

RELAZIONE ILLUSTRATIVA

1. La legge delega

Il presente schema di decreto legislativo realizza la delega di cui all'articolo 18 della legge 22 aprile 2021, n. 53, “Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020”, nel seguito indicata semplicemente con “legge delega”, recante

Principi e criteri direttivi per l'adeguamento della normativa nazionale alle disposizioni del titolo III, Quadro di certificazione della cybersicurezza, del regolamento (UE) 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).

In particolare, il Governo, ai sensi del comma 1, è chiamato ad adottare, entro dodici mesi dalla data di entrata in vigore della suddetta legge (ovvero entro il termine del 7/5/2022), uno o più decreti legislativi per l'adeguamento della normativa nazionale al Titolo III del regolamento (UE) 2019/881, nel seguito indicato semplicemente come “regolamento europeo”.

Va tuttavia precisato che il regolamento europeo pone per gli stati membri adempimenti nazionali a far data già dal 28/6/2021. In particolare, l'articolo 69, paragrafo 2 del regolamento europeo, prevede con decorrenza posticipata di due anni rispetto alla sua entrata in vigore, ovvero al 28 giugno 2021, l'attuazione nazionale degli articoli 58, 60, 61, 63, 64 e 65.

Il regolamento europeo mira ad introdurre regole armonizzate in tutta l'Unione Europea per la certificazione di cybersicurezza di prodotti TIC (Tecnologie dell'Informazione e delle Comunicazioni), servizi TIC e processi TIC. Tuttavia, i primi effetti concreti sull'ordinamento dei singoli stati membri avverranno soltanto attraverso la successiva adozione di sistemi europei di certificazione della cybersicurezza elaborati per specifici ambiti¹ e la cui introduzione è prevista nei prossimi anni con atti di esecuzione della Commissione Europea (art. 49, par. 7). In particolare, l'introduzione di nuovi sistemi di certificazione avrà i seguenti effetti (art. 57) sugli ordinamenti nazionali:

- i sistemi di certificazione stabiliranno regole armonizzate nell'UE per la certificazione di cybersicurezza per specifici ambiti;
- i sistemi di certificazione europei, con la loro adozione, abrogheranno gli eventuali sistemi nazionali di certificazione della cybersicurezza esistenti che dovessero sovrapporsi con i nuovi sistemi europei essendo operativi sullo stesso ambito indirizzato da un sistema di certificazione europeo;
- con l'adozione di un sistema europeo di certificazione gli stati membri dovranno astenersi dall'introdurre sistemi nazionali di certificazione per lo stesso ambito.

Gli elementi di un sistema europeo di certificazione sono definiti dall'articolo 54, paragrafo 1 del regolamento europeo e sono riconducibili alle seguenti aree principali:

¹ Sono in corso di elaborazione sistemi europei di certificazione della cybersicurezza per i seguenti ambiti: certificazioni in base allo standard Common Criteria, servizi cloud, reti 5G. Con la pubblicazione del piano di sviluppo della Commissione Europea (art. 47 del regolamento europeo) per i prossimi anni si prevede l'adozione sistemi di certificazione specifici anche per i dispositivi IoT (Internet of Things), e per gli IACS (industrial automation and control systems).



- ambito, oggetto e scopo di un sistema europeo di certificazione;
- standard e specifiche tecniche, criteri e metodi di valutazione, di riferimento a fronte dei quali sono emessi certificati e dichiarazioni UE di conformità per prodotti TIC, servizi TIC, processi TIC;
- requisiti per l'accreditamento e l'autorizzazione degli organismi di valutazione della conformità abilitati ad emettere certificati, le regole per la conservazione dei loro registri e le informazioni supplementari da conservare assieme ai certificati sul processo di valutazione;
- regole di utilizzo di eventuali marchi ed etichette;
- regole per il controllo di conformità dei certificati e delle dichiarazioni UE, il loro mantenimento, la segnalazione di vulnerabilità rilevate successivamente all'emissione di un certificato o dichiarazione UE, periodo di validità dei certificati, modalità di rilascio, modifica e revoca dei certificati;
- formati e procedure per la formazione e notifica dei certificati e dichiarazioni UE di conformità;
- condizioni per il mutuo riconoscimento dei certificati UE con paesi terzi.

