La valutazione della conformità e la certificazione non possono garantire di per sé la cibersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati. Si tratta piuttosto di procedure e metodologie tecniche volte ad attestare che i prodotti TIC, servizi TIC e processi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio nelle norme tecniche.

(78) La scelta della certificazione appropriata e dei relativi requisiti di sicurezza da parte degli utenti dei certificati europei di cibersicurezza dovrebbe fondarsi su un'analisi dei rischi associati all'uso di un prodotto TIC, servizio TIC o processo TIC. Conseguentemente, il livello di affidabilità dovrebbe essere commisurato al livello del rischio associato al previsto uso di un prodotto TIC, servizio TIC o processo TIC.

([19]) 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).

(79) I sistemi europei di certificazione della cibersicurezza potrebbero prevedere che la valutazione della conformità sia effettuata sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC o processi TIC («autovalutazione della conformità»). In tal caso dovrebbe essere sufficiente che il fabbricante o il fornitore di prodotti TIC, servizi TIC o processi TIC effettui direttamente tutti i controlli per garantire che i prodotti TIC, servizi TIC o processi TIC siano conformi al sistema europeo di certificazione della cibersicurezza. L'autovalutazione della conformità dovrebbe essere considerata idonea per prodotti TIC, servizi TIC o processi TIC a bassa complessità che presentano un basso livello di rischio per l'interesse pubblico, ad esempio progettazione e meccanismi di produzione semplici. Inoltre, l'autovalutazione della conformità dovrebbe essere consentita solo per i prodotti TIC, servizi TIC o processi TIC che corrispondono al livello di affidabilità «di base».

(80) I sistemi europei di certificazione della cibersicurezza potrebbero prevedere sia l'autovalutazione della conformità sia la certificazione di prodotti TIC, servizi TIC e processi TIC. In tale caso, il sistema dovrebbe comprendere mezzi chiari e comprensibili che consentano ai consumatori o altri utenti di distinguere tra i prodotti TIC, servizi TIC o processi TIC riguardo ai quali il fabbricante o fornitore di prodotti TIC, servizi TIC e processi TIC è responsabile della valutazione di prodotti TIC, servizi TIC e processi TIC certificati da terzi.

(81) I fabbricanti o fornitori di prodotti TIC, servizi TIC o processi TIC che effettuano un'autovalutazione della conformità dovrebbero poter rilasciare e firmare la dichiarazione UE di conformità nell'ambito della procedura di valutazione della conformità. Una dichiarazione UE di conformità è un documento che attesta che un prodotto TIC, servizio TIC o processo TIC specifico è conforme ai requisiti del sistema europeo di certificazione della cibersicurezza. Rilasciando e firmando la dichiarazione UE di conformità, il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC si assume la responsabilità della conformità del prodotto TIC, servizio TIC o processo TIC con i requisiti di legge del sistema europeo di certificazione della cibersicurezza. Una copia della dichiarazione UE di conformità dovrebbe essere trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

(82) I fabbricanti o fornitori di prodotti TIC, servizi TIC o processi TIC dovrebbero mettere a disposizione della competente autorità nazionale di certificazione della cibersicurezza, per un periodo stabilito nel sistema europeo di certificazione della cibersicurezza interessato, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC, servizi TIC o processi TIC al pertinente sistema europeo di certificazione della cibersicurezza. La documentazione tecnica dovrebbe precisare i requisiti applicabili nell'ambito del sistema e riguardare la progettazione, la fabbricazione e il funzionamento del prodotto TIC, servizio TIC o processo TIC per quanto rileva ai fini dell'autovalutazione della conformità. La documentazione tecnica dovrebbe essere compilata in modo da permettere di valutare se un prodotto TIC, servizio TIC o processo TIC sia conforme ai requisiti applicabili nell'ambito di tale sistema.

(83) La governance del quadro europeo di certificazione della cibersicurezza tiene conto della partecipazione degli Stati membri e dell'adeguato coinvolgimento dei portatori di interessi e stabilisce il ruolo della Commissione durante l'intero processo di pianificazione e di proposta, richiesta, preparazione, adozione e revisione dei sistemi europei di certificazione della cibersicurezza.

(84) È opportuno che la Commissione prepari, con il sostegno del gruppo europeo per la certificazione della cibersicurezza (*European Cybersecurity Certification Group* — «ECCG») e del gruppo dei portatori di interessi per la certificazione della cibersicurezza e dopo una consultazione ampia e aperta, un programma di lavoro progressivo dell'Unione per i sistemi europei di certificazione della cibersicurezza e lo pubblichi sotto forma di strumento non vincolante. Il programma di lavoro progressivo dell'Unione dovrebbe consistere in un documento strategico atto a consentire al settore, alle autorità nazionali e agli organismi di normazione, in particolare, di prepararsi in anticipo ai futuri sistemi europei di certificazione della sicurezza. Il programma di lavoro progressivo dell'Unione dovrebbe includere una panoramica pluriennale delle richieste di proposte di sistemi che la Commissione intende presentare all'ENISA ai fini della loro preparazione in base a motivi specifici. La Commissione dovrebbe tenere conto del programma di lavoro progressivo dell'Unione nella preparazione del suo programma continuativo per la normazione delle TIC e delle richieste di normazione alle organizzazioni europee di normazione. In considerazione della rapida introduzione e diffusione di nuove tecnologie, dell'emergere di rischi connessi alla cibersicurezza prima sconosciuti e degli sviluppi legislativi e del mercato, è opportuno autorizzare la Commissione o l'ECCG a chiedere all'ENISA di preparare proposte di sistemi che non siano stati previsti nel programma di lavoro progressivo dell'Unione. In siffatti casi, la Commissione e l'ECCG dovrebbero inoltre valutare la necessità di tale richiesta, tenendo conto degli scopi e obiettivi generali del presente regolamento e la necessità di assicurare la continuità per quanto riguarda la pianificazione e l'uso delle risorse da parte dell'ENISA.

A seguito di una simile richiesta, l'ENISA dovrebbe preparare senza indebiti ritardi le proposte di sistemi per prodotti TIC, servizi TIC e processi TIC specifici. La Commissione dovrebbe valutare l'impatto positivo e negativo della sua richiesta sullo specifico mercato interessato, in particolare sulle PMI, sull'innovazione, sugli ostacoli all'accesso a tale mercato e sui costi per gli utenti finali. La Commissione, sulla base dei sistemi preparati dall'ENISA, dovrebbe essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza fissati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Detti elementi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti TIC, servizi TIC e processi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato («di base», «sostanziale» o «elevato»), nonché i livelli di valutazione ove applicabili. L'ENISA dovrebbe poter respingere, in casi debitamente giustificati, una richiesta dell'ECCG. Tali decisioni dovrebbero essere assunte dal consiglio di amministrazione e dovrebbero essere debitamente motivate.

(85) L'ENISA dovrebbe gestire un sito web che fornisca informazioni sui sistemi europei di certificazione della cibersicurezza e che li pubblicizzi, in cui figurino, tra l'altro, le richieste di preparazione di una proposta di sistema e il riscontro ricevuto nella procedura di consultazione effettuata dall'ENISA durante la fase di preparazione. Il sito web dovrebbe anche fornire informazioni sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità rilasciati ai sensi del presente regolamento, incluse le informazioni sulla revoca e sulla scadenza di tali certificati e dichiarazioni. Il sito web dovrebbe inoltre indicare i sistemi nazionali di certificazione della cibersicurezza che sono stati sostituiti da un sistema europeo di certificazione della cibersicurezza.

(86) Il livello di affidabilità di un sistema europeo di certificazione è la base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfi i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza. Allo scopo di garantire la coerenza del quadro europeo di certificazione della cibersicurezza, un sistema europeo di certificazione della cibersicurezza dovrebbe poter specificare i livelli di affidabilità per i certificati europei di cibersicurezza e le dichiarazioni UE di conformità rilasciati nell'ambito di detto sistema. Ciascun certificato europeo di cibersicurezza potrebbe far riferimento a uno dei livelli di affidabilità: «di base», «sostanziale» o «elevato», mentre la dichiarazione UE di conformità potrebbe far riferimento solo al livello di affidabilità «di base». I livelli di affidabilità fornirebbero il rigore e la specificità corrispondenti della valutazione del prodotto TIC, servizio TIC o processo TIC e sarebbero caratterizzati in riferimento alle specifiche tecniche, norme e procedure correlate, tra cui i controlli tecnici, l'obiettivo delle quali è attenuare o prevenire gli incidenti. Ciascun livello di affidabilità dovrebbe essere coerente nei vari settori in cui la certificazione si applica.

(87) Un sistema europeo di certificazione della cibersicurezza potrebbe precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia usata. I livelli di valutazione dovrebbero corrispondere a uno dei livelli di affidabilità ed essere associati a un'idonea combinazione di componenti dell'affidabilità. Per tutti i livelli di affidabilità, il prodotto TIC, servizio TIC o processo TIC dovrebbe contenere alcune funzioni sicure, specificate nel sistema, che possono comprendere una configurazione sicura già predisposta in fabbrica, un codice firmato, aggiornamenti sicuri e tecniche utilizzate per ostacolare lo sfruttamento delle vulnerabilità (*exploit mitigations*) nonché la piena protezione della memoria a impilaggio o della memoria *heap*. Dette funzioni dovrebbero essere soggette a sviluppo e manutenzione utilizzando approcci allo sviluppo centrati sulla sicurezza e strumenti ad essi associati onde assicurare che meccanismi efficaci di software e di hardware siano inclusi in maniera affidabile.

(88) Per il livello di affidabilità «di base», la valutazione dovrebbe essere guidata almeno dai seguenti componenti di affidabilità: la valutazione dovrebbe comprendere almeno un riesame della documentazione tecnica del prodotto TIC, servizio TIC o processo TIC da parte dell'organismo di valutazione della conformità. Se la certificazione comprende processi TIC, dovrebbe essere soggetto a riesame tecnico anche il processo usato per la progettazione, lo sviluppo e la manutenzione del prodotto TIC o servizio TIC. Se un sistema europeo di certificazione della cibersicurezza prevede un'autovalutazione della conformità, dovrebbe essere sufficiente che il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC abbia effettuato un'autovalutazione della conformità del prodotto TIC, servizio TIC o processo TIC al sistema di certificazione.

(89) Per il livello di affidabilità «sostanziale», la valutazione, oltre ai requisiti per il livello di affidabilità «di base», dovrebbe essere guidata almeno dalla verifica della conformità delle funzionalità di sicurezza del prodotto TIC, servizio TIC o processo TIC alla documentazione tecnica ad esso relativa.

(90) Per il livello di affidabilità «elevato», la valutazione, oltre ai criteri requisiti per il livello di affidabilità «sostanziale», dovrebbe essere guidata almeno da un test di efficacia che accerti la resistenza delle funzionalità di sicurezza di un prodotto TIC, servizio TIC o processo TIC nei confronti di complessi ciberattacchi perpetrati da persone che dispongono di abilità e risorse significative.

(91) Il ricorso alla certificazione europea della cibersicurezza e alle dichiarazioni UE di conformità dovrebbe restare volontario, salvo disposizioni contrarie previste dal diritto dell'Unione o dalla normativa degli Stati membri adottata in conformità del diritto dell'Unione. In mancanza di un diritto dell'Unione armonizzato, gli Stati membri possono adottare regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cibersicurezza in virtù della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([20]). Gli Stati membri ricorrono anche alla certificazione europea della cibersicurezza nell'ambito degli appalti pubblici e della direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([21]).

(92) In alcuni settori potrebbe essere necessario in futuro imporre specifici requisiti di cibersicurezza e rendere obbligatoria la relativa certificazione in relazione a taluni prodotti TIC, servizi TIC o processi TIC, al fine di aumentare il livello di cibersicurezza nell'Unione. La Commissione dovrebbe vigilare periodicamente sull'impatto dei sistemi europei di certificazione della cibersicurezza adottati sulla disponibilità di prodotti TIC, servizi TIC e processi TIC sicuri nel mercato interno e valutare periodicamente il livello di utilizzo dei sistemi di certificazione da parte dei fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC nell'Unione. L'efficacia dei sistemi europei di certificazione della cibersicurezza e l'opportunità di rendere obbligatori sistemi specifici dovrebbero essere valutate alla luce della normativa dell'Unione in materia di cibersicurezza, in particolare la direttiva (UE) 2016/1148, tenendo in considerazione la sicurezza delle reti e dei sistemi informativi utilizzati dagli operatori di servizi essenziali.

(93) I certificati europei di cibersicurezza e le dichiarazioni UE di conformità dovrebbero aiutare gli utenti finali a compiere scelte consapevoli. I prodotti TIC, servizi TIC e processi TIC che siano stati certificati o per i quali sia stata rilasciata una dichiarazione UE di conformità dovrebbero pertanto essere accompagnati da informazioni strutturate adeguate al livello tecnico atteso nell'utente finale previsto. Tutte queste informazioni dovrebbero essere disponibili online e, ove opportuno, in forma fisica. L'utente finale dovrebbe avere accesso alle informazioni relative al numero di riferimento del sistema di certificazione, al livello di affidabilità, alla descrizione dei rischi connessi alla cibersicurezza associati al prodotto TIC, servizio TIC o processo TIC, e all'autorità o organismo che ha rilasciato il certificato, o dovrebbe poter ottenere una copia del certificato europeo di cibersicurezza. Inoltre, l'utente finale dovrebbe essere informato della politica di assistenza in materia di cibersicurezza —ossia per quanto tempo l'utente finale può aspettarsi di ricevere aggiornamenti o patch per la cibersicurezza — del fabbricante o fornitore di prodotti TIC, servizi TIC e processi TIC. Se del caso, dovrebbero essere forniti orientamenti sulle azioni da compiere o sui parametri che l'utente finale può applicare per mantenere o aumentare la cibersicurezza del prodotto TIC o del servizio TIC e informazioni di contatto del punto di contatto unico a cui fare capo e da cui ricevere assistenza in caso di ciberattacchi (oltre alle segnalazioni automatiche). Tali informazioni dovrebbero essere aggiornate periodicamente e rese disponibili su un sito web che fornisca informazioni sui sistemi europei di certificazione della cibersicurezza.

(94) Al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti TIC, servizi TIC o processi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere da una data stabilita dalla Commissione mediante atti di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione della cibersicurezza di prodotti TIC, servizi TIC o processi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza in vigore. Non si dovrebbe tuttavia impedire agli Stati membri di adottare o mantenere in vigore sistemi nazionali di certificazione della cibersicurezza per motivi di sicurezza nazionale. Gli Stati membri dovrebbero informare la Commissione e l'ECCG dell'eventuale intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza. La Commissione e l'ECCG dovrebbero valutare l'impatto dei nuovi sistemi nazionali di certificazione della cibersicurezza sul corretto funzionamento del mercato interno, tenendo conto anche dell'eventuale interesse strategico di richiedere invece un sistema europeo di certificazione della cibersicurezza.

(95) I sistemi europei di certificazione della cibersicurezza sono volti ad armonizzare nell'Unione le pratiche in tale settore. Devono contribuire ad accrescere il livello di cibersicurezza nell'Unione. La progettazione dei sistemi europei di certificazione della cibersicurezza dovrebbe tener conto delle innovazioni nel campo della cibersicurezza e consentirne lo sviluppo.

([20]) 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).

([21]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014 sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

(96) I sistemi europei di certificazione della cibersicurezza dovrebbero tener conto degli attuali metodi di sviluppo di software e hardware e, in particolare, dell'impatto di frequenti aggiornamenti del software e del firmware sui singoli certificati europei di cibersicurezza. I sistemi europei di certificazione della cibersicurezza dovrebbero specificare le condizioni alle quali un aggiornamento possa rendere necessario sottoporre nuovamente a certificazione un prodotto TIC, servizio TIC o processo TIC oppure ridurre l'ambito di applicazione di uno specifico certificato europeo di cibersicurezza, tenuto conto dei possibili effetti negativi dell'aggiornamento sulla conformità ai requisiti di sicurezza del certificato.

(97) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC dovrebbero poter presentare domande di certificazione dei loro prodotti TIC, servizi TIC e processi TIC all'organismo di valutazione della conformità di propria scelta, ovunque nell'Unione. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo nazionale di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni e dovrebbe essere rinnovato alle stesse condizioni, purché l'organismo di valutazione della conformità continui a soddisfare i requisiti. Gli organismi di accreditamento dovrebbero limitare, sospendere o revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono state, o non sono più, soddisfatte o se l'organismo di valutazione della conformità viola le disposizioni del presente regolamento.

(98) Riferimenti nella legislazione nazionale a norme nazionali che non sono più applicabili a seguito dell'entrata in vigore di un sistema europeo di certificazione della cibersicurezza possono costituire una fonte di confusione. Gli Stati membri dovrebbero quindi tener conto dell'adozione di un sistema di certificazione europeo della cibersicurezza nella propria legislazione nazionale.

(99) Al fine di ottenere norme equivalenti in tutta l'Unione, agevolare il reciproco riconoscimento e promuovere l'accettazione generale dei certificati europei di cibersicurezza e delle dichiarazioni UE di conformità, è necessario istituire un sistema di valutazione inter pares tra le autorità nazionali di certificazione della cibersicurezza. La valutazione inter pares dovrebbe riguardare le procedure per vigilare sulla conformità dei prodotti TIC, servizi TIC e processi TIC con i certificati europei di cibersicurezza, per monitorare gli obblighi dei fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC che effettuano l'autovalutazione della conformità, per monitorare gli organismi di valutazione della conformità e l'adeguatezza delle competenze del personale degli organismi che rilasciano certificati di livello di affidabilità «elevato». La Commissione dovrebbe poter stabilire, mediante atti di esecuzione, almeno un piano quinquennale per le valutazioni inter pares e stabilire i criteri e le metodologie di funzionamento del sistema di valutazione inter pares.

(100) Fatto salvo il sistema generale di valutazione inter pares che tutte le autorità nazionali di certificazione della cibersicurezza devono istituire nell'ambito del quadro europeo di certificazione della cibersicurezza, taluni sistemi di certificazione possono includere un meccanismo di valutazione inter pares per gli organismi che rilasciano certificati europei di cibersicurezza per prodotti TIC, servizi TIC e processi TIC con un livello di affidabilità «elevato» nel quadro di tali sistemi. L'ECCG dovrebbe sostenere l'attuazione di tali meccanismi di valutazione inter pares. Le valutazioni inter pares dovrebbero in particolare valutare se gli organismi interessati svolgono i rispettivi compiti in maniera armonizzata e possono comprendere meccanismi di impugnazione. I risultati delle valutazioni inter pares dovrebbero essere resi pubblici. Gli organismi interessati possono adottare le opportune misure per adeguare le proprie prassi e competenze di conseguenza.

(101) Gli Stati membri dovrebbero designare una o più autorità nazionale di certificazione della cibersicurezza per vigilare sulla conformità agli obblighi derivanti dal presente regolamento. L'autorità nazionale di certificazione della cibersicurezza può essere un'autorità già esistente o una nuova autorità. Gli Stati membri dovrebbero altresì avere facoltà di designare, previo accordo con un altro Stato membro, una o più autorità nazionali di certificazione della cibersicurezza nel territorio di tale altro Stato membro.

(102) In particolare, l'autorità nazionale di certificazione della cibersicurezza dovrebbe monitorare e far applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC stabiliti nel suo territorio in relazione alla dichiarazione UE di conformità, assistere gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità mettendo a loro disposizione le proprie competenze e pertinenti informazioni, autorizzare gli organismi di valutazione della conformità a svolgere i loro compiti qualora questi soddisfino i requisiti supplementari previsti in un sistema europeo di certificazione della cibersicurezza e monitorare i pertinenti sviluppi nel settore della certificazione della cibersicurezza. Le autorità nazionali di certificazione della cibersicurezza dovrebbero anche trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza che sono da loro rilasciati o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità, ove tali certificati indichino

un livello di affidabilità «elevato», svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Le autorità nazionali di certificazione della cibersicurezza dovrebbero inoltre cooperare con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante la condivisione scambio di informazioni sugli eventuali prodotti TIC, servizi TIC o processi TIC non conformi ai requisiti del presente regolamento o a specifici sistemi europei di certificazione della cibersicurezza. La Commissione dovrebbe facilitare tale condivisione di informazioni mettendo a disposizione un sistema di sostegno generale delle informazioni elettroniche, ad esempio il sistema di informazione e comunicazione per la vigilanza del mercato (ICSMS) e il sistema d'informazione rapida sui prodotti non alimentari pericolosi (RAPEX) già impiegati dalle autorità di vigilanza del mercato a norma del regolamento (CE) n. 765/2008.

(103) Al fine di garantire un'applicazione coerente del quadro europeo di certificazione della cibersicurezza, dovrebbe essere costituito un ECCG costituito dai rappresentanti delle autorità nazionali di certificazione della cibersicurezza o di altre autorità nazionali competenti. I compiti principali dell'ECCG dovrebbero consistere nel consigliare e nell'assistere la Commissione nelle attività volte ad assicurare un'attuazione e un'applicazione coerenti del quadro europeo di certificazione della cibersicurezza, nell'assistere e nel cooperare strettamente con l'ENISA nella preparazione delle proposte di sistemi europei di certificazione della cibersicurezza, in casi debitamente giustificati nell'incaricare l'ENISA di preparare una proposta di sistema, nell'adottare pareri indirizzati all'ENISA in merito alle proposte di sistemi e nell'adottare pareri indirizzati sul mantenimento e la revisione degli attuali sistemi europei di certificazione della cibersicurezza. L'ECCG dovrebbe agevolare lo scambio di buone prassi e di competenze tra le diverse autorità nazionali di certificazione della cibersicurezza responsabili dell'autorizzazione degli organismi di valutazione della conformità e del rilascio dei certificati europei di cibersicurezza.

(104) Al fine di accrescere la consapevolezza e facilitare l'accettazione dei futuri sistemi europei di cibersicurezza, la Commissione può emanare orientamenti generali o settoriali in materia di cibersicurezza, ad esempio orientamenti sulle buone prassi o sul comportamento responsabile in tale ambito, sottolineando l'effetto positivo dell'utilizzo di prodotti TIC, servizi TIC e processi TIC certificati.

(105) Allo scopo di agevolare ulteriormente gli scambi e riconoscendo il carattere globale delle catene di fornitura di TIC, l'Unione può concludere, conformemente all'articolo 218 del trattato sul funzionamento dell'Unione europea (TFUE), accordi per il reciproco riconoscimento di certificati europei di cibersicurezza. La Commissione, tenuto conto del parere dell'ENISA e dell'ECCG, può raccomandare l'apertura dei negoziati pertinenti. Ciascun sistema europeo di certificazione della cibersicurezza dovrebbe prevedere condizioni specifiche per tali accordi per il reciproco riconoscimento con i paesi terzi.

(106) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire 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 ([22]).

(107) La procedura d'esame dovrebbe essere utilizzata per l'adozione degli atti di esecuzione sui sistemi europei di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC; per l'adozione degli atti di esecuzione sulle modalità di conduzione delle indagini da parte dell'ENISA; per l'adozione degli atti di esecuzione su un piano di valutazione inter pares delle autorità nazionali di certificazione della cibersicurezza nonché per l'adozione degli atti di esecuzione sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di certificazione della cibersicurezza alla Commissione.

(108) L'operato dell'ENISA dovrebbe essere soggetto a una valutazione periodica e indipendente. La valutazione dovrebbe tenere conto del conseguimento degli obiettivi da parte dell'ENISA, delle sue pratiche di lavoro e della pertinenza dei suoi compiti, in particolare i compiti relativi alla cooperazione operativa a livello di Unione. La valutazione dovrebbe altresì valutare l'impatto, l'efficacia e l'efficienza del quadro europeo di certificazione della cibersicurezza. In caso di riesame, la Commissione dovrebbe valutare come possa essere rafforzato il ruolo dell'ENISA come punto di riferimento per pareri e competenze e dovrebbe anche valutare la possibilità di un ruolo dell'ENISA nel sostenere la valutazione di prodotti TIC, servizi TIC e processi e i servizi TIC di paesi terzi che non rispettano le regole dell'Unione, ove tali prodotti, servizi e processi entrino nell'Unione.

([22]) 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).

(109) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della loro portata e dei loro effetti, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(110) Il regolamento (UE) n. 526/2013 dovrebbe essere abrogato,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento stabilisce:

a) gli obiettivi, i compiti e gli aspetti organizzativi relativi all'ENISA, («Agenzia dell'Unione europea per la cibersicurezza»); e

b) un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

Il quadro di cui al primo comma, lettera b), si applica fatte salve disposizioni specifiche di altri atti giuridici dell'Unione in materia di certificazione volontaria o obbligatoria.

2. Il presente regolamento fa salve le competenze degli Stati membri per quanto riguarda le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

Articolo 2

Definizioni

Ai fini del presente regolamento si intende per:

1) «cibersicurezza»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;

2) «rete e sistema informativo»: una rete e un sistema informativo quale definito all'articolo 4, punto 1), della direttiva (UE) 2016/1148;

3) «strategia nazionale per la sicurezza della rete e dei sistemi informativi»: una strategia nazionale per la sicurezza della rete e dei sistemi informativi quale definita all'articolo 4, punto 3), della direttiva (UE) 2016/1148;

4) «operatore di servizi essenziali»: un operatore di servizi essenziali quale definito all'articolo 4, punto 4), della direttiva (UE) 2016/1148;

5) «fornitore di servizio digitale»: un fornitore di servizio digitale quale definito all'articolo 4, punto 6), della direttiva (UE) 2016/1148;

6) «incidente»: un incidente quale definito all'articolo 4, punto 7), della direttiva (UE) 2016/1148;

7) «trattamento dell'incidente»: qualsiasi trattamento dell'incidente quale definito all'articolo 4, punto 8), della direttiva (UE) 2016/1148;

8) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;

9) «sistema europeo di certificazione della cibersicurezza»: una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC;

10) «sistema nazionale di certificazione della cibersicurezza»: una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, servizi TIC e processi TIC che rientrano nell'ambito di applicazione del sistema specifico;

11) «certificato europeo di cibersicurezza»: un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

12) «prodotto TIC»: un elemento o un gruppo di elementi di una rete o di un sistema informativo;

13) «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;

14) «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;

15) «accreditamento»: l'accreditamento quale definito all'articolo 2, punto 10), del regolamento (CE) n. 765/2008;

16) «organismo nazionale di accreditamento»: un organismo nazionale di accreditamento quale definito all'articolo 2, punto 11), del regolamento (CE) n. 765/2008;

17) «valutazione della conformità»: una valutazione della conformità ai sensi dell'articolo 2, punto 12), del regolamento (CE) n. 765/2008;

18) «organismo di valutazione della conformità»: un organismo di valutazione della conformità quale definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008;

19) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

20) «specifica tecnica»: un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC o un processo TIC deve soddisfare o le relative procedure di valutazione della conformità;

21) «livello di affidabilità»: base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC o processo TIC è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC o processo TIC interessato;

22) «autovalutazione di conformità»: un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC che valuta se tali prodotti TIC, servizi TIC e processi TIC soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersicurezza.

TITOLO II

ENISA — (AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA)

CAPO I

Mandato e obiettivi

Articolo 3

Mandato

1. L'ENISA svolge i compiti che le sono attribuiti ai sensi del presente regolamento allo scopo di conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersicurezza. L'ENISA funge da punto di riferimento per pareri e competenze in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione.

Svolgendo i compiti che le sono attribuiti ai sensi del presente regolamento, l'ENISA contribuisce a ridurre la frammentazione nel mercato interno.

2. L'ENISA svolge i compiti che le sono attribuiti dagli atti giuridici dell'Unione che stabiliscono le misure per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza.

3. Nello svolgimento dei suoi compiti, l'ENISA agisce in maniera indipendente, evitando nel contempo la duplicazione delle attività degli Stati membri e tenendo conto delle competenze esistenti degli Stati membri.

4. L'ENISA sviluppa le proprie risorse, incluse le capacità e abilità tecniche e umane, necessarie al fine di svolgere i compiti attribuitile ai sensi del presente regolamento.

Articolo 4

Obiettivi

1. L'ENISA opera come centro di competenze nel campo della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite, alle informazioni che mette a disposizione, alla trasparenza delle procedure, ai metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.

2. L'ENISA assiste le istituzioni, gli organi e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cibersicurezza, ivi comprese le politiche settoriali in materia di cibersicurezza.

3. L'ENISA sostiene lo sviluppo delle capacità e la preparazione nell'Unione, assistendo le istituzioni, gli organi e gli organismi dell'Unione, nonché gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersicurezza.

4. L'ENISA promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza.

5. L'ENISA contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.

6. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno. L'ENISA contribuisce all'istituzione e al mantenimento di un apposito quadro europeo di certificazione della cibersicurezza, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC e dei processi TIC in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.

7. L'ENISA promuove un elevato livello di consapevolezza in materia di cibersicurezza, incluse l'igiene informatica e l'alfabetizzazione informatica, tra cittadini, organizzazioni e imprese.

CAPO II

Compiti

Articolo 5

Sviluppo e attuazione delle politiche e della normativa dell'Unione

L'ENISA contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione:

1) prestando assistenza e consulenza per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel campo della cibersicurezza e delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cibersicurezza, in particolare fornendo un parere indipendente, analisi nonché svolgendo lavori preparatori;

2) assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche emanando pareri e orientamenti, fornendo consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

3) assistendo gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nello sviluppo e nella promozione di politiche sulla cibersicurezza che sostengano la disponibilità generale o l'integrità del carattere fondamentale pubblico di una rete Internet aperta;

4) contribuendo ai lavori del gruppo di cooperazione di cui all'articolo 11 della direttiva (UE) 2016/1148, mettendo a disposizione le proprie competenze e fornendo assistenza;

5) sostenendo:

   a) lo sviluppo e l'attuazione della politica dell'Unione nel settore dell'identificazione elettronica e dei servizi fiduciari, in particolare fornendo consulenza e emanando orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti,

   b) la promozione di un livello di sicurezza più elevato delle comunicazioni elettroniche, anche fornendo consulenza e competenze e agevolando lo scambio delle migliori pratiche tra le autorità competenti,

   c) gli Stati membri nell'attuazione di aspetti specifici relativi alla cibersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e vita privata, anche fornendo su richiesta un parere al comitato europeo per la protezione dei dati;

6) sostenendo il riesame periodico delle attività politiche dell'Unione con la preparazione di una relazione annuale sullo stato di attuazione del relativo quadro giuridico per quanto riguarda:

   a) le informazioni sulle notifiche degli incidenti degli Stati membri trasmesse dal punto di contatto unico al gruppo di cooperazione, a norma dell'articolo 10, paragrafo 3, della direttiva (UE) 2016/1148,

   b) le sintesi delle notifiche di violazioni della sicurezza o perdita di integrità ricevute dai prestatori di servizi fiduciari trasmesse dagli organismi di vigilanza all'ENISA, a norma dell'articolo 19, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([23]);

   c) le notifiche relative a incidenti di sicurezza trasmesse dai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, trasmesse dalle autorità competenti all'ENISA, a norma dell'articolo 40 della direttiva (UE) 2018/1972.

([23]) 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).

Articolo 6

Sviluppo delle capacità

1. L'ENISA assiste:

a) gli Stati membri nell'impegno a migliorare la prevenzione, la rilevazione e l'analisi delle minacce informatiche e degli incidenti, come pure la capacità di reazione agli stessi, fornendo loro le conoscenze e le competenze necessarie;

b) gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nella definizione e attuazione di politiche di divulgazione delle vulnerabilità su base volontaria;

c) le istituzioni, gli organi e gli organismi dell'Unione nel loro impegno a migliorare la prevenzione, la rilevazione e l'analisi delle minacce informatiche e degli incidenti, come pure a migliorare le loro capacità di reazione a tali minacce e incidenti, in particolare tramite un sostegno adeguato alla CERT-UE;

d) gli Stati membri nello sviluppo di CSIRT nazionali, ove richiesto a norma dell'articolo 9, paragrafo 5, della direttiva (UE) 2016/1148;

e) gli Stati membri nello sviluppo di strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, ove richiesto a norma dell'articolo 7, paragrafo 2, della direttiva (UE) 2016/1148, e promuove la diffusione di tali strategie in tutta l'Unione e prende nota del progresso della loro attuazione allo scopo di promuovere le migliori pratiche;

f) le istituzioni dell'Unione nello sviluppo e nella revisione di strategie dell'Unione in materia di cibersicurezza, nella promozione della loro diffusione e nel monitoraggio dei progressi compiuti nella loro attuazione;

g) i CSIRT nazionali e dell'Unione nell'innalzare il livello delle loro capacità, anche attraverso la promozione del dialogo e degli scambi di informazioni, al fine di assicurare che, tenuto conto dello stato dell'arte, tutti i CSIRT possiedano una serie comune di capacità minime e operino secondo le migliori pratiche;

h) gli Stati membri, mediante la periodica organizzazione di esercitazioni di cibersicurezza a livello di Unione di cui all'articolo 7, paragrafo 5, almeno ogni due anni e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

i) i pertinenti enti pubblici, attraverso l'offerta di formazione sulla cibersicurezza, se del caso in cooperazione con i portatori di interessi;

j) il gruppo di cooperazione, nello scambio di migliori pratiche, in particolare per quanto riguarda l'identificazione degli operatori di servizi essenziali da parte degli Stati membri, a norma dell'articolo 11, paragrafo 3, lettera l), della direttiva (UE) 2016/1148, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

2. L'ENISA sostiene la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulle procedure da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Articolo 7

Cooperazione operativa a livello di Unione

1. L'ENISA sostiene la cooperazione operativa tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e tra i portatori di interessi.

2. L'ENISA coopera a livello operativo e stabilisce sinergie con le istituzioni, gli organi e gli organismi dell'Unione, compresa la CERT-UE, con i servizi che si occupano della criminalità informatica e con le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di affrontare questioni di interesse comune, anche:

a) scambiando conoscenze e migliori pratiche;

b) fornendo consulenza ed emanando orientamenti sulle questioni pertinenti relative alla cibersicurezza;

c) stabilendo le disposizioni pratiche per l'esecuzione di compiti specifici, previa consultazione della Commissione.

3. L'ENISA svolge le funzioni di segretariato della rete di CSIRT, a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2016/1148, e in tale veste sostiene attivamente la condivisione delle informazioni e la cooperazione tra i suoi membri.

4. L'ENISA sostiene gli Stati membri nella cooperazione operativa nell'ambito della rete di CSIRT, mediante:

a) consigli su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi e, su richiesta di uno o più Stati membri, consigli in relazione a una specifica minaccia informatica;

b) l'assistenza, su richiesta di uno o più Stati membri, nella valutazione di incidenti aventi un impatto rilevante o sostanziale, tramite la messa a disposizione di competenze e l'agevolazione della gestione tecnica di tali incidenti, ivi compreso in particolare il sostegno alla condivisione volontaria di informazioni pertinenti e soluzioni tecniche tra gli Stati membri;

c) l'analisi delle vulnerabilità e degli incidenti sulla base delle informazioni pubblicamente disponibili o delle informazioni fornite volontariamente dagli Stati membri a tale scopo; e

d) su richiesta di uno o più Stati membri, il sostegno in relazione a indagini tecniche ex post sugli incidenti aventi un impatto rilevante o sostanziale ai sensi della direttiva (UE) 2016/1148.

Nello svolgimento di questi compiti, l'ENISA e la CERT-UE intraprendono una cooperazione strutturata per beneficiare delle sinergie ed evitare la duplicazione delle attività.

5. L'ENISA organizza periodicamente esercitazioni di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nell'organizzazione di esercitazioni di cibersicurezza. Tali esercitazioni di cibersicurezza a livello di Unione possono includere elementi tecnici, operativi o strategici. Ogni due anni l'ENISA organizza un'esercitazione globale su vasta scala.

Ove opportuno, l'ENISA inoltre contribuisce e aiuta ad organizzare esercitazioni di cibersicurezza settoriali insieme alle organizzazioni pertinenti che partecipano anche alle esercitazioni di cibersicurezza a livello di Unione.

6. L'ENISA elabora periodicamente, in stretta cooperazione con gli Stati membri, una relazione approfondita sulla situazione tecnica della cibersicurezza nell'Unione in merito agli incidenti e alle minacce informatiche, sulla base di informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro, dai CSIRT degli Stati membri o dai punti di contatto unici istituiti dalla direttiva (UE) 2016/1148, in entrambi i casi su base volontaria, dall'EC3 e dalla CERT-UE.

7. L'ENISA contribuisce a sviluppare una risposta cooperativa, a livello di Unione e di Stati membri, agli incidenti o alle crisi su vasta scala di carattere transfrontaliero connessi alla cibersicurezza, soprattutto:

a) aggregando e analizzando le relazioni delle fonti nazionali di dominio pubblico o condivise su base volontaria al fine di contribuire a creare una consapevolezza comune della situazione;

b) assicurando un flusso di informazioni efficiente e la disponibilità di meccanismi di attivazione tra la rete di CSIRT e i responsabili delle decisioni politiche e tecniche a livello di Unione;

c) agevolando, su richiesta, la gestione tecnica di tali incidenti o crisi, anche, in particolare, sostenendo la condivisione volontaria di soluzioni tecniche tra gli Stati membri;

d) sostenendo le istituzioni, gli organi e gli organismi dell'Unione e, su richiesta, gli Stati membri nella comunicazione pubblica in merito a tali incidenti o crisi;

e) verificando i piani di cooperazione per rispondere a tali incidenti o crisi a livello di Unione e sostenendo gli Stati membri, su loro richiesta, nella verifica di tali piani a livello nazionale.

Articolo 8

Mercato, certificazione della cibersicurezza e normazione

1. L'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC, come stabilito al titolo III del presente regolamento:

a) monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza secondo l'articolo 54, paragrafo 1, lettera c), in assenza di norme;

b) preparando proposte di sistemi europei di certificazione della cibersicurezza («proposte di sistemi») per prodotti TIC, servizi TIC e processi TIC conformemente all'articolo 49;

c) valutando i sistemi europei di certificazione della cibersicurezza adottati, conformemente all'articolo 49, paragrafo 8;

d) partecipando a valutazioni inter pares a norma dell'articolo 59, paragrafo 4;

e) assistendo la Commissione nel provvedere alle funzioni di segretariato dell'ECCG a norma dell'articolo 62, paragrafo 5.

2. L'ENISA provvede alle funzioni di segretariato del gruppo dei portatori di interessi per la certificazione della cibersicurezza a norma dell'articolo 22, paragrafo 4.

3. L'ENISA elabora e pubblica orientamenti e sviluppa buone pratiche in merito ai requisiti di cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC, in cooperazione con le autorità nazionali di certificazione della cibersicurezza e con il settore in modo formale, strutturato e trasparente.

4. L'ENISA contribuisce a uno sviluppo delle capacità relative ai processi di valutazione e certificazione mediante l'elaborazione e la pubblicazione di orientamenti, nonché fornendo sostegno agli Stati membri, su loro richiesta.

5. L'ENISA facilita la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC.

6. L'ENISA redige, in collaborazione con gli Stati membri e con il settore, pareri e orientamenti riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali, nonché riguardanti le norme già esistenti, comprese le norme nazionali degli Stati membri, ai sensi dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148.

7. L'ENISA effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante sia della domanda che dell'offerta, al fine di promuovere tale mercato nell'Unione.

Articolo 9

Conoscenze e informazioni

L'ENISA:

a) esegue analisi delle tecnologie emergenti e fornisce valutazioni su temi specifici in relazione agli impatti previsti, dal punto di vista sociale, giuridico, economico e regolamentare, delle innovazioni tecnologiche sulla cibersicurezza;

b) effettua analisi strategiche a lungo termine delle minacce informatiche e degli incidenti al fine di individuare le tendenze emergenti e contribuire a prevenire gli incidenti;

c) fornisce, in cooperazione con esperti delle autorità degli Stati membri e con i pertinenti portatori di interessi, consulenza, orientamenti e migliori pratiche per la sicurezza della rete e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148 e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva;

d) raggruppa, organizza e mette a disposizione del pubblico, tramite un portale dedicato, informazioni sulla cibersicurezza fornite dalle istituzioni, dagli organi e dagli organismi dell'Unione e informazioni sulla cibersicurezza fornite su base volontaria dagli Stati membri e dai portatori di interessi del settore pubblico e privato;

e) raccoglie e analizza le informazioni pubblicamente disponibili sugli incidenti di rilievo e redige relazioni al fine di fornire orientamenti ai cittadini, alle organizzazioni e alle imprese in tutta l'Unione.

Articolo 10

Sensibilizzazione e istruzione

L'ENISA:

a) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini, organizzazioni e imprese, anche per quanto concerne l'igiene informatica e l'alfabetizzazione informatica;

b) organizza regolarmente, in collaborazione con gli Stati membri, con le istituzioni, gli organi e gli organismi dell'Unione e con il settore, campagne di sensibilizzazione al fine di rafforzare la cibersicurezza e la sua visibilità nell'Unione e incoraggiare un ampio dibattito pubblico;

c) assiste gli Stati membri nei loro sforzi di sensibilizzazione e promuove l'istruzione in materia di cibersicurezza;

d) incoraggia un miglior coordinamento e scambio di migliori pratiche tra gli Stati membri per la sensibilizzazione e l'istruzione in materia di cibersicurezza.

Articolo 11

Ricerca e innovazione

Per quanto riguarda la ricerca e l'innovazione, l'ENISA:

a) fornisce consulenza alle istituzioni, agli organi e agli organismi dell'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel campo della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce informatiche attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

b) partecipa, qualora la Commissione gliene abbia delegato i poteri, alla fase di attuazione dei programmi di finanziamento per la ricerca e l'innovazione o in qualità di beneficiario;

c) contribuisce all'agenda strategica di ricerca e innovazione a livello dell'Unione nel campo della cibersicurezza.

Articolo 12

Cooperazione internazionale

L'ENISA contribuisce all'impegno dell'Unione nella cooperazione con i paesi terzi e le organizzazioni internazionali, nonché all'interno dei pertinenti quadri di cooperazione internazionale, per promuovere la cooperazione internazionale sulle questioni connesse alla cibersicurezza:

a) impegnandosi, ove opportuno, in qualità di osservatore e nell'organizzazione delle esercitazioni internazionali, nonché analizzando i risultati di tali esercitazioni e comunicandoli al consiglio di amministrazione;

b) agevolando, su richiesta della Commissione, lo scambio di migliori pratiche;

c) fornendo competenze specialistiche alla Commissione, su richiesta della stessa;

d) fornendo consulenza e assistenza alla Commissione su questioni concernenti gli accordi con i paesi terzi per il riconoscimento reciproco dei certificati di cibersicurezza, in collaborazione con l'ECCG istituito a norma dell'articolo 62.

CAPO III

Organizzazione dell'ENISA

Articolo 13

Struttura dell'ENISA

La struttura amministrativa e di gestione dell'ENISA è composta da:

a) un consiglio di amministrazione;

b) un comitato esecutivo;

c) un direttore esecutivo;

d) un gruppo consultivo ENISA;

e) una rete di funzionari nazionali di collegamento.

Section 1

Consiglio di amministrazione

Articolo 14

Composizione del consiglio di amministrazione

1. Il consiglio di amministrazione è composto da un membro nominato da ciascuno Stato membro e due membri nominati dalla Commissione. Tutti i membri hanno diritto di voto.

2. Ciascun membro del consiglio di amministrazione ha un supplente. Il supplente rappresenta il membro assente.

3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle loro pertinenti abilità gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza di genere equilibrata nel consiglio di amministrazione.

4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di quattro anni. Il mandato è rinnovabile.

Articolo 15

Funzioni del consiglio di amministrazione

1. Il consiglio di amministrazione:

a) stabilisce gli orientamenti generali del funzionamento dell'ENISA e assicura che operi secondo le regole e i principi stabiliti dal presente regolamento; assicura inoltre la coerenza del lavoro dell'ENISA con le attività svolte dagli Stati membri e a livello di Unione;

b) adotta il progetto di documento unico di programmazione dell'ENISA di cui all'articolo 24 prima che sia trasmesso alla Commissione per parere;

c) adotta il documento unico di programmazione dell'ENISA, tenendo conto del parere della Commissione;

d) vigila sull'attuazione della programmazione annuale e pluriennale contenuta nel documento unico di programmazione;

e) adotta il bilancio annuale dell'ENISA ed esercita altre funzioni in relazione al bilancio dell'ENISA a norma del capo IV;

f) valuta e adotta la relazione annuale consolidata sulle attività dell'ENISA, inclusi i conti e una descrizione di come l'ENISA ha conseguito i propri indicatori di risultato, trasmette, entro il 1º luglio dell'anno successivo, sia la relazione annuale che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti, e rende pubblica la relazione annuale;

g) adotta la regolamentazione finanziaria applicabile all'ENISA in conformità dell'articolo 32;

h) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;

i) adotta regole per la prevenzione e la gestione dei conflitti di interesse in relazione ai suoi membri;

j) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalle relazioni di revisione contabile e valutazioni interne o esterne;

k) adotta il proprio regolamento interno, comprese regole per le decisioni provvisorie sulla delega di compiti specifici, a norma dell'articolo 19, paragrafo 7;

l) esercita, nei confronti del personale dell'ENISA, i poteri conferiti dallo statuto dei funzionari («statuto dei funzionari») e dal regime applicabile agli altri agenti dell'Unione europea («regime applicabile agli altri agenti»), stabiliti nel regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([24]) all'autorità che ha il potere di nomina e all'autorità abilitata a concludere i contratti di assunzione («poteri dell'autorità che ha il potere di nomina») a norma del paragrafo 2 del presente articolo;

m) adotta le disposizioni di esecuzione dello statuto dei funzionari e del regime applicabile agli altri agenti secondo la procedura di cui all'articolo 110 dello statuto dei funzionari;

n) nomina il direttore esecutivo e, se del caso, ne proroga il mandato o lo rimuove dall'incarico, a norma dell'articolo 36;

o) nomina un contabile, che può essere il contabile della Commissione, che opera in piena indipendenza nell'esercizio delle sue funzioni;

p) prende tutte le decisioni sull'istituzione delle strutture interne dell'ENISA e, se necessario, sulla relativa modifica, in considerazione delle necessità per l'attività dell'ENISA e secondo una gestione di bilancio sana;

q) autorizza l'istituzione di accordi di lavoro in relazione all'articolo 7;

r) autorizza l'istituzione o la conclusione di accordi di lavoro conformemente all'articolo 42.

2. In conformità dell'articolo 110 dello statuto dei funzionari, il consiglio di amministrazione adotta una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i poteri di autorità che ha il potere di nomina e stabilisce le condizioni di sospensione della delega di poteri. Il direttore esecutivo può subdelegare tali poteri.

([24]) GU L 56 del 4.3.1968, pag. 1.

3. Qualora circostanze eccezionali lo richiedano, il consiglio di amministrazione può adottare una decisione per sospendere temporaneamente la delega al direttore esecutivo dei poteri di autorità che ha il potere di nomina e tutti i poteri di autorità che ha il potere di nomina che il direttore esecutivo abbia subdelegato ed esercitarli esso stesso o delegarli a uno dei suoi membri o a un membro del personale diverso dal direttore esecutivo.