L'introduzione graduale di sistemi di certificazione europei della cybersicurezza permetterà di ridurre il livello di frammentazione del Mercato Unico dell'Unione Europea realizzando anche il mutuo riconoscimento dei certificati di cybersicurezza tra tutti gli stati membri ovunque emessi nell'Unione Europea, elevando al contempo il livello di affidabilità di prodotti TIC, servizi TIC e processi TIC dal punto di vista della sicurezza informatica. In particolare, la certificazione di cybersicurezza per un prodotto TIC, servizio TIC e processo TIC confermerà l'effettiva aderenza a standard e specifiche tecniche per la realizzazione di misure di contrasto ai rischi di sicurezza informatica.

Come già evidenziato, seppur lo strumento, in quanto regolamento europeo, entrato in vigore il 28/6/2019, sia direttamente applicabile in tutti gli stati membri, per potersi attuare, ha bisogno di alcune riforme preliminari che sono in capo a ciascuno stato membro e riguardano principalmente gli articoli 58, 60, 61, 63, 64 e 65. In particolare, per il contesto nazionale sono da ricomprendere necessariamente nello schema di decreto legislativo le seguenti riforme:

- l'istituzione di una autorità nazionale di certificazione della cybersicurezza (art. 58, par. 1), con il compito principale di far rispettare nel proprio territorio nazionale le disposizioni del Titolo III e dei successivi sistemi europei di certificazione adottati nell'Unione ed il compito accessorio di emissione dei certificati di livello elevato,
- e la conseguente definizione di un quadro sanzionatorio (art 65) che permetterà alle autorità nazionali di far rispettare il regolamento europeo ed i successivi sistemi di certificazione adottati nell'Unione Europea.

A tal fine, il presente schema di decreto legislativo mira ad attuare le riforme necessarie per rendere il nuovo quadro europeo di certificazione, di cui al Titolo III del regolamento europeo, operativo a livello nazionale in vista dei successivi sistemi europei di certificazione che saranno via via adottati nell'Unione Europea.

Nell'ambito del mandato conferito per l'attuazione del Titolo III, il Governo, ai sensi del comma 2, è tenuto ad osservare oltreché i principi e criteri direttivi generali di cui all'articolo 32 della legge n. 234 del 2012, anche i seguenti criteri direttivi specifici:

- a) *designare il Ministero dello sviluppo economico quale autorità competente ai sensi del paragrafo 1 dell'articolo 58 del regolamento (UE) 2019/881;*



- b) *individuare l'organizzazione e le modalità per lo svolgimento dei compiti e l'esercizio dei poteri dell'autorità di cui alla lettera a), attribuiti ai sensi dell'articolo 58 e dell'articolo 56, paragrafi 5 e 6, del regolamento (UE) 2019/881;*
- c) *definire il sistema delle sanzioni applicabili ai sensi dell'articolo 65 del regolamento (UE) 2019/881, prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati ad apposito capitolo dello stato di previsione dell'Ministero dello sviluppo economico per finalità di ricerca e formazione in materia di certificazione della cybersicurezza; le sanzioni amministrative pecuniarie non devono essere inferiori nel minimo a 15.000 euro e non devono essere superiori nel massimo a 5.000.000 di euro;*
- d) *prevedere, in conformità all'articolo 58, paragrafi 7 e 8, del regolamento (UE) 2019/881, il potere dell'autorità di cui alla lettera a) di revocare i certificati rilasciati ai sensi dell'articolo 56, paragrafi 4 e 5, lettera b), emessi sul territorio nazionale, salvo diverse disposizioni dei singoli sistemi europei di certificazione adottati ai sensi dell'articolo 49 di detto regolamento.*

2. Gli effetti del decreto-legge 14 giugno 2021, n. 82 sulla legge delega

Il successivo decreto-legge 14 giugno 2021, n. 82, convertito con Legge 4 agosto 2021, n. 109, ha inciso sull'articolo 18 della Legge 53/2021 con due disposizioni:

- con l'articolo 7, comma 1, lett. e) del decreto-legge, la nuova Agenzia per la cybersicurezza nazionale assume la funzione di Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento europeo;
- in base all'articolo 16, comma 12, lettera b) del decreto-legge “*ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale*”.

Con la prima disposizione, è operata di fatto un'abrogazione implicita del criterio direttivo specifico a), in quanto l'Agenzia per la cybersicurezza nazionale ha già assunto, col suddetto decreto al posto del Ministero dello sviluppo economico, la funzione di autorità nazionale di certificazione della cybersicurezza ai sensi dell'art. 58 del regolamento europeo, anticipando la designazione nazionale di tale autorità prevista per lo schema di decreto legislativo di cui al comma 1, dell'art. 18 della L. 53/2021.

In base alla seconda disposizione i riferimenti al Ministero dello sviluppo economico in tutti i criteri di delega sono sostituiti con i riferimenti alla nuova Agenzia per la cybersicurezza nazionale, con effetto in particolare sul criterio direttivo specifico c), divenendo l'Agenzia per la cybersicurezza nazionale, oltreché il soggetto già designato quale autorità nazionale di certificazione della cybersicurezza, anche destinataria degli introiti delle sanzioni di cui all'art. 65 del regolamento europeo.

Ciò premesso l'ambito in cui il Governo è chiamato ad operare nell'attuazione dell'art. 18 della legge 53/2021 è costituito, oltre che dai criteri direttivi generali della L. n. 234/2012, dai soli criteri direttivi specifici b)-d), dal momento che il criterio direttivo specifico a) è stato superato dalla disposizione di cui all'articolo 7, comma 2, lett. e), del decreto legge 82/2021.

Quindi, il Governo, in primo luogo, è delegato a definire per l'autorità nazionale di certificazione della cybersicurezza, già individuata, l'organizzazione e le modalità operative (criterio direttivo specifico b)) per le attività di vigilanza nazionale (art. 58, paragrafi 7-8 del regolamento europeo),



che costituiscono l'ambito prevalente di azione dell'autorità, assieme alle attività di rilascio dei certificati (art. 56, paragrafi 5(a) e 6), che si aggiungono come funzioni accessorie dell'autorità per esercitare un maggiore controllo sul mercato delle certificazioni di cybersicurezza.

Il quadro sanzionatorio da introdurre (criterio direttivo specifico c)) prevedrà sanzioni pecuniarie tra i 15.000 euro ed i 5.000.000 di euro ed i relativi introiti saranno riassegnati all'Agenzia per la cybersicurezza nazionale per le finalità di ricerca e formazione in materia di certificazione della cybersicurezza.

Sarà inoltre conferito all'autorità, in quanto responsabile a livello nazionale del rispetto del Titolo III e successivi sistemi di certificazione, il potere di "revocare" certificati emessi ai sensi dell'articolo 56, paragrafi 4 e 5 (criterio direttivo specifico d)). Ovvero, i certificati per i livelli di certificazione di base e sostanziale, emessi normalmente da organismi di certificazione diversi dell'autorità (salvo l'eccezione di cui all'art. 56, par. 5, lett. a)) e che operano senza la supervisione diretta dell'autorità in ogni processo di certificazione, potranno essere revocati dall'Agenzia, ammenoché le disposizioni dello specifico sistema di certificazione nell'ambito del quale è emesso il certificato disponga diversamente. A tal proposito, è da evidenziare che l'autorità italiana, tra i poteri minimi riservati a tutte le autorità dal regolamento europeo al paragrafo 8, dispone già del potere di revoca dei certificati di livello elevato (articolo 58, par. 8, lett. e)). Il criterio direttivo specifico di cui alla lettera d) della legge delega estende quindi tale potere di revoca dell'autorità anche ai livelli di base e sostanziale (art. 56, parr. 4-5). La facoltà di estendere in ambito nazionale i poteri delle autorità nazionali di certificazione della cybersicurezza rispetto ai poteri già conferiti in sede europea dal regolamento europeo, all'art. 58, par. 8, lett. a)-f), è reso possibile dalla formulazione dello stesso paragrafo, che elenca i poteri delle autorità nazionali come un insieme minimo e non completo di possibili poteri. In particolare, il paragrafo 8 dell'articolo 58 del regolamento europeo riporta quanto segue.