Articolo 16

Presidente del consiglio di amministrazione

Il consiglio di amministrazione elegge tra i propri membri un presidente e un vicepresidente, a maggioranza dei due terzi dei membri. Il loro mandato è di quattro anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Articolo 17

Riunioni del consiglio di amministrazione

1. Il consiglio di amministrazione si riunisce su convocazione del suo presidente.

2. Il consiglio di amministrazione tiene almeno due riunioni ordinarie l'anno. Si riunisce inoltre in seduta straordinaria su richiesta del suo presidente, della Commissione o di almeno un terzo dei suoi membri.

3. Il direttore esecutivo partecipa alle riunioni del consiglio di amministrazione, ma non ha diritto di voto.

4. I membri del gruppo consultivo ENISA possono partecipare alle riunioni del consiglio di amministrazione su invito del presidente, ma non hanno diritto di voto.

5. Alle riunioni del consiglio di amministrazione, i membri del consiglio di amministrazione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno del consiglio di amministrazione.

6. L'ENISA provvede alle funzioni di segretariato del consiglio di amministrazione.

Articolo 18

Modalità di voto del consiglio di amministrazione

1. Il consiglio di amministrazione adotta le proprie decisioni a maggioranza dei suoi membri.

2. La maggioranza di due terzi dei membri del consiglio di amministrazione è necessaria per l'adozione del documento unico di programmazione e del bilancio annuale, nonché per la nomina del direttore esecutivo, la proroga del suo mandato o la sua rimozione dall'incarico.

3. Ogni membro dispone di un voto. In assenza di un membro, il supplente è abilitato a esercitare il diritto di voto del membro.

4. Il presidente del consiglio di amministrazione partecipa al voto.

5. Il direttore esecutivo non partecipa al voto.

6. Il regolamento interno del consiglio di amministrazione stabilisce le regole dettagliate concernenti la votazione, in particolare le circostanze in cui un membro può agire per conto di un altro.

Section 2

Comitato esecutivo

Articolo 19

Comitato esecutivo

1. Il consiglio di amministrazione è assistito da un comitato esecutivo.

2. Il comitato esecutivo:

a) prepara le decisioni che dovranno essere adottate dal consiglio di amministrazione;

b) insieme con il consiglio di amministrazione, garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'OLAF, nonché dalle relazioni di revisione contabile e valutazioni interne ed esterne;

c) fatte salve le responsabilità del direttore esecutivo stabilite all'articolo 20, fornisce assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione sulle questioni amministrative e di bilancio di cui all'articolo 20.

3. Il comitato esecutivo consta di cinque membri. I membri del comitato esecutivo sono nominati tra i membri del consiglio di amministrazione. Uno dei membri è il presidente del consiglio di amministrazione, che può anche presiedere il comitato esecutivo, e un altro è un rappresentante della Commissione. Le nomine dei membri del comitato esecutivo mirano ad assicurare l'equilibrio di genere nel comitato esecutivo. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.

4. La durata del mandato dei membri del comitato esecutivo è di quattro anni. Il mandato è rinnovabile.

5. Il comitato esecutivo si riunisce almeno una volta ogni tre mesi. Il presidente del comitato esecutivo convoca riunioni supplementari su richiesta dei suoi membri.

6. Il consiglio di amministrazione stabilisce il regolamento interno del comitato esecutivo.

7. Se necessario per ragioni di urgenza, il comitato esecutivo può prendere determinate decisioni provvisorie a nome del consiglio di amministrazione, in particolare su questioni di gestione amministrativa, tra cui la sospensione della delega dei poteri dell'autorità che ha il potere di nomina e le questioni di bilancio. Tali decisioni provvisorie sono notificate al consiglio di amministrazione senza indebiti ritardi. Il consiglio di amministrazione decide poi se approvare o rigettare la decisione provvisoria entro 3 mesi dalla sua adozione. Il comitato esecutivo non adotta per conto del consiglio di amministrazione decisioni richiedono l'approvazione di una maggioranza di due terzi dei membri del consiglio di amministrazione.

Section 3

Direttore esecutivo

Articolo 20

Funzioni del direttore esecutivo

1. L'ENISA è diretta dal suo direttore esecutivo, che è indipendente nell'esercizio delle sue funzioni. Il direttore esecutivo risponde al consiglio di amministrazione.

2. Su richiesta, il direttore esecutivo riferisce al Parlamento europeo sull'esercizio delle sue funzioni. Il Consiglio può invitare il direttore esecutivo a riferire sull'esercizio delle sue funzioni.

3. Il direttore esecutivo ha la responsabilità di:

a) provvedere all'amministrazione corrente dell'ENISA;

b) attuare le decisioni adottate dal consiglio di amministrazione;

c) preparare il documento unico di programmazione e presentarlo al consiglio di amministrazione per approvazione prima di trasmetterlo alla Commissione;

d) attuare il documento unico di programmazione e riferire in merito al consiglio di amministrazione;

e) elaborare la relazione annuale consolidata sulle attività dell'ENISA, compresa l'attuazione del suo programma di lavoro annuale, e presentarla al consiglio di amministrazione per valutazione e adozione;

f) predisporre un piano d'azione che dia seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti;

g) predisporre un piano d'azione che dia seguito alle conclusioni delle relazioni di revisione contabile interne ed esterne e delle indagini dell'OLAF e riferire due volte l'anno alla Commissione sui progressi compiuti e periodicamente al consiglio di amministrazione;

h) predisporre il progetto della regolamentazione finanziaria applicabile all'ENISA di cui all'articolo 32;

i) predisporre il progetto di stato di previsione delle entrate e delle spese dell'ENISA e l'esecuzione del bilancio;

j) proteggere gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, se del caso, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive;

k) elaborare una strategia antifrode dell'ENISA e presentarla al consiglio di amministrazione per approvazione;

l) sviluppare e mantenere i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con i portatori di interessi;

m) scambiare periodicamente opinioni e informazioni con le istituzioni, gli organi e gli organismi dell'Unione riguardo alle loro attività in materia di cibersicurezza, al fine di garantire la coerenza nello sviluppo e nell'attuazione delle politiche dell'Unione;

n) svolgere gli altri compiti attribuiti al direttore esecutivo dal presente regolamento.

4. In base alle esigenze e nell'ambito degli obiettivi e dei compiti dell'ENISA, il direttore esecutivo può istituire gruppi di lavoro ad hoc composti da esperti, anche esperti inviati dalle autorità competenti degli Stati membri. Il direttore esecutivo ne informa il consiglio di amministrazione in anticipo. Le procedure relative in particolare alla composizione dei gruppi di lavoro, alla nomina degli esperti dei gruppi di lavoro da parte del direttore esecutivo e al funzionamento dei gruppi di lavoro sono specificati nel regolamento interno dell'ENISA.

5. Se necessario, per svolgere i compiti dell'ENISA in maniera efficiente ed efficace e in base a un'adeguata analisi costi-benefici, il direttore esecutivo può decidere di istituire uno o più uffici locali in uno o più Stati membri. Prima di decidere di istituire un ufficio locale, il direttore esecutivo chiede il parere degli Stati membri interessati, compreso lo Stato membro che ospita la sede dell'ENISA, e ottiene il previo consenso della Commissione e del consiglio di amministrazione. In caso di disaccordo durante il processo di consultazione tra il direttore esecutivo e gli Stati membri interessati, la questione è sottoposta all'esame del Consiglio. Il numero complessivo dei membri del personale in tutti gli uffici locali è ridotto al minimo e non supera il 40 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede. Il numero dei membri del personale in ciascuno degli uffici locali non supera il 10 % del numero totale dei membri del personale dell'ENISA nello Stato membro che ne ospita la sede.

La decisione di istituire un ufficio locale precisa la gamma di attività che devono essere espletate presso l'ufficio locale al fine di evitare costi inutili e duplicazioni di funzioni amministrative dell'ENISA.

Section 4

Gruppo consultivo ENISA, gruppo dei portatori di interessi per la certificazione della cibersicurezza e rete dei funzionari nazionali di collegamento

Articolo 21

Gruppo consultivo ENISA

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce in maniera trasparente il gruppo consultivo ENISA, composto da esperti riconosciuti che rappresentano i pertinenti portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le PMI, gli operatori di servizi essenziali, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati in conformità della direttiva (UE) 2018/1972, delle organizzazioni europee di normazione nonché delle autorità di contrasto e delle autorità di controllo preposte alla protezione dei dati. Il consiglio di amministrazione si adopera per garantire un opportuno equilibrio geografico e di genere, nonché un equilibrio tra i diversi gruppi di portatori di interessi.

2. Le procedure per il gruppo consultivo ENISA, in particolare per quanto riguarda la composizione, la proposta del direttore esecutivo di cui al paragrafo 1, il numero e la nomina dei membri e il funzionamento del gruppo consultivo ENISA, sono specificati nel regolamento interno dell'ENISA e resi pubblici.

3. Il gruppo consultivo ENISA è presieduto dal direttore esecutivo o da qualsiasi altra persona nominata dal direttore esecutivo caso per caso.

4. Il mandato dei membri del gruppo consultivo ENISA è di due anni e mezzo. I membri del consiglio di amministrazione non possono essere membri del gruppo consultivo ENISA. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare alle riunioni del gruppo consultivo ENISA e a partecipare alle sue attività. Possono essere invitati a partecipare alle riunioni del gruppo consultivo ENISA e alle sue attività i rappresentanti di altri organismi che siano considerati pertinenti dal direttore esecutivo e non siano membri di tale gruppo.

5. Il gruppo consultivo ENISA fornisce consulenza all'ENISA relativamente allo svolgimento dei suoi compiti, tranne per quanto concerne l'applicazione delle disposizioni del titolo III del presente regolamento. In particolare, esso consiglia il direttore esecutivo ai fini della stesura di una proposta relativa al programma di lavoro annuale dell'ENISA e della comunicazione con i relativi portatori di interessi sulle questioni inerenti al programma di lavoro annuale.

6. Il gruppo consultivo ENISA informa periodicamente il consiglio di amministrazione sulle sue attività.

Articolo 22

Gruppo dei portatori di interessi per la certificazione della cibersicurezza

1. È istituito il gruppo dei portatori di interessi per la certificazione della cibersicurezza.

2. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza è composto da membri selezionati tra esperti riconosciuti che rappresentano i pertinenti portatori di interessi. La Commissione, a seguito di un invito aperto e trasparente, seleziona su proposta dell'ENISA i membri del gruppo dei portatori di interessi per la certificazione della cibersicurezza garantendo un equilibrio tra i diversi gruppi di portatori di interessi, nonché un opportuno equilibrio geografico e di genere.

3. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza:

a) fornisce consulenza alla Commissione sulle questioni strategiche riguardanti il quadro europeo di certificazione della cibersicurezza;

b) su richiesta, fornisce consulenza all'ENISA su questioni generali e strategiche concernenti i compiti della stessa in materia di mercato, certificazione della cibersicurezza e normazione;

c) assiste la Commissione nell'elaborazione del programma di lavoro progressivo dell'Unione di cui all'articolo 47;

d) formula un parere sul programma di lavoro progressivo dell'Unione a norma dell'articolo 47, paragrafo 4; e,

e) in casi urgenti, fornisce consulenza alla Commissione e all'ECCG in merito alla necessità di sistemi di certificazione supplementari non inclusi nel programma di lavoro progressivo dell'Unione, come previsto dagli articoli 47 e 48.

4. Il gruppo dei portatori di interessi per la certificazione della cibersicurezza è copresieduto dai rappresentanti della Commissione e dell'ENISA ed è quest'ultima ad assicurarne il segretariato.

Articolo 23

Rete dei funzionari nazionali di collegamento

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce una rete dei funzionari nazionali di collegamento composta da rappresentanti di tutti gli Stati membri («funzionari nazionali di collegamento»). Ciascuno Stato membro designa un rappresentante nella rete dei funzionari nazionali di collegamento. Le riunioni della rete dei funzionari nazionali di collegamento possono svolgersi in diverse formazioni di esperti.

2. In particolare, la rete dei funzionari nazionali di collegamento agevola lo scambio di informazioni tra l'ENISA e gli Stati membri e sostiene l'ENISA nella diffusione, in tutta l'Unione, delle attività, dei risultati e delle raccomandazioni che la riguardano alle pertinenti parti interessate.

3. I funzionari nazionali di collegamento fungono da punto di contatto a livello nazionale per agevolare la cooperazione tra l'ENISA e gli esperti nazionali nel contesto dell'attuazione del programma di lavoro annuale dell'ENISA.

4. Mentre i funzionari nazionali di collegamento cooperano strettamente con i rappresentanti del consiglio di amministrazione dei rispettivi Stati membri, la rete dei funzionari nazionali di collegamento in sé non duplica il lavoro del consiglio di amministrazione o di altri consessi dell'Unione.

5. Le funzioni e le procedure relative alla rete dei funzionari nazionali di collegamento sono specificate nel regolamento interno dell'ENISA e rese pubbliche.

Section 5

Funzionamento

Articolo 24

Documento unico di programmazione

1. L'ENISA opera in conformità di un documento unico di programmazione contenente la programmazione annuale e pluriennale, che include tutte le attività pianificate.

2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti dalla Commissione, predispone un progetto di documento unico di programmazione contenente la pianificazione annuale e pluriennale delle risorse finanziarie e umane corrispondenti, secondo quanto previsto all'articolo 32 del regolamento delegato (UE) n. 1271/2013 della Commissione ([25]).

3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1 e lo trasmette al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, unitamente a eventuali successive versioni aggiornate di tale documento.

4. Il documento unico di programmazione diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione ed è adeguato secondo necessità.

([25]) Regolamento delegato (UE) n. 1271/2013 della Commissione, del 30 settembre 2013, che stabilisce il regolamento finanziario quadro degli organismi di cui all'articolo 208 del regolamento (UE, Euratom) n. 966/2012 del Parlamento europeo e del Consiglio (GU L 328 del 7.12.2013, pag. 42).

5. Il programma di lavoro annuale comprende gli obiettivi dettagliati e i risultati attesi, compresi gli indicatori di risultato. Esso contiene inoltre una descrizione delle azioni da finanziare e un'indicazione delle risorse finanziarie e umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio per attività e gestione per attività. Il programma di lavoro annuale è coerente con il programma di lavoro pluriennale di cui al paragrafo 7. Indica chiaramente i compiti aggiunti, modificati o soppressi rispetto all'esercizio finanziario precedente.

6. Quando all'ENISA è assegnato un nuovo compito, il consiglio di amministrazione modifica il programma di lavoro annuale adottato. Le modifiche sostanziali del programma di lavoro annuale sono adottate con la stessa procedura di quella applicabile al programma di lavoro annuale iniziale. Il consiglio di amministrazione può delegare al direttore esecutivo il potere di apportare modifiche non sostanziali al programma di lavoro annuale.

7. Il programma di lavoro pluriennale definisce la programmazione strategica generale, compresi gli obiettivi, i risultati attesi e gli indicatori di prestazione. Riporta inoltre la programmazione delle risorse, compresi il bilancio pluriennale e il personale.

8. La programmazione delle risorse è aggiornata ogni anno. La programmazione strategica è aggiornata secondo necessità, in particolare per adattarla all'esito della valutazione di cui all'articolo 67.

Articolo 25

Dichiarazione di interessi

1. I membri del consiglio di amministrazione, il direttore esecutivo, come pure i funzionari distaccati dagli Stati membri a titolo temporaneo, rendono ciascuno una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza. Le dichiarazioni sono precise e complete, presentate ogni anno per iscritto e aggiornate ogniqualvolta sia necessario.

2. I membri del consiglio di amministrazione, il direttore esecutivo e gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano ciascuno in modo preciso e completo, al più tardi all'inizio di ogni riunione, qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del giorno e si astengono dal partecipare alle discussioni e alle votazioni inerenti tali punti.

3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per le regole sulle dichiarazioni di interessi di cui ai paragrafi 1 e 2.

Articolo 26

Trasparenza

1. L'ENISA svolge le proprie attività con un livello elevato di trasparenza e nel rispetto dell'articolo 28.

2. L'ENISA provvede a che al pubblico e alle parti interessate siano fornite informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 25.

3. Il consiglio di amministrazione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività dell'ENISA.

4. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2.

Articolo 27

Riservatezza

1. Fatto salvo l'articolo 28, l'ENISA non rivela a terzi le informazioni da essa trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato.

2. I membri del consiglio di amministrazione, il direttore esecutivo, i membri del gruppo consultivo ENISA, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'ENISA, compresi i funzionari distaccati dagli Stati membri a titolo temporaneo, rispettano gli obblighi di riservatezza dell'articolo 339 TFUE anche dopo la cessazione delle proprie funzioni.

3. L'ENISA stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di riservatezza di cui ai paragrafi 1 e 2.

4. Se necessario ai fini dell'esecuzione dei compiti dell'ENISA, il consiglio di amministrazione decide di consentire all'ENISA di trattare informazioni classificate. In questo caso, l'ENISA, in accordo con i servizi della Commissione, adotta regole in materia di sicurezza che applichino i principi di sicurezza enunciati nelle decisioni (UE, Euratom) 2015/443 ([26]) e 2015/444 ([27]) della Commissione. Tali regole in materia di sicurezza disciplinano, tra l'altro, lo scambio, il trattamento e la conservazione di informazioni classificate.

Articolo 28

Accesso ai documenti

1. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dall'ENISA.

2. Entro il 28 dicembre 2019, il consiglio di amministrazione adotta disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

3. Le decisioni adottate dall'ENISA a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono formare oggetto di una denuncia presentata al Mediatore europeo a norma dell'articolo 228 TFUE o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 TFUE.

CAPO IV

Formazione e struttura del bilancio dell'ENISA

Articolo 29

Formazione del bilancio dell'ENISA

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo e lo trasmette al consiglio di amministrazione, corredato di un progetto di tabella dell'organico. Le entrate e le spese devono risultare in pareggio.

2. Ogni anno il consiglio di amministrazione elabora, sulla base del progetto di stato di previsione, uno stato di previsione delle entrate e delle spese dell'ENISA per l'esercizio finanziario successivo.

3. Entro il 31 gennaio di ogni anno il consiglio di amministrazione invia lo stato di previsione, come parte integrante del progetto di documento unico di programmazione, alla Commissione e ai paesi terzi con cui l'Unione ha concluso accordi di cui all'articolo 42, paragrafo 2.

4. Sulla base dello stato di previsione, la Commissione iscrive le stime che ritiene necessarie, per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale dell'Unione, nel progetto di bilancio generale dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente all'articolo 314 TFUE.

5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo dell'Unione all'ENISA.

6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico dell'ENISA.

([26]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

([27]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

7. Insieme al documento unico di programmazione, il consiglio di amministrazione adotta il bilancio dell'ENISA. Il bilancio dell'ENISA diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Ove necessario, il consiglio di amministrazione modifica il bilancio e il documento unico di programmazione dell'ENISA per conformarli al bilancio generale dell'Unione.

Articolo 30

Struttura del bilancio dell'ENISA

1. Fatte salve altre risorse, le entrate dell'ENISA comprendono:

a) un contributo dal bilancio generale dell'Unione;

b) entrate con destinazione specifica volte a finanziare spese specifiche conformemente alla regolamentazione finanziaria di cui all'articolo 32;

c) finanziamenti dell'Unione sotto forma di accordi di delega o di sovvenzioni ad hoc secondo la regolamentazione finanziaria di cui all'articolo 32 e le disposizioni dei pertinenti strumenti di sostegno alle politiche dell'Unione;

d) contributi dei paesi terzi che partecipano ai lavori dell'ENISA di cui all'articolo 42;

e) eventuali contributi volontari degli Stati membri, in denaro o in natura.

Gli Stati membri che versano contributi volontari ai sensi del primo comma, lettera e), non possono rivendicare alcun diritto o servizio specifico per effetto di tale contributo.

2. Le spese dell'ENISA comprendono la retribuzione del personale, l'assistenza amministrativa e tecnica, le spese infrastrutturali e di esercizio, nonché quelle conseguenti a contratti con terzi.

Articolo 31

Esecuzione del bilancio dell'ENISA

1. Il direttore esecutivo è responsabile dell'esecuzione del bilancio dell'ENISA.

2. Il revisore contabile interno della Commissione esercita nei confronti dell'ENISA le stesse competenze di cui dispone nei confronti dei servizi della Commissione.

3. Il contabile dell'ENISA comunica i conti provvisori per l'esercizio (anno N) al contabile della Commissione e alla Corte dei conti entro il 1º marzo dell'esercizio successivo (anno N + 1).

4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti provvisori dell'ENISA a norma dell'articolo 246 del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio ([28]), il contabile dell'ENISA redige i conti definitivi dell'ENISA sotto la propria responsabilità e li presenta al consiglio di amministrazione per parere.

5. Il consiglio di amministrazione formula un parere sui conti definitivi dell'ENISA.

6. Entro il 31 marzo dell'anno N + 1, il direttore esecutivo trasmette la relazione sulla gestione di bilancio e finanziaria al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.

7. Entro il 1º luglio dell'anno N + 1, il contabile dell'ENISA trasmette i conti definitivi dell'ENISA, accompagnati dal parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, al contabile della Commissione e alla Corte dei conti.

([28]) Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1).

8. Contemporaneamente ai conti definitivi dell'ENISA, il contabile dell'ENISA trasmette altresì alla Corte dei conti, e in copia al contabile della Commissione, una dichiarazione ad essi relativa.

9. Entro il 15 novembre dell'anno N + 1 il direttore esecutivo pubblica i conti definitivi dell'ENISA nella *Gazzetta ufficiale dell'Unione europea*.

10. Entro il 30 settembre dell'anno N + 1 il direttore esecutivo invia alla Corte dei conti una risposta alle osservazioni da essa formulate e ne trasmette copia al consiglio di amministrazione e alla Commissione.

11. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo, tutte le informazioni necessarie al corretto svolgimento della procedura di discarico per l'esercizio in causa, in conformità dell'articolo 261, paragrafo 3, del regolamento (UE, Euratom) 2018/1046.

12. Il Parlamento europeo, su raccomandazione del Consiglio, concede il discarico al direttore esecutivo, entro il 15 maggio dell'anno N + 2, per l'esecuzione del bilancio dell'esercizio N.

Articolo 32

Regolamentazione finanziaria

La regolamentazione finanziaria applicabile all'ENISA è adottata dal consiglio di amministrazione previa consultazione della Commissione. Essa si discosta dal regolamento delegato (UE) n. 1271/2013 solo per esigenze specifiche di funzionamento dell'ENISA e previo accordo della Commissione.

Articolo 33

Lotta antifrode

1. Per facilitare la lotta contro la frode, la corruzione e altre attività illecite ai sensi del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio ([29]), entro il 28 dicembre 2019 l'ENISA aderisce all'accordo interistituzionale del 25 maggio 1999 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo interne alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) ([30]). L'ENISA adotta opportune disposizioni valide per l'insieme dei propri dipendenti, utilizzando i modelli riportati nell'allegato di tale accordo.

2. La Corte dei conti ha potere di verifica, esercitabile su documenti e mediante ispezioni in loco, su tutti i beneficiari di sovvenzioni, i contraenti e i subcontraenti che hanno beneficiato di fondi dell'Unione da parte dell'ENISA.

3. L'OLAF può eseguire indagini, compresi controlli e verifiche sul posto, in conformità delle disposizioni e delle procedure stabilite dal regolamento (UE, Euratom) n. 883/2013 e dal regolamento (Euratom, CE) n. 2185/96 del Consiglio ([31]), per accertare casi di frode, corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dall'ENISA.

4. Fatti salvi i paragrafi 1, 2 e 3, gli accordi di cooperazione con paesi terzi o organizzazioni internazionali, i contratti, le convenzioni di sovvenzione e le decisioni di sovvenzione dell'ENISA contengono disposizioni che autorizzano esplicitamente la Corte dei conti e l'OLAF a procedere a tali revisioni contabili e indagini conformemente alle loro rispettive competenze.

([29]) Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

([30]) GU L 136 del 31.5.1999, pag. 15.

([31]) Regolamento (Euratom, CE) n 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2).

CAPO V

Personale

Articolo 34

Disposizioni generali

Al personale dell'ENISA si applicano lo statuto dei funzionari, il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per dare applicazione allo statuto dei funzionari e al regime applicabile agli altri agenti.

Articolo 35

Privilegi e immunità

All'ENISA e al suo personale si applica il protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea, allegato al TUE e al TFUE.

Articolo 36

Direttore esecutivo

1. Il direttore esecutivo è assunto come agente temporaneo dell'ENISA ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.

2. Il direttore esecutivo è nominato dal consiglio di amministrazione in base a un elenco di candidati proposto dalla Commissione, secondo una procedura di selezione aperta e trasparente.

3. Ai fini della conclusione del contratto di lavoro del direttore esecutivo, l'ENISA è rappresentata dal presidente del consiglio di amministrazione.

4. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione è invitato a fare una dichiarazione dinanzi alla commissione competente del Parlamento europeo e a rispondere alle domande dei deputati.

5. La durata del mandato del direttore esecutivo è di cinque anni. Entro la fine di tale periodo, la Commissione esegue una valutazione della prestazione del direttore esecutivo e dei compiti e delle sfide futuri dell'ENISA.

6. Il consiglio di amministrazione adotta le decisioni riguardanti la nomina del direttore esecutivo, la proroga del suo mandato e la sua rimozione dall'incarico in conformità dell'articolo 18, paragrafo 2.

7. Su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di amministrazione può prorogare il mandato del direttore esecutivo una sola volta, per cinque anni.

8. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo. Entro i tre mesi che precedono tale proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.

9. Il direttore esecutivo il cui mandato sia stato prorogato non partecipa a un'altra procedura di selezione per lo stesso posto.

10. Il direttore esecutivo può essere rimosso dall'incarico solo su decisione del consiglio di amministrazione, su proposta della Commissione.

Articolo 37

Esperti nazionali distaccati e altro personale

1. L'ENISA può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze. Lo statuto dei funzionari e il regime applicabile agli altri agenti non si applicano a tale personale.

2. Il consiglio di amministrazione adotta una decisione che stabilisce le regole relative al distacco di esperti nazionali presso l'ENISA.

CAPO VI

Disposizioni generali relative all'ENISA

Articolo 38

Status giuridico dell'ENISA

1. L'ENISA è un organismo dell'Unione ed è dotata di personalità giuridica.

2. L'ENISA gode, in ciascuno Stato membro, della più ampia capacità giuridica riconosciuta alle persone giuridiche dal diritto nazionale. In particolare, può acquistare o alienare beni mobili e immobili e stare in giudizio.

3. L'ENISA è rappresentata dal direttore esecutivo.

Articolo 39

Responsabilità dell'ENISA

1. La responsabilità contrattuale dell'ENISA è disciplinata dal diritto applicabile al contratto.

2. La Corte di giustizia dell'Unione europea è competente a giudicare in virtù di clausole compromissorie contenute nel contratto concluso dall'ENISA.

3. In materia di responsabilità extracontrattuale, l'ENISA è obbligata al risarcimento dei danni cagionati da essa o dai membri del suo personale nell'esercizio delle loro funzioni, secondo i principi generali comuni agli ordinamenti degli Stati membri.

4. La Corte di giustizia dell'Unione europea è competente a conoscere delle controversie relative al risarcimento dei danni di cui al paragrafo 3.

5. La responsabilità personale del personale dell'ENISA nei confronti dell'ENISA è disciplinata dalle disposizioni pertinenti che si applicano al personale dell'ENISA.

Articolo 40

Regime linguistico

1. All'ENISA si applica il regolamento n. 1 del Consiglio ([32]). Gli Stati membri e gli altri organismi designati dagli Stati membri possono rivolgersi all'ENISA e ottenere la risposta in una delle lingue ufficiali delle istituzioni dell'Unione di loro scelta.

2. I servizi di traduzione necessari per il funzionamento dell'ENISA sono forniti dal Centro di traduzione degli organismi dell'Unione europea.

Articolo 41

Protezione dei dati personali

1. Il trattamento dei dati personali da parte dell'ENISA è soggetto al regolamento (UE) 2018/1725.

2. Il consiglio di amministrazione adotta le norme di attuazione di cui all'articolo 45, paragrafo 3, del regolamento (UE) 2018/1725. Il consiglio di amministrazione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (UE) 2018/1725 da parte dell'ENISA.

([32]) Regolamento del Consiglio n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU 17 del 6.10.1958, pag. 385).

Articolo 42

Cooperazione con paesi terzi e organizzazioni internazionali

1. Nella misura necessaria ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'ENISA può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'ENISA può istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali, previa approvazione da parte della Commissione. Detti accordi di lavoro non creano obblighi giuridici per l'Unione e gli Stati membri.

2. L'ENISA è aperta alla partecipazione di paesi terzi che abbiano concluso con l'Unione accordi in tal senso. Nell'ambito delle pertinenti disposizioni di tali accordi, sono istituiti accordi di lavoro che specificano, in particolare, la natura, la portata e le modalità di partecipazione di detti paesi terzi ai lavori dell'ENISA, e comprendono disposizioni sulla partecipazione alle iniziative intraprese dall'ENISA, sui contributi finanziari e sul personale. In materia di personale, tali accordi di lavoro rispettano in ogni caso lo statuto dei funzionari e il regime applicabile agli altri agenti.

3. Il consiglio di amministrazione adotta una strategia per le relazioni con paesi terzi e organizzazioni internazionali riguardo a questioni che rientrano tra le competenze dell'ENISA. La Commissione garantisce che l'ENISA operi nell'ambito del proprio mandato e del quadro istituzionale vigente stipulando accordi di lavoro adeguati con il direttore esecutivo.

Articolo 43

Regole in materia di sicurezza per la protezione delle informazioni sensibili non classificate e delle informazioni classificate

Previa consultazione della Commissione, l'ENISA adotta regole in materia di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni sensibili non classificate e delle ICUE di cui alle decisioni (UE, Euratom) 2015/443 e 2015/444. Le regole in materia di sicurezza dell'ENISA includono le disposizioni che disciplinano lo scambio, il trattamento e la conservazione di tali informazioni.

Articolo 44

Accordo sulla sede e condizioni operative

1. Le necessarie disposizioni relative all'insediamento dell'ENISA nello Stato membro ospitante e alle strutture che quest'ultimo deve mettere a disposizione nonché le regole specifiche applicabili in tale Stato membro al direttore esecutivo, ai membri del consiglio di amministrazione, al personale dell'ENISA e ai membri delle rispettive famiglie sono fissate in un accordo di sede concluso tra l'ENISA e lo Stato membro ospitante, previa approvazione del consiglio di amministrazione.

2. Lo Stato membro che ospita l'ENISA fornisce le migliori condizioni possibili volte a garantire il corretto funzionamento dell'ENISA, tenendo conto dell'accessibilità della sede, dell'esistenza di strutture scolastiche adeguate per i figli del personale, di un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi dei membri del personale.

Articolo 45

Controllo amministrativo

L'operato dell'ENISA è sottoposto al controllo del Mediatore europeo in conformità dell'articolo 228 TFUE.

TITOLO III

QUADRO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Articolo 46

Quadro europeo di certificazione della cibersicurezza

1. È istituito il quadro europeo di certificazione della cibersicurezza al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC.

2. Il quadro europeo di certificazione della cibersicurezza prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita.

Articolo 47

Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza

1. La Commissione pubblica un programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza («programma di lavoro progressivo dell'Unione») in cui sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza.

2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.

3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC e processi TIC o delle relative categorie è giustificata sulla base di una o più delle seguenti motivazioni:

a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC o processi TIC e in particolare in relazione al rischio di frammentazione;

b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri;

c) la domanda di mercato;

d) gli sviluppi nel panorama delle minacce informatiche;

e) la richiesta di preparazione di una specifica proposta di sistema da parte del'ECCG.

4. La Commissione tiene nella debita considerazione i pareri in merito al progetto di programma di lavoro progressivo dell'Unione espressi dall'ECCG e dal gruppo dei portatori di interessi per la certificazione della cibersicurezza.

5. Il primo programma di lavoro progressivo dell'Unione è pubblicato entro il 28 giugno 2020. Il programma di lavoro progressivo dell'Unione è aggiornato almeno ogni tre anni e più spesso se necessario.

Articolo 48

Richiesta di un sistema europeo di certificazione della cibersicurezza

1. La Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente sulla base del programma di lavoro progressivo dell'Unione.

2. In casi debitamente giustificati la Commissione o l'ECCG può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente non incluso nel programma di lavoro progressivo dell'Unione. Il programma di lavoro progressivo dell'Unione è aggiornato di conseguenza.

Articolo 49

Preparazione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza

1. A seguito di una richiesta della Commissione ai sensi dell'articolo 48, l'ENISA prepara una proposta di sistema che soddisfi i requisiti di cui agli articoli 51, 52 e 54.

2. A seguito di una richiesta dell'ECCG a norma dell'articolo 48, paragrafo 2, l'ENISA può preparare una proposta di sistema che soddisfi i requisiti di cui agli articoli 51, 52 e 54. Qualora respinga tale richiesta, l'ENISA motiva il proprio rifiuto. Ogni decisione di rifiuto della richiesta è presa dal consiglio di amministrazione.

3. Nella preparazione di una proposta di sistema, l'ENISA consulta tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo.

4. Per ciascuna proposta di sistema, l'ENISA istituisce un gruppo di lavoro ad hoc in conformità dell'articolo 20, paragrafo 4, con l'obiettivo di fornire all'ENISA consulenza e competenze specifiche.

5. L'ENISA coopera strettamente con l'ECCG. L'ECCG fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e adotta un parere sulla proposta.

6. L'ENISA tiene nella massima considerazione il parere dell'ECCG prima di trasmettere alla Commissione la proposta di sistema preparata in conformità dei paragrafi 3, 4 e 5. Il parere dell'ECCG non vincola l'ENISA e la sua assenza non impedisce all'ENISA di trasmettere la proposta di sistema alla Commissione.

7. La Commissione, sulla base della proposta di sistema preparata dall'ENISA, può adottare atti di esecuzione, prevedendo un sistema europeo di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC che soddisfano i requisiti di cui agli articoli 51, 52 e 54. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

8. Almeno ogni cinque anni l'ENISA valuta ogni sistema europeo di certificazione della cibersicurezza adottato, tenendo conto del riscontro ricevuto dalle parti interessate. Se necessario, la Commissione o l'ECCG può chiedere all'ENISA di avviare il processo di sviluppo di una proposta riveduta di sistema in conformità dell'articolo 48 e del presente articolo.

Articolo 50

Sito web sui sistemi europei di certificazione della cibersicurezza

1. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza, sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità, e li pubblicizza, comprese le informazioni sui certificati europei di cibersicurezza che non sono più validi, sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità revocati e scaduti e sul repertorio di link a informazioni sulla cibersicurezza fornite a norma dell'articolo 55.

2. Ove applicabile, il sito web di cui al paragrafo 1 indica inoltre i sistemi di certificazione della cibersicurezza nazionali che sono stati sostituiti da un sistema europeo di certificazione della cibersicurezza.

Articolo 51

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:

a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC;

c) le persone, i programmi o le macchine autorizzati devono poter accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

d) individuare e documentare le dipendenze e vulnerabilità note;

e) registrare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

f) fare in modo che si possa verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso, che sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

g) verificare che i prodotti TIC, i servizi TIC e i processi TIC non contengano vulnerabilità note;

h) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;

i) i prodotti TIC, i servizi TIC e i processi TIC devono essere sicuri fin dalla progettazione e per impostazione predefinita;

j) il software e l'hardware dei prodotti TIC, dei servizi TIC e dei processi TIC devono essere aggiornati, non contenere vulnerabilità pubblicamente note e devono disporre di meccanismi per effettuare aggiornamenti protetti.

Articolo 52

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC e i processi TIC uno o più dei seguenti livelli di affidabilità: «di base», «sostanziale» o «elevato». Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente.

2. I certificati europei di cibersicurezza e le dichiarazioni UE di conformità si riferiscono a qualsiasi livello di affidabilità specificato nel sistema europeo di certificazione della cibersicurezza nell'ambito del quale si rilascia il certificato europeo di cibersicurezza o la dichiarazione UE di conformità.

3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersicurezza pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti della valutazione a cui deve essere sottoposto il prodotto TIC, servizio TIC o processo TIC.

4. Il certificato o la dichiarazione UE di conformità si riferiscono a specifiche tecniche, norme e procedure ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli

5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità «di base» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

6. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «sostanziale» assicura che i prodotti TIC, servizi TIC e processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

7. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «elevato» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.

8. I sistemi europei di certificazione della cibersicurezza possono precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia di valutazione utilizzata. Ciascun livello di valutazione corrisponde a uno dei livelli di affidabilità ed è definito da un'idonea combinazione di componenti dell'affidabilità.

Articolo 53

Autovalutazione della conformità

1. Un sistema europeo di certificazione della cibersicurezza può consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC o processi TIC. Tale autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, servizi TIC e processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità «di base».

2. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC si assume la responsabilità della conformità del prodotto TIC, servizio TIC o processo TIC ai requisiti previsti in tale sistema.

3. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC rende disponibile all'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema. Una copia della dichiarazione UE di conformità è trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

4. Il rilascio di una dichiarazione UE di conformità è volontario, salvo diversamente specificato nel diritto dell'Unione o degli Stati membri.

5. Le dichiarazioni UE di conformità sono riconosciute in tutti gli Stati membri.

Articolo 54

Elementi dei sistemi europei di certificazione della cibersicurezza

1. Un sistema europeo di certificazione della cibersicurezza comprende almeno i seguenti elementi:

a) l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo o le categorie di prodotti TIC, servizi TIC o processi TIC coperti;

b) una chiara descrizione dello scopo del sistema e delle modalità con cui le norme, i metodi di valutazione e i livelli di affidabilità selezionati corrispondono alle esigenze degli utenti del sistema previsti;

c) i riferimenti alle norme internazionali, europee o nazionali applicate nella valutazione o, laddove tali norme non siano disponibili o adeguate, alle specifiche tecniche che rispettano le prescrizioni enunciate all'allegato II del regolamento (UE) n. 1025/2012 oppure, se tali specifiche non sono disponibili, alle specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema europeo di certificazione della cibersicurezza;

d) se del caso, uno o più livelli di affidabilità;

e) l'indicazione se l'autovalutazione della conformità sia autorizzata nell'ambito del sistema;

f) se del caso, requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cibersicurezza;

g) i criteri e i metodi di valutazione specifici da utilizzare, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi di sicurezza di cui all'articolo 51 sono stati conseguiti;

h) se del caso, le informazioni che sono necessarie per la certificazione e che un richiedente deve fornire agli organismi di valutazione della conformità o che deve altrimenti mettere a loro disposizione;

i) le condizioni alle quali possono essere utilizzati gli eventuali marchi o etichette previsti dal sistema;

j) le regole per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC ai requisiti dei certificati europei di cibersicurezza o delle dichiarazioni UE di conformità, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;

k) se del caso, le condizioni per il rilascio, il mantenimento, la prosecuzione e il rinnovo dei certificati europei di cibersicurezza, nonché le condizioni per l'estensione o la riduzione del campo di applicazione della certificazione;

l) le regole riguardanti le conseguenze per i prodotti TIC, servizi TIC e processi TIC che sono stati certificati o per i quali è stata rilasciata una dichiarazione UE di conformità ma che non sono conformi ai requisiti del sistema;

m) le regole riguardanti il modo in cui segnalare e trattare le vulnerabilità della cibersicurezza nei prodotti TIC, servizi TIC e processi TIC precedentemente non rilevate;

n) se del caso, le regole riguardanti la conservazione dei registri da parte degli organismi di valutazione della conformità;

o) l'individuazione dei sistemi nazionali o internazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti TIC, servizi TIC e processi TIC, requisiti di sicurezza, criteri e metodi di valutazione nonché livelli di affidabilità;

p) il contenuto e il formato dei certificati europei di cibersicurezza e le dichiarazioni UE di conformità da rilasciare;

q) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti da rendere disponibili da parte del fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC;

r) il periodo massimo di validità dei certificati europei di cibersicurezza rilasciati nell'ambito del sistema;

s) la politica di divulgazione dei certificati europei di cibersicurezza rilasciati, modificati o revocati nell'ambito del sistema;

t) le condizioni per il riconoscimento reciproco dei sistemi di certificazione con i paesi terzi;

u) se del caso, le regole riguardanti eventuali meccanismi di valutazione inter pares istituito dal sistema per le autorità o gli organismi che rilasciano certificati europei di cibersicurezza per il livello di affidabilità «elevato» a norma dell'articolo 56, paragrafo 6. Tali meccanismi non pregiudicano la valutazione inter pares di cui all'articolo 59;

v) il formato e le procedure che i fabbricanti o i fornitori di prodotti TIC, servizi TIC o processi TIC devono rispettare nel fornire e aggiornare le informazioni supplementari sulla cibersicurezza a norma dell'articolo 55.

2. I requisiti specificati del sistema europeo di certificazione della cibersicurezza devono essere coerenti con gli obblighi di legge applicabili, in particolare quelli derivanti dal diritto armonizzato dell'Unione.

3. Se un atto giuridico specifico dell'Unione lo prevede, un certificato o una dichiarazione UE di conformità rilasciati nell'ambito di un sistema europeo di certificazione della cibersicurezza possono essere utilizzati per dimostrare la presunzione di conformità agli obblighi imposti da tale atto giuridico.

4. In assenza di diritto armonizzato dell'Unione, anche il diritto degli Stati membri può disporre che un sistema europeo di certificazione della cibersicurezza possa essere utilizzato per stabilire la presunzione di conformità agli obblighi di legge.

Articolo 55

Informazioni supplementari sulla cibersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati

1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC certificati o prodotti TIC, servizi TIC o processi per i quali è stata rilasciata una dichiarazione UE di conformità rende pubblicamente disponibili le seguenti informazioni supplementari sulla cibersicurezza:

a) orientamenti e raccomandazioni che assistano gli utenti finali nel configurare, installare, avviare, operare e mantenere in modo sicuro i prodotti TIC o servizi TIC;

b) il periodo durante il quale agli utenti finali sarà offerta assistenza di sicurezza, in particolare per quanto concerne la disponibilità di aggiornamenti connessi alla cibersicurezza;

c) informazioni di contatto del fabbricante o fornitore e metodi accettati per ricevere informazioni sulle vulnerabilità dagli utenti finali e dai ricercatori nel settore della sicurezza;

d) un riferimento ad archivi online in cui siano elencate le vulnerabilità comunicate al pubblico relative al prodotto TIC, servizio TIC o processo TIC e a tutti i relativi consigli in materia di cibersicurezza.

2. Le informazioni di cui al paragrafo 1 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, almeno fino alla scadenza del certificato europeo di cibersicurezza o della dichiarazione UE di conformità corrispondenti.

Articolo 56

Certificazione della cibersicurezza

1. I prodotti TIC, i servizi TIC e i processi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 sono considerati conformi ai requisiti di tale sistema.

2. La certificazione della cibersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o degli Stati membri.

3. La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e migliorare il funzionamento del mercato interno. La prima valutazione di questo genere è effettuata entro il 31 dicembre 2023 e le successive valutazioni sono effettuate almeno ogni due anni. Sulla base dei risultati di tali valutazioni, la Commissione individua i prodotti TIC, servizi TIC e processi TIC coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione.

In via prioritaria la Commissione si concentra sui settori elencati all'allegato II della direttiva (UE) 2016/1148, che sono sottoposti a valutazione al più tardi due anni dopo l'adozione del primo sistema europeo di certificazione della cibersicurezza.

Nel preparare la valutazione la Commissione:

a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC 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 TIC, i servizi TIC o i processi TIC in questione;

b) tiene conto dell'esistenza e dell'attuazione di diritto degli Stati membri e dei paesi terzi in materia;

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

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

e) propone il modo più rapido ed efficace per realizzare la transizione da un sistema di certificazione volontario a uno obbligatorio.

4. Gli organismi di valutazione della conformità di cui all'articolo 60 rilasciano certificati europei di cibersicurezza ai sensi del presente articolo che fanno riferimento a un livello di affidabilità «di base» o «sostanziale» sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza adottato dalla Commissione a norma dell'articolo 49.

5. In deroga al paragrafo 4, in casi debitamente giustificati un sistema europeo di certificazione della cibersicurezza può prevedere che i certificati europei di cibersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico. Detto ente è uno dei seguenti:

a) un'autorità nazionale di certificazione della cibersicurezza ai sensi dell'articolo 58, paragrafo 1; o

b) un organismo pubblico accreditato come organismo di valutazione della conformità a norma dell'articolo 60, paragrafo 1.

6. Ove un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 richieda un livello di affidabilità «elevato», il certificato europeo di cibersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza oppure, nei casi seguenti, da un organismo di valutazione della conformità:

a) previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità; o

b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cibersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

7. La persona fisica o giuridica che presenta i prodotti TIC, servizi TIC o processi TIC per la certificazione mette a disposizione dell'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersicurezza, o dell'organismo di valutazione della conformità di cui all'articolo 60 tutte le informazioni necessarie a espletare la certificazione.

8. Il titolare di un certificato europeo di cibersicurezza informa l'autorità o l'organismo di cui all'articolo 7 delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC o processi TIC certificati che possono incidere sulla conformità ai requisiti relativi alla certificazione. Tale autorità o organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersicurezza interessata.

9. Un certificato europeo di cibersicurezza è rilasciato per il periodo indicato nel sistema europeo di certificazione della cibersicurezza e può essere rinnovato, purché continuino a essere soddisfatti i requisiti pertinenti.

10. I certificati europei di cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.

Articolo 57

Sistemi e certificati nazionali di certificazione della cibersicurezza

1. Fatto salvo il paragrafo 3 del presente articolo, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC e processi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 49, paragrafo 7. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC e processi TIC non coperti da un sistema europeo di certificazione della cibersicurezza restano in vigore.

2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per prodotti TIC, servizi TIC e processi TIC già coperti da un sistema europeo di certificazione della cibersicurezza in vigore.

3. I certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza e coperti da un sistema europeo di certificazione della cibersicurezza restano validi fino alla loro data di scadenza.

4. Al fine di evitare la frammentazione del mercato interno, gli Stati membri informano la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza.

Articolo 58

Autorità nazionali di certificazione della cibersicurezza

1. Ciascuno Stato membro designa una o più autorità nazionali di certificazione della cibersicurezza nel suo territorio oppure, con l'accordo di un altro Stato membro, designa una o più autorità nazionali di certificazione della cibersicurezza stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.

2. Ciascuno Stato membro comunica alla Commissione l'identità delle autorità nazionali di certificazione della cibersicurezza designate. Se uno Stato membro designa più di una autorità, comunica alla Commissione anche i compiti assegnati a ciascuna di tali autorità.

3. Fatti salvi l'articolo 56, paragrafo 5, lettera a), e l'articolo 56, paragrafo 6, ciascuna autorità nazionale di certificazione della cibersicurezza è indipendente dai soggetti sui quali vigila per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale.