“Ciascuna autorità nazionale di certificazione della cibersicurezza dispone almeno dei seguenti poteri: ...” a cui seguono i poteri di cui alle successive lettere a)-f)

Da tale formulazione si deduce che in aggiunta ai poteri esplicitamente conferiti a tutte le autorità nazionali nell'Unione Europea di cui alle successive lettere a) – f), è possibile prevedere a livello del singolo stato membro ulteriori poteri. Pertanto, con il criterio direttivo specifico d) di cui all'articolo 18, comma 2 della legge delega, si è scelto di estendere il potere di revoca dei certificati dell'autorità nazionale in Italia anche ai livelli di affidabilità sostanziale e di base, ad esempio per meglio tutelare particolari interessi pubblici e diritti fondamentali.

3. Lo schema di decreto legislativo

Ciò premesso, definiti gli obiettivi e gli spazi d'intervento per il Governo in base all'art. 18 della legge delega ed al successivo decreto-legge 14 giugno 2021, n. 82, si sceglie di operare attraverso un singolo schema decreto legislativo recante tutte le riforme necessarie per rendere operativo il Titolo III del regolamento europeo a livello nazionale.

Lo schema di decreto è inviato alle Camere ai sensi dell'articolo 31 della legge n. 234 del 2012, in forza del richiamo di cui all'articolo 1 della legge di delegazione 2019-2020 (l. n. 53 del 2021)”.

Lo schema di decreto legislativo proposto si compone quindi di 15 articoli suddivisi in 5 capi.



Il **CAPO I** “Disposizioni generali” contiene gli articoli da 1 a 3.

L'**articolo 1** “Oggetto e ambito di applicazione” definisce l'ambito d'intervento del decreto legislativo che riguarda in primo luogo l'attuazione nazionale del Titolo III di cui al comma 1 della legge delega.

Al **comma 1** si introduce l'oggetto dello schema di decreto legislativo finalizzato all'adeguamento della normativa nazionale al nuovo quadro europeo di certificazione della cybersicurezza, introdotto mediante le disposizioni del Titolo III del regolamento europeo.

Al **comma 2** lett. a) e c) si richiamano quindi i sopracitati criteri direttivi specifici b) e c) di cui al comma 2 della legge delega quali finalità principali del decreto legislativo. Al comma 2, lett. b) si individuano inoltre le modalità di cooperazione con le altre autorità di vigilanza del mercato pertinenti e l'organismo di accreditamento nazionale (art. 58 par. 7 lett. a), c), g), h) e par. 9 del regolamento europeo), che rientrano nei compiti di vigilanza nazionale dell'autorità.

Si evidenzia infine al **comma 3**, coerentemente con l'art. 1, par. 2 del regolamento europeo, che non sono interessate dal decreto legislativo *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.*

L'**articolo 2** “Trattamento dei dati personali” dispone che il trattamento dei dati personali in applicazione del decreto legislativo sia effettuato, in accordo con il regolamento europeo per la protezione dei dati personali (regolamento (UE) 2016/679) e con il codice per la protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196 vigente).

L'**articolo 3** “Definizioni” include i principali termini richiamati nel testo e derivanti in primo luogo dallo stesso regolamento europeo (Cybersecurity Act), dal regolamento (CE) 765/2008 (su cui si basa il Cybersecurity Act) riguardante la vigilanza del mercato dell'Unione Europea, dal regolamento (UE) n. 1025/2012 sulla normazione europea, assieme ad alcune nuove definizioni. In particolare, per comodità si definisce con il termine conciso “Agenzia”, abbreviando Agenzia per la cybersicurezza nazionale, per riferirsi all'autorità nazionale di certificazione della cybersicurezza designata per l'Italia. Col termine “Regolamento” si indica il Titolo III del regolamento europeo. Con “quadro della europeo di certificazione” si intende il Regolamento ed i successivi sistemi europei di certificazione della cybersicurezza adottati nell'Unione Europea. Con il termine “Organismo di Accreditamento” si indica l'organismo di accreditamento nazionale designato in Italia ai sensi del regolamento (CE) 765/2008. Con il termine “abilitazione”, che non è definito dal regolamento europeo, si introduce un processo di verifica di requisiti ad opera dell'Agenzia per poter inserire un esperto o un laboratorio di prova in un elenco di soggetti dei quali si avvale l'Agenzia nella sua attività di vigilanza o di rilascio dei certificati a livello nazionale. Si introducono anche le definizioni dei due elenchi di esperti e laboratori di prova abilitati ad operare rispettivamente nelle attività di vigilanza nazionale e rilascio dei certificati per conto dell'Agenzia. Si introduce inoltre la definizione di Organismo di Certificazione della Sicurezza Informatica (OCSI), quale organismo di certificazione dell'Agenzia, ai sensi dell'articolo 60, paragrafo 2 del regolamento europeo e già introdotto operativo con DCPM 30 ottobre 2003 in seno all'ex Ministero delle comunicazioni.

Il **Capo II** “Autorità nazionale, attività nazionale ed internazionale” contiene gli articoli da 4 a 9.



L'**articolo 4** "Designazione dell'autorità nazionale di certificazione della cybersicurezza, organizzazione e procedure per lo svolgimento dei compiti in ambito nazionale di certificazione della cybersicurezza" include i principali elementi per l'identificazione e l'organizzazione dell'autorità nazionale di certificazione della cybersicurezza italiana.

In particolare, il **comma 1** individua l'autorità competente per la certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento europeo nell'Agenzia per la cybersicurezza nazionale di cui all'art. 5, del decreto-legge 14 giugno 2021, n. 82, già designata ai sensi all'art. 7, comma 1, lett. e), dello stesso decreto.

Il **comma 2** individua nei successivi articoli del Capo II e nell'articolo 11 le modalità operative generali dell'autorità, che riguardano la vigilanza nazionale, il rilascio dei certificati e la valutazione dei laboratori di prova e organismi di certificazione, l'attività di ricerca, formazione e sperimentazione e la gestione dei reclami, rinviando a successivo provvedimento dell'Agenzia ai sensi dell'articolo 5, comma 3 del DPCM 223/2021 (regolamento di organizzazione dell'Agenzia) gli aspetti di maggior dettaglio da specificare per ciascun articolo, ove necessario.

Con il fine di garantire quanto previsto dall'articolo 58, par. 4, del Regolamento – e cioè che le attività delle autorità nazionali di certificazione della cybersicurezza relative al rilascio di certificati europei di cybersicurezza siano rigorosamente separate dalle attività di vigilanza e siano svolte indipendentemente le une dalle altre – si prevede che tali attività saranno attestate nell'ambito di due distinte Divisioni di cui all'art. 4, comma 4, del Regolamento di organizzazione dell'ACN (DPCM n. 223/2021).

Infine, in attuazione dell'art. 58, par. 6 e par. 7.(h) si dispone per un coinvolgimento diretto dell'Agenzia in seno ai comitati di riferimento per la cooperazione europea previsti dal regolamento europeo ai sensi dell'art. 62 (lo European Cybersecurity Certification Group) e art. 66 (Comitato).

Il **comma 3**, in attuazione dell'art. 58, par. 5, la dotazione finanziaria necessaria per lo svolgimento dei compiti ad essa attribuiti, rimandando all'articolo 14, comma 1, l'individuazione della necessaria copertura economica.

L'**articolo 5** "Vigilanza nazionale" realizza le disposizioni di cui all'art. 58, par. 7 ed 8 del regolamento europeo, nelle quali sono individuati i compiti delle autorità nazionali dei singoli stati membri, da svolgersi anche in cooperazione con le altre autorità di vigilanza del mercato competenti e con gli organismi nazionali di accreditamento, ed i poteri da esercitare.