4. Gli Stati membri assicurano che le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati europei di cibersicurezza di cui all'articolo 56, paragrafo 5, lettera a), e dell'articolo 56, paragrafo 6, siano rigorosamente separate dalle attività di vigilanza indicate nel presente articolo e che tali attività siano svolte indipendentemente le une dalle altre.

5. Gli Stati membri provvedono affinché le autorità nazionali di certificazione della cibersicurezza dispongano di risorse adeguate per l'esercizio dei loro poteri e per l'esecuzione efficiente ed efficace dei loro compiti.

6. Ai fini dell'effettiva attuazione del presente regolamento, è opportuno che le autorità nazionali di certificazione della cibersicurezza partecipino in modo attivo, efficace, efficiente e sicuro all'ECCG.

7. Le autorità nazionali di certificazione della cibersicurezza:

a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti;

b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi di tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza;

c) fatto salvo l'articolo 60, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento;

d) monitorano e vigilano sulle attività degli organismi pubblici di cui all'articolo 56, paragrafo 5;

e) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità violino le prescrizioni del presente regolamento;

f) trattano i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 53, e svolgono le indagini opportune sull'oggetto di tali reclami e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole;

g) trasmettono all'ENISA e all'ECCG una relazione sintetica annuale sulle attività svolte ai sensi del presente paragrafo, lettere b), c) e d), o del paragrafo 8;

h) cooperano con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti TIC, servizi TIC e processi TIC non conformi ai requisiti del presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza; e

i) sorvegliano gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza.

8. Ciascuna autorità nazionale di certificazione della cibersicurezza dispone almeno dei seguenti poteri:

a) richiedere agli organismi di valutazione della conformità, ai titolari di certificati europei della cibersicurezza e agli emittenti di dichiarazioni UE di conformità di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;

b) condurre indagini, sotto forma di verifiche contabili, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità allo scopo di verificarne l'osservanza del presente titolo;

c) adottare misure appropriate, nel rispetto del diritto nazionale, per accertare che gli organismi di valutazione della conformità, i titolari di certificati europei di cibersicurezza e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

d) ottenere accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersicurezza al fine di svolgere indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;

e) revocare, conformemente al diritto nazionale, i certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o i certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, qualora tali certificati non siano conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

f) irrogare sanzioni conformemente al diritto nazionale, a norma dell'articolo 65, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.

9. Le autorità nazionali di certificazione della cibersicurezza cooperano tra di loro e con la Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti TIC, servizi TIC e processi TIC.

Articolo 59

Valutazione inter pares

1. Al fine di ottenere norme equivalenti in tutta l'Unione relativamente ai certificati europei di cibersicurezza e alle dichiarazioni UE di conformità, le autorità nazionali di certificazione della cibersicurezza sono soggette a una valutazione inter pares.

2. La valutazione inter pares è effettuata sulla base di criteri e procedure di valutazione solidi e trasparenti, in particolare per quanto riguarda i requisiti in termini strutturali, di risorse umane e procedurali, la riservatezza e i reclami.

3. La valutazione inter pares esamina:

a) ove applicabile, se le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati europei di cibersicurezza di cui all'articolo 56, paragrafo 5, lettera a), e all'articolo 56, paragrafo 6, siano rigorosamente separate dalle attività di vigilanza indicate all'articolo 58 e se tali attività siano svolte indipendentemente le une dalle altre;

b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i certificati europei di cibersicurezza a norma dell'articolo 58, paragrafo 7, lettera a);

c) le procedure di monitoraggio e applicazione degli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC a norma dell'articolo 58, paragrafo 7, lettera b);

d) le procedure di monitoraggio, autorizzazione e vigilanza delle attività degli organismi di valutazione della conformità;

e) ove applicabile, se il personale delle autorità o degli organismi che rilasciano certificati di livello di affidabilità «elevato» a norma dell'articolo 56, paragrafo 6, disponga di competenze adeguate.

4. La valutazione inter pares è effettuata da almeno due autorità nazionali di certificazione della cibersicurezza di altri Stati membri e dalla Commissione, e ha luogo almeno una volta ogni cinque anni. L'ENISA può partecipare alla valutazione inter pares.

5. La Commissione può adottare atti di esecuzione che definiscano un piano almeno quinquennale per la valutazione inter pares e fissino i criteri riguardanti la composizione del gruppo di valutazione inter pares, la metodologia da utilizzare in tale valutazione nonché il calendario, la frequenza e altri compiti connessi. Nell'adottare tali atti di esecuzione, la Commissione tiene debitamente conto delle opinioni dell'ECCG. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

6. L'ECCG esamina i risultati delle valutazioni inter pares, redige sintesi che possono essere rese pubbliche e, se necessario, formula orientamenti o raccomandazioni in merito ad azioni o a misure che devono essere adottate dai soggetti interessati.

Articolo 60

Organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008. Tale accreditamento è rilasciato solo se l'organismo di valutazione della conformità soddisfa i requisiti indicati nell'allegato del presente regolamento.

2. Ove un certificato europeo di cibersicurezza sia rilasciato da un'autorità nazionale di certificazione della cibersicurezza a norma dell'articolo 56, paragrafo 5, lettera a), e dell'articolo 56, paragrafo 6, l'organismo di certificazione dell'autorità nazionale di certificazione della cibersicurezza è accreditato come organismo di valutazione della conformità a norma del presente articolo, paragrafo 1.

3. Qualora i sistemi europei di certificazione della cibersicurezza stabiliscano requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'autorità nazionale di certificazione della cibersicurezza a svolgere i compiti previsti da tali sistemi.

4. L'accreditamento di cui al paragrafo 1 è rilasciato agli organismi di valutazione della conformità per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni, purché l'organismo di valutazione della conformità continui a soddisfare i requisiti di cui al presente articolo. Entro un termine ragionevole, gli organismi nazionali di accreditamento adottano tutte le misure necessarie per limitare, sospendere o revocare l'accreditamento di un organismo di valutazione della conformità rilasciato in virtù del paragrafo 1 se le condizioni per l'accreditamento non sono state soddisfatte o non sono più soddisfatte oppure se l'organismo di valutazione della conformità viola il presente regolamento.

Articolo 61

Notifica

1. Per ciascun sistema europeo di certificazione della cibersicurezza le autorità nazionali di certificazione della cibersicurezza notificano alla Commissione gli organismi di valutazione della conformità che sono stati accreditati e, se del caso, autorizzati a norma dell'articolo 60, paragrafo 3, a rilasciare certificati europei di cibersicurezza a determinati livelli di affidabilità di cui all'articolo 52. Le autorità nazionali di certificazione della cibersicurezza notificano alla Commissione, senza indebito ritardo, ogni successiva modifica degli stessi.

2. Un anno dopo l'entrata in vigore di un sistema europeo di certificazione della cibersicurezza, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco degli organismi di valutazione della conformità notificati nell'ambito di tale sistema.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco degli organismi di valutazione della conformità notificati entro due mesi dalla data di ricevimento di tale notifica.

4. Un'autorità nazionale di certificazione della cibersicurezza può presentare alla Commissione una richiesta di rimozione di un organismo di valutazione della conformità notificato da tale autorità dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricevimento della richiesta dell'autorità nazionale di certificazione della cibersicurezza.

5. La Commissione può adottare atti di esecuzione per stabilire le circostanze, i formati e le procedure per le notifiche di cui al presente articolo, paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.

Articolo 62

Gruppo europeo per la certificazione della cibersicurezza

1. È istituito il gruppo europeo per la certificazione della cibersicurezza («ECCG»).

2. L'ECCG è composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o da rappresentanti di altre autorità nazionali competenti. Un membro dell'ECCG non rappresenta più di due Stati membri.

3. I portatori di interessi e le parti terze interessate possono essere invitati a presenziare alle riunioni dell'ECCG e a partecipare ai suoi lavori.

4. L'ECCG ha i seguenti compiti:

a) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti del presente titolo, in particolare per quanto riguarda il programma di lavoro progressivo dell'Unione, le questioni relative alla politica in materia di certificazione della cibersicurezza, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersicurezza;

b) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema ai sensi dell'articolo 49;

c) adottare un parere sulle proposte di sistemi preparate dall'ENISA ai sensi dell'articolo 49;

d) chiedere all'ENISA di preparare proposte di sistemi ai sensi dell'articolo 48, paragrafo 2;

e) adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

f) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cibersicurezza;

g) agevolare la cooperazione tra le autorità nazionali di certificazione della cibersicurezza di cui al presente titolo attraverso lo sviluppo della capacità e lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti della certificazione della cibersicurezza;

h) sostenere l'attuazione dei meccanismi di valutazione inter pares in conformità delle regole fissate da un sistema europeo di certificazione della cibersicurezza ai sensi dell'articolo 54, paragrafo 1, lettera u);

i) agevolare l'allineamento dei sistemi europei di certificazione della cibersicurezza alle norme riconosciute a livello internazionale, rivedendo tra l'altro i sistemi europei di certificazione della cibersicurezza esistenti e, ove opportuno, rivolgendo raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale.

5. Con l'assistenza dell'ENISA, la Commissione presiede l'ECCG e svolge le funzioni di segretariato per lo stesso, conformemente all'articolo 8, paragrafo 1, lettera e).

Articolo 63

Diritto di presentare un reclamo

1. Le persone fisiche e giuridiche hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di cibersicurezza o, se il reclamo riguarda un certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità che agisce conformemente all'articolo 56, paragrafo 6, all'autorità nazionale di certificazione della cibersicurezza competente.

2. L'autorità o l'organismo a cui à stato presentato il reclamo informa il reclamante dello stato del procedimento e della decisione adottata e informa il reclamante del diritto a un ricorso giurisdizionale effettivo di cui all'articolo 64.

Articolo 64

Diritto a un ricorso giurisdizionale effettivo

1. Fatti salvi eventuali ricorsi amministrativi o altri ricorsi extragiudiziali, le persone fisiche e giuridiche hanno diritto a un ricorso giurisdizionale effettivo per quanto riguarda:

a) le decisioni assunte dall'autorità o dall'organismo di cui all'articolo 63, paragrafo 1, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cibersicurezza detenuto da tali persone fisiche e giuridiche;

b) il mancato intervento relativamente a un reclamo presentato all'autorità o all'organismo di cui all'articolo 63, paragrafo 1.

2. I procedimenti a norma del presente articolo sono presentati dinanzi ai tribunali dello Stato membro in cui ha sede l'autorità o l'organismo contro cui è mosso il ricorso giurisdizionale.

Articolo 65

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente titolo e di violazione dei sistemi europei di certificazione della cibersicurezza e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.

TITOLO IV

DISPOSIZIONI FINALI

Articolo 66

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, paragrafo 4, lettera b), del regolamento (UE) n. 182/2011.

Articolo 67

Valutazione e riesame

1. Entro il 28 giugno 2024, e successivamente ogni cinque anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'ENISA e delle sue prassi di lavoro, l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro fornito all'ENISA in relazione alle sue attività. Se ritiene che il mantenimento dell'ENISA non sia più giustificato alla luce degli obiettivi, del mandato e dei compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'ENISA.

2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e di migliorare il funzionamento del mercato interno.

3. La valutazione esamina se siano necessari requisiti essenziali di cibersicurezza per l'accesso al mercato interno onde impedire l'ingresso nel mercato dell'Unione di prodotti TIC, servizi TIC e processi TIC che non rispettano i requisiti di base in materia di cibersicurezza.

4. Entro il 28 giugno 2024, e successivamente ogni 5 anni, la Commissione trasmette la relazione di valutazione unitamente alle sue conclusioni al Parlamento europeo, al Consiglio e al consiglio di amministrazione. I risultati della relazione sono resi pubblici.

Articolo 68

Abrogazione e sostituzione

1. Il regolamento (UE) n. 526/2013 è abrogato con effetto a decorrere dal 27 giugno 2019.

2. I riferimenti al regolamento (UE) n. 526/2013 e all'ENISA istituita da tale regolamento si intendono fatti al presente regolamento e all'ENISA istituita dal presente regolamento.

3. L'ENISA istituita dal presente regolamento sostituisce l'ENISA istituita dal regolamento (UE) n. 526/2013 per quanto riguarda diritti di proprietà, accordi, obblighi di legge, contratti di lavoro, impegni finanziari e responsabilità. Tutte le decisioni del consiglio di amministrazione e del comitato esecutivo adottate in conformità del regolamento (UE) n. 526/2013 restano valide, purché siano conformi al presente regolamento.

4. L'ENISA è istituita per un periodo indeterminato a decorrere dal 27 giugno 2019.

5. Il direttore esecutivo nominato a norma dell'articolo 24, paragrafo 4, del regolamento (UE) n. 526/2013 resta in carica ed esercita le funzioni di direttore esecutivo ai sensi dell'articolo 20 del presente regolamento per la restante durata del mandato. Le altre condizioni contrattuali rimangono invariate.

6. I membri del consiglio di amministrazione e i loro supplenti nominati a norma dell'articolo 6 del regolamento (UE) n. 526/2013 restano in carica ed esercitano le funzioni del consiglio di amministrazione ai sensi dell'articolo 15 del presente regolamento per la restante durata del mandato.

Articolo 69

Entrata in vigore

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Gli articoli 58, 60, 61, 63, 64 e 65 si applicano dal 28 giugno 2021.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO

REQUISITI CHE GLI ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ DEVONO SODDISFARE

Gli organismi di valutazione della conformità che desiderano essere accreditati devono soddisfare i requisiti elencati in appresso:

1. L'organismo di valutazione della conformità è istituito a norma del diritto interno e ha personalità giuridica.

2. L'organismo di valutazione della conformità è un organismo terzo, indipendente dall'organizzazione o dai prodotti TIC, servizi TIC o processi TIC che valuta.

3. Un organismo appartenente a un'associazione d'imprese o a una federazione professionale che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura, nell'assemblaggio, nell'utilizzo o nella manutenzione dei prodotti TIC, servizi TIC o processi TIC che valuta può essere ritenuto un organismo di valutazione della conformità, a condizione che siano dimostrate la sua indipendenza e l'assenza di qualsiasi conflitto di interesse.

4. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non sono né il progettista, né il fabbricante, né il fornitore, né l'installatore, né l'acquirente, né il proprietario, né l'utilizzatore, né il responsabile della manutenzione del prodotto TIC, servizio TIC o processo TIC sottoposto a valutazione, né il rappresentante autorizzato di uno di questi soggetti. Tale divieto non preclude l'uso dei prodotti TIC valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità o il loro uso per scopi privati.

5. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intervengono direttamente nella progettazione, fabbricazione o costruzione, nella commercializzazione, nell'installazione, nell'uso o nella manutenzione dei prodotti TIC, servizi TIC o processi TIC sottoposti a valutazione, né rappresentano i soggetti impegnati in tali attività. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intraprendono attività alcuna che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle loro attività di valutazione della conformità. Tale divieto vale in particolare per i servizi di consulenza.

6. Se un organismo di valutazione della conformità è di proprietà di un ente o un'istituzione pubblici o è gestito da questi ultimi, l'indipendenza e l'assenza di conflitti di interessi tra l'autorità nazionale di certificazione della cibersicurezza e l'organismo di valutazione della conformità sono garantite e documentate.

7. Gli organismi di valutazione della conformità garantiscono che le attività delle loro affiliate e dei loro subappaltatori non abbiano effetti negativi sulla riservatezza, sull'obiettività o sull'imparzialità delle loro attività di valutazione della conformità.

8. Gli organismi di valutazione della conformità e il loro personale eseguono le attività di valutazione della conformità con il massimo dell'integrità professionale e della competenza tecnica richieste e sono liberi da qualsivoglia pressione e incentivo che possa influenzare il loro giudizio o i risultati delle loro attività di valutazione, anche pressioni e incentivi di natura finanziaria, in particolare da parte di persone o gruppi di persone interessati ai risultati di tali attività.

9. Un organismo di valutazione della conformità è in grado di effettuare tutti i compiti di valutazione della conformità ad esso attribuiti ai sensi del presente regolamento, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità. Eventuali subappalti o consultazioni di personale esterno sono adeguatamente documentati, non prevedono alcun intermediario e sono oggetto di un accordo scritto che contempli, tra l'altro, la riservatezza e i conflitti di interessi. L'organismo di valutazione della conformità in questione si assume la piena responsabilità dei compiti svolti.

10. In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo, categoria o sottocategoria di prodotti TIC, servizi TIC o processi TIC, l'organismo di valutazione della conformità dispone:

    a) di personale avente conoscenze tecniche ed esperienza sufficiente e appropriata per eseguire i compiti di valutazione della conformità;

    b) di descrizioni delle procedure in base alle quali si svolge la valutazione della conformità, si garantisce la trasparenza di tali procedure e la possibilità di riprodurle. Predispone una politica e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato ai sensi dell'articolo 61 dalle altre attività;

c) di procedure per svolgere le attività che tengano debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto TIC, servizio TIC o processo TIC in questione e della natura di massa o seriale del processo produttivo.

11. L'organismo di valutazione della conformità dispone dei mezzi necessari per eseguire i compiti tecnici e amministrativi connessi alle attività di valutazione della conformità in modo appropriato e ha accesso a tutti gli strumenti e impianti occorrenti.

12. Le persone addette alle attività di valutazione della conformità dispongono di quanto segue:

a) una formazione tecnica e professionale solida che includa tutte le attività di valutazione della conformità;

b) soddisfacenti conoscenze delle prescrizioni relative alle valutazioni della conformità che eseguono e un'adeguata autorità per eseguire tali valutazioni;

c) una conoscenza e una comprensione adeguate dei requisiti e delle norme di prova applicabili;

d) la capacità di elaborare certificati, registri e relazioni a dimostrazione del fatto che le valutazioni sono state effettuate.

13. È garantita l'imparzialità dell'organismo di valutazione della conformità, dei suoi alti dirigenti, delle persone addette alle attività di valutazione della conformità e di tutti i subcontraenti.

14. La remunerazione degli alti dirigenti e delle persone addette alle attività di valutazione della conformità non dipende dal numero di valutazioni della conformità eseguite o dai risultati di tali valutazioni.

15. Gli organismi di valutazione della conformità sottoscrivono un contratto di assicurazione per la responsabilità civile, a meno che detta responsabilità non sia direttamente coperta dallo Stato membro a norma del diritto nazionale o che lo Stato membro stesso non sia direttamente responsabile della valutazione della conformità.

16. L'organismo di valutazione della conformità e il personale, i comitati, le controllate e i subcontraenti dello stesso e qualsiasi organismo associato o membro del personale di organismi esterni di un organismo di valutazione della conformità sono tenuti al mantenimento della riservatezza e al segreto professionale per tutto ciò di cui vengono a conoscenza nell'esercizio dei loro compiti di valutazione della conformità ai sensi del presente regolamento o di qualsiasi disposizione di diritto interno di applicazione del presente regolamento, tranne laddove la divulgazione sia richiesta dal diritto dell'Unione o dello Stato membro cui tali persone sono soggette, e tranne per quanto riguarda le autorità competenti degli Stati membri in cui esercitano le loro attività. Sono tutelati i diritti di proprietà intellettuale. L'organismo di valutazione della conformità dispone di procedure documentate riguardo ai requisiti di cui al presente punto.

17. Con l'eccezione del punto 16, i requisiti del presente allegato non precludono in alcun modo gli scambi di informazioni tecniche e di orientamenti regolamentari tra un organismo di valutazione della conformità e una persona che richieda la certificazione o stia valutando se richiedere la certificazione.

18. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque e ragionevoli, tenendo conto degli interessi delle PMI in relazione alle tariffe.

19. Gli organismi di valutazione della conformità sono conformi ai requisiti della pertinente norma armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità che effettuano la certificazione dei prodotti TIC, servizi TIC o processi TIC.

20. Gli organismi di valutazione della conformità si assicurano che i laboratori di prova utilizzati ai fini della valutazione della conformità siano conformi ai requisiti della pertinente norma armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento dei laboratori che effettuano prove.

DIRETTIVE

DIRETTIVA (UE) 2019/882DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019

sui requisiti di accessibilità dei prodotti e dei servizi

(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 [1],

deliberando secondo la procedura legislativa ordinaria [2],

considerando quanto segue:

(1) La presente direttiva ha lo scopo di contribuire al corretto funzionamento del mercato interno mediante il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di requisiti di accessibilità per determinati prodotti e servizi, in particolare eliminando e prevenendo gli ostacoli alla libera circolazione di determinati prodotti e servizi accessibili derivanti dall'eterogeneità dei requisiti di accessibilità negli Stati membri. Ciò aumenterebbe la disponibilità di prodotti e servizi accessibili nel mercato interno e migliorerebbe l'accessibilità delle pertinenti informazioni.

(2) La domanda di prodotti e servizi accessibili è elevata e il numero di persone con disabilità dovrebbe, secondo le previsioni, aumentare in modo significativo. Un ambiente in cui i prodotti e i servizi sono più accessibili rende possibile una società più inclusiva e facilita la vita indipendente delle persone con disabilità. In tale contesto, si dovrebbe tenere conto del fatto che nell'Unione la disabilità è più diffusa tra le donne che tra gli uomini.

(3) La presente direttiva definisce le persone con disabilità in modo conforme alla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (UNCRPD), adottata il 13 dicembre 2006, di cui l'Unione è parte dal 21 gennaio 2011 e che tutti gli Stati membri hanno ratificato. L'UNCRPD annovera tra le persone con disabilità «quanti hanno minorazioni fisiche, mentali, intellettuali o sensoriali a lungo termine che in interazione con varie barriere possono impedire la loro piena ed effettiva partecipazione nella società su una base di eguaglianza con gli altri». La presente direttiva promuove la piena ed effettiva parità di partecipazione migliorando l'accesso ai prodotti e servizi generici che grazie alla loro progettazione iniziale o al loro successivo adattamento rispondono alle esigenze specifiche delle persone con disabilità.

(4) Beneficerebbero della presente direttiva anche altre persone con limitazioni funzionali, come le persone anziane, le donne in gravidanza e le persone che viaggiano con bagaglio. Il concetto di «persone con limitazioni funzionali» di cui alla presente direttiva comprende le persone con minorazioni fisiche, mentali, intellettive o sensoriali, con minorazioni connesse con l'età, o altre condizioni connesse alle prestazioni del corpo umano, permanenti o temporanee, che in interazione con varie barriere determinano un accesso limitato ai prodotti e servizi causando una situazione che richiede l'adeguamento di tali prodotti e servizi alle loro esigenze specifiche.

(5) Le disparità esistenti tra le disposizioni legislative, regolamentari e amministrative degli Stati membri riguardanti l'accessibilità dei prodotti e dei servizi per le persone con disabilità, creano ostacoli alla libera circolazione di prodotti e servizi e falsano la concorrenza effettiva nel mercato interno. Per taluni prodotti e servizi, tali disparità rischiano di aumentare nell'Unione dopo l'entrata in vigore dell'UNCRPD. Gli operatori economici, in particolare le piccole e medie imprese (PMI), risentono in modo particolare di tali ostacoli.

[1] GU C 303 del 19.8.2016, pag. 103.

[2] Posizione del Parlamento europeo del 13 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.

(6) Le differenze in materia di requisiti nazionali di accessibilità scoraggiano i singoli professionisti, le PMI e le microimprese in particolare dall'avviare iniziative imprenditoriali al di fuori del proprio mercato nazionale. Attualmente, i requisiti di accessibilità nazionali, o anche regionali o locali, predisposti dagli Stati membri differiscono per quanto riguarda sia la copertura sia il livello di dettaglio. Tali differenze incidono negativamente sulla competitività e sulla crescita a causa dei costi aggiuntivi sostenuti per lo sviluppo e la commercializzazione di prodotti e servizi accessibili per ciascun mercato nazionale.

(7) I consumatori di prodotti e servizi accessibili e di tecnologie assistive devono far fronte a prezzi elevati a causa della scarsa concorrenza tra i fornitori. La frammentazione tra le normative nazionali riduce i vantaggi derivanti dalla condivisione di esperienze con omologhi nazionali e internazionali potrebbe apportare in relazione agli sviluppi sociali e tecnologici.

(8) Il ravvicinamento delle misure nazionali a livello dell'Unione è pertanto necessario per il corretto funzionamento del mercato interno allo scopo di porre fine alla frammentazione del mercato dei prodotti e dei servizi accessibili, creare economie di scala, agevolare la mobilità e il commercio transfrontalieri e aiutare gli operatori economici a concentrare le risorse sull'innovazione anziché impiegarle per coprire le spese derivanti da una legislazione frammentaria all'interno dell'Unione.

(9) I vantaggi dell'armonizzazione dei requisiti di accessibilità per il mercato interno sono stati dimostrati dall'applicazione della direttiva 2014/33/UE del Parlamento europeo e del Consiglio ([3]) relativa agli ascensori del regolamento (CE) n. 661/2009 del Parlamento europeo e del Consiglio ([4]) riguardante il settore dei trasporti.

(10) Nella dichiarazione n. 22 sui portatori di handicap allegata al trattato di Amsterdam, la Conferenza dei rappresentanti degli Stati membri ha convenuto che, nell'elaborazione di misure a norma dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), le istituzioni dell'Unione debbano tenere conto delle esigenze dei portatori di handicap.

(11) L'obiettivo generale della Commissione del 6 maggio 2015 «Una strategia per il mercato unico digitale per l'Europa» è fornire i benefici economici e sociali sostenibili provenienti da un mercato unico digitale connesso, agevolando quindi il commercio e promuovendo l'occupazione nell'Unione. I consumatori dell'Unione non beneficiano ancora pienamente, in termini di prezzi e possibilità di scelta, dei vantaggi che il mercato unico può offrire, in quanto le operazioni transfrontaliere online sono ancora molto limitate. Anche la frammentazione limita la domanda di operazioni transfrontaliere di commercio elettronico. Occorre inoltre un intervento concordato per garantire che le persone con disabilità possano accedere integralmente ai contenuti elettronici, ai servizi di comunicazione elettronica e ai servizi di media audiovisivi. È pertanto necessario armonizzare i requisiti di accessibilità in tutto il mercato unico digitale e garantire che tutti i cittadini dell'Unione possano trarne beneficio, a prescindere dalle loro abilità.

(12) Da quando l'Unione è divenuta parte della UNCRPD, le disposizioni di tale convenzione sono divenute parte integrante dell'ordinamento giuridico dell'Unione e vincolano le istituzioni dell'Unione e gli Stati membri.

(13) La UNCRPD dispone che le parti adottino misure adeguate a garantire alle persone con disabilità, su base di uguaglianza con gli altri, l'accesso all'ambiente fisico, ai trasporti, all'informazione e alle comunicazioni, compresi i sistemi e le tecnologie di informazione e comunicazione, e ad altre attrezzature e servizi aperti o forniti al pubblico, sia nelle aree urbane che in quelle rurali. Il comitato delle Nazioni Unite sui diritti delle persone con disabilità ha riscontrato la necessità di creare un quadro legislativo con parametri concreti, applicabili e temporalmente definiti per monitorare la graduale attuazione dell'accessibilità.

(14) L'UNCRPD invita le parti a intraprendere o promuovere la ricerca e lo sviluppo, nonché a incoraggiare la messa a disposizione e l'uso di nuove tecnologie, tra cui tecnologie dell'informazione e della comunicazione, ausili alla mobilità, dispositivi e tecnologie di sostegno, adatte alle persone con disabilità. L'UNCRPD invita altresì a dare priorità alle tecnologie dai costi più accessibili.

([3]) Direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori (GU L 96 del 29.3.2014, pag. 251).

([4]) Regolamento (CE) n. 661/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, sui requisiti dell'omologazione per la sicurezza generale dei veicoli a motore, dei loro rimorchi e sistemi, componenti ed entità tecniche ad essi destinati (GU L 200 del 31.7.2009, pag. 1).

(15) L'entrata in vigore dell'UNCRPD nell'ordinamento giuridico degli Stati membri comporta la necessità di adottare disposizioni nazionali supplementari sull'accessibilità dei prodotti e dei servizi. In assenza di interventi da parte dell'Unione, tali disposizioni porterebbero a un ulteriore aumento delle disparità fra le disposizioni legislative, regolamentari ed amministrative degli Stati membri.

(16) È pertanto necessario agevolare l'attuazione dell'UNCRPD nell'Unione prevedendo regole comuni dell'Unione. La presente direttiva contribuisce altresì agli sforzi degli Stati membri volti a rispettare, in modo armonizzato, i rispettivi impegni nazionali e obblighi in materia di accessibilità derivanti dall'UNCRPD.

(17) La comunicazione della Commissione del 15 novembre 2010 «Strategia europea sulla disabilità 2010-2020: un rinnovato impegno per un'Europa senza barriere», in linea con l'UNCRPD e, individua l'accessibilità come uno degli otto ambiti d'azione, la definisce una condizione indispensabile per la partecipazione alla società e mira a garantire l'accessibilità dei prodotti e dei servizi.

(18) La determinazione dei prodotti e dei servizi che rientrano nell'ambito di applicazione della presente direttiva è basata su un'analisi eseguita durante la preparazione della valutazione d'impatto che ha individuato i prodotti e servizi pertinenti destinati alle persone con disabilità per i quali gli Stati membri hanno adottato o presumibilmente adotteranno requisiti di accessibilità nazionali divergenti che perturbano il funzionamento del mercato interno.

(19) Al fine di garantire l'accessibilità dei servizi che rientrano nell'ambito di applicazione della presente direttiva, anche i prodotti utilizzati per la prestazione di tali servizi con cui il consumatore interagisce dovrebbero rispettare i requisiti di accessibilità applicabili della presente direttiva.

(20) Anche se un servizio, o parte di esso, è subappaltato a terzi, non dovrebbe essere compromessa l'accessibilità a tale servizio e i fornitori di servizi dovrebbero rispettare gli obblighi della presente direttiva. I fornitori di servizi dovrebbero inoltre assicurare una formazione appropriata e continua del personale per garantire che esso disponga di una preparazione adeguata sull'utilizzo dei prodotti e dei servizi accessibili. Tale formazione dovrebbe riguardare questioni quali la trasmissione di informazioni, la consulenza e la pubblicità.

(21) Si dovrebbero introdurre requisiti di accessibilità nel modo meno oneroso possibile per gli operatori economici e gli Stati membri.

(22) È necessario specificare i requisiti di accessibilità per l'immissione sul mercato di prodotti e servizi che rientrano nell'ambito di applicazione della presente direttiva al fine di garantire la loro libera circolazione nel mercato interno.

(23) La presente direttiva dovrebbe rendere obbligatori i requisiti funzionali di accessibilità e questi dovrebbero essere stabiliti in termini di obiettivi generali. Tali requisiti dovrebbero essere sufficientemente precisi da creare obblighi giuridicamente vincolanti e sufficientemente dettagliati da consentire di valutare la conformità al fine di garantire il buon funzionamento del mercato interno per i prodotti e i servizi contemplati dalla presente direttiva, nonché lasciare un determinato margine di flessibilità per consentire l'innovazione.

(24) La presente direttiva contiene una serie di criteri funzionali di prestazione relativi alle modalità di funzionamento di prodotti e servizi. Tali criteri non sono intesi come un'alternativa generale ai requisiti di accessibilità stabiliti dalla presente direttiva, ma dovrebbero essere utilizzati soltanto in circostanze molto specifiche. I suddetti criteri dovrebbero essere applicati a funzioni o caratteristiche specifiche di tali prodotti o servizi, per renderli accessibili, quando i requisiti di accessibilità della presente direttiva non trattano una o più di tali funzioni o caratteristiche specifiche. In aggiunta, nel caso che un requisito di accessibilità contenga requisiti tecnici specifici, e nel prodotto o nel servizio sia fornita una soluzione tecnica alternativa a detti requisiti tecnici, tale soluzione tecnica alternativa dovrebbe essere comunque conforme ai pertinenti requisiti di accessibilità, e dovrebbe produrre un'accessibilità equivalente o maggiore, applicando i pertinenti criteri funzionali di prestazione.

(25) La presente direttiva dovrebbe applicarsi ai sistemi hardware informatici generici per consumatori. Affinché detti sistemi funzionino in maniera accessibile, anche i loro sistemi operativi dovrebbero essere accessibili. Tali sistemi hardware informatici sono caratterizzati dalla multifunzionalità e dalla capacità di eseguire, con il software adeguato, le operazioni informatiche più comuni richieste dai consumatori e sono destinati ad essere utilizzati dai consumatori. I personal computer, compresi i computer da tavolo (desktop), i notebook, gli smartphone e i tablet,

sono esempi di tali sistemi hardware informatici. I computer specializzati incorporati in prodotti elettronici di consumo non costituiscono sistemi hardware informatici generici per consumatori. La presente direttiva non dovrebbe applicarsi, su base individuale, ai singoli componenti con funzioni specifiche in quanto tali, come ad esempio una scheda madre o un chip di memoria, che sono usati o potrebbero essere usati in un tale sistema.

(26) La presente direttiva dovrebbe inoltre includere i terminali di pagamento, inclusi entrambe i loro hardware e software, e taluni terminali self-service interattivi comprendenti, inclusi entrambe i loro hardware e software, destinati a essere utilizzati per la fornitura di servizi contemplati dalla presente direttiva: ad esempio, gli sportelli automatici; le macchine per l'emissione di biglietti che garantiscono l'accesso a servizi, quali i distributori di titoli di trasporto e le macchine per l'emissione di biglietti per la gestione delle file negli uffici bancari; i terminali per il check-in; e i terminali self-service interattivi per la fornitura di informazioni, compresi gli schermi informativi interattivi.

(27) Tuttavia, alcuni terminali self-service interattivi per la fornitura di informazioni installati come parti integranti di veicoli, aeromobili, navi o materiale rotabile dovrebbero essere esclusi dall'ambito di applicazione della presente direttiva, in quanto fanno parte di tali veicoli, aeromobili, navi o materiale rotabile che non sono contemplati dalla presente direttiva.

(28) La presente direttiva dovrebbe inoltre applicarsi ai servizi di comunicazione elettronica, comprese le comunicazioni di emergenza, di cui alla direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio ([5]). Attualmente, le misure adottate dagli Stati membri per garantire l'accesso delle persone con disabilità divergono e non sono armonizzate in tutto il mercato interno. Garantire l'applicazione degli stessi requisiti di accessibilità in tutta l'Unione consentirà di realizzare economie di scala agli operatori economici attivi in più di uno Stato membro e agevolerà l'accesso efficace delle persone con disabilità sia nel loro Stato membro che quando viaggiano tra Stati membri. Affinché i servizi di comunicazione elettronica, comprese le comunicazioni di emergenza, siano accessibili, i fornitori dovrebbero fornire, in aggiunta alla comunicazione vocale, il testo in tempo reale e i servizi di conversazione globale qualora offrano un video, garantendo la sincronizzazione di tutti questi strumenti di comunicazione. Oltre ai requisiti della presente direttiva, gli Stati membri dovrebbero, conformemente alla direttiva (UE) 2018/1972, poter individuare un fornitore di servizi di ritrasmissione utilizzabile dalle persone con disabilità.

(29) La presente direttiva armonizza i requisiti di accessibilità per i servizi di comunicazione elettronica e i relativi prodotti e integra la direttiva (UE) 2018/1972, che stabilisce requisiti in materia di accesso e scelta equivalenti per gli utenti finali con disabilità. La direttiva (UE) 2018/1972 stabilisce anche, nell'ambito degli obblighi di servizio universale, requisiti in materia di accessibilità economica dei servizi di accesso a Internet e di comunicazione vocale, nonché di accessibilità economica e disponibilità delle relative apparecchiature terminali, attrezzature specifiche e servizi per i consumatori con disabilità.

(30) La presente direttiva dovrebbe altresì contemplare le apparecchiature terminali con capacità informatiche interattive per consumatori, prevedibilmente destinate ad essere utilizzate principalmente per accedere ai servizi di comunicazione elettronica. Ai fini della presente direttiva si dovrebbe ritenere che tali apparecchiature comprendano le apparecchiature utilizzate per l'accesso ai suddetti servizi di comunicazione elettronica come ad esempio un router o un modem.

(31) Ai fini della presente direttiva, accesso a servizi di media audiovisivi dovrebbe significare che i servizi che forniscono accesso ai contenuti audiovisivi devono essere accessibili, come pure i meccanismi che consentono agli utenti con disabilità di utilizzare le loro tecnologie assistive. I servizi che forniscono accesso a servizi di media audiovisivi potrebbero comprendere siti web, applicazioni online, applicazioni basate su set-top box e scaricabili, servizi per dispositivi mobili, comprese le applicazioni mobili, e relativi lettori multimediali, nonché servizi di televisione connessa. L'accessibilità dei servizi di media audiovisivi è disciplinata dalla direttiva 2010/13/UE del Parlamento europeo e del Consiglio ([6]), con l'eccezione dell'accessibilità alle guide elettroniche ai programmi (*electronic programme guides* — EPG) che sono comprese nella definizione di servizi che forniscono accesso a servizi di media audiovisivi a cui si applica la presente direttiva.

(32) Nell'ambito dei servizi di trasporto passeggeri aerei, su autobus, ferroviari e per vie navigabili, la presente direttiva dovrebbe tra l'altro disciplinare la fornitura di informazioni relative ai servizi di trasporto comprese le informazioni di viaggio in tempo reale tramite siti web, servizi per dispositivi mobili, schermi informativi interattivi e terminali

([5]) 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).

([6]) Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (GU L 95 del 15.4.2010, pag. 1).

self-service
interattivi di cui i passeggeri con disabilità hanno bisogno per viaggiare. Ciò potrebbe includere le informazioni sui prodotti e servizi di trasporto passeggeri offerti dal fornitore di servizi, le informazioni prima del viaggio, le informazioni durante il viaggio e le informazioni fornite quando un servizio subisce una cancellazione o un ritardo alla partenza. Altri elementi d'informazione potrebbero comprendere, ad esempio, informazioni su prezzi e promozioni.

(33) La presente direttiva dovrebbe disciplinare anche i siti web, i servizi per dispositivi mobili, comprese le applicazioni mobili sviluppate o messe a disposizione da operatori di servizi di trasporto passeggeri rientranti nell'ambito di applicazione della presente direttiva o a loro nome, i servizi di biglietteria elettronica, i biglietti elettronici e i terminali self-service interattivi.

(34) La definizione dell'ambito di applicazione della presente direttiva per quanto riguarda i servizi di trasporto passeggeri aerei, con autobus, ferroviari e per vie navigabili dovrebbe basarsi sulla legislazione settoriale in vigore in materia di diritti dei passeggeri. Qualora la presente direttiva non si applichi a determinati tipi di servizi di trasporto, gli Stati membri dovrebbero incoraggiare i fornitori di servizi ad applicare i requisiti di accessibilità pertinenti della presente direttiva.

(35) La direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio ([7]) prevede già l'obbligo, per gli enti pubblici che forniscono servizi di trasporto, compresi i servizi di trasporto urbani e extraurbani e dei servizi di trasporto regionale, di rendere accessibili i loro siti web. La presente direttiva prevede esenzioni per le microimprese che forniscono servizi, compresi i servizi di trasporto urbani e extraurbani e dei servizi di trasporto regionale. Inoltre, presente direttiva prevede obblighi finalizzati ad assicurare che i siti web di commercio elettronico siano accessibili. Poiché la presente direttiva reca obblighi per la grande maggioranza dei fornitori di servizi di trasporto privati a rendere accessibili i loro siti web, per quanto riguarda la vendita online dei biglietti, non è necessario introdurre nella presente direttiva ulteriori requisiti per i siti web dei fornitori di servizi di trasporto urbani e extraurbani e dei fornitori di servizi di trasporto regionali.

(36) Alcuni elementi dei requisiti di accessibilità, in particolare in relazione alla fornitura di informazioni di cui alla presente direttiva, sono già disciplinati dal diritto dell'Unione in vigore nel settore del trasporto passeggeri. Si tratta di elementi del regolamento (CE) n. 261/2004 del Parlamento europeo e del Consiglio ([8]), del regolamento (CE) n. 1107/2006 del Parlamento europeo e del Consiglio ([9]), del regolamento (CE) n. 1371/2007 del Parlamento europeo e del Consiglio ([10]), del regolamento (UE) n. 1177/2010 del Parlamento europeo e del Consiglio ([11]), e del regolamento (UE) n. 181/2011 del Parlamento europeo e del Consiglio ([12]). Si tratta inoltre degli atti pertinenti adottati sulla base della direttiva 2008/57/CE del Parlamento europeo e del Consiglio ([13]). Per ragioni di coerenza normativa, i requisiti di accessibilità fissati dai tali regolamenti e atti dovrebbero continuare ad applicarsi come prima. Tuttavia, i requisiti supplementari della presente direttiva dovrebbero integrare i requisiti esistenti, migliorando il funzionamento del mercato interno nel settore dei trasporti e recando beneficio alle persone con disabilità.

(37) Alcuni elementi dei servizi di trasporto non dovrebbero rientrare nell'ambito di applicazione della presente direttiva se prestati al di fuori del territorio degli Stati membri, anche se il servizio è destinato al mercato dell'Unione. Per quanto riguarda tali elementi, un operatore di servizi di trasporto passeggeri dovrebbe essere tenuto a garantire la conformità ai requisiti previsti presente direttiva soltanto per la parte del servizio fornita all'interno del territorio dell'Unione. Tuttavia, per quanto riguarda il trasporto aereo, i vettori aerei dell'Unione dovrebbero essere tenuti ad assicurare che i requisiti applicabili di cui alla presente direttiva siano soddisfatti anche nel caso di voli in partenza

([7]) Direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici (GU L 327 del 2.12.2016, pag. 1).
([8]) Regolamento (CE) n. 261/2004 del Parlamento europeo e del Consiglio, dell'11 febbraio 2004, che istituisce regole comuni in materia di compensazione ed assistenza ai passeggeri in caso di negato imbarco, di cancellazione del volo o di ritardo prolungato e che abroga il regolamento (CEE) n. 295/91 (GU L 46 del 17.2.2004, pag. 1).
([9]) Regolamento (CE) n. 1107/2006 del Parlamento europeo e del Consiglio, del 5 luglio 2006, relativo ai diritti delle persone con disabilità e delle persone a mobilità ridotta nel trasporto aereo (GU L 204 del 26.7.2006, pag. 1).
([10]) Regolamento (CE) n. 1371/2007 del Parlamento europeo e del Consiglio, del 23 ottobre 2007, relativo ai diritti e agli obblighi dei passeggeri nel trasporto ferroviario (GU L 315 del 3.12.2007, pag. 14).
([11]) Regolamento (UE) n. 1177/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, relativo ai diritti dei passeggeri che viaggiano via mare e per vie navigabili interne e che modifica il regolamento (CE) n. 2006/2004 (GU L 334 del 17.12.2010, pag. 1).
([12]) Regolamento (UE) n. 181/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, relativo ai diritti dei passeggeri nel trasporto effettuato con autobus e che modifica il regolamento (CE) n. 2006/2004 (GU L 55 del 28.2.2011, pag. 1).
([13]) Direttiva 2008/57/CE del Parlamento europeo e del Consiglio, del 17 giugno 2008, relativa all'interoperabilità del sistema ferroviario comunitario (GU L 191 del 18.7.2008, pag. 1).

da un aeroporto situato in un paese terzo e diretti verso un aeroporto situato nel territorio di uno Stato membro. Inoltre, tutti i vettori aerei, compresi quelli che non sono titolari di una licenza rilasciata nell'Unione, dovrebbero essere tenuti ad assicurare che i requisiti applicabili previsti dalla presente direttiva siano soddisfatti nel caso di voli in partenza dal territorio dell'Unione e diretti verso il territorio di un paese terzo.

(38) Le autorità urbane dovrebbero essere incoraggiate a integrare l'accessibilità senza barriere nei servizi di trasporto urbano nei loro piani di mobilità urbana sostenibile e a pubblicare regolarmente un elenco delle migliori pratiche in materia di accessibilità senza barriere ai trasporti pubblici urbani e alla mobilità.

(39) Il diritto dell'Unione in materia di servizi bancari e finanziari mira a proteggere e a informare i consumatori di tali servizi in tutta l'Unione ma non include requisiti di accessibilità. Al fine di consentire alle persone con disabilità di utilizzare tali servizi in tutta l'Unione, anche quando sono forniti mediante siti web e servizi per dispositivi mobili, incluse le applicazioni mobili, di prendere decisioni in piena cognizione di causa e sentirsi sicuri di essere protetti adeguatamente su una base di uguaglianza con gli altri consumatori, nonché al fine di garantire condizioni di parità per i fornitori di servizi, la presente direttiva dovrebbe stabilire requisiti di accessibilità comuni per alcuni servizi bancari e finanziari forniti ai consumatori.

(40) I requisiti di accessibilità adeguati dovrebbero inoltre applicarsi ai metodi di identificazione, alla firma elettronica e ai servizi di pagamento poiché essi sono necessari per concludere transazioni nell'ambito dei servizi bancari per consumatori.

(41) I file di libri elettronici sono basati su una codificazione elettronica che consente la circolazione e la consultazione di opere dell'ingegno prevalentemente di tipo grafico e testuale. Il grado di precisione di tale codificazione determina l'accessibilità dei file di libri elettronici, in particolare per quanto riguarda la qualificazione dei diversi elementi costitutivi delle opere e la descrizione standardizzata della loro struttura. L'interoperabilità in termini di accessibilità dovrebbe ottimizzare la compatibilità di tali file con i programmi utenti e le tecnologie assistive attuali e future. Le caratteristiche specifiche di volumi speciali come i fumetti, i libri per bambini e i libri d'arte dovrebbero essere prese in considerazione alla luce di a tutti i requisiti di accessibilità applicabili. L'esistenza di requisiti di accessibilità divergenti negli Stati membri renderebbe difficile per gli editori e gli altri operatori economici beneficiare dei vantaggi del mercato interno, potrebbe creare problemi d'interoperabilità con i lettori di libri elettronici (e-reader) e limiterebbe l'accesso per i consumatori con disabilità. Nel contesto dei libri elettronici, il concetto di fornitore di servizi potrebbe includere gli editori e gli altri operatori economici coinvolti nella distribuzione.

È riconosciuto che le persone con disabilità continuano a incontrare ostacoli nell'accesso ai contenuti protetti da diritti d'autore e diritti connessi e che talune misure sono già state adottate per affrontare tale situazione ad esempio mediante l'adozione della direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio ([14]) e il regolamento (UE) 2017/1563 del Parlamento europeo e del Consiglio ([15]), e che in futuro potrebbero essere adottate a tale riguardo ulteriori misure dell'Unione.

(42) La presente direttiva definisce i servizi di commercio elettronico come servizi forniti a distanza, tramite siti web e applicazioni mobili, per via elettronica e su richiesta individuale di un consumatore, al fine di concludere un contratto di consumo. Ai fini di tale definizione per «a distanza» si intende che il servizio è fornito senza la presenza simultanea delle parti; per «per via elettronica» si intende un servizio inviato all'origine e ricevuto a destinazione mediante mezzi elettronici di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è trasmesso, inoltrato e ricevuto in tutti i suoi elementi via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici; per «su richiesta individuale di un consumatore» si intende che il servizio è fornito su richiesta individuale. Data la crescente importanza dei servizi di commercio elettronico e il loro carattere altamente tecnologico, è importante disporre di requisiti di accessibilità armonizzati.