Il **comma 1** in particolare individua le funzioni di *vigilanza oggettiva* dell'Agenzia con riferimento ai *certificati di cybersicurezza* e alle *dichiarazioni UE di conformità* di cui all'articolo 58, paragrafo 7, lettere a)-b) del regolamento europeo e di *vigilanza soggettiva* con riferimento ai fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8 del Regolamento. Inoltre ai sensi delle lettere c)-e) l'Agenzia sostiene ed assiste l'Organismo di Accreditamento nel monitoraggio degli organismi di valutazione della conformità, vigila sugli organismi di valutazione della conformità pubblici e sospende, limita e revoca l'autorizzazione degli organismi di valutazione della conformità, quando previsto dal sistema europeo di certificazione, dandone notizia all'organismo nazionale di accreditamento.

Il **comma 2** stabilisce che l'autorità nazionale in Italia nei compiti di vigilanza, ai sensi dell'articolo 58, paragrafo 7 del regolamento europeo, coopera con altre autorità nazionali ed europee. Il comma 2 prevede che fra le autorità nazionali con cui stabilire una cooperazione vi sono le Forze dell'ordine, in quanto l'esercizio di alcuni poteri ispettivi dell'autorità nazionale di cui all'articolo 58 del paragrafo 8 del regolamento europeo potrebbe essere ostacolato dal soggetto sottoposto anche non volontariamente alle attività ispettive dell'autorità. A tal proposito, va osservato che solo nell'ambito di uno specifico sistema di certificazione settoriale potranno definirsi in maggior dettaglio le modalità di cooperazione con gli organi di Polizia, non essendo definito il contesto specifico di operatività dell'autorità direttamente dal regolamento europeo. Nel decreto legislativo si configura la semplice possibilità di



collaborazione con gli organi di Polizia, potendo un successivo provvedimento dell’Agenzia ai sensi dell’articolo 4, comma 2, anche attraverso successivi emendamenti ed integrazioni, ai sensi dell’articolo 15, adattarsi alle esigenze specifiche di un sistema di certificazione, definire le effettive modalità operative per ogni sistema europeo di certificazione, inclusi gli aspetti di cooperazione con le Forze di polizia.

Il **comma 3** individua i poteri dell’Agenzia in base all’articolo 58, paragrafo 8 del regolamento europeo e, in accordo con il criterio direttivo specifico ex art. 18, comma 2 lett. d) della legge delega, estende² il potere di revoca³ dei certificati ad opera dell’Agenzia, già previsto dal regolamento europeo all’articolo 58, paragrafo 8, lettera e) per il livello di affidabilità elevato, anche ai certificati di livello di base e sostanziale. In particolare, l’attività di vigilanza dell’Agenzia può prevedere sanzioni pecuniarie ed accessorie e prelievi di prodotti.

Il **comma 4** individua le casistiche di revoca dei certificati da parte dell’Agenzia. I soggetti destinatari di provvedimenti di revoca da parte dell’Agenzia sono sia gli organismi di valutazione della conformità emittenti certificati di livello elevato (come già stabilito dall’articolo 58, paragrafo 8, lettera e) del regolamento europeo), sia gli organismi di valutazione della conformità emittenti certificati di livello di base e sostanziale (in base al criterio direttivo specifico di cui alla lettera d) dell’art. 18 della L. 53/2021). In primo luogo, a seguito dell’accertamento di un certificato non conforme, il certificato è revocato in tre casi:

- a) se il certificato ha livello di affidabilità elevato;
- b) se il certificato ha livello di affidabilità di base o sostanziale nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale ai sensi dell’allegato II del decreto legislativo 18 maggio 2018, n. 65 e successive modificazioni o servizio di comunicazione elettronica ai sensi del decreto legislativo 1 agosto 2003, n. 259 e successive modificazioni o alla salute o all’incolumità personale;
- c) se previsto espressamente dallo specifico sistema europeo di certificazione.