([14]) Direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio, del 13 settembre 2017, relativa a taluni utilizzi consentiti di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa, e che modifica la direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (GU L 242 del 20.9.2017, pag. 6).

([15]) Regolamento (UE) 2017/1563 del Parlamento europeo e del Consiglio, del 13 settembre 2017, relativo allo scambio transfrontaliero tra l'Unione e i paesi terzi di copie in formato accessibile di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa (GU L 242 del 20.9.2017, pag. 1).

(43) Gli obblighi di accessibilità relativi a servizi di commercio elettronico della presente direttiva dovrebbero applicarsi alla vendita online di qualsiasi prodotto o servizio, e dovrebbero pertanto applicarsi anche alla vendita di prodotti o servizi contemplati in quanto tali dalla presente direttiva.

(44) Le misure relative all'accessibilità della raccolta delle comunicazioni di emergenza dovrebbero essere adottate senza pregiudicare né incidere in alcun modo sull'organizzazione dei servizi di emergenza, che resta di esclusiva competenza degli Stati membri.

(45) Conformemente alla direttiva (UE) 2018/1972, gli Stati membri devono provvedere affinché gli utenti finali con disabilità abbiano accesso ai servizi di emergenza mediante le comunicazioni di emergenza e in modo equivalente a quelli utilizzati dagli altri utenti finali in conformità del diritto dell'Unione che armonizza i requisiti di accessibilità dei prodotti e dei servizi. La Commissione e le autorità nazionali di regolamentazione o le altre autorità competenti devono adottare misure adeguate per assicurare che gli utenti finali con disabilità, mentre viaggiano in altri Stati membri, possano accedere ai servizi di emergenza su un piano di parità con gli altri utenti finali ove possibile senza alcuna preregistrazione. Tali misure mirano a garantire l'interoperabilità tra gli Stati membri devono basarsi quanto più possibile sulle norme o specifiche europee stabilite conformemente alle disposizioni dell'articolo 39 della direttiva (UE) 2018/1972. Tali misure non impediscono agli Stati membri di adottare ulteriori requisiti al fine di perseguire gli obiettivi di cui a tale direttiva. In alternativa al rispetto dei requisiti di accessibilità stabiliti dalla presente direttiva per quanto riguarda la raccolta delle comunicazioni di emergenza per gli utenti con disabilità, gli Stati membri dovrebbero poter individuare un fornitore terzo di servizi di ritrasmissione utilizzabile dalle persone con disabilità per comunicare con il centro di raccolta delle chiamate di emergenza, fino a che tali centri siano in grado di utilizzare i servizi di comunicazione elettronica tramite protocolli Internet per garantire l'accessibilità della raccolta delle comunicazioni di emergenza. In ogni caso, gli obblighi della presente direttiva non dovrebbero essere intesi nel senso di limitare o ridurre alcun obbligo a beneficio degli utenti finali con disabilità, compreso l'accesso equivalente ai servizi di comunicazione elettronica e ai servizi di emergenza così come gli obblighi di accessibilità di cui alla direttiva (UE) 2018/1972.

(46) La direttiva (UE) 2016/2102 definisce i requisiti di accessibilità per i siti web e le applicazioni mobili degli enti pubblici, nonché altri aspetti correlati, in particolare i requisiti riguardanti la conformità dei siti web e delle applicazioni mobili interessati. Tuttavia, detta direttiva prevede un elenco specifico di eccezioni. Eccezioni analoghe riguardano la presente direttiva. Alcune attività che hanno luogo attraverso i siti web e le applicazioni mobili degli enti del settore pubblico, come i servizi di trasporto passeggeri o i servizi di commercio elettronico, che rientrano nell'ambito di applicazione della presente direttiva, dovrebbero inoltre essere conformi ai requisiti di accessibilità applicabili della presente direttiva al fine di garantire che la vendita online di prodotti e servizi sia accessibile alle persone con disabilità, a prescindere dal fatto che il venditore sia un operatore economico pubblico o privato. I requisiti di accessibilità della presente direttiva dovrebbero essere allineati ai requisiti della direttiva (UE) 2016/2102, nonostante le differenze, ad esempio, nel monitoraggio, nelle relazioni e nell'attuazione.

(47) I quattro principi dell'accessibilità dei siti web e delle applicazioni mobili, quali utilizzati nella direttiva (UE) 2016/2102, sono: percepibilità, nel senso che le informazioni e i componenti dell'interfaccia utente devono essere presentabili agli utenti in modalità percepibili; utilizzabilità, nel senso che i componenti e la navigazione dell'interfaccia utente devono essere utilizzabili; comprensibilità, nel senso che le informazioni e il funzionamento dell'interfaccia utente devono essere comprensibili; e solidità, nel senso che i contenuti devono essere abbastanza solidi da poter essere interpretati con sicurezza da una vasta gamma di programmi utente, comprese le tecnologie assistive. Detti principi sono altresì rilevanti per la presente direttiva.

(48) Gli Stati membri dovrebbero adottare tutte le misure adeguate a garantire che, laddove i prodotti e i servizi disciplinati dalla presente direttiva siano conformi ai requisiti di accessibilità applicabili, la loro libera circolazione nell'Unione non sia impedita per motivi relativi ai requisiti di accessibilità.

(49) In alcune situazioni, requisiti comuni di accessibilità dell'ambiente costruito agevolerebbero la libera circolazione dei servizi connessi e delle persone con disabilità. La presente direttiva dovrebbe consentire pertanto agli Stati membri di includere l'ambiente costruito utilizzato per fornire i servizi nell'ambito di applicazione della presente direttiva, in modo da garantire la conformità ai requisiti di accessibilità di cui all'allegato III.

(50) L'accessibilità dovrebbe essere conseguita mediante la soppressione e la prevenzione sistematiche delle barriere, preferibilmente attraverso il principio della progettazione universale o della «progettazione per tutti», che contribuisce a garantire alle persone con disabilità un accesso su base di uguaglianza con gli altri. Secondo l'UNCRPD, con tale approccio si intende la progettazione di prodotti, ambienti, programmi e servizi utilizzabili da tutte le persone, nella misura più estesa possibile, senza il bisogno di adattamenti o di progettazioni specializzate. In linea con l'UNCRPD, la «progettazione universale» non esclude i dispositivi assistivi per particolari gruppi di persone con disabilità, qualora ve ne sia l'esigenza». Inoltre, l'accessibilità non dovrebbe escludere l'applicazione di soluzioni

appropriate se richiesto dal diritto nazionale o dell'Unione. I concetti di accessibilità e di progettazione universale dovrebbero essere interpretati in linea con l'osservazione generale n. 2(2014) - articolo 9: Accessibilità, quale redatta dal Comitato sui diritti delle persone con disabilità.

(51) I prodotti e i servizi rientranti nell'ambito di applicazione della presente direttiva non rientrano automaticamente nell'ambito di applicazione della direttiva 93/42/CEE del Consiglio ([16]). Tuttavia, alcune tecnologie assistive che sono dispositivi medici potrebbero rientrare nell'ambito di applicazione di tale direttiva.

(52) Le PMI e le microimprese forniscono lavoro alla maggioranza degli occupati nell'Unione. Esse sono di fondamentale importanza per la crescita futura, ma molto spesso si trovano di fronte a difficoltà e ostacoli nello sviluppo dei loro prodotti o servizi, in particolare nel contesto transfrontaliero. È quindi necessario facilitare il lavoro delle PMI e delle microimprese armonizzando le disposizioni nazionali in materia di accessibilità e mantenendo nel contempo le garanzie necessarie.

(53) Affinché possano beneficiare della presente direttiva, le microimprese e le PMI devono realmente soddisfare i requisiti della raccomandazione 2003/361/CE della Commissione ([17]), e della giurisprudenza pertinente, volti a prevenire l'elusione delle sue norme.

(54) Al fine di garantire la coerenza della legislazione dell'Unione, la presente direttiva dovrebbe basarsi sulla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio ([18]) in quanto riguarda prodotti già oggetto di altri atti dell'Unione, pur riconoscendo le caratteristiche specifiche dei requisiti di accessibilità della presente direttiva.

(55) Tutti gli operatori economici che rientrano nell'ambito di applicazione della presente direttiva e che intervengono nella catena di fornitura e distribuzione dovrebbero garantire che siano messi a disposizione sul mercato solo prodotti conformi alla presente direttiva. Lo stesso dovrebbe applicarsi agli operatori economici che forniscono servizi. È necessario ripartire in modo chiaro e proporzionato gli obblighi corrispondenti al ruolo di ciascun operatore economico nel processo di fornitura e distribuzione.

(56) Gli operatori economici dovrebbero essere responsabili della conformità dei prodotti e dei servizi in relazione al ruolo che rivestono nella catena di fornitura, in modo da garantire un elevato livello di protezione dell'accessibilità e una concorrenza leale sul mercato dell'Unione.

(57) Gli obblighi della presente direttiva dovrebbero applicarsi indistintamente agli operatori economici del settore pubblico e del settore privato.

(58) Il fabbricante, che possiede conoscenze dettagliate del processo di progettazione e di produzione, è nella posizione migliore per eseguire la valutazione completa della conformità. Se la responsabilità della conformità dei prodotti incombe al fabbricante, le autorità di vigilanza del mercato dovrebbero svolgere un ruolo essenziale nel verificare se i prodotti messi a disposizione nell'Unione sono fabbricati in conformità del diritto dell'Unione.

(59) Gli importatori e i distributori dovrebbero essere coinvolti nei compiti di vigilanza del mercato eseguiti dalle autorità nazionali e parteciparvi attivamente, fornendo alle autorità competenti tutte le informazioni necessarie sul prodotto in questione.

(60) Gli importatori dovrebbero garantire che i prodotti originari di paesi terzi che entrano nel mercato dell'Unione siano conformi alla presente direttiva, e in particolare che i fabbricanti abbiano effettuato adeguate procedure di valutazione della conformità di tali prodotti.

(61) All'atto dell'immissione di un prodotto sul mercato, gli importatori dovrebbero indicare sul prodotto il loro nome, la loro denominazione commerciale registrata o il loro marchio d'impresa, e l'indirizzo al quale possono essere contattati.

([16]) Direttiva 93/42/CEE del Consiglio, del 14 giugno 1993, concernente i dispositivi medici (GU L 169 del 12.7.1993, pag. 1).
([17]) 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).
([18]) Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

(62) I distributori dovrebbero garantire che la manipolazione del prodotto non incida negativamente sulla sua conformità ai requisiti di accessibilità della presente direttiva.

(63) Qualsiasi operatore economico che immetta sul mercato un prodotto con il proprio nome o marchio d'impresa oppure modifichi un prodotto già immesso sul mercato in modo che possa incidere sulla conformità ai requisiti applicabili, dovrebbe esserne considerato il fabbricante e assumere quindi i relativi obblighi.

(64) Per motivi di proporzionalità, i requisiti di accessibilità dovrebbero applicarsi soltanto nella misura in cui non impongano un onere sproporzionato agli operatori economici interessati o nella misura in cui non richiedano un cambiamento significativo dei prodotti e servizi che comporterebbe una loro modifica sostanziale alla luce della presente direttiva. Dovrebbero tuttavia essere istituiti meccanismi di controllo per verificare la legittimità delle deroghe all'applicabilità dei requisiti di accessibilità.

(65) La presente direttiva dovrebbe seguire il principio «pensare anzitutto in piccolo» e tenere conto degli oneri amministrativi che le PMI si trovano ad affrontare. Essa dovrebbe fissare norme poco gravose in termini di valutazione della conformità e stabilire clausole di salvaguardia per gli operatori economici, anziché prevedere eccezioni e deroghe generali per tali imprese. Di conseguenza, al momento di stabilire le regole per la selezione e l'attuazione delle procedure di valutazione della conformità più appropriate, bisognerebbe prendere in considerazione la situazione delle PMI e limitare gli obblighi di valutazione della conformità ai requisiti di accessibilità in modo che non impongano un onere sproporzionato per le PMI. Le autorità di vigilanza del mercato dovrebbero inoltre operare in modo proporzionato rispetto alle dimensioni delle imprese e alla limitata natura seriale o non seriale della produzione in questione, senza creare inutili ostacoli alle piccole e medie imprese e senza compromettere la protezione dell'interesse pubblico.

(66) In casi eccezionali, in cui l'osservanza dei requisiti di accessibilità della presente direttiva impongano un onere sproporzionato per gli operatori economici, questi ultimi dovrebbero essere tenuti a conformarvisi soltanto nella misura in cui non impongano un onere sproporzionato. In tali casi debitamente giustificati, non sarebbe ragionevolmente possibile per un operatore economico applicare pienamente uno o più dei requisiti di accessibilità della presente direttiva. Tuttavia, l'operatore economico dovrebbe rendere quanto più possibile accessibile un servizio o un prodotto rientrante nell'ambito di applicazione della presente direttiva applicando tali requisiti nella misura in cui non impongano un onere sproporzionato. I requisiti di accessibilità che l'operatore economico non ha ritenuto che impongano un onere sproporzionato dovrebbero applicarsi pienamente. Le eccezioni alla conformità a uno o più requisiti di accessibilità dovute all'onere sproporzionato che gli stessi impongono non dovrebbero andare oltre lo stretto necessario, al fine di limitare detto onere per quanto riguarda il particolare prodotto o servizio interessato in ogni singolo caso. Per misure che imporrebbero un onere sproporzionato si dovrebbero intendere le misure che imporrebbero all'operatore economico un onere aggiuntivo eccessivo sotto il profilo organizzativo o finanziario, pur tenendo conto del probabile beneficio che ne deriverebbe per le persone con disabilità in linea con i criteri stabiliti nella presente direttiva. Sulla base di queste considerazioni dovrebbero essere definiti criteri al fine di consentire sia agli operatori economici che alle autorità pertinenti di confrontare le varie situazioni e di valutare l'eventuale esistenza di un onere sproporzionato in modo sistematico. Nel valutare in quale misura i requisiti di accessibilità non possano essere soddisfatti a causa dell'onere sproporzionato che imporrebbero, si dovrebbe tener conto soltanto di motivi legittimi. La mancanza di carattere prioritario, di tempo o di conoscenze non dovrebbe essere considerata un motivo legittimo.

(67) La valutazione globale del carattere sproporzionato dell'onere dovrebbe essere effettuata avvalendosi dei criteri di cui all'allegato VI. Essa dovrebbe essere documentata dall'operatore economico tenendo conto dei pertinenti criteri. I fornitori di servizi dovrebbero riesaminare la valutazione del carattere sproporzionato dell'onere almeno ogni cinque anni.

(68) L'operatore economico dovrebbe informare le autorità pertinenti che sono state invocate le disposizioni della presente direttiva relative alla modifica sostanziale e/o all'onere sproporzionato. Solo su richiesta delle autorità pertinenti l'operatore economico dovrebbe fornire una copia della valutazione in cui spiega perché il suo prodotto o servizio non è pienamente accessibile, adducendo la prova del carattere sproporzionato dell'onere o della modifica sostanziale, o di entrambe.

(69) Se, sulla base della valutazione prescritta, un fornitore di servizi conclude che l'obbligo di assicurare che, tutti i terminali self-service utilizzati per la prestazione dei servizi contemplati dalla presente direttiva siano conformi ai requisiti di accessibilità della presente direttiva, costituirebbe un onere sproporzionato, il fornitore di servizi dovrebbe comunque applicare tali requisiti nella misura in cui non gli impongono un onere sproporzionato. Di conseguenza, i fornitori di servizi dovrebbero valutare la misura in cui un livello minimo di accessibilità di tutti i terminali self-service o un numero limitato di terminali self-service pienamente accessibili permetterebbe loro di evitare che un onere sproporzionato sia loro imposto, e dovrebbe essere loro richiesto di soddisfare i requisiti di accessibilità della presente direttiva solo in tale misura.

(70) Le microimprese si distinguono da tutte le altre imprese per il fatto di disporre di risorse umane, fatturato annuo o bilancio annuo limitati. Per le microimprese, pertanto, l'onere di soddisfare i requisiti di accessibilità assorbe in generale una quota maggiore delle loro risorse umane e finanziarie rispetto alle altre imprese ed è più probabile che rappresenti una quota sproporzionata dei costi. Una percentuale significativa dei costi sostenuti dalle microimprese deriva dalla compilazione e dall'archiviazione di documenti e registri per dimostrare la propria conformità ai vari requisiti previsti dal diritto dell'Unione. Mentre tutti gli operatori economici contemplati dalla presente direttiva dovrebbero essere in grado di valutare la proporzionalità del rispetto dei requisiti di accessibilità della presente direttiva e dovrebbero conformarsi ad essi solo nella misura in cui non siano sproporzionati, imporre alle microimprese che forniscono servizi di procedere a una siffatta valutazione costituirebbe, di per sé, un onere sproporzionato. I requisiti e gli obblighi della presente direttiva non dovrebbero pertanto applicarsi alle microimprese che forniscono servizi rientranti nell'ambito di applicazione della presente direttiva.

(71) Al fine di ridurre l'imposizione di oneri amministrativi sproporzionati, è opportuno che la presente direttiva preveda requisiti e obblighi meno rigorosi per le microimprese che trattano prodotti che rientrano nell'ambito di applicazione della presente direttiva.

(72) Se alcune microimprese sono esenti dagli obblighi della presente direttiva, tutte le microimprese dovrebbero essere incoraggiate a fabbricare, importare o distribuire prodotti e a fornire servizi conformi ai requisiti di accessibilità della presente direttiva al fine di rafforzare la loro competitività e potenziale di crescita nel mercato interno. Gli Stati membri dovrebbero pertanto fornire alle microimprese orientamenti e strumenti per facilitare l'applicazione delle misure nazionali di recepimento della presente direttiva.

(73) Tutti gli operatori economici, all'atto di immettere o di mettere a disposizione sul mercato prodotti o di fornire servizi sul mercato, dovrebbero agire in modo responsabile e in piena conformità alle prescrizioni giuridiche applicabili.

74) Per facilitare la valutazione della conformità ai requisiti di accessibilità applicabili è necessario introdurre una presunzione di conformità per i prodotti e i servizi conformi alle norme armonizzate volontarie adottate ai sensi del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([19]) al fine di formulare specifiche tecniche dettagliate di tali requisiti. La Commissione ha già formulato alle organizzazioni europee di normazione una serie di richieste di normazione in materia di accessibilità, quali i mandati di normazione M/376, M/473 e M/420, che sarebbero rilevanti per la preparazione delle norme armonizzate.

(75) Il regolamento (UE) n. 1025/2012 prevede una procedura relativa alle obiezioni formali alle norme armonizzate che non sono ritenute conformi ai requisiti della presente direttiva.

(76) Le norme europee dovrebbero essere orientate al mercato, tenere conto dell'interesse pubblico nonché degli obiettivi strategici chiaramente formulati nella richiesta rivolta dalla Commissione a una o più organizzazioni europee di normazione di elaborare norme armonizzate, e dovrebbero basarsi su un consenso. In mancanza di norme armonizzate e ove necessario ai fini dell'armonizzazione del mercato interno, la Commissione dovrebbe essere in grado di adottare, in determinati casi, atti di esecuzione che stabiliscano specifiche tecniche comuni per i requisiti di accessibilità della presente direttiva. Il ricorso alle specifiche tecniche dovrebbe essere limitato a tali casi. La Commissione dovrebbe poter adottare specifiche tecniche, ad esempio, quando il processo di normazione è bloccato a causa della mancanza di consenso tra le parti interessate o tale situazione crea ritardi ingiustificati nella definizione di una norma armonizzata, ad esempio perché la qualità richiesta non è raggiunta. La Commissione dovrebbe lasciare tempo sufficiente tra l'adozione di una richiesta a una o più organizzazioni europee di normazione di elaborare norme armonizzate e l'adozione di una specifica tecnica relativa allo stesso requisito di accessibilità. La Commissione non dovrebbe poter adottare una specifica tecnica senza avere precedentemente tentato di garantire la copertura dei requisiti di accessibilità da parte del sistema europeo di normazione, tranne nel caso in cui la Commissione possa dimostrare che le specifiche tecniche rispettano i requisiti di cui all'allegato II del regolamento (UE) n. 1025/2012.

(77) Nell'ottica di istituire nel modo più efficace possibile norme armonizzate e specifiche tecniche che rispettino i requisiti di accessibilità per i prodotti e i servizi della presente direttiva, la Commissione dovrebbe, ove possibile, coinvolgere nel processo le organizzazioni europee di coordinamento che rappresentano le persone con disabilità e tutte le altre parti interessate.

([19]) 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).

(78) Per garantire un accesso efficace alle informazioni a fini di vigilanza del mercato, le informazioni necessarie per dichiarare la conformità a tutti gli atti dell'Unione applicabili dovrebbero essere rese disponibili in un'unica dichiarazione UE di conformità. Al fine di ridurre gli oneri amministrativi a carico degli operatori economici, essi dovrebbero poter includere in tale unica dichiarazione UE di conformità tutte le singole dichiarazioni di conformità pertinenti.

(79) Per la valutazione della conformità dei prodotti, la presente direttiva dovrebbe utilizzare il controllo interno della produzione del «Modulo A», descritto nell'allegato II della decisione n. 768/2008/CE, in quanto consente agli operatori economici di dimostrare e alle autorità competenti di garantire che i prodotti messi a disposizione sul mercato sono conformi ai requisiti di accessibilità senza imporre un onere indebito.

(80) Nell'effettuare la sorveglianza del mercato dei prodotti e nel verificare la conformità dei servizi, le autorità dovrebbero altresì verificare se le valutazioni di conformità, compresa se del caso la valutazione di un'alterazione essenziale o dell'onere sproporzionato, siano state correttamente effettuate. Le autorità dovrebbero adempiere ai loro obblighi in cooperazione con le persone con disabilità e con le organizzazioni che le rappresentano e che rappresentano i loro interessi.

(81) Per i servizi, le informazioni necessarie a valutare la conformità ai requisiti di accessibilità della presente direttiva dovrebbero essere fornite nelle condizioni generali o in un documento equivalente, fatta salva la direttiva 2011/83/UE del Parlamento europeo e del Consiglio ([20]).

(82) La marcatura CE, che indica la conformità di un prodotto ai requisiti di accessibilità della presente direttiva, è la conseguenza visibile di un processo complessivo che comprende la valutazione della conformità in senso lato. La presente direttiva dovrebbe seguire i principi generali che disciplinano la marcatura CE del regolamento (CE) n. 765/2008, del Parlamento europeo e del Consiglio ([21]), che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti. Oltre a rendere la dichiarazione di conformità UE, il fabbricante dovrebbe informare i consumatori, in modo efficace sotto il profilo dei costi, sull'accessibilità dei prodotti.

(83) In conformità del regolamento (CE) n. 765/2008, apponendo la marcatura CE sul prodotto il fabbricante dichiara la conformità del prodotto a tutti i requisiti di accessibilità applicabili e se ne assume la piena responsabilità.

(84) In conformità della decisione n. 768/2008/CE, gli Stati membri hanno la responsabilità di garantire, per i prodotti, una vigilanza forte ed efficiente del mercato sul proprio territorio e dovrebbero conferire poteri e risorse sufficienti alle proprie autorità di vigilanza del mercato.

(85) Gli Stati membri dovrebbero verificare la conformità dei servizi agli obblighi della presente direttiva e dare seguito ai reclami o alle relazioni concernenti casi di non conformità al fine di garantire che siano state adottate misure correttive.

(86) La Commissione potrebbe, se del caso, adottare, in consultazione con le parti interessate, orientamenti non vincolanti volti a sostenere il coordinamento tra le autorità di vigilanza del mercato e le autorità responsabili del controllo della conformità dei servizi. La Commissione e gli Stati membri dovrebbero poter avviare iniziative allo scopo di condividere risorse e conoscenze delle autorità.

(87) Gli Stati membri dovrebbero essere tenuti a provvedere affinché le autorità di vigilanza del mercato e le autorità responsabili della conformità dei servizi verifichino la conformità degli operatori economici ai criteri di cui all'allegato VI, in conformità dei capi VIII e IX. Gli Stati membri dovrebbero poter designare un organismo specializzato per adempiere agli obblighi delle autorità di vigilanza del mercato o delle autorità responsabili della conformità dei servizi previsti dalla presente direttiva. Gli Stati membri dovrebbero poter decidere che le competenze di tale organismo specializzato debbano essere limitate all'ambito di applicazione della presente direttiva o ad alcune sue parti, fatti salvi gli obblighi degli Stati membri a norma del regolamento (CE) n. 765/2008.

([20]) Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio (GU L 304 del 22.11.2011, pag. 64).

([21]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

(88) È opportuno istituire una procedura di salvaguardia da applicare in caso di disaccordo tra Stati membri sulle misure adottate da uno Stato membro, in base alla quale le parti interessate siano informate delle misure di cui è prevista l'adozione in relazione a prodotti non conformi ai requisiti di accessibilità della presente direttiva. La procedura di salvaguardia dovrebbe consentire alle autorità di vigilanza del mercato, in cooperazione con gli operatori economici interessati, di intervenire in una fase più precoce per quanto riguarda tali prodotti.

(89) Qualora gli Stati membri e la Commissione concordino sul fatto che una misura adottata da uno Stato membro è giustificata, non dovrebbero essere previsti ulteriori interventi della Commissione, ad eccezione dei casi in cui la non conformità possa essere attribuita a carenze di una norma armonizzata o delle specifiche tecniche.

(90) Le direttive 2014/24/UE ([22]) e 2014/25/UE ([23]) del Parlamento europeo e del Consiglio sugli appalti pubblici, che definiscono le procedure di aggiudicazione degli appalti pubblici e concorsi pubblici di progettazione per talune forniture (prodotti), servizi e lavori, stabiliscono che, per tutti gli appalti destinati all'uso da parte di persone fisiche, che si tratti della popolazione o del personale dell'amministrazione aggiudicatrice o dell'ente aggiudicatore, le specifiche tecniche sono elaborate, salvo in casi debitamente giustificati, in modo da tenere conto dei criteri di accessibilità per le persone con disabilità o di una progettazione per tutti gli utenti. Inoltre, tali direttive prevedono che, qualora i requisiti di accessibilità obbligatori siano adottati con un atto giuridico dell'Unione, le specifiche tecniche debbano essere stabilite mediante riferimento ad esse per quanto riguarda l'accessibilità per le persone con disabilità o la progettazione per tutti gli utenti. La presente direttiva dovrebbe stabilire requisiti di accessibilità obbligatori per i prodotti e i servizi da essa contemplati. Per i prodotti e i servizi che non rientrano nell'ambito di applicazione della presente direttiva, i requisiti di accessibilità della stessa non sono vincolanti. Tuttavia, l'utilizzo di tali requisiti di accessibilità per soddisfare i pertinenti obblighi stabiliti in atti dell'Unione diversi dalla presente direttiva faciliterebbe l'attuazione dell'accessibilità e contribuirebbe alla certezza del diritto e al ravvicinamento dei requisiti di accessibilità in tutta l'Unione. Non si dovrebbe impedire alle autorità di stabilire requisiti di accessibilità che vanno oltre quelli di cui all'allegato I della presente direttiva.

(91) La presente direttiva non dovrebbe modificare la natura obbligatoria o volontaria delle disposizioni in materia di accessibilità in altri atti dell'Unione.

(92) La presente direttiva dovrebbe applicarsi solo alle procedure di appalto per le quali è stato inviato l'avviso di indizione di gara ovvero, qualora non sia previsto l'avviso di indizione di gara, laddove l'amministrazione aggiudicatrice o l'ente aggiudicatore abbia avviato la procedura di appalto dopo la data di applicazione della presente direttiva.

(93) Al fine di garantire la corretta applicazione della presente direttiva, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del TFUE riguardo all'ulteriore precisazione dei requisiti di accessibilità che non possono, per la loro stessa natura, produrre il loro effetto atteso a meno di essere ulteriormente specificati in atti giuridici vincolanti dell'Unione; alla modifica del periodo durante il quale gli operatori economici devono essere in grado di identificare qualsiasi altro operatore economico che ha fornito loro un prodotto o al quale essi hanno fornito un prodotto; e all'ulteriore specificazione dei criteri pertinenti che l'operatore economico deve prendere in considerazione per valutare se la conformità ai requisiti di accessibilità imporrebbe un onere sproporzionato. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([24]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(94) Al fine di garantire condizioni uniformi di esecuzione della presente direttiva, dovrebbero essere conferite alla Commissione competenze di esecuzione per quanto riguarda le specifiche tecniche. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([25]).

([22]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

([23]) Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE (GU L 94 del 28.3.2014, pag. 243).

([24]) GU L 123 del 12.5.2016, pag. 1.

([25]) 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).

(95) Gli Stati membri dovrebbero garantire che esistano mezzi idonei ed efficaci per assicurare il rispetto delle disposizioni della presente direttiva e dovrebbero stabilire pertanto adeguati meccanismi di controllo, come il controllo a posteriori da parte delle autorità di vigilanza del mercato, al fine di verificare la legittimità della deroga all'applicazione dei requisiti di accessibilità. In sede di esame dei ricorsi riguardanti l'accessibilità, gli Stati membri dovrebbero rispettare il principio generale di buona amministrazione, e in particolare l'obbligo dei funzionari di garantire che sia adottata una decisione su ciascun ricorso entro un termine ragionevole.

(96) Per agevolare l'attuazione uniforme della presente direttiva, la Commissione dovrebbe istituire un gruppo di lavoro composto dalle pertinenti autorità e parti interessate per facilitare lo scambio di informazioni e di migliori prassi e per fornire consulenza. È opportuno incoraggiare la cooperazione tra le autorità e le parti interessate, comprese le persone con disabilità e le organizzazioni che le rappresentano, tra l'altro per migliorare la coerenza nell'applicazione delle disposizioni della presente direttiva riguardanti i requisiti di accessibilità e per controllare l'attuazione delle sue disposizioni sulla modifica sostanziale e l'onere sproporzionato.

(97) Visto il quadro normativo esistente in materia di ricorsi nei settori contemplati dalle direttive 2014/24/UE e 2014/25/UE, le disposizioni della presente direttiva relative all'applicazione e alle sanzioni non dovrebbero applicarsi alle procedure di appalto soggette agli obblighi imposti dalla presente direttiva. Tale esclusione lascia impregiudicati gli obblighi degli Stati membri derivanti dai trattati di adottare tutte le misure necessarie per garantire l'applicazione e l'efficacia del diritto dell'Unione.

(98) Le sanzioni dovrebbero essere adeguate rispetto alla natura delle violazioni e alle circostanze, affinché non fungano da alternativa all'adempimento, da parte degli operatori economici, degli obblighi di rendere accessibili i loro prodotti o servizi.

(99) Gli Stati membri dovrebbero garantire che, conformemente al diritto dell'Unione in vigore, siano disponibili meccanismi alternativi di risoluzione delle controversie che consentano di risolvere i presunti casi di non conformità alla presente direttiva prima che vengano aditi i tribunali o gli organi amministrativi competenti.

(100) Conformemente alla dichiarazione politica comune del 28 settembre 2011 degli Stati membri e della Commissione sui documenti esplicativi ([26]), gli Stati membri si sono impegnati a garantire, in casi giustificati, che la notifica delle loro misure di recepimento sia accompagnata da uno o più documenti che chiariscano il rapporto tra gli elementi costitutivi della direttiva e le parti corrispondenti degli strumenti nazionali di recepimento. Per quanto riguarda la presente direttiva, il legislatore ritiene che la trasmissione di tali documenti sia giustificata.

(101) Al fine di concedere ai fornitori di servizi un periodo di tempo sufficiente per adeguarsi ai requisiti della presente direttiva, è necessario prevedere un periodo transitorio di cinque anni a decorrere dalla data di applicazione della presente direttiva, durante il quale non occorre che i prodotti utilizzati per la fornitura di un servizio immessi sul mercato prima di tale data siano conformi ai requisiti di accessibilità della presente direttiva, a meno che non siano sostituiti dai fornitori di servizi nel corso del periodo transitorio. Visti il costo e il lungo ciclo di vita dei terminali self-service, è opportuno prevedere che, quando sono utilizzati per la prestazione di servizi, tali terminali possano continuare ad essere utilizzati fino alla fine della loro vita economica, purché non siano sostituiti durante tale periodo, il quale non è superiore a 20 anni.

(102) I requisiti di accessibilità della presente direttiva dovrebbero applicarsi ai prodotti immessi sul mercato e ai servizi forniti dopo la data di applicazione delle misure nazionali di recepimento della presente direttiva, compresi i prodotti usati e di seconda mano importati da un paese terzo e immessi sul mercato dopo tale data.

(103) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea («Carta»). La presente direttiva mira, in particolare, a garantire il pieno rispetto dei diritti delle persone con disabilità di beneficiare di misure intese a garantirne l'autonomia, l'inserimento sociale e professionale e la partecipazione alla vita della comunità, e intende promuovere l'applicazione degli articoli 21, 25 e 26 della Carta.

(104) Poiché l'obiettivo della presente direttiva, vale a dire l'eliminazione degli ostacoli alla libera circolazione di determinati prodotti e servizi accessibili al fine di contribuire al corretto funzionamento del mercato interno, non può essere conseguito in misura sufficiente dagli Stati membri in quanto richiede l'armonizzazione di disposizioni diverse attualmente esistenti nei rispettivi ordinamenti giuridici, ma può essere conseguito meglio a livello di Unione, definendo requisiti di accessibilità e disposizioni comuni per il funzionamento del mercato interno, l'Unione può intervenire in base 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,

([26]) GU C 369 del 17.12.2011, pag. 14.

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

La presente direttiva ha lo scopo di contribuire al corretto funzionamento del mercato interno mediante il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di requisiti di accessibilità per determinati prodotti e servizi, in particolare eliminando e prevenendo gli ostacoli alla libera circolazione dei prodotti e servizi disciplinati dalla presente direttiva derivanti dall'eterogeneità dei requisiti di accessibilità negli Stati membri.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai prodotti seguenti immessi sul mercato dopo il 28 giugno 2025:

a) sistemi hardware e sistemi operativi informatici generici per consumatori per tali sistemi hardware;

b) i terminali self-service seguenti:

   i) terminali di pagamento;

   ii) i terminali self-service seguenti destinati alla fornitura dei servizi disciplinati dalla presente direttiva:

      — sportelli automatici;

      — macchine per l'emissione di biglietti;

      — terminali per il check-in;

      — terminali self-service interattivi destinati alla fornitura di informazioni, a eccezione dei terminali installati come parti integranti di veicoli, aeromobili, navi o materiale rotabile;

c) apparecchiature terminali con capacità informatiche interattive per consumatori utilizzate per i servizi di comunicazione elettronica;

d) apparecchiature terminali con capacità informatiche interattive per consumatori utilizzate per accedere a servizi di media audiovisivi; e

e) lettori di libri elettronici (e-reader).

2. Fatto salvo l'articolo 32, la presente direttiva si applica ai servizi seguenti forniti ai consumatori dopo il 28 giugno 2025:

a) servizi di comunicazione elettronica, a eccezione di servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina;

b) servizi che forniscono accesso a servizi di media audiovisivi;

c) gli elementi seguenti relativi ai servizi di trasporto passeggeri aerei, con autobus, ferroviari e per vie navigabili, ad eccezione dei servizi di trasporto urbani, extraurbani, e regionali, per i quali si applicano solo gli elementi di cui al punto v):

   i) siti web;

   ii) servizi per dispositivi mobili, comprese le applicazioni mobili;

   iii) biglietti elettronici e servizi di biglietteria elettronica;

   iv) fornitura di informazioni relative ai servizi di trasporto, comprese le informazioni di viaggio in tempo reale; per quanto riguarda gli schermi informativi ciò si limita agli schermi interattivi situati nel territorio dell'Unione; e

v) terminali self-service interattivi situati nel territorio dell'Unione, a eccezione di quelli installati come parti integranti su veicoli, aeromobili, navi e materiale rotabile utilizzati per la fornitura di una qualsiasi parte di tali servizi di trasporto passeggeri;

d) servizi bancari per consumatori;

e) libri elettronici (e-book) e software dedicati; e

f) servizi di commercio elettronico.

3. La presente direttiva si applica alla raccolta delle comunicazioni di emergenza effettuate verso il numero unico di emergenza europeo «112».

4. La presente direttiva non si applica ai contenuti di siti web e alle applicazioni mobili seguenti:

a) media basati sul tempo preregistrati pubblicati prima del 28 giugno 2025;

b) formati di file per ufficio pubblicati prima del 28 giugno 2025;

c) carte e servizi di cartografia online, qualora per le carte destinate alla navigazione le informazioni essenziali siano fornite in modalità digitale accessibile;

d) contenuti di terzi che non sono né finanziati né sviluppati dall'operatore economico interessato né sottoposti al suo controllo;

e) contenuti di siti web e applicazioni mobili considerati archivi nel senso che contengono soltanto contenuti che non sono stati aggiornati o rielaborati dopo il 28 giugno 2025.

5. La presente direttiva fa salva la direttiva (UE) 2017/1564 e il regolamento (UE) n. 2017/1563.

Articolo 3

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) «persone con disabilità»: coloro che hanno minorazioni fisiche, mentali, intellettuali o sensoriali a lungo termine che in interazione con varie barriere possono impedire la loro piena ed effettiva partecipazione nella società su una base di eguaglianza con gli altri;

2) «prodotto»: sostanza, preparato o merce fabbricati attraverso un processo di fabbricazione, diversi da alimenti, mangimi, piante e animali vivi, prodotti di origine umana e prodotti di piante ed animali collegati direttamente alla loro futura riproduzione;

3) «servizio»: un servizio quale definito all'articolo 4, punto 1, della direttiva 2006/123/CE del Parlamento europeo e del Consiglio ([27]);

4) «fornitore di servizi»: una persona fisica o giuridica che fornisce un servizio sul mercato dell'Unione o si offre di fornire tale servizio ai consumatori nell'Unione;

5) «servizi di media audiovisivi»: i servizi definiti all'articolo 1, paragrafo 1, lettera a), della direttiva 2010/13/UE;

6) «servizi che forniscono accesso a servizi di media audiovisivi»: servizi trasmessi da reti di comunicazione elettronica che sono utilizzati per individuare, selezionare, ricevere informazioni sui servizi di media audiovisivi e visualizzare tali servizi e tutte le caratteristiche correlate, quali sottotitoli per non udenti e ipoudenti, audiodescrizione, sottotitoli parlati e interpretazione in lingua dei segni, derivanti dall'attuazione di misure per rendere i servizi accessibili ai sensi dell'articolo 7 della direttiva 2010/13/UE; e includono guide elettroniche ai programmi (*electronic programme guides* — EPG).

7) «apparecchiature terminali con capacità informatiche interattive per consumatori utilizzate per accedere a servizi di media audiovisivi»: apparecchiature il cui scopo principale è fornire accesso ai servizi di media audiovisivi;

([27]) Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno (GU L 376 del 27.12.2006, pag. 36).

8) «servizio di comunicazione elettronica»: i servizi di comunicazione elettronica quali definiti all'articolo 2, punto 4, della direttiva (UE) 2018/1972;

9) «servizio di conversazione globale»: il servizio di conversazione globale quale definito all'articolo 2, punto 35, della direttiva (UE) 2018/1972;

10) «centro di raccolta delle chiamate di emergenza» o «PSAP»: un centro di raccolta delle chiamate di emergenza o PSAP quale definito all'articolo 2, punto 36, della direttiva (UE) 2018/1972;

11) «PSAP più idoneo»: uno PSAP più idoneo quale definito all'articolo 2, punto 37, della direttiva (UE) 2018/1972;

12) «comunicazione di emergenza»: la comunicazione di emergenza quale definita all'articolo 2, punto 38, della direttiva (UE) 2018/1972;

13) «servizio di emergenza»: il servizio di emergenza quale definito all'articolo 2, punto 39, della direttiva (UE) 2018/1972;

14) «testo in tempo reale»: una forma di conversazione testuale in situazioni punto a punto o in conferenza tra più punti, in cui il testo introdotto è inviato in modo tale che la comunicazione è percepita dall'utente come continua, carattere per carattere;

15) «messa a disposizione sul mercato»: la fornitura sul mercato dell'Unione, nel corso di un'attività commerciale, a titolo oneroso o gratuito, di un prodotto destinato a essere distribuito, consumato o usato;

16) «immissione sul mercato»: la prima messa a disposizione di un prodotto sul mercato dell'Unione;

17) «fabbricante»: una persona fisica o giuridica che fabbrica un prodotto oppure lo fa progettare o fabbricare e lo commercializza apponendovi il proprio nome o marchio d'impresa;

18) «rappresentante autorizzato»: una persona fisica o giuridica stabilita nell'Unione che ha ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti;

19) «importatore»: una persona fisica o giuridica stabilita nell'Unione che immette sul mercato dell'Unione un prodotto originario di un paese terzo;

20) «distributore»: una persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o dall'importatore, che mette un prodotto a disposizione sul mercato;

21) «operatore economico»: il fabbricante, il rappresentante autorizzato, l'importatore, il distributore o il fornitore di servizi;

22) «consumatore»: una persona fisica che acquista il prodotto in questione o è destinatario del servizio in questione per fini che non rientrano nella sua attività commerciale, industriale, artigianale o professionale;

23) «microimpresa»: un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di EUR;

24) «piccole e medie imprese» o «PMI»: la categoria di imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR o il cui totale di bilancio annuo non supera i 43 milioni di EUR, ma che non comprende le microimprese;

25) «norma armonizzata»: una norma armonizzata quale definita all'articolo 2, punto 1, lettera c), del regolamento (UE) n. 1025/2012;

26) «specifiche tecniche »: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012 che costituisce un mezzo per conformarsi ai requisiti di accessibilità applicabili a un prodotto o servizio;

27) «ritiro»: qualsiasi provvedimento volto a impedire la messa a disposizione sul mercato di un prodotto nella catena di fornitura;

28) «servizi bancari per consumatori»: la fornitura ai consumatori dei servizi bancari e finanziari seguenti:

a) i contratti di credito contemplati dalla direttiva 2008/48/CE del Parlamento europeo e del Consiglio ([28]) o dalla direttiva 2014/17/UE del Parlamento europeo e del Consiglio ([29]);

b) i servizi definiti ai punti 1, 2, 4 e 5 della sezione A e ai punti 1, 2, 4 e 5 della sezione B dell'allegato I della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([30]);

c) i servizi di pagamento quali definiti all'articolo 4, punto 3), della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio ([31]);

d) i servizi collegati al conto di pagamento quali definiti all'articolo 2, punto 3), della direttiva 2014/92/UE del Parlamento europeo e del Consiglio ([32]); e

e) la moneta elettronica quale definita all'articolo 2, punto 2), della direttiva 2009/110/CE del Parlamento europeo e del Consiglio ([33]);

29) «terminale di pagamento»: un dispositivo che il cui scopo principale è consentire di effettuare pagamenti tramite l'uso di strumenti di pagamento quali definiti all'articolo 4, punto 14, della direttiva (UE) 2015/2366 presso un punto vendita fisico ma non in un contesto virtuale;

30) «servizi di commercio elettronico»: i servizi forniti a distanza, tramite siti web e servizi per dispositivi mobili, per via elettronica e su richiesta individuale di un consumatore al fine di concludere un contratto di consumo;

31) «servizi di trasporto passeggeri aerei»: i servizi aerei passeggeri commerciali quali definiti all'articolo 2, lettera l), del regolamento (CE) n. 1107/2006, in partenza, in transito o in arrivo presso un aeroporto, quando l'aeroporto è situato nel territorio di uno Stato membro, inclusi i voli in partenza da un aeroporto situato in un paese terzo diretti verso un aeroporto situato nel territorio di uno Stato membro quando i servizi sono assicurati da vettori aerei dell'Unione;

32) «servizi di trasporto passeggeri con autobus»: i servizi di cui all'articolo 2, paragrafi 1 e 2, del regolamento (UE) n. 181/2011;

33) «servizi di trasporto passeggeri ferroviari»: tutti i servizi di trasporto ferroviario di passeggeri di cui all'articolo 2, paragrafo 1, del regolamento (CE) n. 1371/2007, a eccezione dei servizi di cui all'articolo 2, paragrafo 2, dello stesso regolamento;

34) «servizi di trasporto passeggeri per vie navigabili»: i servizi di trasporto passeggeri di cui all'articolo 2, paragrafo 1, del regolamento (UE) n. 1177/2010, ad eccezione dei servizi di cui all'articolo 2, paragrafo 2, del medesimo regolamento;

35) «servizi di trasporto urbani ed extraurbani»: i servizi urbani ed extraurbani quali definiti all'articolo 3, punto 6), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([34]); ma ai fini della presente direttiva, tale definizione comprende solo i modi di trasporto seguenti: ferroviario, con autobus e pullman, metropolitana, tram e filobus;

([28]) Direttiva 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE (GU L 133 del 22.5.2008, pag. 66).

([29]) Direttiva 2014/17/UE del Parlamento europeo e del Consiglio, del 4 febbraio 2014, in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali e recante modifica delle direttive 2008/48/CE e 2013/36/UE e del regolamento (UE) n. 1093/2010 (GU L 60 del 28.2.2014, pag. 34).

([30]) 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).

([31]) Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).

([32]) Direttiva 2014/92/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sulla comparabilità delle spese relative al conto di pagamento, sul trasferimento del conto di pagamento e sull'accesso al conto di pagamento con caratteristiche di base (GU L 257 del 28.8.2014, pag. 214).

([33]) Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

([34]) 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).

36) «servizi di trasporto regionali»: i servizi regionali quali definiti all'articolo 3, punto 7), della direttiva 2012/34/UE; ma ai fini della presente direttiva, tale definizione comprende solo i modi di trasporto seguenti: ferroviario, con autobus e pullman, metropolitana, tram e filobus;

37) «tecnologia assistiva»: qualsiasi elemento, parte di apparecchiatura, servizio o sistema di prodotti, compresi i software, utilizzato per accrescere, mantenere, sostituire o migliorare le capacità funzionali delle persone con disabilità oppure per alleviare o compensare minorazioni, limitazioni dell'attività o restrizioni della partecipazione;

38) «sistema operativo»: il software che, tra l'altro, gestisce l'interfaccia con l'hardware periferico, programma le operazioni, assegna la memoria e presenta all'utente un'interfaccia di default quando non vi sono applicazioni in esecuzione, compresa un'interfaccia grafica utente, indipendentemente dal fatto che tale software costituisca una parte integrante dell'hardware informatico generico per consumatori o sia un software a sé stante destinato a essere utilizzato per mezzo di un hardware informatico generico per consumatori; ma tale definizione esclude il boot loader, il basic input-output system o altri firmware necessari nella fase di avvio o al momento dell'installazione del sistema operativo;

39) «sistema hardware informatico generico per consumatori»: la combinazione di hardware che forma un computer completo, caratterizzato dalla multifunzionalità e dalla capacità di eseguire, con il software adeguato, le operazioni informatiche più comuni richieste dai consumatori e destinato ad essere utilizzato dai consumatori; compresi personal computer, in particolare i computer da tavolo (desktop), i notebook, gli smartphone e i tablet;

40) «capacità informatica interattiva»: funzionalità che sostiene l'interazione uomo-dispositivo consentendo il trattamento e la trasmissione di dati, voce o video o una qualsiasi combinazione dei predetti;

41) «libro elettronico (e-book) e software dedicati»: il servizio consistente nella fornitura di file digitali che trasmettono la versione elettronica di un libro così da potervi accedere e navigare e da renderne possibile la lettura e l'utilizzo, nonché il software, ivi inclusi i servizi per dispositivi mobili comprese le applicazioni mobili, destinato a consentire le operazioni di accesso, navigazione, lettura e utilizzo di tali file digitali, ed esclude i software di cui alla definizione (42);

42) «lettore di libro elettronico (e-reader)»: apparecchiatura dedicata, comprendente sia hardware che software, utilizzata ai fini dell'accesso ai file di libri elettronici, della navigazione al loro interno, della loro lettura e del loro utilizzo;

43) «biglietti elettronici»: un sistema in cui un titolo di trasporto, sotto forma di biglietti singoli o multipli, abbonamenti o credito di viaggio, è archiviato in forma elettronica in una tessera di trasporto fisica o in un altro dispositivo anziché essere stampato su un biglietto cartaceo;

44) «servizi di biglietteria elettronica»: un sistema in cui i biglietti di trasporto dei passeggeri sono acquistati, incluso online, utilizzando un dispositivo dotato di capacità informatica interattiva e forniti all'acquirente in forma elettronica, che consentano la loro stampa su carta o di essere visualizzati, al momento del viaggio, utilizzando un dispositivo mobile dotato di capacità informatica interattiva.

CAPO II

Requisiti di accessibilità e libera circolazione

Articolo 4

Requisiti di accessibilità

1. Gli Stati membri provvedono affinché, conformemente ai paragrafi 2, 3 e 5 del presente articolo, fatto salvo l'articolo 14, gli operatori economici immettano sul mercato solo i prodotti e forniscano solo i servizi che siano conformi ai requisiti di accessibilità di cui all'allegato I.

2. Tutti i prodotti elencati devono essere conformi ai requisiti di accessibilità di cui alla sezione I dell'allegato I.

Tutti i prodotti, esclusi i terminali self-service, devono essere conformi ai requisiti di accessibilità di cui alla sezione II dell'allegato I.

3. Fatto salvo il paragrafo 5 del presente articolo, tutti i servizi, ad eccezione dei servizi di trasporto urbani, extraurbani e regionali, sono conformi ai requisiti di accessibilità di cui alla sezione III dell'allegato I.

Fatto salvo il paragrafo 5 del presente articolo, tutti i servizi devono essere conformi ai requisiti di accessibilità di cui alla sezione IV dell'allegato I.

4. Gli Stati membri possono decidere, alla luce delle circostanze nazionali, che l'ambiente costruito utilizzato dai clienti dei servizi contemplati dalla presente direttiva si conformi ai requisiti di accessibilità di cui all'allegato III, al fine di ottimizzarne l'utilizzo da parte delle persone con disabilità.

5. Le microimprese che forniscono servizi sono esentate dall'osservanza dei requisiti di accessibilità di cui al paragrafo 3 del presente articolo e da qualsiasi obbligo relativo al rispetto di detti requisiti.

6. Gli Stati membri forniscono orientamenti e strumenti alle microimprese per facilitare l'applicazione delle misure nazionali di recepimento della presente direttiva. Gli Stati membri elaborano tali strumenti in consultazione con le parti interessate.

7. Gli Stati membri possono fornire agli operatori economici degli esempi indicativi, contenuti nell'allegato II, di possibili soluzioni che contribuiscono a soddisfare i requisiti di accessibilità di cui all'allegato I.

8. Gli Stati membri provvedono affinché la raccolta delle comunicazioni di emergenza effettuate verso il numero unico di emergenza europeo «112», da parte dello PSAP più idoneo sia conforme agli specifici requisiti di accessibilità di cui alla sezione V dell'allegato I, nel modo che più si adatta all'organizzazione nazionale dei sistemi di emergenza.

9. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 26 a integrazione dell'allegato I specificando ulteriormente i requisiti di accessibilità che non possono, per la loro stessa natura, produrre il loro effetto atteso a meno di essere ulteriormente specificati in atti giuridici vincolanti dell'Unione, come i requisiti relativi all'interoperabilità.

Articolo 5

Diritto dell'Unione in vigore nel settore del trasporto passeggeri

I servizi conformi ai requisiti sulla fornitura di informazioni accessibili e sulle informazioni sull'accessibilità di cui ai regolamenti (CE) n. 261/2004, (CE) n. 1107/2006, (CE) n. 1371/2007, (UE) n. 1177/2010 e(UE) n. 181/2011, nonché agli atti pertinenti adottati sulla base della direttiva 2008/57/CE, sono ritenuti conformi ai requisiti corrispondenti della presente direttiva. Qualora la presente direttiva preveda requisiti supplementari rispetto a quelli stabiliti da detti regolamenti e atti, tali requisiti supplementari si applicano integralmente.

Articolo 6

Libera circolazione

Gli Stati membri non ostacolano, per motivi relativi ai requisiti di accessibilità, la messa a disposizione sul mercato nel loro territorio di prodotti o la fornitura nel loro territorio di servizi conformi alla presente direttiva.

CAPO III

Obblighi degli operatori economici che trattano prodotti

Articolo 7

Obblighi dei fabbricanti

1. All'atto dell'immissione dei loro prodotti sul mercato, i fabbricanti garantiscono che essi siano stati progettati e fabbricati conformemente ai requisiti di accessibilità applicabili della presente direttiva.

2. I fabbricanti preparano la documentazione tecnica in conformità dell'allegato IV ed eseguono o fanno eseguire la procedura di valutazione della conformità di cui al medesimo allegato.

Qualora la conformità di un prodotto ai requisiti di accessibilità applicabili sia stata dimostrata con tale procedura, i fabbricanti redigono una dichiarazione UE di conformità e appongono la marcatura CE.

3. I fabbricanti conservano la documentazione tecnica e la dichiarazione UE di conformità per un periodo di cinque anni dalla data di immissione sul mercato del prodotto.

4. I fabbricanti garantiscono che siano predisposte le procedure necessarie affinché la produzione in serie continui a essere conforme alla presente direttiva. Si tiene debitamente conto delle modifiche della progettazione o delle caratteristiche del prodotto, nonché delle modifiche delle norme armonizzate o delle specifiche tecniche in riferimento alle quali è dichiarata la conformità di un prodotto.

5. I fabbricanti garantiscono che sui loro prodotti sia apposto un numero di tipo, di lotto, di serie oppure qualsiasi altro elemento che ne consenta l'identificazione, oppure, qualora le dimensioni o la natura del prodotto non lo consentano, che le informazioni prescritte siano fornite sull'imballaggio o in un documento di accompagnamento del prodotto.

6. I fabbricanti indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio d'impresa e l'indirizzo al quale possono essere contattati sul prodotto oppure, ove ciò non sia possibile, sull'imballaggio o in un documento di accompagnamento del prodotto. L'indirizzo deve indicare un unico punto dove il fabbricante può essere contattato. I dati di recapito sono redatti in una lingua facilmente comprensibile per gli utilizzatori finali e le autorità di vigilanza del mercato.

7. I fabbricanti garantiscono che il prodotto sia accompagnato da istruzioni e informazioni sulla sicurezza in una lingua che può essere facilmente compresa dai consumatori e dagli altri utenti finali, secondo quanto determinato dallo Stato membro interessato. Tali istruzioni e informazioni, nonché l'eventuale etichettatura, sono chiare, comprensibili e intelligibili.

8. I fabbricanti che ritengono o hanno motivo di credere che un prodotto che hanno immesso sul mercato non sia conforme alla presente direttiva adottano immediatamente le misure correttive necessarie per rendere conforme tale prodotto o, se del caso, per ritirarlo. Inoltre, qualora il prodotto non sia conforme ai requisiti di accessibilità della presente direttiva, i fabbricanti ne informano immediatamente le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione il prodotto, indicando in particolare i dettagli relativi alla non conformità e a eventuali misure correttive adottate. In tali casi, i fabbricanti tengono un registro dei prodotti che non sono conformi ai requisiti di accessibilità applicabili e dei relativi reclami.

9. I fabbricanti, a seguito di una richiesta motivata di un'autorità nazionale competente, forniscono a quest'ultima tutte le informazioni e la documentazione necessarie per dimostrare la conformità del prodotto in una lingua che può essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi azione adottata per eliminare la non conformità ai requisiti di accessibilità applicabili dei prodotti che hanno immesso sul mercato, in particolare rendendoli conformi ai requisiti di accessibilità applicabili.

Articolo 8

Rappresentanti autorizzati

1. Il fabbricante può nominare, mediante mandato scritto, un rappresentante autorizzato.

Gli obblighi di cui all'articolo 7, paragrafo 1, e l'elaborazione della documentazione tecnica non rientrano nel mandato del rappresentante autorizzato.

2. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. Il mandato consente al rappresentante autorizzato di eseguire almeno i compiti seguenti:

a) tenere a disposizione delle autorità di vigilanza dei mercati la dichiarazione UE di conformità e la documentazione tecnica per un periodo di cinque anni;

b) fornire a un'autorità nazionale competente che ne faccia richiesta motivata tutte le informazioni e la documentazione necessarie per dimostrare la conformità del prodotto;

c) cooperare con le autorità nazionali competenti, su loro richiesta, a qualsiasi azione adottata per eliminare la non conformità ai requisiti di accessibilità applicabili dei prodotti che rientrano nel loro mandato.

Articolo 9

Obblighi degli importatori

1. Gli importatori immettono sul mercato solo prodotti conformi.

2. Prima di immettere un prodotto sul mercato, gli importatori assicurano che il fabbricante abbia eseguito la procedura di valutazione della conformità stabilita all'allegato IV. Essi assicurano che il fabbricante abbia redatto la documentazione tecnica prescritta dall'allegato II, che il prodotto rechi il marchio CE e sia accompagnato dai documenti prescritti e che il fabbricante abbia rispettato i requisiti di cui all'articolo 7, paragrafi 5 e 6.

3. L'importatore, se ritiene o ha motivo di credere che un prodotto non sia conforme ai requisiti di accessibilità applicabili della presente direttiva, non immette il prodotto sul mercato finché non sia stato reso conforme. Inoltre, quando un prodotto non è conforme ai requisiti di accessibilità applicabili, l'importatore ne informa il fabbricante e le autorità di vigilanza del mercato.

4. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio d'impresa e l'indirizzo al quale possono essere contattati sul prodotto oppure, ove ciò non sia possibile, sull'imballaggio o in un documento di accompagnamento del prodotto. I dati di recapito sono redatti in una lingua facilmente comprensibile per gli utilizzatori finali e le autorità di vigilanza del mercato.

5. Gli importatori garantiscono che il prodotto sia accompagnato da istruzioni e informazioni sulla sicurezza in una lingua che può essere facilmente compresa dai consumatori e dagli altri utenti finali, secondo quanto determinato dallo Stato membro interessato.

6. Gli importatori garantiscono che, mentre un prodotto è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto non ne pregiudichino la conformità ai requisiti di accessibilità applicabili

7. Gli importatori tengono una copia della dichiarazione UE di conformità a disposizione delle autorità di vigilanza del mercato per un periodo di cinque anni e provvedono affinché, su richiesta, la documentazione tecnica possa essere messa a disposizione di tali autorità.

8. Gli importatori che ritengono o hanno motivo di credere che un prodotto che hanno immesso sul mercato non sia conforme alla presente direttiva adottano immediatamente le misure correttive necessarie per rendere conforme tale prodotto o, se del caso, per ritirarlo. Inoltre, qualora il prodotto non sia conforme ai requisiti di accessibilità applicabili, gli importatori ne informano immediatamente le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione il prodotto, indicando in particolare i dettagli relativi alla non conformità e ad eventuali misure correttive adottate. In tali casi, gli importatori tengono un registro dei prodotti che non sono conformi ai requisiti di accessibilità applicabili e dei relativi reclami.

9. Gli importatori, a seguito di una richiesta motivata di un'autorità nazionale competente, forniscono a quest'ultima tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un prodotto in una lingua che può essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi azione adottata per eliminare la non conformità ai requisiti di accessibilità applicabili dei prodotti che hanno immesso sul mercato.

Articolo 10

Obblighi dei distributori

1. Quando mettono un prodotto a disposizione sul mercato, i distributori agiscono con la dovuta attenzione in relazione ai requisiti della presente direttiva.

2. Prima di mettere un prodotto a disposizione sul mercato, i distributori verificano che esso rechi la marcatura CE, che sia accompagnato dai documenti prescritti e da istruzioni e informazioni sulla sicurezza in una lingua che può essere facilmente compresa dai consumatori e dagli altri utenti finali nello Stato membro in cui il prodotto deve essere messo a disposizione sul mercato e che il fabbricante e l'importatore si siano conformati ai requisiti di cui, rispettivamente, all'articolo 7, paragrafi 5 e 6, e all'articolo 9, paragrafo 4.

3. Il distributore, se ritiene o ha motivo di credere che un prodotto non sia conforme ai requisiti di accessibilità applicabili della presente direttiva, non immette il prodotto sul mercato finché non sia stato reso conforme. Inoltre, quando un prodotto non è conforme ai requisiti di accessibilità applicabili, il distributore ne informa il fabbricante o l'importatore e le autorità di vigilanza del mercato.

4. I distributori garantiscono che, mentre un prodotto è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto non ne pregiudichino la conformità ai requisiti di accessibilità applicabili.

5. I distributori che ritengono o hanno motivo di credere che un prodotto che hanno reso disponibile sul mercato non sia conforme alla presente direttiva si assicurano che siano adottate le misure correttive necessarie per rendere conforme tale prodotto o, se del caso, per ritirarlo. Inoltre, qualora il prodotto non sia conforme ai requisiti di accessibilità applicabili, i distributori ne informano immediatamente le autorità nazionali competenti degli Stati membri in cui hanno messo a disposizione il prodotto, indicando in particolare i dettagli relativi alla non conformità e a qualsiasi misura correttiva adottata.

6. I distributori, a seguito della richiesta motivata di un'autorità nazionale competente, forniscono a quest'ultima tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un prodotto. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi azione adottata per eliminare la non conformità ai requisiti di accessibilità applicabili dei prodotti che hanno reso disponibili sul mercato.

Articolo 11

Casi in cui gli obblighi dei fabbricanti si applicano agli importatori e ai distributori

Un importatore o un distributore che immette un prodotto sul mercato con il proprio nome o marchio d'impresa oppure modifica un prodotto già immesso sul mercato in modo tale che la conformità ai requisiti della presente direttiva possa esserne condizionata è considerato un fabbricante ai fini della presente direttiva ed è soggetto agli obblighi del fabbricante di cui all'articolo 7.

Articolo 12

Identificazione degli operatori economici che trattano prodotti

1. Gli operatori economici di cui agli articoli da 7 a 10 indicano alle autorità di vigilanza che ne facciano richiesta:

a) ogni altro operatore economico che abbia fornito loro un prodotto;

b) ogni altro operatore economico cui essi abbiano fornito un prodotto.

2. Gli operatori economici di cui agli articoli da 7 a 10 sono in grado di presentare le informazioni di cui al paragrafo 1 del presente articolo per un periodo di cinque anni dal momento in cui sia stato loro fornito il prodotto e per un periodo di cinque anni dal momento in cui essi abbiano fornito il prodotto.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 26, di modificare la presente direttiva per modificare il periodo di cui al paragrafo 2 del presente articolo relativamente a prodotti specifici. Tale periodo modificato è superiore a cinque anni ed è proporzionale alla vita economica utile del prodotto in questione.

CAPO IV

Obblighi dei fornitori di servizi

Articolo 13

Obblighi dei fornitori di servizi

1. I fornitori di servizi assicurano di progettare e fornire servizi in conformità dei requisiti di accessibilità della presente direttiva.

2. I fornitori di servizi preparano le informazioni necessarie in conformità dell'allegato V e spiegano come i servizi soddisfino i requisiti di accessibilità applicabili. Le informazioni sono messe a disposizione del pubblico in forma scritta e orale, anche in modo da essere accessibili a persone con disabilità. I fornitori di servizi conservano tali informazioni finché il servizio è operativo.

3. Fatto salvo l'articolo 32, i fornitori di servizi assicurano che siano predisposte procedure affinché la fornitura di servizi continui a essere conforme ai requisiti di accessibilità applicabili. Le variazioni delle caratteristiche della fornitura del servizio, dei requisiti di accessibilità applicabili e delle norme armonizzate o delle specifiche tecniche in riferimento a cui il servizio è dichiarato conforme ai requisiti di accessibilità sono prese adeguatamente in considerazione dai fornitori di servizi.

4. In caso di non conformità, i fornitori di servizi adottano le misure correttive necessarie per rendere il servizio conforme ai requisiti di accessibilità applicabili. Inoltre, qualora il servizio non sia conforme ai requisiti di accessibilità applicabili, i fornitori di servizi ne informano immediatamente le autorità nazionali competenti degli Stati membri in cui il servizio è fornito, indicando in particolare i dettagli relativi alla non conformità e a eventuali misure correttive adottate.

5. I fornitori di servizi, a seguito di una richiesta motivata di un'autorità competente, forniscono a quest'ultima tutte le informazioni necessarie per dimostrare la conformità del servizio ai requisiti di accessibilità applicabili. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi azione adottata per rendere il servizio conforme a tali requisiti

CAPO V

Modifica sostanziale di prodotti o servizi e onere sproporzionato per gli operatori economici

Articolo 14

Modifica sostanziale e onere sproporzionato

1. I requisiti di accessibilità di cui all'articolo 4 si applicano soltanto nella misura in cui la conformità:

a) non richieda una modifica sostanziale di un prodotto o di un servizio tale da comportare la modifica sostanziale della sua natura stessa; e

b) non comporti l'imposizione di un onere sproporzionato agli operatori economici interessati.

2. Gli operatori economici valutano se la conformità ai requisiti di accessibilità di cui all'articolo 4 introdurrebbe una modifica fondamentale o, sulla base dei pertinenti criteri di cui all'allegato VI, imporrebbe un onere sproporzionato, come previsto al paragrafo 1 del presente articolo.

3. Gli operatori economici documentano la valutazione di cui al paragrafo 2. Gli operatori economici conservano tutti i risultati pertinenti per un periodo di cinque anni, calcolati a decorrere, a seconda dei casi, dall'ultima messa a disposizione di un prodotto sul mercato o dall'ultima fornitura di un servizio. Su richiesta delle autorità di vigilanza del mercato o delle autorità responsabili del controllo della conformità dei servizi, a seconda dei casi, gli operatori economici forniscono alle autorità una copia della valutazione di cui al paragrafo 2.

4. In deroga al paragrafo 3, le microimprese che trattano prodotti sono esenti dal requisito di documentare la loro valutazione. Se tuttavia un'autorità di vigilanza del mercato lo richiede, le microimprese che trattano prodotti e che hanno scelto di invocare il paragrafo 1 forniscono all'autorità gli elementi fattuali relativi alla valutazione di cui al paragrafo 2.

5. I fornitori di servizi che invocano il paragrafo 1, lettera b), per quanto riguarda ogni categoria o tipo di servizio, rinnovano la loro valutazione sul fatto che l'onere sia o meno sproporzionato:

a) quando il servizio offerto è modificato; o

b) su richiesta delle autorità responsabili del controllo della conformità dei servizi; e

c) in ogni caso, almeno ogni cinque anni.

6. Qualora gli operatori economici ricevano finanziamenti provenienti da fonti, pubbliche o private, diverse dalle risorse dell'operatore, cioè forniti al fine di migliorare l'accessibilità, non hanno diritto di invocare il paragrafo 1, lettera b).

7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 26 a integrazione dell'allegato VI specificando ulteriormente i pertinenti criteri di cui l'operatore economico deve tenere conto per la valutazione di cui al paragrafo 2 del presente articolo. Al momento di specificare ulteriormente tali criteri, la Commissione tiene conto dei potenziali vantaggi non soltanto per le persone con disabilità, ma anche per le persone con limitazioni funzionali.

Se necessario, la Commissione adotta il primo di tali atti delegati entro il 28 giugno 2020. Tale atto comincia ad applicarsi non prima del 28 giugno 2025.

8. Qualora gli operatori economici invochino il paragrafo 1 per uno specifico prodotto o servizio, essi ne informano le autorità di vigilanza del mercato o le autorità responsabili della conformità dei servizi competenti dello Stato membro in cui il prodotto specifico è immesso sul mercato o è fornito il servizio specifico.

Il primo comma non si applica alle microimprese.

CAPO VI

Norme armonizzate e specifiche tecniche dei prodotti e dei servizi

Articolo 15

Presunzione di conformità

1. I prodotti e i servizi conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* sono considerati conformi ai requisiti di accessibilità della presente direttiva nella misura in cui tali norme o parti di esse contemplino tali requisiti.

2. La Commissione richiede, conformemente all'articolo 10 del regolamento (UE) n. 1025/2012, a una o più organizzazioni europee di normazione di elaborare norme armonizzate per i requisiti di accessibilità dei prodotti di cui all'allegato I. La Commissione trasmette il primo di tali progetti di richiesta al comitato interessato entro il 28 giugno 2021.

3. La Commissione può adottare atti di esecuzione che stabiliscano specifiche tecniche conformi ai requisiti di accessibilità della presente direttiva se sono soddisfatte le condizioni seguenti:

a) in assenza di riferimenti a norme armonizzate pubblicati nella *Gazzetta ufficiale dell'Unione europea* a norma del regolamento (UE) n. 1025/2012; e

b) oppure:

   i) la Commissione ha chiesto a una o più organizzazioni europee di normazione di elaborare una norma armonizzata e vi sono ritardi indebiti nella procedura di normazione o la richiesta non è stata accettata da nessuna organizzazione europea di normazione; o

ii) la Commissione può dimostrare che una specifica tecnica rispetta i requisiti di cui all'allegato II del regolamento (UE) n. 1025/2012, a eccezione del requisito che le specifiche tecniche avrebbero dovuto essere sviluppate da un'organizzazione senza scopo di lucro.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 27, paragrafo 2.

4. I prodotti e i servizi conformi alle specifiche tecniche o a parti di esse sono considerati conformi ai requisiti di accessibilità della presente direttiva nella misura in cui dette specifiche tecniche o parti di esse contemplino tali requisiti.

CAPO VII

Conformità dei prodotti e marcatura ce

Articolo 16

Dichiarazione UE di conformità dei prodotti

1. La dichiarazione UE di conformità attesta che è stata dimostrata la conformità ai requisiti di accessibilità applicabili. Qualora in via eccezionale si sia fatto ricorso all'articolo 14, la dichiarazione UE di conformità attesta quali requisiti di accessibilità sono soggetti a tale eccezione.

2. La dichiarazione UE di conformità ha la struttura tipo di cui all'allegato III della decisione n. 768/2008/CE. Essa contiene gli elementi specificati all'allegato IV della presente direttiva ed è regolarmente aggiornata. I requisiti concernenti la documentazione tecnica evitano l'imposizione di un onere indebito per le microimprese e le PMI. La dichiarazione è tradotta nella lingua o nelle lingue richieste dallo Stato membro in cui il prodotto è immesso sul mercato o messo a disposizione.

3. Se al prodotto si applicano più atti dell'Unione che prescrivono una dichiarazione UE di conformità, viene compilata un'unica dichiarazione UE di conformità in rapporto a tali atti dell'Unione. La dichiarazione contiene gli estremi degli atti interessati, compresi i riferimenti della loro pubblicazione.

4. Con la dichiarazione UE di conformità il fabbricante si assume la responsabilità della conformità del prodotto ai requisiti della presente direttiva.

Articolo 17

Principi generali della marcatura CE dei prodotti

La marcatura CE è soggetta ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

Articolo 18

Regole e condizioni per l'apposizione della marcatura CE

1. La marcatura CE è apposta sul prodotto o sulla sua targhetta segnaletica in modo visibile, leggibile e indelebile. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del prodotto, il marchio è apposto sull'imballaggio e sui documenti di accompagnamento.

2. La marcatura CE è apposta prima che il prodotto sia immesso sul mercato.

3. Gli Stati membri si avvalgono dei meccanismi esistenti per garantire un'applicazione corretta del regime che disciplina la marcatura CE e promuovono le azioni opportune in caso di uso improprio di tale marcatura.

CAPO VIII

Vigilanza del mercato dei prodotti e procedura di salvaguardia dell'unione

Articolo 19

Vigilanza del mercato dei prodotti

1. Ai prodotti si applicano l'articolo 15, paragrafo 3, gli articoli da 16 a 19, l'articolo 21, gli articoli da 23 a 28 e l'articolo 29, paragrafi 2 e 3, del regolamento (CE) n. 765/2008.

2. Nell'effettuare la sorveglianza del mercato dei prodotti, le autorità di vigilanza del mercato competenti, qualora l'operatore economico abbia invocato l'articolo 14 della presente direttiva:

a) verificano se la valutazione di cui all'articolo 14 sia stata effettuata dall'operatore economico;

b) riesaminano tale valutazione e i relativi risultati, compreso l'uso corretto dei criteri di cui all'allegato VI; e

c) controllano la conformità ai requisiti di accessibilità applicabili.

3. Gli Stati membri provvedono affinché le informazioni detenute dalle autorità di vigilanza del mercato in merito alla conformità degli operatori economici ai requisiti di accessibilità applicabili della presente direttiva e in merito alla valutazione di cui all'articolo 14 siano messe a disposizione dei consumatori su loro richiesta e in un formato accessibile, salvo nel caso in cui tali informazioni non possano essere fornite per i motivi di riservatezza previsti all'articolo 19, paragrafo 5, del regolamento (CE) n. 765/2008.

Articolo 20

Procedura a livello nazionale per i prodotti non conformi ai requisiti di accessibilità applicabili

1. Qualora le autorità di vigilanza del mercato di uno degli Stati membri abbiano sufficienti ragioni per ritenere che un prodotto contemplato dalla presente direttiva non sia conforme ai requisiti di accessibilità applicabili, esse effettuano una valutazione del prodotto interessato rispetto a tutti i requisiti di cui alla presente direttiva. Gli operatori economici interessati cooperano pienamente a tal fine con le autorità di vigilanza del mercato.

Se, attraverso la valutazione di cui al primo comma, le autorità di vigilanza del mercato concludono che il prodotto non rispetta i requisiti di cui alla presente direttiva, esse chiedono senza ritardo all'operatore economico interessato di adottare tutte le misure correttive del caso al fine di rendere il prodotto conforme ai suddetti requisiti entro un termine ragionevole e proporzionato alla natura della non conformità, da esse stabilito.

Le autorità di vigilanza del mercato chiedono all'operatore economico interessato di ritirare il prodotto dal mercato entro un termine supplementare ragionevole solo qualora l'operatore economico interessato non abbia adottato misure correttive adeguate entro il termine di cui al secondo comma del presente paragrafo.

L'articolo 21 del regolamento (CE) n. 765/2008 si applica alle misure di cui al secondo e al terzo comma del presente paragrafo.

2. Qualora ritengano che la non conformità non sia limitata al territorio nazionale, le autorità di vigilanza del mercato informano la Commissione e gli altri Stati membri dei risultati della valutazione e delle misure che hanno chiesto all'operatore economico di adottare.

3. L'operatore economico garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i prodotti interessati che ha messo a disposizione sul mercato in tutta l'Unione.

4. Qualora l'operatore economico interessato non adotti le misure correttive adeguate entro il periodo di cui al paragrafo 1, terzo comma, le autorità di vigilanza del mercato adottano tutte le opportune misure provvisorie per vietare o limitare la messa a disposizione del prodotto sul loro mercato nazionale o per ritirarlo da tale mercato.

Esse informano senza ritardo la Commissione e gli altri Stati membri di tali misure.

5. Le informazioni di cui al secondo comma paragrafo 4 includono tutti gli elementi disponibili, in particolare i dati necessari all'identificazione del prodotto non conforme, la sua origine, la natura della presunta non conformità e i requisiti di accessibilità ai quali il prodotto non è conforme, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dall'operatore economico interessato. In particolare, le autorità di vigilanza del mercato indicano se la non conformità sia dovuta:

a) alla mancata rispondenza del prodotto ai requisiti di accessibilità applicabili; o

b) alle carenze nelle norme armonizzate o nelle specifiche tecniche di cui all'articolo 15 che conferiscono la presunzione di conformità.

6. Gli Stati membri che non siano quello che ha avviato la procedura di cui al presente articolo comunicano senza ritardo alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del prodotto interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.

7. Qualora, entro tre mesi dal ricevimento delle informazioni di cui al secondo comma del paragrafo 4, né uno Stato membro né la Commissione sollevino obiezioni contro la misura provvisoria adottata da uno Stato membro, tale misura è ritenuta giustificata.

8. Gli Stati membri provvedono affinché siano adottate senza ritardo le opportune misure restrittive, quali il ritiro del prodotto dal loro mercato, in relazione al prodotto in questione.

Articolo 21

Procedura di salvaguardia dell'Unione

1. Qualora, in esito alla procedura di cui all'articolo 20, paragrafi 3 e 4, vengano sollevate obiezioni contro una misura adottata da uno Stato membro o qualora la Commissione abbia elementi di prova ragionevoli che suggeriscano che una misura nazionale sia contraria al diritto dell'Unione, la Commissione si consulta senza ritardo con gli Stati membri e con l'operatore o gli operatori economici interessati e valuta la misura nazionale. In base ai risultati di tale valutazione, la Commissione decide se la misura nazionale sia o meno giustificata.

La Commissione indirizza la propria decisione a tutti gli Stati membri e la comunica immediatamente ad essi e all'operatore o agli operatori economici interessati.

2. Se la misura nazionale di cui al paragrafo 1 è ritenuta giustificata, tutti gli Stati membri adottano le misure necessarie a garantire che il prodotto non conforme sia ritirato dal loro mercato e ne informano la Commissione. Se la misura nazionale è ritenuta ingiustificata, lo Stato membro interessato la revoca.

3. Se la misura nazionale di cui al paragrafo 1 del presente articolo è ritenuta giustificata e la non conformità del prodotto è attribuita a carenze nelle norme armonizzate di cui all'articolo 20, paragrafo 5, lettera b), la Commissione applica la procedura di cui all'articolo 11 del regolamento (UE) n. 1025/2012.

4. Se la misura nazionale di cui al paragrafo 1 del presente articolo è ritenuta giustificata e la non conformità del prodotto è attribuita alle carenze nelle specifiche tecniche di cui all'articolo 20, paragrafo 5, lettera b), la Commissione adotta senza ritardo un atto di esecuzione che modifica o abroga la specifica tecnicadi cui trattasi. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 27, paragrafo 2.

Articolo 22

Non conformità formale

1. Fatto salvo l'articolo 20, uno Stato membro che giunga a una delle conclusioni riportate di seguito chiede all'operatore economico interessato di porre fine alla non conformità contestata:

a) la marcatura CE è stata apposta in violazione dell'articolo 30 del regolamento (CE) n. 765/2008 o dell'articolo 18 della presente direttiva;

b) il marchio CE non è stato apposto;

c) la dichiarazione UE di conformità non è stata compilata;

d) la dichiarazione UE di conformità non è stata compilata correttamente;

e) la documentazione tecnica non è disponibile o è incompleta;

f) le informazioni di cui all'articolo 7, paragrafo 6, o all'articolo 9, paragrafo 4, sono assenti, false o incomplete;

g) qualsiasi altro requisito amministrativo di cui all'articolo 7 o all'articolo 9 non è rispettato.

2. Se la non conformità di cui al paragrafo 1 permane, lo Stato membro interessato adotta tutte le misure opportune per limitare o proibire la messa a disposizione sul mercato del prodotto o garantisce che sia ritirato dal mercato.

CAPO IX

Conformità dei servizi

Articolo 23

Conformità dei servizi

1. Gli Stati membri istituiscono, attuano e periodicamente aggiornano procedure adeguate al fine di:

a) verificare la conformità dei servizi ai requisiti della presente direttiva, compresa la valutazione di cui all'articolo 14 alla quale si applica mutatis mutandis l'articolo 19, paragrafo 2;

b) dare seguito ai reclami o alle relazioni riguardanti problemi di non conformità ai requisiti di accessibilità della presente direttiva;

c) verificare che l'operatore economico abbia adottato le necessarie misure correttive.

2. Gli Stati membri designano le autorità responsabili che sono competenti per l'attuazione delle procedure di cui al paragrafo 1 riguardo alla conformità dei servizi.

Gli Stati membri garantiscono che il pubblico sia informato dell'esistenza, dell'ambito di competenza, dell'identità, del lavoro e delle decisioni delle autorità di cui al primo comma. Su richiesta, tali autorità mettono a disposizione tali informazioni in formati accessibili.

CAPO X

Requisiti di accessibilità in altri atti dell'unione

Articolo 24

Accessibilità nel quadro di altri atti dell'Unione

1. Per quanto riguarda i prodotti e i servizi di cui all'articolo 2 della presente direttiva, i requisiti di accessibilità di cui all'allegato I costituiscono i requisiti di accessibilità obbligatori ai sensi dell'articolo 42, paragrafo 1, della direttiva 2014/24/UE e dell'articolo 60, paragrafo 1, della direttiva 2014/25/UE.

2. Un prodotto o servizio le cui caratteristiche, i cui elementi o le cui funzioni sono conformi ai requisiti di accessibilità di cui all'allegato I della presente direttiva conformemente alla sezione VI dello stesso è considerato conforme ai pertinenti obblighi stabiliti in atti dell'Unione diversi dalla presente direttiva, per quanto concerne l'accessibilità, per tali caratteristiche, elementi o funzioni, salvo altrimenti disposto in tali altri atti.

Articolo 25

Norme armonizzate e specifiche tecniche per altri atti dell'Unione

La conformità alle norme armonizzate e alle specifiche tecniche, o a parti di esse, adottate ai sensi dell'articolo 15, crea una presunzione di conformità con l'articolo 24, nella misura in cui tali norme e specifiche tecniche, o parti di esse, soddisfano i requisiti di accessibilità della presente direttiva.

CAPO XI

Atti delegati, competenze di esecuzione e disposizioni finali

Articolo 26

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 4, paragrafo 9, è conferito alla Commissione per un periodo indeterminato a decorrere dal 27 giugno 2019.

Il potere di adottare atti delegati di cui all'articolo 12, paragrafo 3, e all'articolo 14, paragrafo 7, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 27 giugno 2019. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 4, paragrafo 9, all'articolo 12, paragrafo 3, e all'articolo 14, paragrafo 7, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale del 13 aprile 2016 «Legiferare meglio».

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 4, paragrafo 9, dell'articolo 12, paragrafo 3, e dell'articolo 14, paragrafo 7, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 27

Procedura di comitato

1. La Commissione è assistita da un comitato. Tale comitato 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.

Articolo 28

Gruppo di lavoro

La Commissione istituisce un gruppo di lavoro composto da rappresentanti delle autorità di vigilanza del mercato, delle autorità responsabili della conformità dei servizi e delle parti interessate, compresi rappresentanti delle organizzazioni delle persone con disabilità.

Il gruppo di lavoro:

a) agevola lo scambio di informazioni e migliori pratiche tra le autorità e le parti interessate;

b) promuove la cooperazione tra le autorità e le parti interessate su questioni relative all'attuazione della presente direttiva al fine di migliorare la coerenza nell'applicazione dei requisiti di accessibilità della presente direttiva e di monitorare con attenzione l'attuazione dell'articolo 14; e

c) fornisce consulenza, in particolare alla Commissione, segnatamente in merito all'attuazione degli articoli 4 e 14.

Articolo 29

Applicazione

1. Gli Stati membri garantiscono che esistano mezzi adeguati ed efficaci per assicurare il rispetto delle disposizioni della presente direttiva.

2. I mezzi di cui al paragrafo 1 comprendono:

a) disposizioni in base alle quali un consumatore può, a norma della legislazione nazionale, adire i tribunali o gli organi amministrativi competenti per garantire che le disposizioni nazionali di recepimento della presente direttiva siano rispettate;

b) disposizioni in base alle quali gli organismi pubblici o le associazioni, le organizzazioni o altri soggetti giuridici privati che abbiano un legittimo interesse a garantire che la presente direttiva sia rispettata possono, a norma della legislazione nazionale, adire i tribunali o gli organi amministrativi competenti per conto o a sostegno della persona che si ritiene lesa, con la sua approvazione, in qualsiasi procedimento giudiziario o amministrativo diretto a far rispettare gli obblighi stabiliti dalla presente direttiva.

3. Il presente articolo non si applica alle procedure di aggiudicazione degli appalti disciplinate dalla direttiva 2014/24/UE o dalla direttiva 2014/25/UE.

Articolo 30

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni nazionali adottate conformemente alla presente direttiva e adottano tutte le misure necessarie per garantirne l'attuazione.

2. Le sanzioni previste sono effettive, proporzionate e dissuasive. Le sanzioni sono inoltre accompagnate da misure correttive efficaci in caso di non conformità dell'operatore economico.

3. Gli Stati membri notificano senza ritardo tali norme e misure alla Commissione, nonché eventuali successive modifiche delle stesse.

4. Le sanzioni tengono conto dell'entità della non conformità, compresi la sua gravità e il numero di unità di prodotti o servizi non conformi interessati, nonché del numero di persone colpite.

5. Il presente articolo non si applica alle procedure di aggiudicazione degli appalti disciplinate dalla direttiva 2014/24/UE o dalla direttiva 2014/25/UE.

Articolo 31

Recepimento

1. Entro il 28 giugno 2022, gli Stati membri adottano e pubblicano le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

2. Essi applicano tali disposizioni a decorrere dal 28 giugno 2025.

3. In deroga al paragrafo 2 del presente articolo, gli Stati membri possono decidere di applicare le disposizioni relative agli obblighi di cui all'articolo 4, paragrafo 8, al più tardi a decorrere dal 28 giugno 2027.

4. Le misure 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.

5. Gli Stati membri comunicano alla Commissione il testo delle misure principali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

6. Gli Stati membri che si avvalgono della possibilità di cui all'articolo 4, paragrafo 4, comunicano alla Commissione il testo delle principali misure di diritto interno che essi adottano a tal fine e riferiscono alla Commissione in merito ai progressi compiuti nella loro attuazione.

Articolo 32

Misure transitorie

1. Fatto salvo il paragrafo 2 del presente articolo, gli Stati membri prevedono un periodo transitorio che termina il 28 giugno 2030 durante il quale i fornitori di servizi possono continuare a prestare i loro servizi utilizzando prodotti che utilizzavano in modo legittimo prima di tale data per fornire servizi analoghi.

I contratti di servizi conclusi prima del 28 giugno 2025 possono essere mantenuti invariati fino alla loro scadenza, ma per non più di cinque anni da tale data.

2. Gli Stati membri possono disporre che i terminali self-service utilizzati in modo legittimo dai fornitori di servizi per la fornitura di servizi prima del 28 giugno 2025 possano continuare a essere utilizzati per la fornitura di servizi analoghi fino alla fine della loro vita economica utile, ma per non più di venti anni dalla loro messa in funzione.

Articolo 33

Relazione e riesame

1. Entro il 28 giugno 2030 e successivamente ogni cinque anni, la Commissione presenta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni una relazione sull'applicazione della presente direttiva.

2. Alla luce degli sviluppi sociali, economici e tecnologici, le relazioni esaminano, tra l'altro, l'evoluzione dell'accessibilità dei prodotti e servizi, l'eventuale *lock-in* tecnologico o gli eventuali ostacoli all'innovazione e l'impatto della presente direttiva sugli operatori economici e sulle persone con disabilità. Le relazioni valutano altresì se l'applicazione dell'articolo 4, paragrafo 4, abbia contribuito al ravvicinamento dei requisiti di accessibilità divergenti relativi all'ambiente costruito dei servizi di trasporto passeggeri, dei servizi bancari per consumatori e dei centri di servizi ai clienti di operatori di servizi di comunicazione elettronica, ove possibile, con l'obiettivo di consentire il loro progressivo allineamento ai requisiti di accessibilità di cui all'allegato III.

La relazione valuta inoltre se l'applicazione della presente direttiva, in particolare le sue disposizioni volontarie, abbia contribuito al ravvicinamento dei requisiti di accessibilità relativi all'ambiente costruito che costituisce lavori rientranti nell'ambito di applicazione della direttiva 2014/23/UE del Parlamento europeo e del Consiglio ([35]), della direttiva 2014/24/UE e della direttiva 2014/25/UE.

Le relazioni esaminano inoltre le conseguenze per il funzionamento del mercato interno dell'applicazione dell'articolo 14 della presente direttiva, anche sulla base delle informazioni ricevute conformemente all'articolo 14, paragrafo 8, se disponibili, nonché dell'esenzione delle microimprese. La relazione stabilisce se la presente direttiva ha raggiunto i suoi obiettivi e se sarebbe opportuno includere nuovi prodotti o servizi nel suo ambito di applicazione, o escluderne alcuni prodotti o servizi, e individua, ove possibile, gli ambiti in cui è possibile ridurre gli oneri in vista di un'eventuale revisione della presente direttiva.

Se necessario, la Commissione propone opportune misure, che potrebbero includere misure legislative.

([35]) Direttiva 2014/23/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sull'aggiudicazione dei contratti di concessione (GU L 94 del 28.3.2014, pag. 1).

3. Gli Stati membri comunicano alla Commissione, in tempo utile, tutte le informazioni necessarie per consentire alla Commissione di redigere tale relazione.

4. Le relazioni della Commissione tengono conto dei pareri delle parti economiche e delle organizzazioni non governative interessate, incluse le organizzazioni che rappresentano le persone con disabilità.

Articolo 34

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

Articolo 35

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO I

REQUISITI DI ACCESSIBILITÀ PER PRODOTTI E SERVIZI

Sezione I

Requisiti generali di accessibilità relativi a tutti i prodotti disciplinati dalla presente direttiva ai sensi dell'articolo 2, paragrafo 1

I prodotti devono essere progettati e prodotti in modo da ottimizzarne l'uso prevedibile da parte di persone con disabilità e devono essere accompagnati, se possibile mediante indicazione al loro interno o su di essi, da informazioni accessibili sul loro funzionamento e sulle loro caratteristiche di accessibilità.

1. Requisiti relativi alla fornitura di informazioni:

   a) le informazioni sull'uso del prodotto riportate sul prodotto stesso (etichettatura, istruzioni e avvertenze) devono essere:

      i) rese disponibili attraverso più di un canale sensoriale;

      ii) presentate in modo comprensibile;

      iii) presentate agli utenti in modalità percepibili;

      iv) presentate in caratteri di dimensioni e forme idonee, tenendo conto delle condizioni d'uso prevedibili e usando un contrasto sufficiente nonché una spaziatura regolabile tra lettere, righe e paragrafi;

   b) le istruzioni per l'uso del prodotto, qualora non riportate sul prodotto stesso, ma rese disponibili durante l'uso del prodotto o mediante altri mezzi come un sito web, comprese le funzioni di accessibilità del prodotto, le modalità per la loro attivazione e la loro interoperabilità con le soluzioni assistive, devono essere disponibili pubblicamente quando il prodotto è immesso sul mercato e devono:

      i) essere rese disponibili attraverso più di un canale sensoriale;

      ii) essere presentate in modo comprensibile;

      iii) essere presentate agli utenti in modalità percepibili;

      iv) essere presentate in caratteri di dimensioni e forme idonee, tenendo conto delle condizioni d'uso prevedibili e usando un contrasto sufficiente nonché una spaziatura regolabile tra lettere, righe e paragrafi;

      v) essere rese disponibili, con riferimento al contenuto, in formati testuali utilizzabili per la produzione di formati assistivi alternativi fruibili in modi diversi e attraverso più di un canale sensoriale;

      vi) essere accompagnate da una presentazione alternativa di eventuale contenuto non testuale;

      vii) includere una descrizione dell'interfaccia utente del prodotto (gestione, comando e feedback, input e output), che è fornita conformemente al punto 2; per ognuno dei punti di cui al punto 2 la descrizione deve indicare se il prodotto presenta tali caratteristiche;

      viii) includere una descrizione della funzionalità del prodotto, messa a disposizione con funzioni volte a rispondere alle esigenze delle persone con disabilità conformemente al punto 2; per ognuno dei punti di cui al punto 2 la descrizione deve indicare se il prodotto presenta tali caratteristiche;

      ix) includere una descrizione di come il software e l'hardware del prodotto si interfacciano con i dispositivi assistivi; la descrizione deve includere un elenco dei dispositivi assistivi che sono stati testati unitamente al prodotto.

2. Progettazione interfaccia utente e funzionalità:

   il prodotto, compresa la sua interfaccia utente, presenta caratteristiche, elementi e funzioni che consentono alle persone con disabilità l'accesso, la percezione, l'utilizzo, la comprensione e il comando del prodotto facendo in modo che:

   a) qualora consenta la comunicazione, compresi la comunicazione interpersonale, l'utilizzo, l'informazione, il comando e l'orientamento, il prodotto utilizzi più di un canale sensoriale, anche offrendo alternative ai canali visivo, uditivo, vocale e tattile;

   b) qualora utilizzi il canale vocale, il prodotto renda disponibili alternative alla parola e all'intervento vocale per la comunicazione, l'utilizzo, il comando e l'orientamento;

c) qualora utilizzi elementi visivi, il prodotto renda disponibili ingrandimento, luminosità e contrasto flessibili per la comunicazione, l'informazione e l'utilizzo, oltre a garantire l'interoperabilità con programmi e dispositivi assistivi per navigare nell'interfaccia;

d) qualora utilizzi colori per trasmettere informazioni, indicare un'azione, richiedere una risposta o individuare elementi, il prodotto renda disponibile un'alternativa ai colori;

e) qualora utilizzi segnali acustici per trasmettere informazioni, indicare un'azione, richiedere una risposta o individuare elementi, il prodotto renda disponibile un'alternativa ai segnali acustici;

f) qualora utilizzi elementi visivi, il prodotto renda disponibili modalità flessibili per migliorare la chiarezza dell'immagine;

g) qualora utilizzi l'audio, il prodotto renda disponibili all'utente il controllo del volume e della velocità e migliori caratteristiche audio, comprese la riduzione di segnali acustici provenienti da prodotti nelle vicinanze che fanno interferenza, nonché la chiarezza del suono;

h) qualora richieda un utilizzo e un comando manuali, il prodotto renda disponibili il comando sequenziale e alternative al controllo della motricità fine, evitando i comandi simultanei per la manipolazione, e utilizzi parti riconoscibili al tatto;

i) il prodotto non presenti modalità di funzionamento che richiedono una grande estensione e molta forza;

j) il prodotto non scateni crisi di epilessia fotosensibile;

k) il prodotto tuteli la riservatezza dell'utente durante l'utilizzo delle caratteristiche di accessibilità;

l) il prodotto offra un'alternativa all'identificazione e al comando biometrici;

m) il prodotto garantisca la coerenza della funzionalità e conceda tempo sufficiente e flessibile per l'interazione;

n) il prodotto renda disponibile software e hardware che si interfaccino con i dispositivi assistivi;

o) il prodotto sia conforme ai requisiti settoriali seguenti:

   i) i terminali self-service:

      — offrono la tecnologia di sintesi vocale (text-to-speech);

      — consentono l'utilizzo di cuffie auricolari personali;

      — qualora il tempo di risposta sia limitato, allertano l'utente attraverso più di un canale sensoriale;

      — prevedono la possibilità di prolungare il tempo assegnato;

      — dispongono di un adeguato contrasto e di eventuali tasti e comandi riconoscibili a livello tattile;

      — non prevedono l'attivazione di una caratteristica di accessibilità per permetterne l'accensione all'utente che ne ha bisogno;

      — se il prodotto utilizza audio o segnali acustici, deve essere compatibile con dispositivi e tecnologie assistivi disponibili a livello dell'Unione, comprese le tecnologie uditive quali audioprotesi, telecoil, impianti cocleari e dispositivi assistivi per l'udito;

   ii) i lettori di libri elettronici (e-book) offrono la tecnologia di sintesi vocale (*text-to-speech*);

   iii) le apparecchiature terminali con capacità informatiche interattive per consumatori utilizzate per la fornitura di servizi di comunicazione elettronica:

      — consentono l'elaborazione di testo in tempo reale qualora tali prodotti dispongano della capacità testuale oltre a quella vocale e supportano un audio ad alta fedeltà;

      — consentono, quando dispongono di capacità video in aggiunta a testo e voce o in combinazione con questi ultimi, il ricorso alla conversazione globale, compresi voce sincronizzata, testo in tempo reale e video, con una risoluzione che consenta la comunicazione mediante la lingua dei segni;

      — consentono la connessione senza fili efficace a tecnologie uditive;

      — non interferiscono con i dispositivi assistivi.

iv) le apparecchiature terminali con capacità informatiche interattive per consumatori utilizzate per accedere a servizi di media audiovisivi mettono a disposizione delle persone con disabilità gli elementi di accessibilità offerti dal fornitore di servizi di media audiovisivi per l'accesso, la selezione, il comando e la personalizzazione da parte dell'utente e per la trasmissione ai dispositivi assistivi.

3. Servizi di assistenza:

se disponibili, i servizi di assistenza (sportelli di assistenza, centri di assistenza telefonica, assistenza tecnica, servizi di ritrasmissione e servizi di formazione) forniscono informazioni circa l'accessibilità dei prodotti e la loro compatibilità con le tecnologie assistive, in modi di comunicazione accessibili.

Sezione II

Requisiti di accessibilità relativi a tutti I prodotti di cui all'Articolo 2, paragrafo 1, ad eccezione dei terminali self-service di cui all'Articolo 2, paragrafo 1, lettera b)

In aggiunta ai requsiti della sezione I, l'imballaggio e le istruzioni relativi ai prodotti contemplati dalla presente sezione devono essere resi accessibili, al fine di ottimizzarne l'uso prevedibile da parte di persone con disabilità, devono essere resi accessibili. Ciò implica che:

a) le informazioni sull'imballaggio del prodotto, comprese le informazioni ivi riportate (ad esempio apertura e chiusura, uso, smaltimento) e, se fornite, quelle relative alle caratteristiche di accessibilità del prodotto siano rese accessibili e, ove possibile, tali informazioni accessibili siano siano riportate sull'imballaggio;

b) le istruzioni per l'installazione, la manutenzione, lo stoccaggio e lo smaltimento del prodotto, che non sono rese disponibili sul prodotto stesso ma tramite altri mezzi, quali un sito web, siano rese pubblicamente disponibili quando il prodotto è immesso sul mercato e rispettino i requisiti seguenti:

i) essere disponibili attraverso più di un canale sensoriale;

ii) essere presentate in modo comprensibile;

iii) essere presentate agli utenti in modalità percepibili;

iv) essere presentate in caratteri di dimensioni e forme idonee, tenendo conto delle condizioni d'uso prevedibili e usando un contrasto sufficiente nonché una spaziatura regolabile tra lettere, righe e paragrafi;

v) avere un contenuto disponibile in formati testuali utilizzabili per la produzione di formati assistivi alternativi fruibili in modi diversi e attraverso più di un canale sensoriale, e

vi) ove presentino elementi dal contenuto non testuale, essere accompagnate da una presentazione alternativa di tale contenuto.

Sezione III

Requisiti generali di accessibilità relativi a tutti i servizi disciplinati dalla presente Direttiva ai sensi dell'Articolo 2, paragrafo 2

La fornitura dei servizi, al fine di ottimizzarne l'uso prevedibile da parte di persone con disabilità, deve essere realizzata:

a) garantendo l'accessibilità dei prodotti utilizzati per la fornitura del servizio in conformità della sezione I e, se del caso, della sezione II del presente allegato;

b) fornendo informazioni in merito al funzionamento del servizio e, nel caso in cui siano utilizzati prodotti nella fornitura del servizio, al suo collegamento con tali prodotti nonché informazioni sulle loro caratteristiche di accessibilità e sull'interoperabilità con le strutture e i dispositivi assistivi:

i) rendendo le informazioni disponibili attraverso più di un canale sensoriale;

ii) presentando le informazioni in modo comprensibile;

iii) presentando le informazioni agli utenti in modalità percepibili;

iv) rendendo il contenuto delle informazioni disponibile in formati testuali utilizzabili per la produzione di formati assistivi alternativi fruibili in modi diversi dall'utente e attraverso più di un canale sensoriale;

v) presentando caratteri di dimensioni e forme idonee, tenendo conto delle condizioni d'uso prevedibili e usando un contrasto sufficiente nonché una spaziatura regolabile tra lettere, righe e paragrafi;

vi) integrando eventuale contenuto non testuale con una presentazione alternativa di tale contenuto; e

vii) rendendo disponibili le informazioni elettroniche, necessarie per la fornitura del servizio, in modo coerente e adeguato, facendo in modo che siano percepibili, utilizzabili, comprensibili e solide;

c) rendendo i siti web, comprese le applicazioni online e i servizi per dispositivi mobili correlati - tra cui le applicazioni mobili - accessibili in modo coerente e adeguato, facendo in modo che siano percepibili, utilizzabili, comprensibili e solidi;

d) se disponibili, tramite servizi di assistenza (sportelli di assistenza, centri di assistenza telefonica, assistenza tecnica, servizi di ritrasmissione e servizi di formazione) che forniscono informazioni circa l'accessibilità dei servizi e la loro compatibilità con le tecnologie assistive, in modi di comunicazione accessibili.

Sezione IV

Ulteriori requisiti di accessibilità relativi a servizi specifici

La fornitura dei servizi, al fine di ottimizzarne l'uso prevedibile da parte di persone con disabilità, deve essere realizzata includendo funzioni, prassi, strategie e procedure, nonché modifiche al funzionamento del servizio, mirate a rispondere alle esigenze delle persone con disabilità e a garantire l'interoperabilità con le tecnologie assistive:

a) Servizi di comunicazione elettronica, tra cui le comunicazioni di emergenza di cui all'articolo 109, paragrafo 2, della direttiva (UE) 2018/1972:

i) rendere disponibile un testo in tempo reale oltre alla comunicazione vocale;

ii) consentire la conversazione globale qualora sia offerto il video in aggiunta alla comunicazione vocale;

iii) fare in modo che le comunicazioni di emergenza che utilizzano voce e testo (compreso testo in tempo reale) siano sincronizzate e che, qualora sia offerto il video, siano altresì sincronizzate come conversazione globale e trasmesse dal fornitore del servizio di comunicazione elettronica allo PSAP più idoneo.

b) Servizi che forniscono accesso ai servizi di media audiovisivi:

i) fornire guide elettroniche ai programmi (*electronic programme guides* — EPG) che siano percepibili, utilizzabili, comprensibili e solide e offrano informazioni sulla disponibilità di accessibilità;

ii) fare in modo che gli elementi di accessibilità (servizi di accesso) dei servizi di media audiovisivi, quali i sottotitoli per non udenti e ipoudenti, l'audio-descrizione, i sottotitoli parlati e l'interpretazione in lingua dei segni, siano trasmessi interamente con una qualità adeguata a una visualizzazione precisa e sincronizzati con suono e video, consentendo nel contempo il controllo della loro visualizzazione e del loro utilizzo da parte dell'utente.

c) Servizi di trasporto passeggeri aerei, con autobus, ferroviari e per vie navigabili ad eccezione dei servizi di trasporto urbani ed extraurbani e dei servizi di trasporto regionali:

i) garantire la fornitura di informazioni sull'accessibilità dei veicoli, delle infrastrutture circostanti, e sull'ambiente costruito e sull'assistenza per le persone con disabilità.

ii) garantire la fornitura di informazioni sui sistemi di biglietteria intelligente (prenotazione elettronica, prenotazione di biglietti ecc.), informazioni di viaggio in tempo reale (orari, informazioni su perturbazioni del traffico, servizi di collegamento, connessioni con altri mezzi di trasporto ecc.) e ulteriori informazioni sui servizi (ad esempio, personale delle stazioni, ascensori guasti o servizi temporaneamente indisponibili).

d) Servizi di trasporto urbani ed extraurbani e servizi di trasporto regionali: garantire l'accessibilità dei terminali self-service utilizzati nella fornitura del servizio in conformità della sezione I del presente allegato.

e) Servizi bancari per consumatori:

i) fornire metodi di identificazione, firme elettroniche, sicurezza e servizi di pagamento che siano percepibili, utilizzabili, comprensibili e solidi;

ii) fare in modo che le informazioni siano comprensibili, con un grado di complessità limitato al livello B2 (intermedio avanzato) del Quadro comune europeo di riferimento per le lingue del Consiglio d'Europa.

f) Libri elettronici (e-book):

i) garantire che il libro elettronico, qualora contenga audio in aggiunta al testo, renda disponibili testo e audio sincronizzati;

ii) garantire che i file digitali del libro elettronico non impediscano alla tecnologia assistiva di funzionare correttamente;

iii) garantire l'accesso al contenuto, la navigazione all'interno del contenuto e dell'impostazione grafica del file, compresa l'impostazione grafica dinamica, l'offerta di struttura, flessibilità e possibilità di scelta nella presentazione del contenuto.

iv) consentire riproduzioni alternative del contenuto e la sua interoperabilità con una serie di tecnologie assistive in modo che esso sia percepibile, utilizzabile, comprensibile e solido;

v) consentirne la scoperta fornendo informazioni mediante metadati sulle loro caratteristiche di accessibilità;

vi) garantire che le misure relative alla gestione dei diritti digitali (DRM) non blocchino le caratteristiche di accessibilità.

g) Servizi di commercio elettronico:

i) fornire le informazioni riguardanti l'accessibilità dei prodotti e dei servizi venduti qualora tali informazioni siano fornite dall'operatore economico responsabile;

ii) garantire l'accessibilità della funzionalità per l'identificazione, la sicurezza e il pagamento qualora sia fornita come parte del servizio anziché di un prodotto, rendendola percepibile, utilizzabile, comprensibile e solida;

iii) fornire metodi di identificazione, firme elettroniche e servizi di pagamento che siano percepibili, utilizzabili, comprensibili e solidi.

Sezione V

Specifici requisiti di accessibilità relativi alla raccolta delle comunicazioni di emergenza effettuate verso il numero unico di emergenza Europeo «112» da parte dello PSAP più idoneo

Al fine di ottimizzarne l'uso prevedibile da parte di persone con disabilità, la raccolta delle comunicazioni di emergenza effettuate verso il numero unico di emergenza europeo «112» da parte dello PSAP più idoneo è realizzata includendo funzioni, prassi, strategie, procedure e modifiche mirate a rispondere alle esigenze delle persone con disabilità.

Le comunicazioni di emergenza effettuate verso il numero unico di emergenza europeo «112» ricevono adeguata risposta, nel modo che più si adatta all'organizzazione nazionale dei sistemi di emergenza, presso lo PSAP più idoneo, utilizzando gli stessi mezzi di comunicazione utilizzati dal richiedente, vale a dire mediante voce sincronizzata e testo (compreso testo in tempo reale), o, qualora sia offerto il video, voce, testo (compreso testo in tempo reale) e video sincronizzati come conversazione globale.

Sezione VI

Requisiti di accessibilità relativi a caratteristiche, elementi o funzioni di prodotti e servizi ai sensi dell'Articolo 24, paragrafo 2

La presunzione di conformità ai pertinenti obblighi stabiliti in altri atti dell'Unione per quanto riguarda le caratteristiche, gli elementi o le funzioni dei prodotti e dei servizi prevede i requisiti seguenti:

1. Prodotti:

a) l'accessibilità delle informazioni riguardanti il funzionamento e le caratteristiche di accessibilità relative ai prodotti è conforme agli elementi corrispondenti di cui alla sezione I, punto 1, del presente allegato, vale a dire le informazioni sull'uso del prodotto riportate sul prodotto stesso e le istruzioni per l'uso del prodotto non riportate sul prodotto stesso ma rese disponibili durante l'uso del prodotto o mediante altri mezzi come un sito web;

b) l'accessibilità delle caratteristiche, degli elementi e delle funzioni della progettazione dell'interfaccia utente e della funzionalità dei prodotti è conforme ai corrispondenti requisiti di accessibilità di tale progettazione dell'interfaccia utente o della funzionalità, ai sensi della sezione I, punto 2, del presente allegato;

c) l'accessibilità dell'imballaggio, comprese le informazioni ivi indicate e le istruzioni ai fini dell'installazione, della manutenzione, dello stoccaggio e dello smaltimento del prodotto che non sono riportate sul prodotto stesso ma rese disponibili attraverso altri mezzi come un sito web, ad eccezione dei terminali self-service, è conforme ai corrispondenti requisiti di accessibilità di cui alla sezione II del presente allegato.

2. Servizi:

l'accessibilità delle caratteristiche, degli elementi e delle funzioni dei servizi è conforme ai corrispondenti requisiti di accessibilità per tali caratteristiche, elementi e funzioni indicati nelle sezioni relative ai servizi del presente allegato.

Sezione VII

Criteri funzionali di prestazione

Al fine di ottimizzare l'uso prevedibile da parte di persone con disabilità, qualora i requisiti di accessibilità di cui alle sezioni da I a VI del presente allegato non riguardino una o più funzioni della progettazione e della produzione dei prodotti o della fornitura di servizi, tali funzioni o mezzi sono resi accessibili in linea con i relativi criteri funzionali di prestazione.

Se i requisiti di accessibilità includono requisiti tecnici specifici, è possibile applicare i criteri funzionali di prestazione in alternativa a uno o più requisiti tecnici specifici solo ed esclusivamente se l'applicazione dei criteri funzionali di prestazione pertinenti è conforme ai requisiti di accessibilità ed è stabilito che la progettazione e la produzione dei prodotti e la fornitura dei servizi comportano un livello di accessibilità equivalente o superiore con riguardo all'uso prevedibile da parte di persone con disabilità.

a) Utilizzo non visivo

Qualora offra modalità di funzionamento visive, il prodotto o servizio prevede almeno una modalità di funzionamento che non richieda la vista.

b) Utilizzo con una visione limitata

Qualora offra modalità di funzionamento visive, il prodotto o servizio prevede almeno una modalità di funzionamento che consenta agli utenti ipovedenti di utilizzare il prodotto.

c) Utilizzo senza percezione di colore

Qualora offra modalità di funzionamento visive, il prodotto o servizio prevede almeno una modalità di funzionamento che non richieda la percezione del colore da parte dell'utente.

d) Utilizzo non uditivo

Qualora offra modalità di funzionamento uditive, il prodotto o servizio prevede almeno una modalità di funzionamento che non richieda l'udito.

e) Utilizzo con ascolto limitato

Qualora offra modalità di funzionamento uditive, il prodotto o servizio prevede almeno una modalità di funzionamento con caratteristiche audio migliorate che consenta all'utente con ridotta capacità uditiva di far funzionare il prodotto.

f) Utilizzo senza capacità vocale

Qualora richieda un intervento vocale da parte dell'utente, il prodotto o servizio prevede almeno una modalità di funzionamento che non lo richieda. Un intervento vocale include qualsiasi tipo di suono orale quali parole, fischi o clic.

g) Utilizzo con manipolazione o sforzo limitati

Qualora richieda interventi manuali, il prodotto o servizio prevede almeno una modalità di funzionamento che consenta agli utenti di utilizzare il prodotto tramite modalità alternative di funzionamento che non richiedano il controllo della motricità fine, la manipolazione, la forza della mano o il funzionamento di più di un controllo contemporaneamente.

h) Utilizzo con ampiezza di movimento limitata

Gli elementi funzionali dei prodotti devono essere alla portata di tutti gli utenti. Qualora offra modalità di funzionamento manuali, il prodotto o servizio prevede almeno una modalità di funzionamento accessibile agli utenti con forza limitata e difficoltà nei movimenti ampi.

i) Riduzione al minimo del rischio di scatenare crisi di epilessia fotosensibile

Qualora offra modalità di funzionamento visive, il prodotto evita modalità di funzionamento che possano scatenare crisi di epilessia fotosensibile.

j) Utilizzo con capacità cognitive limitate

Il prodotto o servizio prevede almeno una modalità di funzionamento con funzionalità che ne semplifichino e ne facilitino l'utilizzo.

k) Riservatezza

Qualora includa funzionalità che garantiscono l'accessibilità, il prodotto o servizio prevede almeno una modalità di funzionamento che tuteli la riservatezza al momento dell'utilizzo di dette funzionalità.

ALLEGATO II

ESEMPI INDICATIVI NON VINCOLANTI DI POSSIBILI SOLUZIONI CHE CONTRIBUISCONO A SODDISFARE I REQUISITI DI ACCESSIBILITÀ DI CUI ALL'ALLEGATO I

SEZIONE I:

ESEMPI DI REQUISITI GENERALI DI ACCESSIBILITÀ RELATIVI A TUTTI I PRODOTTI DISCIPLINATI DALLA PRESENTE DIRETTIVA AI SENSI DELL'ARTICOLO 2, PARAGRAFO 1

REQUISITI DI CUI ALLA SEZIONE I DELL'ALLEGATO I	ESEMPI
1. Fornitura di informazioni	
a)	
i)	Fornire informazioni visive e tattili oppure visive e uditive indicanti il luogo in cui introdurre una carta in un terminale self-service, affinché il terminale possa essere usato da non vedenti e non udenti.
ii)	Utilizzare le stesse parole in modo coerente o secondo una struttura chiara e logica, affinché possano essere comprese meglio da persone con disabilità intellettuali.
iii)	Fornire informazioni in formato a rilievo tattile oppure sonoro oltre a un testo di avvertenza, affinché i non vedenti possano comprenderle.
iv)	Rendere possibile la lettura di un testo da parte di persone con disabilità visive.
b)	
i)	Fornire file elettronici leggibili da un computer mediante software di lettura dello schermo, affinché i non vedenti possano utilizzare le informazioni.
ii)	Utilizzare le stesse parole in modo coerente o secondo una struttura chiara e logica, affinché possano essere comprese meglio da persone con disabilità intellettuali.
iii)	Mettere a disposizione sottotitoli qualora siano fornite istruzioni video.
iv)	Rendere possibile la lettura di un testo da parte di persone con disabilità visive.
v)	Fornire la stampa in Braille, affinché un non vedente possa utilizzare le informazioni.
vi)	Integrare un diagramma con una descrizione testuale che identifichi gli elementi principali o descriva le azioni principali.
vii)	Nessun esempio
viii)	Nessun esempio
ix)	Integrare in uno sportello automatico di banca una presa e un software che consentano l'inserimento di cuffie auricolari tramite le quali ricevere sotto forma di suoni il testo visibile a schermo.

2. Progettazione dell'interfaccia utente e della funzionalità	
a)	Fornire istruzioni sotto forma di voce o testo oppure integrando segnali tattili in un tastierino per consentire ai non vedenti o ipoudenti di interagire con il prodotto.
b)	In un terminale self-service, fornire istruzioni, in aggiunta a quelle vocali, ad esempio sotto forma di testo o immagini per consentire ai non udenti di eseguire l'azione richiesta.
c)	Consentire agli utenti di ingrandire il testo, di zumare su uno specifico pittogramma o di aumentare il contrasto affinché le persone con disabilità visive possano ricevere l'informazione.
d)	Oltre a consentire di scegliere se premere il tasto verde o quello rosso per selezionare un'opzione, indicare sui tasti le opzioni disponibili affinché le persone daltoniche possano operare la scelta.
e)	Quando un computer emette un segnale di errore, fornire un testo scritto o un'immagine indicante l'errore, per consentire ai non udenti di accorgersi dell'errore.
f)	Consentire un maggiore contrasto nelle immagini dinamiche affinché le persone ipovedenti possano vederle.
g)	Consentire all'utente di un telefono di selezionare il volume del suono e di ridurre l'interferenza con le audioprotesi affinché le persone ipoudenti possano utilizzare il telefono.
h)	Ingrandire i tasti degli schermi tattili e distanziarli tra loro, affinché possano essere premuti da persone affette da tremore.
i)	Garantire che i tasti da premere non richiedano molta forza, affinché possano essere usati da persone con disabilità motorie.
j)	Evitare lo sfarfallamento delle immagini, così da non mettere a rischio le persone suscettibili di crisi epilettiche.
k)	Consentire l'utilizzo di cuffie auricolari quando uno sportello automatico di banca fornisce informazioni a voce.
l)	In alternativa al riconoscimento delle impronte digitali, consentire agli utenti che non possono usare le mani di selezionare una password per bloccare o sbloccare un telefono.
m)	Garantire che il software reagisca in modo prevedibile quando si esegue una specifica azione e accordando tempo sufficiente per inserire una password, affinché sia di facile uso per le persone con disabilità intellettuali.
n)	Fornire un collegamento a uno schermo Braille aggiornabile affinché i non vedenti possano utilizzare il computer.
o)	Esempi di requisiti settoriali
i)	Nessun esempio
ii)	Nessun esempio
iii) Primo trattino	Rendere un telefono cellulare in grado di elaborare conversazioni in tempo reale, affinché le persone ipoudenti possano scambiare informazioni in modo interattivo.
iii) quarto trattino	Consentire l'uso contemporaneo di video per mostrare la lingua dei segni e il testo per scrivere un messaggio, affinché due non udenti possano comunicare tra loro oppure con una persona normoudente.

iv)	Garantire che i sottotitoli siano trasmessi dal set-top box affinché siano utilizzati dai non udenti.

3. Servizi di sostegno: Nessun esempio

SEZIONE II:

ESEMPI DI REQUISITI DI ACCESSIBILITÀ RELATIVI A TUTTI I PRODOTTI DI Ci ALL'ARTICOLO 2, PARAGRAFO 1, AD ECCEZIONE DEI TERMINALI SELF-SERVICE DI CUI ALL'ARTICOLO 2, PARGRAFO 1, LETTERA b)

REQUISITI DI CUI ALLA SEZIONE II DELL'ALLEGATO I	ESEMPI
Imballaggio e istruzioni relativi ai prodotti	
a)	Indicare sull'imballaggio che il telefono è dotato di caratteristiche di accessibilità per le persone con disabilità.
b)	
i)	Fornire file elettronici leggibili da un computer mediante software di lettura dello schermo, affinché i non vedenti possano utilizzare le informazioni.
ii)	Utilizzare le stesse parole in modo coerente o secondo una struttura chiara e logica, affinché possano essere comprese meglio da persone con disabilità intellettuali.
iii)	Fornire informazioni in formato a rilievo tattile oppure sonoro accanto a un testo di avvertenza, affinché i non vedenti possano comprenderlo.
iv)	Rendere possibile la lettura di un testo da parte di persone con disabilità visive.
v)	Fornire la stampa in Braille, affinché un non vedente possa leggere le informazioni.
vi)	Integrare un diagramma con una descrizione testuale che identifichi gli elementi principali o descriva le azioni principali.

SEZIONE III:

ESEMPI DI REQUISITI GENERALI DI ACCESSIBILITÀ RELATIVI A TUTTI I SERVIZI DISCIPLINATI DALLA PRESENTE DIRETTIVA AI SENSI DELL'ARTICOLO 2, PARAGRAFO 2

REQUISITI DI CUI ALLA SEZIONE III DELL'ALLEGATO I	ESEMPI
Fornitura di servizi	
a)	Nessun esempio
b)	
i)	Fornire file elettronici leggibili da un computer mediante software di lettura dello schermo, affinché i non vedenti possano utilizzare le informazioni.
ii)	Utilizzare le stesse parole in modo coerente o secondo una struttura chiara e logica, affinché possano essere comprese meglio da persone con disabilità intellettuali.
iii)	Mettere a disposizione sottotitoli qualora siano fornite istruzioni video.

iv)	Consentire a un non vedente di usare un file stampandolo in Braille.
v)	Rendere possibile la lettura di un testo da parte di persone con disabilità visive.
vi)	Integrare un diagramma con una descrizione testuale che identifichi gli elementi principali o descriva le azioni principali.
vii)	Se un prestatore di servizi offre una chiavetta USB contenente informazioni sul servizio, rendere accessibili tali informazioni.
c)	Fornire una descrizione testuale delle immagini, rendendo tutte le funzionalità disponibili tramite tastiera, lasciando tempo sufficiente per leggere, facendo in modo che il contenuto appaia e operi in modo prevedibile, e garantire la compatibilità con le tecnologie assistive, affinché persone con disabilità diverse possano leggere e interagire con un sito web.
d)	Nessun esempio

SEZIONE IV:

ESEMPI DI ULTERIORI REQUISITI DI ACCESSIBILITÀ PER SERVIZI SPECIFICI

REQUISITI DI CUI ALLA SEZIONE IV DELL'ALLEGATO I	ESEMPI
Servizi specifici	
a)	
i)	Consentire a una persona ipoudente di scrivere e ricevere un testo in modo interattivo e in tempo reale.
ii)	Consentire ai non udenti di usare la lingua dei segni per comunicare tra loro.
iii)	Consentire a chi ha un disturbo del linguaggio o dell'udito e sceglie di ricorrere a una combinazione di testo, voce e video di sapere che la comunicazione è trasmessa tramite rete a un servizio di emergenza.
b)	
i)	Consentire a un non vedente di selezionare programmi alla televisione.
ii)	Supportare la possibilità di selezionare, personalizzare e visualizzare i «servizi di accesso» quali sottotitoli per non udenti o ipoudenti, audiodescrizione, sottotitoli parlati e interpretazione in lingua dei segni, fornendo strumenti di connessione senza fili efficace a tecnologie uditive o fornendo agli utenti dispositivi di comando per attivare i «servizi di accesso» ai servizi di media audiovisivi allo stesso livello dei comandi dei media primari.
c)	
i)	Nessun esempio
ii)	Nessun esempio
d)	Nessun esempio
e)	
i)	Rendere i dialoghi di identificazione su schermo leggibili da software di lettura dello schermo affinché possano essere usati dai non vedenti.

ii)	Nessun esempio
f)	
i)	Consentire a una persona dislessica di leggere e contemporaneamente ascoltare il testo.
ii)	Consentire la fornitura di testo e audio sincronizzati o una trascrizione in Braille aggiornabile.
iii)	Consentire a un non vedente di accedere al sommario o cambiare capitolo.
iv)	Nessun esempio
v)	Garantire che il file elettronico contenga informazioni sulle relative caratteristiche di accessibilità, in modo che le persone con disabilità possano esserne informate.
vi)	Garantire che non vi sia blocco, ad esempio che misure tecniche di protezione, informazioni sul regime dei diritti o questioni di interoperabilità non impediscano la lettura ad alta voce del testo ad opera di dispositivi assistivi, in modo tale che gli utenti non vedenti possano leggere il libro.
g)	
i)	Garantire che le informazioni disponibili sulle caratteristiche di accessibilità di un prodotto non siano cancellate.
ii)	Rendere l'interfaccia utente per il servizio di pagamento disponibile a voce, affinché i non vedenti possano effettuare acquisti online in modo indipendente.
iii)	Rendere i dialoghi di identificazione su schermo leggibili da software di lettura dello schermo affinché possano essere usati dai non vedenti.

ALLEGATO III

REQUISITI DI ACCESSIBILITÀ AI FINI DELL'ARTICOLO 4, PARAGRAFO 4, PER QUANTO RIGUARDA L'AMBIENTE COSTRUITO IN CUI SIANO PRESTATI I SERVIZI CHE RIENTRANO NELL'AMBITO DI APPLICAZIONE DELLA PRESENTE DIRETTIVA

Al fine di massimizzare l'uso prevedibile in modo indipendente da parte di persone con disabilità dell'ambiente costruito in cui è fornito il servizio e che è sotto la responsabilità del fornitore di servizi, ai sensi dell'articolo 4, paragrafo 4, l'accessibilità delle zone destinate all'accesso del pubblico deve comprendere gli aspetti seguenti:

a) utilizzo delle relative aree e strutture esterne;

b) percorsi di avvicinamento agli edifici;

c) utilizzo degli accessi;

d) utilizzo dei percorsi di circolazione orizzontale;

e) utilizzo dei percorsi di circolazione verticale;

f) utilizzo delle sale da parte del pubblico;

g) utilizzo delle attrezzature e delle strutture impiegate nella prestazione del servizio;

h) utilizzo dei servizi igienico-sanitari;

i) utilizzo delle uscite, delle vie d'evacuazione e dei concetti della pianificazione delle emergenze;

j) comunicazione e orientamento attraverso più di un canale sensoriale;

k) utilizzo delle strutture e degli edifici per lo scopo previsto;

l) protezione dai rischi ambientali interni ed esterni.

ALLEGATO IV

PROCEDURA DI VALUTAZIONE DELLA CONFORMITÀ - PRODOTTI

1. Controllo interno della produzione

Il controllo interno della produzione è la procedura di valutazione della conformità con cui il fabbricante ottempera agli obblighi di cui ai punti 2, 3 e 4 del presente allegato e garantisce e dichiara, sotto la sua esclusiva responsabilità, che il prodotto interessato soddisfa i pertinenti requisiti della presente direttiva.

2. Documentazione tecnica

Il fabbricante compila la documentazione tecnica. Tale documentazione tecnica consente di valutare la conformità del prodotto ai pertinenti requisiti di accessibilità di cui all'articolo 4 e, nel caso in cui il fabbricante si sia avvalso dell'articolo 14, di dimostrare che i pertinenti requisiti di accessibilità introdurrebbero una modifica sostanziale o imporrebbero un onere sproporzionato. La documentazione tecnica deve specificare solo i requisiti applicabili e illustrare, se necessario ai fini della valutazione, il progetto, la fabbricazione e il funzionamento del prodotto.

La documentazione tecnica deve contenere, laddove applicabile, almeno gli elementi seguenti:

a) una descrizione generale del prodotto;

b) un elenco delle norme armonizzate e di altre specifiche tecniche, i cui riferimenti siano stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, applicate completamente o in parte, e descrizioni delle soluzioni adottate per soddisfare i pertinenti requisiti di accessibilità di cui all'articolo 4 qualora tali norme armonizzate o specifiche tecniche non siano state applicate. In caso di applicazione parziale delle norme armonizzate o delle specifiche tecniche, la documentazione tecnica specifica le parti che sono state applicate.

3. Fabbricazione

Il fabbricante prende i provvedimenti necessari affinché il processo di fabbricazione e di controllo garantisca la conformità dei prodotti alla documentazione tecnica di cui al punto 2 del presente allegato e ai requisiti di accessibilità della presente direttiva.

4. Marcatura CE e dichiarazione di conformità UE

4.1. Il fabbricante appone la marcatura CE di cui alla presente direttiva a ogni singolo prodotto che soddisfa i requisiti applicabili della presente direttiva.

4.2. Il fabbricante compila una dichiarazione scritta di conformità UE per un modello del prodotto. La dichiarazione di conformità UE identifica il prodotto per il quale è stata redatta.

Una copia della dichiarazione di conformità UE è messa a disposizione delle autorità competenti su richiesta.

5. Rappresentante autorizzato

Gli obblighi del fabbricante di cui al punto 4 possono essere adempiuti dal suo rappresentante autorizzato, per suo conto e sotto la sua responsabilità, purché siano specificati nel mandato.

ALLEGATO V

INFORMAZIONI SUI SERVIZI CHE SODDISFANO I REQUISITI DI ACCESSIBILITÀ

1. Il fornitore di servizi include nelle condizioni generali, o in un documento equivalente, informazioni sulla valutazione di come il servizio soddisfi i requisiti di accessibilità di cui all'articolo 4. Tali informazioni precisano i requisiti applicabili e includono, se necessario ai fini della valutazione, il progetto e il funzionamento del servizio. Oltre agli obblighi di informazione per i consumatori di cui alla direttiva 2011/83/UE, le informazioni contengono, laddove applicabile, gli elementi seguenti:

   a) una descrizione generale del servizio in formati accessibili;

   b) descrizioni e spiegazioni necessarie alla comprensione del funzionamento del servizio;

   c) una descrizione del modo in cui il servizio soddisfa i pertinenti requisiti di accessibilità di cui all'allegato I.

2. Per conformarsi al punto 1 del presente allegato il fornitore di servizi può applicare in tutto o in parte le norme armonizzate e altre specifiche tecniche, i cui riferimenti siano stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*.

3. Il fornitore di servizi fornisce le informazioni che dimostrano che il processo di fornitura del servizio e il relativo monitoraggio garantiscono la conformità del servizio al punto 1 del presente allegato e ai requisiti applicabili della presente direttiva.

ALLEGATO VI

CRITERI PER LA VALUTAZIONE DEL CARATTERE SPROPORZIONATO DELL'ONERE

Criteri per l'effettuazione e la documentazione della valutazione:

1. Rapporto tra i costi netti dell'ottemperanza ai requisiti di accessibilità e i costi totali (spese operative e spese in conto capitale) della fabbricazione, distribuzione o importazione del prodotto o della fornitura del servizio per gli operatori economici.

   Elementi da utilizzare per valutare i costi netti della conformità ai requisiti di accessibilità:

   a) criteri relativi alle spese una tantum di organizzazione di cui tenere conto nella valutazione:

      i) spese connesse a risorse umane aggiuntive con competenze in materia di accessibilità;

      ii) spese connesse alla formazione delle risorse umane e all'acquisizione di competenze in materia di accessibilità;

      iii) spese per lo sviluppo di nuovi processi al fine di includere l'accessibilità nello sviluppo del prodotto o nella fornitura del servizio;

      iv) spese connesse allo sviluppo di materiale esplicativo in materia di accessibilità;

      v) spese una tantum per conoscere la legislazione in materia di accessibilità;

   b) criteri connessi alle spese correnti di produzione e sviluppo di cui tenere conto nella valutazione:

      i) spese connesse alla progettazione delle caratteristiche di accessibilità del prodotto o servizio

      ii) spese sostenute durante i processi di fabbricazione

      iii) spese connesse ai test di accessibilità per i prodotti o servizi

      iv) spese connesse alla realizzazione della documentazione.

2. Stima dei costi e dei benefici per gli operatori economici, ivi compresi i processi di produzione e gli investimenti, rispetto al beneficio previsto per le persone con disabilità, tenendo conto del numero e della frequenza d'uso del prodotto o servizio specifico.

3. Rapporto tra i costi netti della conformità ai requisiti di accessibilità e fatturato netto dell'operatore economico.

   Elementi da utilizzare per valutare i costi netti della conformità ai requisiti di accessibilità:

   a) criteri relativi alle spese una tantum di organizzazione di cui tenere conto nella valutazione:

      i) spese connesse a risorse umane aggiuntive con competenze in materia di accessibilità

      ii) spese connesse alla formazione delle risorse umane e all'acquisizione di competenze in materia di accessibilità

      iii) spese per lo sviluppo di nuovi processi al fine di includere l'accessibilità nello sviluppo del prodotto o nella fornitura del servizio

      iv) spese connesse allo sviluppo di materiale esplicativo in materia di accessibilità

      v) spese una tantum per conoscere la legislazione in materia di accessibilità

   b) criteri connessi alle spese correnti di produzione e sviluppo di cui tenere conto nella valutazione:

      i) spese connesse alla progettazione delle caratteristiche di accessibilità del prodotto o servizio;

      ii) spese sostenute durante i processi di fabbricazione;

      iii) spese connesse ai test di accessibilità per i prodotti o servizi;

      iv) spese connesse alla realizzazione della documentazione.

DIRETTIVA (UE) 2019/883 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019

relativa agli impianti portuali di raccolta per il conferimento dei rifiuti delle navi, che modifica la direttiva 2010/65/UE e abroga la direttiva 2000/59/CE

(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 100, paragrafo 2,

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 ([1]),

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) La politica marittima dell'Unione mira a conseguire un elevato livello di sicurezza e protezione dell'ambiente. Questo obiettivo si può raggiungere attraverso il rispetto delle convenzioni, dei codici e delle risoluzioni internazionali, mantenendo nel contempo la libertà di navigazione prevista dalla Convenzione delle Nazioni Unite sul diritto del mare («UNCLOS»).

(2) L'obiettivo di sviluppo sostenibile n. 14 delle Nazioni Unite richiama l'attenzione sulle minacce rappresentate dall'inquinamento marino e da quello da sostanze eutrofizzanti, dall'esaurimento delle risorse e dai cambiamenti climatici, tutte principalmente dovute alle azioni umane. Tali minacce esercitano un'ulteriore pressione sui sistemi ambientali quali la biodiversità e l'infrastruttura naturale, creando nel contempo problemi socioeconomici globali, compresi rischi per la salute e la sicurezza e rischi finanziari. L'Unione deve adoperarsi per proteggere le specie marine e sostenere le persone che dipendono dagli oceani in termini di occupazione, risorse o attività ricreative.

(3) La convenzione internazionale per la prevenzione dell'inquinamento causato da navi («convenzione MARPOL») stabilisce i divieti generali relativi agli scarichi delle navi in mare, ma disciplina altresì le condizioni alle quali alcuni tipi di rifiuti possono essere scaricati nell'ambiente marino. La convenzione MARPOL prescrive che le parti contraenti garantiscano la fornitura di adeguati impianti portuali di raccolta.

(4) L'Unione ha proseguito l'attuazione di alcune parti della convenzione MARPOL mediante la direttiva 2000/59/CE del Parlamento europeo e del Consiglio ([4]), seguendo un approccio portuale. La direttiva 2000/59/CE mira a conciliare gli interessi del buon funzionamento del trasporto marittimo con la tutela dell'ambiente marino.

(5) Negli ultimi vent'anni la convenzione MARPOL e i relativi allegati sono stati oggetto di importanti modifiche che hanno posto in essere norme e divieti più severi per gli scarichi in mare dei rifiuti delle navi.

(6) L'allegato VI della convenzione MARPOL ha introdotto norme relative allo scarico di nuove categorie di rifiuti, in particolare i residui dei sistemi di depurazione dei gas di scarico, costituiti da fanghi e acque di lavaggio. Tali categorie di rifiuti dovrebbero essere incluse nell'ambito di applicazione della presente direttiva.

([1]) GU C 283 del 10.8.2018, pag. 61.
([2]) GU C 461 del 21.12.2018, pag. 220.
([3]) Posizione del Parlamento europeo del 13 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.
([4]) Direttiva 2000/59/CE del Parlamento europeo e del Consiglio, del 27 novembre 2000, relativa agli impianti portuali di raccolta per i rifiuti prodotti dalle navi e i residui del carico (GU L 332 del 28.12.2000, pag. 81).

(7) Gli Stati membri dovrebbero continuare ad adoperarsi a livello dell'Organizzazione marittima internazionale («IMO») per giungere a una considerazione complessiva dell'impatto ambientale generato dagli scarichi delle acque reflue degli scrubber a circuito aperto, comprese misure per contrastare potenziali impatti.

(8) È opportuno incoraggiare gli Stati membri ad adottare misure appropriate, conformemente alla direttiva 2000/60/CE del Parlamento europeo e del Consiglio ([5]), compresi divieti di scarico delle acque reflue degli scrubber a circuito aperto e di taluni residui del carico nelle rispettive acque territoriali.

(9) Il 1º marzo 2018 l'IMO ha adottato la guida consolidata rivista per i gestori e gli utenti degli impianti portuali di raccolta (MEPC.1/Circ. 834/Rev.1) («guida consolidata IMO»), che comprende formati standard per la notifica dei rifiuti, per la ricevuta di conferimento dei rifiuti e per la segnalazione di presunte inadeguatezze rilevate negli impianti portuali di raccolta, nonché i requisiti di segnalazione degli impianti di raccolta dei rifiuti.

(10) Nonostante tali sviluppi normativi, gli scarichi dei rifiuti in mare continuano a verificarsi, comportando costi ambientali, sociali ed economici significativi. Ciò è dovuto a una combinazione di fattori, tra cui l'assenza in alcuni porti di impianti portuali di raccolta adeguati, un'applicazione spesso insufficiente della normativa e la mancanza di incentivi al conferimento dei rifiuti a terra.

(11) La direttiva 2000/59/CE ha contribuito ad aumentare il volume dei rifiuti conferiti agli impianti portuali di raccolta, assicurando tra l'altro che le navi contribuiscano ai costi di tali impianti, indipendentemente dal loro effettivo utilizzo, svolgendo in tal modo un ruolo determinante nella riduzione degli scarichi in mare, come evidenziato nella valutazione della suddetta direttiva effettuata nel quadro del programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione («valutazione REFIT»).

(12) La valutazione REFIT ha dimostrato inoltre che la direttiva 2000/59/CE non è stata pienamente efficace a causa di incoerenze con il quadro della convenzione MARPOL. Gli Stati membri hanno altresì elaborato interpretazioni diverse dei concetti essenziali di tale direttiva, quali l'adeguatezza degli impianti, la notifica anticipata dei rifiuti, l'obbligo di conferimento dei rifiuti agli impianti portuali di raccolta e le esenzioni per le navi in servizio di linea. La valutazione REFIT ha evidenziato la necessità di una maggiore armonizzazione di tali concetti e del pieno allineamento con la convenzione MARPOL, al fine di evitare inutili oneri amministrativi sia per i porti sia per gli utenti degli stessi.

(13) Al fine di allineare la direttiva 2005/35/CE del Parlamento europeo e del Consiglio ([6]) alle pertinenti disposizioni della convenzione MARPOL relative alle norme in materia di scarico, la Commissione dovrebbe valutare l'opportunità di rivedere la suddetta direttiva, in particolare mediante un'estensione del suo ambito di applicazione.

(14) La politica marittima dell'Unione dovrebbe mirare a conseguire un elevato livello di protezione dell'ambiente marino, tenendo conto della diversità delle zone marittime dell'Unione. Tale politica dovrebbe fondarsi sui principi di prevenzione, eliminazione alla fonte dei danni causati all'ambiente marino, nonché sul principio «chi inquina paga».

(15) La presente direttiva dovrebbe essere fondamentale per l'applicazione dei principali fondamenti normativi in campo ambientale nel contesto dei porti e della gestione dei rifiuti delle navi. In particolare, sono adeguati strumenti le direttive 2008/56/CE ([7]) e 2008/98/CE ([8]).

(16) La direttiva 2008/98/CE stabilisce i principi più importanti per la gestione dei rifiuti, compresi il principio «chi inquina paga» e la gerarchia dei rifiuti, che privilegia il riutilizzo e il riciclaggio rispetto ad altre forme di recupero e smaltimento e richiede l'istituzione di sistemi per la raccolta differenziata dei rifiuti. Inoltre, il concetto di responsabilità estesa del produttore è un principio guida del diritto dell'Unione in materia di rifiuti, in base al quale i produttori sono responsabili degli impatti ambientali dei loro prodotti per tutto il loro ciclo di vita. Tali obblighi si applicano anche alla gestione dei rifiuti delle navi.

([5]) Direttiva 2000/60/CE del Parlamento europeo e del Consiglio, del 23 ottobre 2000, che istituisce un quadro per l'azione comunitaria in materia di acque (GU L 327 del 22.12.2000, pag. 1).

([6]) Direttiva 2005/35/CE del Parlamento europeo e del Consiglio, del 7 settembre 2005, relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni, anche penali, per i reati di inquinamento (GU L 255 del 30.9.2005, pag. 11).

([7]) Direttiva 2008/56/CE del Parlamento europeo e del Consiglio, del 17 giugno 2008, che istituisce un quadro per l'azione comunitaria nel campo della politica per l'ambiente marino (direttiva quadro sulla strategia per l'ambiente marino) (GU L 164 del 25.6.2008, pag. 19).

([8]) 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).

(17) La raccolta differenziata dei rifiuti delle navi, compresi le reti da pesca in disuso, è necessaria per garantirne un ulteriore recupero per consentire che siano preparati per il riutilizzo o il riciclaggio nella catena di gestione dei rifiuti a valle e per evitare che provochino danni agli animali e agli ambienti marini. I rifiuti spesso sono separati a bordo delle navi in conformità delle norme e degli standard internazionale e il diritto dell'Unione dovrebbe garantire che gli sforzi per separare i rifiuti a bordo non siano pregiudicati dalla mancanza di organizzazione per la raccolta differenziata a terra.

(18) Ogni anno un ingente quantitativo di plastica finisce nei mari e negli oceani nell'Unione. Sebbene, in gran parte delle zone marittime, la maggior parte dei rifiuti marini è generata da attività a terra, anche il trasporto marittimo, compresi i settori della pesca e della navigazione da diporto, contribuisce in misura importante, scaricando rifiuti quali plastiche e reti da pesca in disuso, che finiscono direttamente in mare.

(19) La direttiva 2008/98/CE invita gli Stati membri a fermare la produzione di rifiuti marini come contributo all'obiettivo di sviluppo sostenibile delle Nazioni Unite di prevenire e ridurre in modo significativo l'inquinamento marino di tutti i tipi.

(20) La comunicazione della Commissione del 2 dicembre 2015, dal titolo «L'anello mancante — Piano d'azione dell'Unione europea per l'economia circolare», aveva riconosciuto, in tale contesto, il ruolo specifico della direttiva 2000/59/CE, garantendo la disponibilità di impianti adeguati per la raccolta dei rifiuti solidi e provvedendo al giusto livello di incentivi e di misure esecutive per il conferimento dei rifiuti agli impianti a terra.

(21) Gli impianti in mare costituiscono una delle fonti di inquinamento marino. Per tale ragione gli Stati membri dovrebbero adottare, ove opportuno, misure sul conferimento dei rifiuti da impianti in mare battenti la loro bandiera o che operano nelle loro acque o entrambi, nonché assicurare il rispetto rigoroso delle norme previste dalla convenzione MARPOL in materia di scarico, applicabili agli impianti in mare.

(22) I rifiuti, in particolare quelli da materie plastiche, provenienti dai fiumi, compresi gli scarichi delle navi adibite alla navigazione interna, sono fra i principali responsabili dell'inquinamento marino. Dette navi dovrebbero pertanto essere soggette a norme rigorose in materia di scarico e conferimento. Oggi, tali norme sono stabilite dalla commissione fluviale pertinente. Ai porti di navigazione interna si applica tuttavia il diritto dell'Unione in materia di rifiuti. Per proseguire gli sforzi tesi ad armonizzare il quadro normativo delle vie navigabili interne dell'Unione, la Commissione è invitata a considerare un regime europeo di norme in materia di scarico e conferimento applicabili alle navi adibite alla navigazione interna, che tenga conto della convenzione sulla raccolta, il deposito e il ritiro di rifiuti nella navigazione sul Reno e nella navigazione interna del 9 settembre 1996.

(23) Ai sensi del regolamento (CE) n. 1224/2009 del Consiglio ([9]), i pescherecci battenti la bandiera di uno Stato membro dispongono a bordo delle attrezzature per il recupero delle reti da pesca perdute. Se le reti da pesca sono state perdute, il comandante del peschereccio deve cercare di recuperarle quanto prima possibile. Se le reti da pesca non possono essere recuperate, entro 24 ore il comandante del peschereccio deve informare le autorità del proprio Stato membro di bandiera. Lo Stato membro di bandiera deve informare a sua volta l'autorità competente dello Stato membro costiero. Le informazioni includono il numero d'identificazione esterno e il nome del peschereccio, il tipo di reti da pesca perdute e il luogo della perdita, nonché le misure messe in atto per recuperarle. I pescherecci di lunghezza inferiore a 12 metri possono essere esentati. Ai sensi della proposta di un regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 1224/2009 del Consiglio, la segnalazione da parte dei pescherecci deve avvenire mediante un giornale di bordo elettronico e gli Stati membri sono tenuti a raccogliere e registrare le informazioni sulle reti da pesca perdute e a fornirle alla Commissione su richiesta. Anche le informazioni raccolte e disponibili nelle ricevute di conferimento dei rifiuti accidentalmente pescati in linea con la presente direttiva potrebbero essere comunicate in questa maniera.

(24) Conformemente alla convenzione internazionale per il controllo e la gestione delle acque di zavorra e dei sedimenti delle navi, che è stata adottata dall'IMO il 13 febbraio 2004 ed è entrata in vigore l'8 settembre 2017, tutte le navi sono obbligate a eseguire le procedure di gestione delle acque di zavorra conformemente alle norme dell'IMO, mentre i porti e i terminali designati per la pulizia e la riparazione delle cisterne di zavorra devono fornire impianti adeguati per la raccolta dei sedimenti.

([9]) Regolamento (CE) n. 1224/2009 del Consiglio, del 20 novembre 2009, che istituisce un regime di controllo unionale per garantire il rispetto delle norme della politica comune della pesca, che modifica i regolamenti (CE) n. 847/96, (CE) n. 2371/2002, (CE) n. 811/2004, (CE) n. 768/2005, (CE) n. 2115/2005, (CE) n. 2166/2005, (CE) n. 388/2006, (CE) n. 509/2007, (CE) n. 676/2007, (CE) n. 1098/2007, (CE) n. 1300/2008, (CE) n. 1342/2008 e che abroga i regolamenti (CEE) n. 2847/93, (CE) n. 1627/94 e (CE) n. 1966/2006 (GU L 343 del 22.12.2009, pag. 1).

(25) Gli impianti portuali di raccolta sono considerati adeguati se sono in grado di rispondere alle esigenze delle navi che utilizzano abitualmente il porto, senza causare loro ingiustificati ritardi, come specificato anche nella guida consolidata IMO e nelle linee guida IMO per garantire l'adeguatezza degli impianti portuali di raccolta dei rifiuti (risoluzione MEPC.83(44)]. L'adeguatezza si riferisce sia alle condizioni operative dell'impianto in considerazione delle esigenze degli utenti, sia alla gestione ambientale degli impianti in conformità del diritto dell'Unione in materia di rifiuti. In taluni casi potrebbe essere difficile valutare se un impianto portuale di raccolta situato al di fuori dell'Unione rispetta tale norma.

(26) Il regolamento (CE) n. 1069/2009 del Parlamento europeo e del Consiglio ([10]) prescrive lo smaltimento in una discarica autorizzata mediante incenerimento o interramento dei rifiuti di cucina e ristorazione provenienti da mezzi di trasporto che effettuano tragitti internazionali, compresi i rifiuti delle navi che fanno scalo nei porti dell'Unione i quali siano stati potenzialmente in contatto a bordo con sottoprodotti di origine animale. Affinché tale prescrizione non limiti la preparazione al riutilizzo e riciclaggio dei rifiuti delle navi, è opportuno adoperarsi, conformemente alla guida consolidata IMO, per separare meglio i rifiuti in modo da evitare potenziali contaminazioni, per esempio dei rifiuti di imballaggio.

(27) Come stabilito nel regolamento (CE) n. 1069/2009, in combinato disposto con il regolamento (UE) n. 142/2011 della Commissione ([11]), i viaggi intra-Unione non sono considerati tragitti internazionali e i rifiuti di cucina e ristorazione generati durante tali viaggi non devono essere inceneriti. Ai sensi della legislazione marittima internazionale [convenzione MARPOL e convenzione internazionale per la salvaguardia della vita umana in mare (SOLAS)], i suddetti viaggi intra-Unione sono tuttavia assimilati ai viaggi internazionali. Al fine di garantire la coerenza del diritto dell'Unione, è opportuno attenersi alle definizioni del regolamento (CE) n. 1069/2009 allorché sono definiti, nella presente direttiva, in combinato disposto con il regolamento (UE) n. 142/2011, l'ambito di applicazione e il trattamento dei rifiuti di cucina e ristorazione provenienti da mezzi di trasporto che effettuano tragitti internazionali.

(28) Al fine di garantire l'adeguatezza degli impianti portuali di raccolta, è essenziale sviluppare, attuare e riesaminare il piano di raccolta e di gestione dei rifiuti, previa consultazione di tutte le parti interessate. Per motivi pratici e organizzativi, i porti limitrofi nella stessa regione geografica potrebbero sviluppare un piano comune, che comprenda la disponibilità di impianti portuali di raccolta in ciascuno dei porti interessati dal piano, fornendo nel contempo un quadro amministrativo comune.

(29) Per i piccoli porti non commerciali può rivelarsi difficile adottare e monitorare i piani di raccolta e di gestione dei rifiuti, per esempio le aree di ormeggio e i porti turistici, che sono interessati da un traffico poco frequente, caratterizzato solo da imbarcazioni da diporto, o che è utilizzato solo per una parte dell'anno. I rifiuti prodotti da questi piccoli porti sono solitamente gestiti dal sistema di gestione dei rifiuti urbani, in conformità dei principi della direttiva 2008/98/CE. Al fine di non sovraccaricare gli enti locali e agevolare la gestione dei rifiuti in detti piccoli porti, dovrebbe essere sufficiente includere i rifiuti prodotti da tali porti nel flusso di rifiuti urbani e gestirli di conseguenza, richiedendo altresì che i porti mettano a disposizione dei loro utenti informazioni relative alla raccolta dei rifiuti e che i porti esentati siano inseriti in un sistema elettronico per consentire un livello minimo di monitoraggio.

(30) Per affrontare il problema dei rifiuti marini in modo efficace, è fondamentale fornire il giusto livello di incentivi per il conferimento dei rifiuti agli impianti portuali di raccolta, in particolare i rifiuti di cui all'allegato V della convenzione MARPOL («allegato V della MARPOL sui rifiuti»). Ciò può essere conseguito attraverso un sistema di recupero dei costi che comporti l'applicazione di una tariffa indiretta. Tale tariffa indiretta dovrebbe essere dovuta indipendentemente dal conferimento dei rifiuti e autorizzare il conferimento dei rifiuti senza aggiungere ulteriori oneri diretti. Dovrebbero essere soggetti all'imposta indiretta anche i settori della pesca e della navigazione da diporto, dato il loro contributo alla produzione di rifiuti marini. Tuttavia, qualora una nave conferisca un quantitativo eccessivo di rifiuti di cui all'allegato V della convenzione MARPOL, in particolare i rifiuti operativi, che superi la massima capacità di stoccaggio dedicata così come menzionata nel modulo di notifica anticipata per il conferimento dei rifiuti, dovrebbe essere possibile addebitare una tariffa diretta supplementare al fine di garantire che i costi relativi al ricevimento di tale quantitativo in eccesso di rifiuti non costituiscano un onere sproporzionato per il sistema di recupero dei costi del porto. Questo anche nel caso in cui la capacità di stoccaggio dedicata dichiarata è sproporzionata o irragionevole.

([10]) Regolamento (CE) n. 1069/2009 del Parlamento europeo e del Consiglio, del 21 ottobre 2009, recante norme sanitarie relative ai sottoprodotti di origine animale e ai prodotti derivati non destinati al consumo umano e che abroga il regolamento (CE) n. 1774/2002 (regolamento sui sottoprodotti di origine animale) (GU L 300 del 14.11.2009, pag. 1).

([11]) Regolamento (UE) n. 142/2011 della Commissione, del 25 febbraio 2011, recante disposizioni di applicazione del regolamento (CE) n. 1069/2009 del Parlamento europeo e del Consiglio recante norme sanitarie relative ai sottoprodotti di origine animale e ai prodotti derivati non destinati al consumo umano, e della direttiva 97/78/CE del Consiglio per quanto riguarda taluni campioni e articoli non sottoposti a controlli veterinari alla frontiera (GU L 54 del 26.2.2011, pag. 1).

(31) In taluni Stati membri sono stati istituiti regimi per fornire un finanziamento alternativo dei costi per la raccolta e la gestione a terra dei rifiuti degli attrezzi da pesca o dei rifiuti accidentalmente pescati, compresi i cosiddetti «sistemi per la pesca dei rifiuti». Tali iniziative dovrebbero essere accolte con favore ed è opportuno incoraggiare gli Stati membri a integrare i sistemi di recupero dei costi istituiti a norma della presente direttiva con i sistemi per la pesca dei rifiuti per coprire i costi dei rifiuti pescati passivamente. È quindi opportuno che tali sistemi di recupero dei costi, che si basano sull'applicazione di una tariffa indiretta del 100 % per i rifiuti di cui all'allegato V della MARPOL, esclusi i residui del carico, non creino un disincentivo alla partecipazione delle comunità dei porti di pesca ai regimi esistenti di conferimento dei rifiuti accidentalmente pescati.

(32) Una nave dovrebbe beneficiare di tariffe ridotte qualora sia progettata, attrezzata o utilizzata per ridurre al minimo i rifiuti, seguendo alcuni criteri che devono essere elaborati mediante competenze di esecuzione attribuite alla Commissione, in linea con le linee guida IMO per l'attuazione dell'allegato V della MARPOL e con le norme elaborate dall'Organizzazione internazionale per la standardizzazione. La riduzione e l'efficiente riciclaggio dei rifiuti si conseguono principalmente mediante l'efficace separazione dei rifiuti a bordo, in linea con le suddette linee guida e norme.

(33) Data la tipologia di traffico, caratterizzato da scali frequenti, il trasporto marittimo a corto raggio sostiene costi notevoli nell'ambito dell'attuale regime per il conferimento dei rifiuti agli impianti portuali di raccolta, poiché deve corrispondere una tariffa per ogni singolo scalo effettuato. Al tempo stesso, il traffico non è sufficientemente pianificato e regolare tale da poter usufruire di un'esenzione dal pagamento e dal conferimento dei rifiuti per questi motivi. Al fine di ridurre gli oneri finanziari a carico del settore, dovrebbero essere applicate tariffe ridotte alle navi in base al tipo di traffico cui sono adibite.

(34) I residui del carico restano di proprietà del proprietario delle merci anche successivamente al loro scarico presso il terminal e possono avere un valore economico. Per questo motivo i residui del carico non dovrebbero essere inclusi nei sistemi di recupero dei costi e nell'applicazione della tariffa indiretta. Gli oneri per il conferimento dei residui del carico dovrebbero essere pagati dall'utente dell'impianto di raccolta del porto, così come indicato nelle convenzioni contrattuali tra le parti interessate o in altre convenzioni locali. I residui del carico comprendono inoltre i resti di carichi oleosi o di carichi liquidi nocivi dopo le operazioni di pulizia, a cui si applicano le norme in materia di scarico di cui agli allegati I e II della convenzione MARPOL e che, a determinate condizioni specificate in detti allegati, non occorre conferire nel porto al fine di evitare costi operativi inutili per le navi e la congestione dei porti.

(35) È opportuno che gli Stati membri incoraggino il conferimento dei residui delle acque di lavaggio delle cisterne contenenti sostanze galleggianti persistenti a viscosità elevata, eventualmente mediante incentivi finanziari adeguati.

(36) Il regolamento (UE) 2017/352 del Parlamento europeo e del Consiglio [12] considera la fornitura di impianti portuali di raccolta come un servizio compreso nel suo ambito di applicazione. Esso prevede norme sulla trasparenza del sistema di tariffazione applicato per l'uso dei servizi portuali, sulla consultazione degli utenti dei porti e sulla gestione delle procedure di reclamo. La presente direttiva va oltre il quadro fornito da tale regolamento e fornisce maggiori dettagli per la predisposizione e il funzionamento dei sistemi di recupero dei costi per gli impianti portuali di raccolta dei rifiuti delle navi e per la trasparenza della struttura dei costi.

(37) Oltre a fornire incentivi per il conferimento di rifiuti, è essenziale prevedere un'applicazione efficace dell'obbligo di conferimento, che dovrebbe seguire un approccio basato sul rischio per il quale è opportuno stabilire un meccanismo unionale di selezione che privilegia il rischio.

(38) Uno dei principali ostacoli all'applicazione efficace dell'obbligo di conferimento è costituito dalla diversa interpretazione e attuazione da parte degli Stati membri della deroga basata sulla sufficiente capacità di stoccaggio. Al fine di evitare che l'applicazione di tale deroga comprometta l'obiettivo principale della presente direttiva, la sufficiente capacità di stoccaggio dovrebbe essere ulteriormente precisata, in particolare rispetto al successivo porto di scalo, e dovrebbe essere determinata in modo armonizzato, in base a una metodologia e a criteri comuni. Nei casi in cui è difficile stabilire se sono disponibili impianti portuali di raccolta adeguati nei porti al di fuori dell'Unione, è essenziale che l'autorità competente valuti attentamente l'applicazione della deroga.

[12] Regolamento (UE) 2017/352 del Parlamento europeo e del Consiglio, del 15 febbraio 2017, che istituisce un quadro normativo per la fornitura di servizi portuali e norme comuni in materia di trasparenza finanziaria dei porti (GU L 57 del 3.3.2017, pag. 1).

(39) È necessaria un'ulteriore armonizzazione del regime delle esenzioni per le navi in servizio di linea con scali frequenti e regolari, e in particolare occorre chiarire i termini e le condizioni che disciplinano tali esenzioni. La valutazione REFIT e la valutazione d'impatto hanno messo in luce che la mancanza di armonizzazione delle condizioni e dell'applicazione delle esenzioni ha provocato oneri amministrativi inutili per le navi e i porti.

(40) Il monitoraggio e l'applicazione dovrebbero essere facilitati mediante un sistema basato sulla comunicazione e sullo scambio di informazioni per via elettronica. A tal fine il sistema informativo e di monitoraggio esistente, istituito a norma della direttiva 2000/59/CE, dovrebbe essere ulteriormente sviluppato e dovrebbe continuare a essere utilizzato sulla base di sistemi di dati elettronici esistenti, in particolare il sistema dell'Unione per lo scambio di dati marittimi (SafeSeaNet), istituito dalla direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([13]), e la banca dati sulle ispezioni, istituita dalla direttiva 2009/16/CE del Parlamento europeo e del Consiglio ([14]) (THETIS). Tale sistema dovrebbe altresì includere le informazioni sugli impianti portuali di raccolta disponibili nei diversi porti.

(41) La direttiva 2010/65/UE del Parlamento europeo e del Consiglio ([15]) semplifica e armonizza le procedure amministrative applicate al trasporto marittimo attraverso l'uso più generalizzato della trasmissione elettronica delle informazioni e la razionalizzazione delle formalità delle segnalazioni. La dichiarazione di La Valletta sulle priorità per la politica UE dei trasporti marittimi fino al 2020, approvata dal Consiglio nelle sue conclusioni dell'8 giugno 2017, ha invitato la Commissione a proporre un seguito adeguato alla revisione di detta direttiva. Una consultazione pubblica sulle formalità di segnalazione delle navi è stata svolta dalla Commissione dal 25 ottobre 2017 al 18 gennaio 2018. Il 17 maggio 2018 la Commissione ha trasmesso al Parlamento europeo e al Consiglio una proposta di regolamento che istituisce un'interfaccia unica marittima europea e abroga la direttiva 2010/65/UE.

(42) La convenzione MARPOL impone alle parti contraenti di mantenere aggiornate le informazioni sui loro impianti portuali di raccolta e di comunicarle all'IMO. A tal fine l'IMO ha istituito una banca dati sugli impianti portuali di raccolta dei rifiuti nel proprio sistema integrato globale di informazione sul traffico marittimo («GISIS»).

(43) Nella sua guida consolidata IMO, l'IMO prevede la segnalazione delle presunte inadeguatezze rilevate negli impianti portuali di raccolta. Secondo tale procedura, una nave dovrebbe segnalare tali inadeguatezze all'amministrazione dello Stato di bandiera, che a sua volta ne deve informare l'IMO e lo Stato di approdo. Lo Stato di approdo dovrebbe esaminare la segnalazione e rispondere adeguatamente, informando l'IMO e lo Stato di bandiera. La segnalazione diretta di tali informazioni sulle presunte inadeguatezze al sistema informativo, di monitoraggio e di applicazione previsto dalla presente direttiva consentirebbe la successiva trasmissione delle suddette informazioni al sistema GISIS, dispensando gli Stati membri, in qualità di Stati di bandiera e di approdo, dall'obbligo di segnalazione all'IMO.

(44) Il sottogruppo sugli impianti portuali di raccolta, che è stato istituito nell'ambito del Forum europeo per il trasporto marittimo sostenibile e che ha riunito una molteplicità di esperti nel campo dell'inquinamento provocato dalle navi e della gestione dei rifiuti delle navi, ha sospeso i lavori nel dicembre 2017 in ragione dell'avvio dei negoziati interistituzionali. Dato che tale sottogruppo ha fornito preziosi orientamenti e consulenze alla Commissione, sarebbe auspicabile costituire un analogo gruppo di esperti con il mandato di scambiare esperienze in merito all'attuazione della presente direttiva.

(45) È importante che le eventuali sanzioni previste dagli Stati membri siano applicate correttamente e siano effettive, proporzionate e dissuasive.

(46) Le buone condizioni di lavoro per il personale portuale che lavora negli impianti portuali di raccolta sono di fondamentale importanza per rendere il settore marittimo sicuro, efficiente e socialmente responsabile, in grado di attirare lavoratori qualificati e garantire condizioni paritarie in tutta Europa. La formazione iniziale e periodica del personale è essenziale per garantire la qualità dei servizi e la protezione dei lavoratori. Le autorità portuali e degli impianti portuali di raccolta dei rifiuti dovrebbero provvedere affinché tutto il personale riceva la formazione necessaria ad acquisire le conoscenze essenziali per lo svolgimento delle proprie funzioni, con particolare attenzione per gli aspetti di salute e di sicurezza connessi alle attività che prevedono l'utilizzo di materiali pericolosi, e affinché i requisiti di formazione siano periodicamente aggiornati per rispondere alle sfide dell'innovazione tecnologica.

([13]) 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).

([14]) Direttiva 2009/16/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa al controllo da parte dello Stato di approdo (GU L 131 del 28.5.2009, pag. 57).

([15]) Direttiva 2010/65/UE del Parlamento europeo e del Consiglio, del 20 ottobre 2010, relativa alle formalità di dichiarazione delle navi in arrivo o in partenza da porti degli Stati membri e che abroga la direttiva 2002/6/CE (GU L 283 del 29.10.2010, pag. 1).

(47) Le competenze conferite alla Commissione per attuare la direttiva 2000/59/CE dovrebbero essere aggiornate in conformità del trattato sul funzionamento dell'Unione europea (TFUE).

(48) È opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE riguardo alla modifica degli allegati della presente direttiva e dei riferimenti agli strumenti internazionali nella misura necessaria per renderli conformi al diritto dell'Unione o per tener conto degli sviluppi a livello internazionale, in particolare a livello dell'IMO; modificando gli allegati della presente direttiva quando ciò è necessario per migliorare le disposizioni di attuazione e controllo da esso stabilite, in particolare in relazione alla notifica e al conferimento dei rifiuti efficaci e alla corretta applicazione delle esenzioni; nonché, in circostanze eccezionali, ove debitamente giustificato da un'appropriata analisi da parte della Commissione e al fine di evitare una minaccia grave e inaccettabile per l'ambiente marino, modificando la presente direttiva nella misura necessaria per evitare tale minaccia, allo scopo di evitare, se necessario, che si applichino modifiche di tali strumenti internazionali ai fini della presente direttiva. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti e che tali consultazioni siano svolte nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([16]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(49) Al fine di fornire i metodi per il calcolo della sufficiente capacità di stoccaggio dedicata; per sviluppare criteri comuni per riconoscere, ai fini della concessione di una tariffa ridotta sui rifiuti delle navi, che la progettazione, le attrezzature e il funzionamento della nave dimostrano che essa produce minori quantità di rifiuti e siano gestiti in modo sostenibile e compatibile con l'ambiente; per definire le metodologie sui dati di monitoraggio sul volume e sulla quantità di rifiuti accidentalmente pescati e il formato delle relazioni; per definire nel dettaglio gli elementi del meccanismo unionale basato sul rischio, è opportuno attribuire 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 ([17]).

(50) Poiché l'obiettivo della presente direttiva, vale a dire la protezione dell'ambiente marino dagli scarichi di rifiuti in mare, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base 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.

(51) L'Unione è caratterizzata da differenze regionali a livello di porti, come dimostra anche la valutazione dell'impatto territoriale eseguita dalla Commissione. I porti differiscono in base all'ubicazione geografica, alle dimensioni, all'assetto amministrativo e proprietario e sono caratterizzati dal tipo di navi che vi fanno scalo abitualmente. I sistemi di gestione dei rifiuti riflettono inoltre le differenze a livello comunale e dell'infrastruttura di gestione dei rifiuti a valle.

(52) L'articolo 349 TFUE impone di tener conto delle caratteristiche specifiche delle regioni ultraperiferiche dell'Unione, segnatamente la Guadalupa, la Guyana francese, la Martinica, Mayotte, la Riunione, Saint Martin, le Azzorre, Madera e le isole Canarie. Per garantire l'adeguatezza e la disponibilità degli impianti portuali di raccolta, potrebbe essere opportuno che gli Stati membri adottino azioni a supporto degli operatori o delle autorità portuali delle suddette regioni dell'Unione per far fronte agli effetti degli svantaggi permanenti di cui a detto articolo. Tali azioni messe a disposizione dagli Stati membri in tale contesto sono esenti dall'obbligo di notifica di cui all'articolo 108, paragrafo 3, TFUE se, al momento della concessione, soddisfano le condizioni previste dal regolamento (UE) n. 651/2014 della Commissione ([18]), adottato ai sensi del regolamento (CE) n. 994/98 del Consiglio ([19]).

(53) È pertanto opportuno abrogare la direttiva 2000/59/CE,

([16]) GU L 123 del 12.5.2016, pag. 1.

([17]) 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).

([18]) Regolamento (UE) n. 651/2014 della Commissione, del 17 giugno 2014, che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del trattato (GU L 187 del 26.6.2014, pag. 1).

([19]) Regolamento (CE) n. 994/98 del Consiglio, del 7 maggio 1998, sull'applicazione degli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea a determinate categorie di aiuti di stato orizzontali (GU L 142 del 14.5.1998, pag. 1).

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Sezione 1

Disposizioni generali

Articolo 1

Oggetto

La presente direttiva ha l'obiettivo di proteggere l'ambiente marino dagli effetti negativi degli scarichi dei rifiuti delle navi che utilizzano porti situati nel territorio dell'Unione e di garantire nel contempo il buon funzionamento del traffico marittimo migliorando la disponibilità e l'uso di adeguati impianti portuali di raccolta dei rifiuti e il conferimento degli stessi presso tali impianti.

Articolo 2

Definizioni

Ai fini della presente direttiva si applicano le seguenti definizioni:

1) «nave»: un'imbarcazione di qualsiasi tipo che opera nell'ambiente marino, compresi i pescherecci, le imbarcazioni da diporto, gli aliscafi, i veicoli a cuscino d'aria, i sommergibili e le imbarcazioni galleggianti;

2) «convenzione MARPOL»: la convenzione internazionale per la prevenzione dell'inquinamento causato da navi, nella versione aggiornata;

3) «rifiuti delle navi»: tutti i rifiuti, compresi i residui del carico, prodotti durante le operazioni di servizio di una nave o durante le operazioni di carico, scarico e pulizia, e che rientrano nell'ambito di applicazione degli allegati I, II, IV, V e VI della convenzione MARPOL, nonché i rifiuti accidentalmente pescati;

4) «rifiuti accidentalmente pescati»: rifiuti raccolti dalle reti durante le operazioni di pesca;

5) «residui del carico»: i resti di qualsiasi materiale che costituisce il carico contenuto a bordo, che rimangono sul ponte, nella stiva o nelle cisterne dopo le operazioni di carico e scarico, comprese le eccedenze di carico e scarico e le fuoriuscite, siano essi umidi, secchi o trascinati dalle acque di lavaggio, a eccezione delle polveri del carico che rimangono sul ponte dopo che questo è stato spazzato o della polvere sulle superfici esterne della nave;

6) «impianto portuale di raccolta»: qualsiasi struttura fissa, galleggiante o mobile che sia in grado di fornire il servizio di raccolta dei rifiuti delle navi;

7) «peschereccio»: qualsiasi nave equipaggiata o utilizzata a fini commerciali per la cattura di pesce o di altre risorse marine viventi;

8) «imbarcazione da diporto»: una nave di qualsiasi tipo, con scafo di lunghezza pari o superiore a 2,5 metri, indipendentemente dal mezzo di propulsione, destinata all'utilizzo per finalità sportive o ricreative e non impegnata in attività commerciali;

9) «porto»: un luogo o un'area geografica cui siano state apportate migliorie e aggiunte attrezzature progettate principalmente per consentire l'attracco di navi, compresa la zona di ancoraggio all'interno della giurisdizione del porto;

10) «sufficiente capacità di stoccaggio»: lo spazio necessario a stoccare i rifiuti a bordo dal momento della partenza fino al successivo porto di scalo, compresi i rifiuti che saranno presumibilmente prodotti nel corso del viaggio;

11) «traffico di linea»: traffico effettuato in base a una lista pubblicata o pianificata di orari di partenza e di arrivo tra porti specificati o in occasione di traversate ricorrenti, secondo un orario riconosciuto;

12) «scali regolari»: viaggi ripetuti dalla stessa nave secondo uno schema costante tra porti individuati o una serie di viaggi da e verso lo stesso porto senza scali intermedi;

13) «scali frequenti»: scali effettuati da una nave nello stesso porto, che si verificano almeno una volta ogni due settimane;

14) «GISIS»: sistema globale integrato di informazione sul traffico marittimo istituito dall'IMO;

15) «trattamento»: operazioni di recupero o smaltimento, inclusa la preparazione prima del recupero o dello smaltimento;

16) «tariffa indiretta»: una tariffa pagata per i servizi svolti dagli impianti portuali di raccolta, indipendentemente dall'effettivo conferimento dei rifiuti da parte delle navi.

I «rifiuti delle navi» di cui al punto 3), sono considerati rifiuti ai sensi dell'articolo 3, punto 1), della direttiva 2008/98/CE.

Articolo 3

Ambito di applicazione

1. La presente direttiva si applica a:

a) tutte le navi, indipendentemente dalla loro bandiera, che fanno scalo o che operano in un porto di uno Stato membro, a esclusione delle navi adibite a servizi portuali ai sensi dell'articolo 1, paragrafo 2, del regolamento (UE) 2017/352, e con l'eccezione delle navi militari da guerra, delle navi ausiliarie o di altre navi possedute o gestite da uno Stato e impiegate, al momento, solo per servizi statali a fini non commerciali;

b) tutti i porti degli Stati membri ove fanno abitualmente scalo le navi cui si applica la lettera a).

Ai fini della presente direttiva, e per evitare ingiustificati ritardi per le navi, gli Stati membri possono decidere di escludere dai loro porti la zona di ancoraggio ai fini dell'applicazione degli articoli 6, 7 e 8.

2. Gli Stati membri adottano misure per garantire che, ove ragionevolmente possibile, le navi escluse dall'ambito di applicazione della presente direttiva conferiscano i loro rifiuti in accordo con la presente direttiva.

3. Gli Stati membri privi di porti o di navi battenti bandiera che rientrano nell'ambito di applicazione della presente direttiva, con l'eccezione degli obblighi di cui al terzo comma del presente paragrafo, possono derogare alle disposizioni della presente direttiva.

Gli Stati membri privi di porti che rientrano nell'ambito di applicazione della presente direttiva possono derogare alle disposizioni della presente direttiva che riguardano soltanto i porti.

Gli Stati membri che intendono avvalersi delle deroghe di cui al presente paragrafo comunicano alla Commissione, entro il 28 giugno 2021, se le pertinenti condizioni sono state soddisfatte e, successivamente, informano la Commissione con cadenza annuale di ogni eventuale modifica ulteriore. Fino a quando gli Stati membri in questione non avranno recepito e attuato la presente direttiva, essi non possono avere porti che rientrano nell'ambito di applicazione della presente direttiva e non possono autorizzare navi, comprese le imbarcazioni che rientrano nell'ambito di applicazione della presente direttiva a battere la loro bandiera.

Sezione 2

Fornitura di impianti portuali di raccolta adeguati

Articolo 4

Impianti portuali di raccolta

1. Gli Stati membri mettono a disposizione impianti portuali di raccolta adeguati a rispondere alle esigenze delle navi che utilizzano abitualmente il porto, senza causare loro ingiustificati ritardi.

2. Gli Stati membri provvedono a che:

a) gli impianti portuali di raccolta dispongano della capacità di ricevere i tipi e i quantitativi di rifiuti delle navi che abitualmente utilizzano tale porto, tenendo conto:

   i) delle esigenze operative degli utenti del porto;

   ii) dell'ubicazione geografica e delle dimensioni di tale porto;

   iii) della tipologia delle navi che vi fanno scalo; e

   iv) delle esenzioni di cui all'articolo 9;

b) le formalità e le modalità operative relative all'utilizzo degli impianti portuali di raccolta siano semplici e rapide ed evitino ingiustificati ritardi alle navi;

c) le tariffe stabilite per il conferimento non creino un disincentivo all'uso degli impianti portuali di raccolta da parte delle navi; e

d) gli impianti portuali di raccolta provvedano a una gestione dei rifiuti delle navi ambientalmente compatibile, conformemente alla direttiva 2008/98/CE e ad altre pertinenti leggi nazionali e dell'Unione sui rifiuti.

Ai fini del primo comma, lettera d), gli Stati membri garantiscono la raccolta differenziata per facilitare il riutilizzo e il riciclaggio dei rifiuti delle navi, nei porti, come previsto nella normativa dell'Unione sui rifiuti, in particolare nella direttiva 2006/66/CE del Parlamento europeo e del Consiglio ([20]), nella direttiva 2008/98/CE e nella direttiva 2012/19/UE del Parlamento europeo e del Consiglio ([21]). Al fine di facilitare tale processo, gli impianti portuali di raccolta possono raccogliere le frazioni di rifiuti differenziate conformemente alle categorie di rifiuti stabilite nella convenzione MARPOL, tenendo conto delle sue linee guida.

Il primo comma, lettera d), si applica fatte salve le prescrizioni più rigorose imposte dal regolamento (CE) n. 1069/2009 per la gestione dei rifiuti di cucina e ristorazione derivanti da trasporti internazionali.

3. Gli Stati membri, in qualità di Stati di bandiera, si avvalgono dei moduli e delle procedure stabilite dall'IMO per notificare all'IMO e alle autorità dello Stato di approdo le presunte inadeguatezze degli impianti portuali di raccolta.

Gli Stati membri, in qualità di Stati di approdo, indagano su tutti i casi di presunta inadeguatezza segnalati e si avvalgono dei moduli e delle procedure stabilite dall'IMO per notificare l'esito dell'indagine all'IMO e allo Stato di bandiera che ha effettuato la segnalazione.

4. Le autorità portuali interessate o, in mancanza di queste, le autorità competenti provvedono affinché le operazioni di conferimento o raccolta dei rifiuti siano realizzate adottando misure di sicurezza sufficienti per evitare rischi sia per le persone che per l'ambiente nei porti disciplinati dalla presente direttiva.

5. Gli Stati membri garantiscono che tutte le parti coinvolte nel conferimento o nella raccolta dei rifiuti delle navi abbiano diritto al risarcimento del danno causato da ritardi ingiustificati.

([20]) Direttiva 2006/66/CE del Parlamento europeo e del Consiglio, del 6 settembre 2006, relativa a pile e accumulatori e ai rifiuti di pile e accumulatori e che abroga la direttiva 91/157/CEE (testo rilevante ai fini del SEE) (GU L 266 del 26.9.2006, pag. 1).

([21]) Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (GU L 197 del 24.7.2012, pag. 38).

Articolo 5

Piani di raccolta e di gestione dei rifiuti

1. Gli Stati membri garantiscono che per ciascun porto sia predisposto e attuato un adeguato piano di raccolta e di gestione dei rifiuti, previa consultazione delle parti interessate, tra cui, in particolare, gli utenti del porto o i loro rappresentanti e, se del caso, le autorità locali competenti, gli operatori dell'impianto portuale di raccolta, le organizzazioni che attuano gli obblighi di responsabilità estesi del produttore e i rappresentanti della società civile. Tale consultazione dovrebbe avvenire sia durante la predisposizione del piano di raccolta e di gestione dei rifiuti sia dopo la sua adozione, in particolare qualora siano stati attuati cambiamenti significativi per quanto riguarda le prescrizioni di cui agli articoli 4, 6 e 7.

Nell'allegato 1 figurano i criteri dettagliati per l'elaborazione del piano di raccolta e di gestione dei rifiuti.

2. Gli Stati membri provvedono a comunicare agli operatori delle navi le seguenti informazioni riportate nei piani di raccolta e di gestione dei rifiuti in merito alla disponibilità di adeguati impianti di raccolta nei loro porti e come sono strutturati i costi, e a renderle disponibili al pubblico e facilmente accessibili in una lingua ufficiale dello Stato membro in cui si trova il porto e, se del caso, in una lingua usata internazionalmente:

a) ubicazione degli impianti portuali di raccolta per ogni banchina di ormeggio e, ove opportuno, il loro orario di lavoro;

b) elenco dei rifiuti delle navi abitualmente gestiti dal porto;

c) elenco dei punti di contatto, degli operatori degli impianti portuali di raccolta e dei servizi offerti;

d) descrizione delle procedure per il conferimento dei rifiuti;

e) descrizione del sistema di recupero dei costi, inclusi sistemi e fondi di gestione dei rifiuti di cui all'allegato 4, se del caso.

Le informazioni di cui al primo comma del presente paragrafo sono rese disponibili anche per via elettronica e aggiornate nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13.

3. Ove necessario per motivi di efficienza, i piani di raccolta e di gestione dei rifiuti possono essere elaborati congiuntamente da due o più porti limitrofi nella stessa regione geografica con l'adeguata partecipazione di ciascun porto, purché siano specificate per ogni singolo porto l'esigenza e la disponibilità degli impianti portuali di raccolta.

4. Gli Stati membri valutano e approvano il piano di raccolta e di gestione dei rifiuti e garantiscono che si procederà a una nuova approvazione al termine di almeno cinque anni dalla precedente approvazione o nuova approvazione, e dopo che si siano verificati significativi cambiamenti operativi nella gestione del porto. Tali cambiamenti possono comprendere modifiche strutturali del traffico diretto al porto, sviluppo di nuove infrastrutture, modifiche della domanda e della fornitura di impianti portuali di raccolta e nuove tecniche di trattamento a bordo.

Gli Stati membri controllano l'attuazione del piano di raccolta e di gestione dei rifiuti del porto. Se durante il periodo di cinque anni di cui al primo comma non si sono verificati cambiamenti significativi, la nuova approvazione può consistere in una convalida dei piani esistenti.

5. I piccoli porti non commerciali, che sono caratterizzati soltanto da un traffico sporadico o scarso di imbarcazioni da diporto, possono essere esentati dai paragrafi da 1 a 4 se i loro impianti portuali di raccolta sono integrati nel sistema di gestione dei rifiuti comunale e se gli Stati membri in cui tali porti sono situati garantiscono che le informazioni relative al sistema di gestione dei rifiuti siano messe a disposizione degli utenti dei porti stessi.

Gli Stati membri in cui tali porti sono situati ne comunicano il nome e l'ubicazione per via elettronica nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13.

Sezione 3

Conferimento dei rifiuti delle navi

Articolo 6

Notifica anticipata dei rifiuti

1. L'operatore, l'agente o il comandante di una nave che rientra nell'ambito di applicazione della direttiva 2002/59/CE, diretto verso un porto dell'Unione, compila in modo autentico e accurato il modulo di cui all'allegato 2 della presente direttiva («notifica anticipata dei rifiuti») e trasmette tutte le informazioni in esso contenute all'autorità o all'organismo designato a tale scopo dallo Stato membro in cui è situato il porto:

a) con almeno 24 ore di anticipo rispetto all'arrivo se il porto di scalo è noto;

b) non appena è noto il porto di scalo, qualora questa informazione sia disponibile a meno di 24 ore dall'arrivo; o

c) al più tardi al momento della partenza dal porto precedente se la durata del viaggio è inferiore a 24 ore.

2. Le informazioni della notifica anticipata dei rifiuti sono riportate per via elettronica nel sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13 della presente direttiva, in conformità delle direttive 2002/59/CE e 2010/65/UE.

3. Le informazioni della notifica anticipata dei rifiuti sono disponibili a bordo, preferibilmente in formato elettronico, almeno fino al successivo porto di scalo e, su richiesta, sono messe a disposizione delle autorità competenti degli Stati membri.

4. Gli Stati membri provvedono a che le informazioni notificate a norma del presente articolo siano esaminate e condivise con le competenti autorità preposte all'applicazione senza incorrere in ritardi.

Articolo 7

Conferimento dei rifiuti delle navi

1. Il comandante di una nave che approda in un porto dell'Unione, prima di lasciare tale porto, conferisce tutti i rifiuti presenti a bordo a un impianto portuale di raccolta tenendo in considerazione le pertinenti norme in materia di scarico previste dalla convenzione MARPOL.

2. Al momento del conferimento l'operatore dell'impianto portuale di raccolta o l'autorità del porto cui i rifiuti sono stati conferiti compila in modo autentico e accurato il modulo di cui all'allegato 3 («ricevuta di conferimento dei rifiuti») e fornisce, senza ingiustificati ritardi, la ricevuta di conferimento dei rifiuti al comandante della nave.

Le disposizioni di cui al primo comma non si applicano ai piccoli porti e senza personale o che sono ubicati in località remote, a condizione che lo Stato membro in cui sono situati tali porti abbia notificato il nome e l'ubicazione di detti porti per via elettronica nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13.

3. L'operatore, l'agente o il comandante di una nave che rientra nell'ambito di applicazione della direttiva 2002/59/CE comunica per via elettronica, prima della partenza, o non appena riceve la ricevuta di conferimento dei rifiuti, le informazioni in essa riportate, nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13 della presente direttiva, in conformità delle direttive 2002/59/CE e 2010/65/UE.

Le informazioni della ricevuta di conferimento dei rifiuti sono disponibili a bordo per almeno due anni, ove opportuno insieme al registro degli idrocarburi, al registro dei carichi, al registro dei rifiuti solidi o al piano di gestione dei rifiuti solidi e, su richiesta, sono messe a disposizione delle autorità degli Stati membri.

4. Fatto salvo il paragrafo 1, una nave può procedere verso il successivo porto di scalo senza aver conferito i rifiuti se:

a) dalle informazioni fornite conformemente agli allegati 2 e 3 risulta la presenza di una sufficiente capacità di stoccaggio dedicata a tutti i rifiuti che sono già stati accumulati e che saranno accumulati nel corso del viaggio previsto della nave fino al successivo porto di scalo; oppure

b) dalle informazioni disponibili a bordo delle navi che non rientrano nell'ambito di applicazione della direttiva 2002/59/CE risulta la presenza di una sufficiente capacità di stoccaggio dedicata a tutti i rifiuti che sono già stati accumulati e che saranno accumulati nel corso del viaggio previsto della nave fino al successivo porto di scalo; oppure

c) la nave fa scalo nella zona di ancoraggio solo per meno di 24 ore o in condizioni meteorologiche avverse, a meno che tale zona sia stata esclusa ai sensi dell'articolo 3, paragrafo 1, secondo comma.

Al fine di garantire l'uniformità per l'applicazione della deroga di cui alle lettere a) e b) del primo comma, la Commissione adotta atti di esecuzione al fine di definire i metodi da utilizzare per il calcolo della sufficiente capacità di stoccaggio dedicata. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 20, paragrafo 2.

5. Uno Stato membro chiede alla nave di conferire, prima della partenza, tutti i propri rifiuti se:

a) sulla base delle informazioni disponibili, comprese le informazioni disponibili per via elettronica nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13 o nel GISIS, non può essere accertato che nel successivo porto di scalo siano disponibili adeguati impianti portuali per la raccolta; o

b) il successivo porto di scalo non è noto.

6. Il paragrafo 4 si applica fatte salve prescrizioni più rigorose a carico delle navi, adottate in base al diritto internazionale.

Articolo 8

Sistemi di recupero dei costi

1. Gli Stati membri assicurano che i costi degli impianti portuali per la raccolta e il trattamento dei rifiuti delle navi, diversi dai residui del carico, siano recuperati mediante la riscossione di tariffe a carico delle navi. Tali costi comprendono gli elementi di cui all'allegato 4.

2. I sistemi di recupero dei costi non costituiscono un incentivo per le navi a scaricare i loro rifiuti in mare. A tale scopo gli Stati membri applicano tutti i seguenti principi nell'elaborazione e nel funzionamento dei sistemi di recupero dei costi:

a) le navi pagano una tariffa indiretta, indipendentemente dal conferimento dei rifiuti agli impianti portuali di raccolta;

b) la tariffa indiretta copre:

   i) i costi amministrativi indiretti;

   ii) una parte significativa dei costi operativi diretti, come stabilito nell'allegato 4, che rappresenta almeno il 30 % del totale dei costi diretti dell'effettivo conferimento dei rifiuti nell'anno precedente, con la possibilità di tenere conto anche dei costi relativi al volume di traffico previsto per l'anno successivo;

c) al fine di prevedere l'incentivo massimo per il conferimento dei rifiuti di cui all'allegato V della convenzione MARPOL, diversi dai residui del carico, per tali rifiuti non si impone alcuna tariffa diretta, allo scopo di garantire un diritto di conferimento senza ulteriori oneri basati sul volume dei rifiuti conferiti, eccetto qualora il volume superi la massima capacità di stoccaggio dedicata menzionata nel modulo di cui all'allegato 2 della presente direttiva; i rifiuti accidentalmente pescati rientrano in questo regime, incluso il diritto di conferimento;

d) per evitare che i costi della raccolta e del trattamento dei rifiuti accidentalmente pescati siano soltanto a carico degli utenti dei porti, ove opportuno gli Stati membri coprono tali costi con le entrate generate da sistemi di finanziamento alternativi, compresi sistemi di gestione dei rifiuti e finanziamenti unionali, nazionali o regionali disponibili;

e) per incoraggiare il conferimento dei residui delle acque di lavaggio delle cisterne contenenti sostanze galleggianti persistenti a viscosità elevata, gli Stati membri possono accordare adeguati incentivi finanziari;

f) la tariffa indiretta non include i costi dei rifiuti dei sistemi di depurazione dei gas di scarico, che sono recuperati in base ai tipi e ai quantitativi di rifiuti conferiti.

3. L'eventuale parte dei costi non coperta dalla tariffa indiretta è recuperata in base ai tipi e ai quantitativi di rifiuti effettivamente conferiti dalla nave.

4. Le tariffe possono essere differenziate sulla base dei seguenti elementi:

a) la categoria, il tipo e le dimensioni della nave;

b) la prestazione di servizi alle navi al di fuori del normale orario di lavoro nel porto; o

c) la natura pericolosa dei rifiuti.

5. Le tariffe sono ridotte sulla base dei seguenti elementi:

a) il tipo di commercio cui è adibita la nave, in particolare quando una nave è adibita al commercio marittimo a corto raggio;

b) la progettazione, le attrezzature e il funzionamento della nave dimostrano che la nave produce minori quantità di rifiuti e li gestisce in modo ambientalmente sostenibile e compatibile.

Entro il 28 giugno 2020, la Commissione adotta atti di esecuzione volti a definire i criteri per stabilire che una nave osserva le prescrizioni di cui alla lettera b) del primo comma, in merito alla gestione dei rifiuti a bordo della nave. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 20, paragrafo 2.

6. Al fine di garantire che le tariffe siano eque, trasparenti, facilmente identificabili e non discriminatorie e che rispecchino i costi degli impianti e dei servizi resi disponibili e, se del caso, utilizzati, l'importo delle tariffe e la base sulla quale sono state calcolate sono messi a disposizione degli utenti dei porti nei piani di raccolta e di gestione dei rifiuti in una lingua ufficiale dello Stato membro in cui è ubicato il porto e, se del caso, in una lingua usata internazionalmente.

7. Gli Stati membri provvedono alla raccolta dei dati di monitoraggio riguardanti il volume e la quantità dei rifiuti accidentalmente pescati e li trasmettono alla Commissione. Sulla base di tali dati di monitoraggio, la Commissione pubblica una relazione entro il 31 dicembre 2022 e successivamente con cadenza biennale.

La Commissione adotta atti di esecuzione per definire le metodologie sui dati di monitoraggio e il formato delle relazioni. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 20, paragrafo 2.

Articolo 9

Esenzioni

1. Gli Stati membri possono esentare una nave che fa scalo nei loro porti dagli obblighi di cui all'articolo 6, all'articolo 7, paragrafo 1, e all'articolo 8 («esenzione»), qualora vi siano prove sufficienti del rispetto delle seguenti condizioni:

a) la nave svolge servizio di linea con scali frequenti e regolari;

b) esiste un accordo che garantisce il conferimento dei rifiuti e il pagamento delle tariffe in un porto lungo il tragitto della nave che:

   i) è comprovato da un contratto firmato con un porto o con un'impresa di gestione dei rifiuti e da ricevute di conferimento dei rifiuti;

   ii) è stato notificato a tutti i porti lungo la rotta della nave; e

   iii) è stato accettato dal porto in cui hanno luogo il conferimento e il pagamento, che può essere un porto dell'Unione o un altro porto, nel quale, come stabilito sulla base delle informazioni comunicate per via elettronica in tale parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13 e nel GISIS, sono disponibili impianti adeguati;

c) l'esenzione non incide negativamente sulla sicurezza marittima, sulla salute, sulle condizioni di vita e di lavoro a bordo o sull'ambiente marino.

2. Qualora sia concessa l'esenzione, lo Stato membro in cui è situato il porto rilascia un certificato di esenzione, in base al formato di cui all'allegato 5, che conferma che la nave rispetta le condizioni e gli obblighi necessari all'applicazione dell'esenzione stessa e ne attesta la durata.

3. Le informazioni di cui al certificato di esenzione sono riportate per via elettronica dagli Stati membri nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13.

4. Gli Stati membri provvedono al monitoraggio e alla corretta applicazione degli accordi in essere relativi alle navi soggette a esenzioni che fanno scalo nei loro porti per il conferimento e il pagamento.

5. Fatta salva l'esenzione concessa, una nave non procede verso il successivo porto di scalo se è presente un'insufficiente capacità di stoccaggio dedicata a tutti i rifiuti che sono già stati accumulati e che saranno accumulati nel corso del viaggio previsto della nave fino al successivo porto di scalo.

Sezione 4

Misure esecutive

Articolo 10

Ispezioni

Gli Stati membri provvedono a ispezioni, anche casuali, per qualsiasi nave per verificarne la conformità alla presente direttiva.

Articolo 11

Impegni di ispezione

1. Ogni Stato membro ispeziona almeno il 15 % del numero totale di singole navi che fanno scalo nei propri porti ogni anno.

Il numero totale di singole navi che fanno scalo in uno Stato membro corrisponde al numero medio di singole navi registrate nel triennio precedente nella parte del sistema informativo, di monitoraggio e di applicazione di cui all'articolo 13.

2. Gli Stati membri rispettano il paragrafo 1 del presente articolo selezionando le navi mediante il meccanismo unionale basato sul rischio.

Al fine di garantire l'armonizzazione delle ispezioni e prevedere condizioni uniformi per la selezione delle navi da ispezionare, la Commissione adotta atti di esecuzione affinché possa definire nel dettaglio gli elementi del meccanismo unionale basato sul rischio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 20, paragrafo 2.

3. Gli Stati membri stabiliscono le procedure di ispezione delle navi che non rientrano nell'ambito di applicazione della direttiva 2002/59/CE al fine di garantire, per quanto possibile, la conformità alla presente direttiva.

Nel definire dette procedure gli Stati membri possono tener conto del meccanismo unionale basato sul rischio di cui al paragrafo 2.

4. Se l'autorità pertinente dello Stato membro non è soddisfatta dei risultati di tale ispezione, fatta salva l'applicazione delle sanzioni di cui all'articolo 16, assicura che la nave non lasci il porto fino a che non avrà conferito i propri rifiuti a un impianto portuale di raccolta in conformità dell'articolo 7.

Articolo 12

Sistema informativo, di monitoraggio e di applicazione

L'attuazione e l'applicazione della presente direttiva sono agevolate dal sistema elettronico di comunicazione e di scambio di informazioni tra gli Stati membri, in conformità degli articoli 13 e 14.

Articolo 13

Comunicazione e scambio di informazioni

1. La comunicazione e lo scambio di informazioni si basano sul sistema dell'Unione per lo scambio di dati marittimi («SafeSeaNet») di cui all'articolo 22 *bis*, paragrafo 3, e all'allegato III della direttiva 2002/59/CE.

2. Gli Stati membri assicurano che le seguenti informazioni siano comunicate per via elettronica entro un tempo ragionevole in conformità della direttiva 2010/65/UE:

a) le informazioni sull'ora effettiva di arrivo e di partenza di ogni nave che rientra nell'ambito di applicazione della direttiva 2002/59/CE che fa scalo in un porto dell'Unione, insieme a un identificativo del porto in questione;

b) le informazioni riportate nella notifica anticipata dei rifiuti di cui all'allegato 2;

c) le informazioni riportate nella ricevuta di conferimento dei rifiuti di cui all'allegato 3;

d) le informazioni riportate nel certificato di esenzione di cui all'allegato 5.

3. Gli Stati membri assicurano che le informazioni elencate all'articolo 5, paragrafo 2, siano disponibili elettronicamente attraverso SafeSeaNet.

Articolo 14

Registrazione delle ispezioni

1. La Commissione elabora, mantiene e aggiorna una banca dati sulle ispezioni a cui sono collegati tutti gli Stati membri e che contiene tutte le informazioni necessarie per attuare il sistema di ispezioni istituito dalla presente direttiva («banca dati sulle ispezioni»). La banca dati sulle ispezioni è basata su quella di cui all'articolo 24 della direttiva 2009/16/CE e ha funzionalità simili.

2. Gli Stati membri assicurano che le informazioni relative alle ispezioni a norma della presente direttiva, comprese le informazioni relative ai casi di non conformità e ai provvedimenti di fermo emessi, siano trasferite senza ritardi alla banca dati sulle ispezioni, non appena:

a) sia stato completato il rapporto di ispezione;

b) sia stato revocato il provvedimento di fermo; o

c) sia stata concessa un'esenzione.

3. La Commissione assicura che la banca dati sulle ispezioni sia completa di qualsiasi dato pertinente comunicato dagli Stati membri ai fini del monitoraggio dell'attuazione della presente direttiva.

La Commissione assicura che la banca dati sulle ispezioni contiene informazioni per il meccanismo unionale basato sul rischio di cui all'articolo 11, paragrafo 2.

La Commissione riesamina periodicamente la banca dati sulle ispezioni per monitorare l'attuazione della presente direttiva e richiamare l'attenzione su eventuali dubbi in merito all'attuazione globale al fine di incentivare un'azione correttiva.

4. Gli Stati membri hanno accesso in qualsiasi momento alle informazioni registrate nella banca dati sulle ispezioni.

Articolo 15

Formazione del personale

Le autorità portuali e le autorità dell'impianto portuale di raccolta provvedono affinché tutto il personale riceva la formazione idonea per lo svolgimento del proprio lavoro sul trattamento dei rifiuti, con particolare attenzione agli aspetti relativi alla salute e alla sicurezza connessi al trattamento di materiali pericolosi. Tali autorità garantiscono altresì che i requisiti di formazione siano regolarmente aggiornati per rispondere alle sfide dell'innovazione tecnologica.

Articolo 16

Sanzioni

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 garantirne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive.

Sezione 5

Disposizioni finali

Articolo 17

Scambio di esperienze

La Commissione provvede all'organizzazione di uno scambio di esperienze tra le autorità nazionali e gli esperti degli Stati membri, compresi quelli del settore privato, della società civile e dei sindacati, in merito all'applicazione della presente direttiva nei porti dell'Unione.

Articolo 18

Procedura di modifica

1. Alla Commissione è conferito il potere di adottare atti delegati in conformità dell'articolo 19 al fine di modificare gli allegati della presente direttiva e i riferimenti agli strumenti dell'IMO nella presente direttiva nella misura necessaria a renderli conformi al diritto dell'Unione o per tenere conto degli sviluppi a livello internazionale, in particolare a livello dell'IMO.

2. Alla Commissione è conferito inoltre il potere di adottare atti delegati conformemente all'articolo 19 per modificare gli allegati qualora ciò si renda necessario per migliorarne i meccanismi stabiliti di attuazione e monitoraggio, in particolare, quelli di cui agli articoli 6, 7 e 9, al fine di provvedere alla notifica e al conferimento dei rifiuti efficaci e alla corretta applicazione delle esenzioni.

3. In casi eccezionali, ove debitamente giustificato da un'adeguata analisi da parte della Commissione e allo scopo di evitare una minaccia grave e inaccettabile all'ambiente marino, alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per modificare la presente direttiva, nella misura necessaria a evitare tale minaccia, allo scopo di non applicare una modifica della convenzione MARPOL ai fini della presente direttiva.

4. Gli atti delegati di cui al presente articolo sono adottati almeno tre mesi prima della scadenza del periodo fissato a livello internazionale per la tacita accettazione della modifica della convenzione MARPOL o della data prevista per l'entrata in vigore di detta modifica.

Nel periodo che precede l'entrata in vigore di detti atti delegati gli Stati membri si astengono da qualsiasi iniziativa volta a integrare la modifica nel diritto nazionale o ad applicare la modifica allo strumento internazionale in questione.

Articolo 19

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 18, paragrafi 1, 2 e 3, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 27 giugno 2019. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 18, paragrafi 1, 2 e 3, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale del «Legiferare meglio»13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 18, paragrafi 1, 2 e 3, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo sia il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 20

Procedura di comitato

1. La Commissione è assistita dal comitato per la sicurezza marittima e la prevenzione dell'inquinamento provocato dalle navi (COSS), istituito dal regolamento (CE) n. 2099/2002 del Parlamento europeo e del Consiglio ([22]). Tale comitato 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.

Articolo 21

Modifica della direttiva 2010/65/UE

Al punto A dell'allegato della direttiva 2010/65/UE, il punto 4 è sostituito dal seguente:

«4. Notifica di rifiuti delle navi, compresi i residui

Articoli 6, 7 e 9 della direttiva (UE) 2019/883 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa agli impianti portuali di raccolta per il conferimento dei rifiuti delle navi, che modifica la direttiva 2010/65/UE e abroga la direttiva 2000/59/CE (GU L 151 del 7.6.2019, pag. 116).».

Articolo 22

Abrogazione

La direttiva 2000/59/CE è abrogata.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva.

Articolo 23

Riesame

1. La Commissione procede a una valutazione della presente direttiva e presenta i risultati della valutazione al Parlamento europeo e al Consiglio entro il 28 giugno 2026. Tale valutazione include altresì una relazione dettagliata sulle migliori azioni in materia di prevenzione e gestione dei rifiuti rilevate a bordo delle navi.

2. Nell'ambito del regolamento (UE) 2016/1625 del Parlamento europeo e del Consiglio ([23]), in occasione della prossima revisione del mandato dell'Agenzia europea per la sicurezza marittima (EMSA), la Commissione valuta l'opportunità di conferire all'EMSA competenze aggiuntive ai fini dell'esecuzione della presente direttiva.

([22]) Regolamento (CE) n. 2099/2002 del Parlamento europeo e del Consiglio, del 5 novembre 2002, che istituisce un comitato per la sicurezza marittima e la prevenzione dell'inquinamento provocato dalle navi (comitato COSS) e recante modifica dei regolamenti in materia di sicurezza marittima e di prevenzione dell'inquinamento provocato dalle navi (GU L 324 del 29.11.2002, pag. 1).

([23]) Regolamento (UE) 2016/1625 del Parlamento europeo e del Consiglio, del 14 settembre 2016, che modifica il regolamento (CE) n. 1406/2002 che istituisce un'Agenzia europea per la sicurezza marittima (GU L 251 del 16.9.2016, pag. 77).

Articolo 24

Attuazione

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 28 giugno 2021. Essi ne informano immediatamente la Commissione.

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.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni principali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 25

Entrata in vigore

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

Articolo 26

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO 1

DISPOSIZIONI PER I PIANI DI RACCOLTA E DI GESTIONE DEI RIFIUTI NEI PORTI

I piani di raccolta e di gestione dei rifiuti nei porti devono riguardare tutti i tipi di rifiuti delle navi che abitualmente fanno scalo in un porto e sono elaborati in conformità delle dimensioni del porto e della tipologia delle navi che vi fanno scalo.

I piani di raccolta e di gestione dei rifiuti nei porti devono includere i seguenti elementi:

a) una valutazione dell'esigenza di impianti portuali di raccolta in funzione delle necessità delle navi che abitualmente fanno scalo nel porto;

b) una descrizione del tipo e della capacità degli impianti portuali di raccolta;

c) una descrizione delle procedure di accettazione e raccolta dei rifiuti delle navi;

d) una descrizione del sistema di recupero dei costi;

e) una descrizione della procedura per la segnalazione delle presunte inadeguatezze rilevate negli impianti portuali di raccolta;

f) una descrizione della procedura per le consultazioni permanenti con gli utenti dei porti, le imprese di gestione dei rifiuti, gli operatori dei terminal e le altre parti interessate; nonché

g) una panoramica del tipo e dei quantitativi di rifiuti conferiti dalle navi e gestiti negli impianti.

I piani di raccolta e di gestione dei rifiuti nei porti possono includere:

a) una sintesi del diritto nazionale pertinente, la procedura e le formalità per il conferimento dei rifiuti agli impianti portuali di raccolta;

b) l'identificazione di un punto di contatto nel porto;

c) una descrizione degli impianti e dei processi di pretrattamento per eventuali flussi specifici di rifiuti nel porto;

d) una descrizione delle modalità di registrazione dell'uso effettivo degli impianti portuali di raccolta;

e) una descrizione delle modalità di registrazione dei quantitativi di rifiuti conferiti dalle navi;

f) una descrizione delle modalità di gestione nel porto dei diversi flussi di rifiuti.

Le procedure di accettazione, raccolta, stoccaggio, trattamento e smaltimento dovrebbero essere del tutto conformi a un programma di gestione ambientale in grado di ridurre progressivamente l'impatto ambientale di queste attività. Tale conformità si presume se le procedure sono conformi al regolamento (CE) n. 1221/2009 del Parlamento europeo e del Consiglio ([1]).

([1]) Regolamento (CE) n. 1221/2009 del Parlamento europeo e del Consiglio, del 25 novembre 2009, sull'adesione volontaria delle organizzazioni a un sistema comunitario di ecogestione e audit (EMAS), che abroga il regolamento (CE) n. 761/2001 e le decisioni della Commissione 2001/681/CE e 2006/193/CE (GU L 342 del 22.12.2009, pag. 1).

ALLEGATO 2

FORMATO STANDARD DEL MODULO DI NOTIFICA ANTICIPATA PER IL CONFERIMENTO DEI RIFIUTI AGLI IMPIANTI PORTUALI DI RACCOLTA

Notifica del conferimento dei rifiuti a: *[inserire il nome del porto di destinazione di cui all'articolo 6 della direttiva (UE) 2019/883]*

Il presente modulo dovrebbe essere conservato a bordo della nave insieme al registro degli idrocarburi, al registro dei carichi, al registro dei rifiuti solidi o al piano di gestione dei rifiuti, come prescritto dalla convenzione MARPOL.

1. DATI DELLA NAVE

1.1. Nome della nave	1.5. Proprietario o operatore:
1.2. Numero IMO:	1.6. Lettere o numero di identificazione:
	Numero MMSI (identificativo del servizio mobile marittimo):
1.3. Stazza lorda:	1.7. Stato di bandiera:
1.4. Tipo di nave: ☐ Petroliera ☐ Chimichiera ☐ Portarinfuse ☐ Container ☐ Nave da carico di altro tipo ☐ Nave passeggeri ☐ Ro-ro ☐ Altro (specificare)	

2. DATI RELATIVI AL VIAGGIO E AL PORTO

2.1. Luogo/nome del terminal:	2.6. Ultimo porto in cui sono stati conferiti i rifiuti:
2.2. Data e ora di arrivo:	2.7. Data dell'ultimo conferimento:
2.3. Data e ora di partenza:	2.8. Porto di conferimento successivo:
2.4. Ultimo porto e paese di scalo:	2.9. Persona che presenta il presente modulo (se diversa dal comandante):
2.5. Porto o paese successivo di scalo (se noto):	

3. TIPO E QUANTITATIVO DI RIFIUTI E CAPACITÀ DI STOCCAGGIO

Tipo	Rifiuti da conferire (m^3)	Massima capacità di stoccaggio dedicata (m^3)	Quantitativo di rifiuti trattenuti a bordo (m^3)	Porto in cui saranno conferiti i rifiuti restanti	Quantitativo stimato di rifiuti che sarà prodotto tra la notifica e il successivo scalo (m^3)
MARPOL allegato I — Idrocarburi					
Acque oleose di sentina					
Residui oleosi (fanghi)					
Acque oleose di lavaggio delle cisterne					
Acque di zavorra sporche					

Tipo	Rifiuti da conferire (m^3)	Massima capacità di stoccaggio dedicata (m^3)	Quantitativo di rifiuti trattenuti a bordo (m^3)	Porto in cui saranno conferiti i rifiuti restanti	Quantitativo stimato di rifiuti che sarà prodotto tra la notifica e il successivo scalo (m^3)
Fanghi e residui di lavaggio delle cisterne					
Altro (specificare)					
MARPOL allegato II — Sostanze liquide nocive (NLS) ([1])					
Sostanza di categoria X					
Sostanza di categoria Y					
Sostanza di categoria Z					
OS - Altre sostanze					
MARPOL allegato IV — Acque reflue					
MARPOL allegato V — Rifiuti solidi					
A. Plastica					
B. Rifiuti alimentari					
C. Rifiuti domestici (ad esempio prodotti di carta, stracci, vetro, metallo, bottiglie, vasellame ecc.)					
D. Olio da cucina					
E. Ceneri prodotte dagli inceneritori					
F. Rifiuti operativi					
G. Carcasse di animali					
H. Attrezzi da pesca					
I. Rifiuti di apparecchiature elettriche ed elettroniche					

([1]) Indicare la designazione ufficiale di trasporto della sostanza liquida nociva coinvolta.

Tipo	Rifiuti da conferire (m^3)	Massima capacità di stoccaggio dedicata (m^3)	Quantitativo di rifiuti trattenuti a bordo (m^3)	Porto in cui saranno conferiti i rifiuti restanti	Quantitativo stimato di rifiuti che sarà prodotto tra la notifica e il successivo scalo (m^3)
J. Residui del carico (1) (dannosi per l'ambiente marino)					
K. Residui del carico (2) (non dannosi per l'ambiente marino)					
MARPOL allegato VI — Relativo all'inquinamento atmosferico					
Sostanze che riducono lo strato di ozono e attrezzature che contengono tali sostanze (3)					
Residui della depurazione dei gas di scarico					

Altri rifiuti, non disciplinati dalla convenzione MARPOL					
Rifiuti accidentalmente pescati					

Note

1. Tali informazioni devono essere usate per i controlli da parte dello Stato di approdo (PSC) e per altri scopi connessi con le ispezioni.
2. Il presente modulo deve essere compilato in ogni sua parte, salvo nel caso in cui la nave sia esentata a norma dell'articolo 9 della direttiva (UE) 2019/883

(1) Può trattarsi di stime. Indicare la designazione ufficiale di trasporto del carico secco.
(2) Può trattarsi di stime. Indicare la designazione ufficiale di trasporto del carico secco.
(3) Derivanti dalle normali attività di manutenzione a bordo.

ALLEGATO 3

FORMATO STANDARD PER LA RICEVUTA DI CONFERIMENTO DEI RIFIUTI

Il rappresentante designato del gestore dell'impianto portuale di raccolta deve fornire il seguente modulo al comandante della nave che ha conferito i rifiuti in conformità dell'articolo 7 della direttiva (UE) 2019/883.

Il presente modulo deve essere conservato a bordo della nave insieme al registro degli idrocarburi, al registro dei carichi, al registro dei rifiuti o al pPiano di gestione dei rifiuti, come prescritto dalla convenzione MARPOL.

1. DATI DELL'IMPIANTO PORTUALE DI RACCOLTA E DEL PORTO

1.1. Luogo/nome del terminal:	
1.2. Gestore/i dell'impianto portuale di raccolta:	
1.3. Gestore/i dell'impianto di trattamento — se diverso dal precedente:	
1.4. Data e ora di conferimento dei rifiuti da:	a:

2. DATI DELLA NAVE

2.1. Nome della nave:						2.5. Proprietario o operatore:		
2.2. Numero IMO:						2.6. Lettere o numero di identificazione: Numero MMSI (identificativo del servizio mobile marittimo):		
2.3. Stazza lorda:						2.7. Stato di bandiera:		
2.4. Tipo di nave:	☐	Petroliera	☐	Chimichiera	☐	Portarinfuse	☐	Container
	☐	Nave da carico di altro tipo	☐	Nave passeggeri	☐	Ro-ro	☐	Altro (specificare)

3. TIPO E QUANTITATIVO DI RIFIUTI RICEVUTI

MARPOL allegato I — Idrocarburi	Quantità (m^3)
Acque oleose di sentina	
Residui oleosi (fanghi)	
Acque oleose di lavaggio delle cisterne	
Acque di zavorra sporche	
Fanghi e residui di lavaggio delle cisterne	
Altro (specificare)	
MARPOL allegato II — Sostanze liquide nocive (NLS)	Quantità (m^3)/Nome (1)
Sostanza di categoria X	
Sostanza di categoria Y	
Sostanza di categoria Z	
AS — Altre sostanze	
MARPOL allegato IV — Acque reflue	Quantità (m^3)

MARPOL allegato V — Rifiuti solidi	Quantità (m^3)
A. Plastica	
B. Rifiuti alimentari	
C. Rifiuti domestici (ad esempio prodotti di carta, stracci, vetro, metallo, bottiglie, vasellame ecc.)	
D. Olio da cucina	
E. Ceneri prodotte dagli inceneritori	
F. Rifiuti operativi	
G. Carcasse di animali	
H. Attrezzi da pesca	
I. Rifiuti di apparecchiature elettriche ed elettroniche	
J. Residui del carico (2) (dannosi per l'ambiente marino)	
K. Residui del carico (2) (non dannosi per l'ambiente marino)	
MARPOL allegato VI — Relativo all'inquinamento atmosferico	Quantità (m^3)
Sostanze che riducono lo strato di ozono e attrezzature che contengono tali sostanze	
Residui della depurazione dei gas di scarico	
Altri rifiuti, non disciplinati dalla convenzione MARPOL	Quantità (m^3)
Rifiuti pescati passivamente	

(1) Indicare la designazione ufficiale di trasporto della sostanza liquida nociva coinvolta.
(2) Indicare la designazione ufficiale di trasporto del carico secco

ALLEGATO 4

CATEGORIE DI COSTI E DI ENTRATE NETTE CONNESSE AL FUNZIONAMENTO E ALL'AMMINISTRAZIONE DEGLI IMPIANTI PORTUALI DI RACCOLTA

Costi diretti	Costi indiretti	Entrate nette
Costi operativi diretti derivanti dall'effettivo conferimento dei rifiuti delle navi, comprese le voci di costo elencate di seguito	Costi amministrativi indiretti derivanti dalla gestione del sistema nel porto, comprese le voci di costo elencate di seguito	Proventi netti derivanti dai sistemi di gestione dei rifiuti e dai finanziamenti nazionali e regionali disponibili, comprese le entrate di cui sotto
— Fornitura di infrastrutture degli impianti portuali di raccolta, compresi container, cisterne, strumenti di lavorazione, chiatte, camion, raccolta dei rifiuti e impianti di trattamento. — Concessioni per l'affitto degli spazi, se del caso, o delle attrezzature necessarie al funzionamento degli impianti portuali di raccolta. — Effettivo funzionamento degli impianti portuali di raccolta: raccolta dei rifiuti delle navi, trasporto dei rifiuti dagli impianti portuali di raccolta per il trattamento finale, manutenzione e pulizia degli impianti portuali di raccolta, costi per il personale, comprese le ore di straordinario, fornitura di elettricità, analisi dei rifiuti e assicurazione. — Preparazione al riutilizzo, riciclaggio o smaltimento dei rifiuti delle navi, compresa la raccolta differenziata dei rifiuti. — Amministrazione: fatturazione, emissione delle ricevute di conferimento dei rifiuti alla nave, comunicazioni.	— Elaborazione e approvazione del piano di raccolta e di gestione dei rifiuti, compresa la sua attuazione ed eventuali audit. — Aggiornamento del piano di raccolta e di gestione dei rifiuti, compresi i costi del lavoro e i costi di consulenza, se del caso. — Organizzazione delle procedure di consultazione per la (ri)valutazione del piano di raccolta e di gestione dei rifiuti. — Gestione dei sistemi di notifica e di recupero dei costi, compresa l'applicazione di tariffe ridotte per le «navi verdi», la fornitura di sistemi informatici a livello dei porti, le analisi statistiche e i costi del lavoro associati. — Organizzazione delle procedure di appalto pubblico per la fornitura di impianti portuali di raccolta, così come il rilascio delle necessarie autorizzazioni per la fornitura di impianti portuali di raccolta nei porti; — Comunicazione di informazioni agli utenti del porto mediante la distribuzione di volantini, l'affissione di cartelli e manifesti nel porto o la pubblicazione delle informazioni sul sito web del porto, nonché trasmissione elettronica delle informazioni come previsto all'articolo 5; — Gestione dei sistemi di gestione dei rifiuti: regimi di responsabilità estesa del produttore, riciclaggio nonché richiesta ed esecuzione di fondi nazionali e regionali; — Altri costi amministrativi: costi di monitoraggio e comunicazione elettronica delle esenzioni di cui all'articolo 9.	— Benefici finanziari netti ottenuti da regimi di responsabilità estesa del produttore; — Altre entrate nette derivanti dalla gestione dei rifiuti, quali i sistemi di riciclaggio; — Finanziamenti nell'ambito del fondo europeo per gli affari marittimi e la pesca (FEAMP); — Altri finanziamenti o sussidi disponibili per i porti per la gestione dei rifiuti e la pesca.

ALLEGATO 5

CERTIFICATO DI ESENZIONE A NORMA DELL'ARTICOLO 9 IN RELAZIONE ALLE PRESCRIZIONI DI CUI AGLI ARTICOLI 6, 7, PARAGRAFO 1, E 8 DELLA DIRETTIVA (UE) 2019/883 NEL/I PORTO/I [INSERIRE PORTO] DI [INSERIRE STATO MEMBRO] [1]

Nome della nave	Lettere o numero di identificazione	Stato di bandiera
[inserire il nome della nave]	*[inserire il numero IMO]*	*[inserire il nome dello Stato di bandiera]*

effettua traffico di linea con scali frequenti e regolari presso il/i seguente/i porto/i ubicato/i in [*inserire nome dello Stato membro*] secondo un calendario o una rotta prestabilita:

[ ]

e fa scalo presso tali porti almeno una volta ogni due settimane:

[ ]

ed esistono accordi che garantiscono il conferimento dei rifiuti e il pagamento delle tariffe al porto o a una terza parte nel porto di:

[ ]

ed è pertanto esentata, in conformità di [*inserire disposizione pertinente nella legislazione nazionale del paese*], *dalle prescrizioni in materia di*:

☐ *obbligo di conferimento dei rifiuti delle navi*;

☐ *notifica anticipata dei rifiuti; e*

☐ *pagamento di una tariffa obbligatoria al seguente porto/ai seguenti porti*:

Il presente certificato è valido fino al [*inserire data*], a meno che i motivi alla base del rilascio del certificato non cambino prima di tale data.

Luogo e data

.....

Nome
Titolo

---

[1] Cancellare la dicitura inutile.

DIRETTIVA (UE) 2019/884 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019

che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1, secondo comma, lettera d),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria ([1]),

considerando quanto segue:

(1) L'Unione si è prefissa l'obiettivo di offrire ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone. Tale obiettivo dovrebbe essere conseguito, tra l'altro, attraverso misure appropriate per prevenire e combattere la criminalità, compresa la criminalità organizzata e il terrorismo.

(2) Detto obiettivo presuppone che le informazioni relative alle decisioni di condanna pronunciate negli Stati membri siano prese in considerazione al di fuori dello Stato membro di condanna in occasione di un nuovo procedimento penale, come stabilito nella decisione quadro 2008/675/GAI del Consiglio ([2]), sia per prevenire nuovi reati.

(3) Il succitato obiettivo implica lo scambio di informazioni estratte dal casellario giudiziale tra le competenti autorità degli Stati membri. Tale scambio di informazioni è organizzato e agevolato dalle norme fissate con decisione quadro 2009/315/GAI del Consiglio ([3]) e dal sistema europeo di informazione sui casellari giudiziali (ECRIS) istituito con decisione 2009/316/GAI del Consiglio ([4]).

(4) L'attuale quadro giuridico di ECRIS tuttavia non risponde sufficientemente alle caratteristiche delle richieste riguardanti cittadini di paesi terzi. Sebbene sia già possibile scambiare informazioni sui cittadini di paesi terzi tramite ECRIS, manca una procedura o un meccanismo comune dell'Unione che consenta di farlo in modo efficace, rapido e preciso.

(5) All'interno dell'Unione le informazioni sui cittadini di paesi terzi non sono raccolte come avviene per i cittadini degli Stati membri negli Stati membri di cittadinanza, ma sono solo conservate negli Stati membri in cui le condanne sono state pronunciate. Pertanto, per ottenere un quadro completo del trascorso criminale di un cittadino di paese terzo è necessario chiedere tali informazioni a tutti gli Stati membri.

(6) Tali «richieste generalizzate» impongono un onere amministrativo sproporzionato a tutti gli Stati membri, compresi quelli che non sono in possesso di informazioni sul cittadino di paese terzo interessato. Nella pratica, tale onere scoraggia gli Stati membri dal chiedere agli altri Stati membri informazioni sui cittadini di paesi terzi, il che ostacola gravemente lo scambio di informazioni tra gli Stati membri e fa sì che l'accesso alle informazioni sui precedenti penali sia limitato a quelle conservate nel proprio casellario nazionale. Di conseguenza, aumenta il rischio che lo scambio di informazioni tra gli Stati membri sia inefficiente e incompleto.

([1]) Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.

([2]) Decisione quadro 2008/675/GAI del Consiglio, del 24 luglio 2008, relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (GU L 220 del 15.8.2008, pag. 32).

([3]) Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziale (GU L 93 del 7.4.2009, pag. 23).

([4]) Decisione 2009/316/GAI del Consiglio, del 6 aprile 2009, che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2009/315/GAI (GU L 93 del 7.4.2009, pag. 33).

(7) Per migliorare la situazione la Commissione ha presentato una proposta che ha portato all'adozione del regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio ([5]) che istituisce un sistema centralizzato a livello dell'Unione, contenente i dati personali di cittadini di paesi terzi condannati al fine di consentire l'individuazione degli Stati membri in possesso di informazioni sulle precedenti condanne («ECRIS-TCN»).

(8) ECRIS-TCN permetterà all'autorità centrale di uno Stato membro di individuare prontamente ed efficacemente in quali altri Stati membri sono conservate informazioni sui precedenti penali di un cittadino di paese terzo, in modo che l'attuale quadro di ECRIS possa essere usato per richiedere tali informazioni a quegli Stati membri conformemente alla decisione quadro 2009/315/GAI.

(9) Lo scambio di informazioni sulle condanne penali è un elemento importante di qualsiasi strategia di lotta alla criminalità e al terrorismo. Il pieno sfruttamento da parte degli Stati membri del potenziale di ECRIS contribuirebbe quindi alla risposta di giustizia penale alla radicalizzazione che porta al terrorismo e all'estremismo violento.

(10) Al fine di rafforzare l'utilità delle informazioni sulle condanne e le interdizioni derivanti da condanne per reati sessuali a danno di minori, la direttiva 2011/93/UE del Parlamento europeo e del Consiglio ([6]) stabilisce l'obbligo per gli Stati membri di adottare le misure necessarie per assicurare che, per assumere una persona per una posizione che comporti un contatto diretto e regolare con minori, le informazioni sulle condanne esistenti per reati sessuali a danno di minori iscritte nel casellario giudiziale o sulle interdizioni esistenti per tali reati siano trasmesse secondo le procedure di cui alla decisione quadro 2009/315/GAI. L'obiettivo di tale meccanismo è garantire che una persona condannata per un reato sessuale a danno di minori non possa occultare tale condanna o interdizione al fine di esercitare un'attività professionale che comporti contatti diretti e regolari con minori in un altro Stato membro.

(11) La presente direttiva è volta a introdurre le necessarie modifiche alla decisione quadro 2009/315/GAI per consentire uno scambio efficace di informazioni sulle condanne di cittadini di paesi terzi tramite ECRIS. Essa obbliga gli Stati membri di adottare le misure necessarie a garantire che le condanne siano corredate di informazioni sulla cittadinanza o sulle cittadinanze della persona condannata, nella misura in cui gli Stati membri dispongano di tali informazioni. Introduce inoltre le procedure di risposta alle richieste di informazioni, garantisce l'integrazione dell'estratto del casellario giudiziale richiesto da un cittadino di paese terzo con le informazioni provenienti da altri Stati membri e prevede le modifiche tecniche necessarie per il funzionamento del sistema di scambio di informazioni.

(12) La direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([7]) dovrebbe applicarsi al trattamento dei dati personali da parte delle autorità nazionali competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([8]) dovrebbe applicarsi al trattamento dei dati personali da parte delle autorità nazionali quando tale trattamento non rientra nell'ambito di applicazione della direttiva (UE) 2016/680.

(13) Al fine di garantire condizioni uniformi di esecuzione della decisione quadro 2009/315/GAI, è opportuno incorporare in tale decisione quadro i principi della decisione 2009/316/GAI e attribuire 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 ([9]).

([5]) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare e sostenere il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) n. 1077/2011 (GU L 135 del 22.5.2019, pag. 1).

([6]) 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).

([7]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

([8]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa 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).

([9]) 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).

(14) L'infrastruttura di comunicazione comune utilizzata per lo scambio delle informazioni estratte dai casellari giudiziali dovrebbe essere la rete di servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni (s-TESTA) o qualsiasi suo ulteriore sviluppo o rete sicura alternativa.

(15) Nonostante la possibilità di avvalersi di programmi finanziari dell'Unione in conformità delle norme applicabili, ogni Stato membro dovrebbe sostenere i propri costi per l'attuazione, la gestione, l'uso e la manutenzione della propria banca dati di casellari giudiziali e per l'attuazione, la gestione, l'uso e la manutenzione degli adeguamenti tecnici necessari per usare ECRIS.

(16) La presente direttiva rispetta diritti e libertà fondamentali sanciti, in particolare, nella Carta dei diritti fondamentali dell'Unione europea, compresi il diritto alla protezione dei dati di carattere personale, i diritti al ricorso giurisdizionale e amministrativo, il principio dell'uguaglianza davanti alla legge, il diritto a un giusto processo, la presunzione d'innocenza e il divieto generale di discriminazione. La presente direttiva dovrebbe essere attuata conformemente a tali diritti e principi.

(17) Poiché l'obiettivo della presente direttiva, vale a dire consentire uno scambio rapido ed efficace di informazioni accurate estratte dai casellari giudiziali relative ai cittadini di paesi terzi, non può essere conseguito in misura sufficiente dagli Stati membri ma, ponendo in essere norme comuni, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(18) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al trattato sul funzionamento dell'Unione europea (TFUE), la Danimarca non partecipa all'adozione della presente direttiva, non è da essa vincolata né è soggetta alla sua applicazione.

(19) A norma degli articoli 1 e 2 nonché dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione della presente decisione, non è da essa vincolata né è soggetta alla sua applicazione.

(20) A norma dell'articolo 3 e dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21, il Regno Unito ha notificato che desidera partecipare all'adozione e all'applicazione della presente direttiva.

(21) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([10]) e ha espresso un parere il 13 aprile 2016 ([11]).

(22) È opportuno pertanto modificare di conseguenza la decisione quadro 2009/315/GAI,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Modifiche della decisione quadro 2009/315/GAI

La decisione quadro 2009/315/GAI è così modificata:

1) l'articolo 1 è sostituito dal seguente:

«*Articolo 1*

Oggetto

La presente decisione quadro

a) definisce le condizioni a cui lo Stato membro di condanna scambia con gli altri Stati membri le informazioni sulle condanne;

([10]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

([11]) GU C 186 del 25.5.2016, pag. 7.

b) definisce gli obblighi che incombono allo Stato membro di condanna e allo Stato membro di cittadinanza della persona condannata («Stato membro di cittadinanza della persona») e precisa i metodi da seguire nel rispondere a una richiesta di informazioni estratte dal casellario giudiziale;

c) istituisce un sistema informatico decentrato per lo scambio delle informazioni sulle condanne basato sulle banche dati di casellari giudiziali di ciascuno Stato membro, il sistema europeo di informazione sui casellari giudiziali (ECRIS).»;

2) all'articolo 2 sono aggiunte le lettere seguenti:

«d) «Stato membro di condanna», lo Stato membro in cui è stata pronunciata una condanna;

e) «cittadino di paese terzo», chiunque non sia cittadino dell'Unione ai sensi dell'articolo 20, paragrafo 1, TFUE, l'apolide o qualsiasi persona la cui cittadinanza è ignota;

f) «dati relativi alle impronte digitali» i dati relativi alle impressioni piatte e rollate delle impronte digitali di ciascun dito;

g) «immagine del volto» le immagini digitalizzate del volto di una persona;

h) «implementazione di riferimento ECRIS» il software sviluppato dalla Commissione e messo a disposizione degli Stati membri per lo scambio delle informazioni sui casellari giudiziali tramite ECRIS.»;

3) all'articolo 4, il paragrafo 1 è sostituito dal seguente:

«1. Ciascuno Stato membro di condanna adotta tutte le misure necessarie per garantire che le condanne comminate nell'ambito del proprio territorio siano corredate di informazioni sulla cittadinanza o sulle cittadinanze della persona condannata qualora tale persona sia un cittadino di un altro Stato membro o un cittadino di paese terzo. Il casellario giudiziale indica se le informazioni sulla cittadinanza non sono note o se la persona condannata è un apolide.»;

4) l'articolo 6 è così modificato:

a) il paragrafo 3 è sostituito dal seguente:

«3. Qualora un cittadino di uno Stato membro chieda informazioni sul proprio casellario giudiziale all'autorità centrale di un altro Stato membro, detta autorità centrale rivolge all'autorità centrale dello Stato membro di cittadinanza una richiesta di estrazione di informazioni e dati a esse attinenti dai casellari giudiziali e include tali informazioni e dati a esse attinenti nell'estratto da fornire all'interessato.»;

b) è inserito il paragrafo seguente:

«3 *bis*. Qualora un cittadino di paese terzo chieda informazioni sul proprio casellario giudiziale all'autorità centrale di uno Stato membro, detta autorità centrale rivolge alle autorità centrali degli Stati membri che possiedono informazioni sui precedenti penali dell'interessato una richiesta di estrazione di informazioni e dati a esse attinenti dal casellario giudiziale e include tali informazioni e dati a esse attinenti nell'estratto da fornire all'interessato.»;

5) l'articolo 7 è così modificato:

a) il paragrafo 4 è sostituito dal seguente:

«4. Qualora una richiesta di informazioni estratte dal casellario giudiziale sulle condanne pronunciate a carico di un cittadino di uno Stato membro sia rivolta ai sensi dell'articolo 6 all'autorità centrale di uno Stato membro che non sia quello di cittadinanza, lo Stato membro richiesto trasmette tali informazioni nella misura prevista dall'articolo 13 della Convenzione europea di assistenza giudiziaria in materia penale.»;

b) è inserito il paragrafo seguente:

«4 *bis*. Qualora una richiesta di informazioni estratte dal casellario giudiziale sulle condanne pronunciate a carico di un cittadino di paese terzo sia presentata ai sensi dell'articolo 6 ai fini di un procedimento penale, lo Stato membro richiesto trasmette le informazioni sulle condanne pronunciate nello Stato membro richiesto e iscritte nei casellari giudiziali e sulle condanne pronunciate in paesi terzi di cui abbia ricevuto notifica e iscritte nei casellari giudiziali.

Se tali informazioni sono richieste a fini diversi da un procedimento penale, si applica di conseguenza il paragrafo 2 del presente articolo.»;

6) all'articolo 8, il paragrafo 2 è sostituito dal seguente:

«2. La risposta alla richiesta di cui all'articolo 6, paragrafi 2, 3 e 3 *bis*, è trasmessa entro venti giorni lavorativi dal ricevimento della richiesta.»;

7) l'articolo 9 è così modificato:

a) al paragrafo 1, i termini «articolo 7, paragrafi 1 e 4» sono sostituiti dai termini «articolo 7, paragrafi 1, 4 e 4 *bis*»;

b) al paragrafo 2, i termini «articolo 7, paragrafi 2 e 4» sono sostituiti dai termini «articolo 7, paragrafi 2, 4 e 4 *bis*»;

c) al paragrafo 3, i termini «articolo 7, paragrafi 1, 2 e 4» sono sostituiti dai termini «articolo 7, paragrafi 1, 2, 4 e 4 *bis*»;

8) l'articolo 11 è così modificato:

a) al paragrafo 1, primo comma, lettera c), è aggiunto il punto seguente:

«iv) immagine del volto.»;

b) i paragrafi da 3 a 7 sono sostituiti dai seguenti:

«3. Le autorità centrali degli Stati membri si trasmettono le seguenti informazioni per via elettronica attraverso ECRIS e in formato standardizzato conformemente alle norme che devono essere stabilite negli atti di esecuzione:

a) le informazioni di cui all'articolo 4;

b) le richieste di cui all'articolo 6;

c) le risposte di cui all'articolo 7; e

d) altre informazioni pertinenti.

4. Ove non fosse disponibile la via di trasmissione di cui al paragrafo 3, le autorità centrali degli Stati membri si trasmettono tutte le informazioni di cui al paragrafo 3 con qualsiasi mezzo che lasci una traccia scritta, in modo tale da consentire all'autorità centrale dello Stato membro ricevente di accertare l'autenticità dell'informazione, tenendo conto della sicurezza della trasmissione.

Se la via di trasmissione di cui al paragrafo 3 non è disponibile per un periodo significativo, lo Stato membro interessato ne informa gli altri Stati membri e la Commissione.

5. Ciascuno Stato membro procede agli adeguamenti tecnici necessari per poter il suo uso del formato standardizzato per trasmettere per via elettronica attraverso ECRIS tutte le informazioni di cui al paragrafo 3 agli altri Stati membri. Ciascuno Stato membro notifica alla Commissione da quale data sarà in grado di effettuare tali trasmissioni.»;

9) sono inseriti gli articoli seguenti:

«*Articolo 11* bis

Sistema europeo di informazione sui casellari giudiziali (ECRIS)

1. Ai fini dello scambio elettronico di informazioni estratte dal casellario giudiziale in conformità della presente decisione quadro, è istituito un sistema informatico decentrato basato sulle banche dati di casellari giudiziali di ciascuno Stato membro, il sistema europeo di informazione sui casellari giudiziali (ECRIS). È composto dai seguenti elementi:

a) implementazione di riferimento ECRIS;

b) infrastruttura di comunicazione comune tra le autorità centrali che forma una rete cifrata.

Per assicurare la riservatezza e l'integrità delle informazioni sui precedenti penali trasmesse ad altri Stati membri, si deve ricorrere a idonee misure tecniche e organizzative, tenendo conto dello stato dell'arte, del costo relativo all'attuazione e dei rischi associati al trattamento delle informazioni.

2. Tutti i dati estratti dai casellari giudiziali sono conservati unicamente nelle banche dati gestite dagli Stati membri.

3. Le autorità centrali degli Stati membri non hanno un accesso diretto alle banche dati di casellari giudiziali degli altri Stati membri.

4. Lo Stato membro interessato è responsabile della gestione dell'implementazione di riferimento ECRIS e delle banche dati che conservano, inviano e ricevono informazioni estratte dai casellari giudiziali. L'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) istituita dal regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio (*) sostiene gli Stati membri nell'ambito dei suoi compiti stabiliti dal regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio (**).

5. La Commissione è responsabile del funzionamento dell'infrastruttura di comunicazione comune. Questa soddisfa i requisiti di sicurezza necessari e risponde pienamente alle esigenze di ECRIS.

6. eu-LISA fornisce, sviluppa ulteriormente e gestisce l'implementazione di riferimento ECRIS.

7. Ciascuno Stato membro sostiene i propri costi per l'attuazione, la gestione, l'uso e la manutenzione della propria banca dati di casellari giudiziali e per l'installazione e l'uso dell'implementazione di riferimento ECRIS.

La Commissione sostiene i costi per l'attuazione, la gestione, l'uso, la manutenzione e il futuro sviluppo dell'infrastruttura di comunicazione comune.

8. Gli Stati membri che utilizzano il proprio software nazionale di implementazione ECRIS a norma dell'articolo 4, paragrafi da 4 a 8, del regolamento (UE) 2019/816 possono continuare a utilizzare il proprio software nazionale di implementazione ECRIS al posto dell'implementazione di riferimento ECRIS, a condizione che soddisfino tutte le condizioni di cui a detti paragrafi.

Articolo 11 ter

Atti di esecuzione

1. La Commissione stabilisce con atti di esecuzione:

a) il formato standardizzato di cui all'articolo 11, paragrafo 3, anche per quanto riguarda le informazioni relative al reato che ha determinato la condanna e le informazioni relative al contenuto della condanna;

b) le norme concernenti l'attuazione tecnica di ECRIS e lo scambio di dati sulle impronte digitali;

c) le altre modalità tecniche per organizzare e agevolare gli scambi di informazioni sulle condanne fra le autorità centrali degli Stati membri, comprese:

i) le modalità per agevolare la comprensione delle informazioni trasmesse e la loro traduzione automatica;

ii) le modalità di scambio delle informazioni per via elettronica, in particolare con riferimento alle specifiche tecniche da usare e, se necessario, alle procedure di scambio applicabili.

2. Gli atti di esecuzione di cui al paragrafo 1 del presente articolo sono adottati secondo la procedura di esame di cui all'articolo 12 *bis*, paragrafo 2.

(*) Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011 (EU) No 1077/2011 (GU L 295 del 21.11.2018, pag. 99).»;

(**) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare e sostenere il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).

10) è inserito l'articolo seguente:

«*Articolo 12* bis

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.

Qualora il comitato non esprima alcun parere, la Commissione non adotta il progetto di atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.»;

11) è inserito l'articolo seguente:

«*Articolo 13* bis

Presentazione di relazioni da parte della Commissione e riesame

1. Entro l'29 giugno 2023, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione della presente decisione quadro. La relazione valuta in che misura gli Stati membri hanno adottato le misure necessarie per conformarsi alla presente decisione quadro, compresa la sua attuazione tecnica.

2. La relazione è corredata, se del caso, di opportune proposte legislative.

3. La Commissione pubblica una relazione periodica sugli scambi delle informazioni estratte dai casellari giudiziali tramite ECRIS e sull'uso di ECRIS-TCN, basata in particolare sulle statistiche fornite da eu-LISA e dagli Stati membri in conformità del regolamento (UE) 2019/816. Essa è pubblicata per la prima volta un anno dopo la presentazione della relazione di cui al paragrafo 1.

4. La relazione della Commissione di cui al paragrafo 3 riguarda, in particolare, il livello di scambio delle informazioni fra Stati membri, anche in riferimento a cittadini di paesi terzi, nonché l'obiettivo delle richieste e il relativo numero, comprese le richieste a fini diversi da un procedimento penale, come i controlli sui precedenti e le richieste di informazioni delle persone interessate in merito ai propri casellari giudiziali.».

Articolo 2

Sostituzione della decisione 2009/316/GAI

La decisione 2009/316/GAI è sostituita in relazione agli Stati membri vincolati dalla presente direttiva, fatti salvi gli obblighi di tali Stati membri relativi al termine di recepimento di tale decisione.

Articolo 3

Recepimento

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 28 giugno 2022. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Esse recano altresì l'indicazione che, nelle disposizioni legislative, regolamentari e amministrative in vigore, i riferimenti alla decisione sostituita dalla presente direttiva si intendono fatti a quest'ultima. Le modalità del riferimento e dell'indicazione sono stabilite dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni principali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

3. Gli Stati membri provvedono agli adeguamenti tecnici di cui all'articolo 11, paragrafo 5, della decisione quadro 2009/315/GAI, come modificata dalla presente direttiva, entro il 28 giugno 2022.

Articolo 4

Entrata in vigore e applicazione

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

L'articolo 2 si applica a decorrere dal 28 giugno 2022.

Articolo 5

Destinatari

Gli Stati membri sono destinatari della presente direttiva conformemente ai trattati.

Fatto a Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ISSN 1977-0707 (edizione elettronica)
ISSN 1725-258X (edizione cartacea)

Ufficio delle pubblicazioni dell'Unione europea
2985 Lussemburgo
LUSSEMBURGO

IT