Il **comma 5** individua le modalità di revoca per i casi stabiliti al comma 4. Nel caso dei certificati di livello elevato la revoca avviene da parte dell’Agenzia. Nel caso di certificati di livello di base o sostanziale la revoca avviene in prima battuta da parte dell’organismo di valutazione della conformità emittente entro 5 giorni su richiesta dell’Agenzia e solo se questi non interviene avviene da parte dell’Agenzia entro i successivi 5 giorni.

² Riguardo all’estensione dei poteri minimi comuni a tutte le autorità europee ai sensi dell’articolo 58, par. 8 ed in particolare del potere di revoca dei certificati si considerino i seguenti punti:

- Tra i vari poteri esplicitamente previsti, alle autorità nazionali europee, ai sensi del regolamento europeo, art. 58, par. 8, lett. e) è già data facoltà di revocare i certificati di livello di affidabilità elevato (art 56, par. 6) emessi o dalla stessa autorità, attraverso il suo organismo di certificazione interno (art. 60, par. 2), o da altro organismo di valutazione della conformità accreditato scelto dall’autorità (art. 56, par. 6, lett a)-b)). Con questo comma 3 del presente articolo il potere di revoca dei certificati per l’autorità è esteso anche ai certificati di livello di base e sostanziale, che sono emessi, ai sensi dell’art. 56, par. 4 o 5, nella maggioranza dei casi, da organismi di valutazione della conformità diversi dallo organismo di certificazione dell’autorità.
- Tra i poteri minimi elencati alla lettera c) è già individuato un potere generale che permette di adottare misure appropriate non specificate per il rispetto del regolamento europeo “adottare misure appropriate, nel rispetto del diritto nazionale, per accertare che gli organismi di valutazione della conformità, i titolari di certificati europei di cybersicurezza e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cybersicurezza”. Tale criterio denota un’ulteriore apertura del regolamento europeo nei confronti delle autorità ad esercitare ulteriori poteri compatibili con la normativa nazionale per assicurare il rispetto del regolamento europeo e successivi sistemi di certificazione.

³ Da evidenziare che con il termine revoca in questo contesto non si intende il significato di cui all’art. 25-quinquies della L. 241/1990 s.m. che riguarda l’annullamento da parte di un’amministrazione di provvedimenti da essa adottati, ma piuttosto il termine revoca è usato in senso estensivo, anche ai certificati di livello di base e sostanziale, rispetto al potere di revoca già previsto dal regolamento europeo all’articolo 58, par. 8, lett. e), riguardante i certificati di livello elevato, indipendentemente dal soggetto emittente per il contesto nazionale italiano.



Il **comma 6** disciplina la modalità di gestione dei certificati non conformi che non sono direttamente revocati in base ai casi stabiliti al comma 4. Al di fuori di questi casi di revoca, l'organismo di valutazione della conformità ha la possibilità di revocare spontaneamente il certificato o ricondurre a conformità il certificato entro 120 giorni, operando delle modifiche al certificato eventualmente a seguito di integrazione dell'attività di valutazione. In caso di mancata revoca o riconduzione nei termini previsti, il certificato decade. La riconduzione a conformità o revoca del certificato sono divulgate in base alle regole definite dallo specifico sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera s) del regolamento europeo. Inoltre, il comma 6 riguarda l'attività di sostegno ed assistenza dell'autorità all'organismo nazionale di accreditamento. In base all'art. 58, par. 7, lett. c), senza arrecare pregiudizio all'eventuale processo di autorizzazione⁴, l'Agenzia presta sostegno ed assistenza all'organismo nazionale di accreditamento, in particolare mettendo a disposizione le competenze dell'autorità e pertinenti informazioni (considerando (102) del regolamento europeo). In tal modo l'accREDITamento degli organismi di valutazione della conformità, a cura dell'organismo nazionale di accREDITamento, può beneficiare del supporto indiretto dell'autorità. Il comma 7 prevede che tali attività siano disciplinate da apposita convenzione o protocollo di intesa fra l'Agenzia e l'organismo nazionale di accREDITamento.

Il **comma 7** stabilisce che l'Agenzia può effettuare l'attività di vigilanza con il coinvolgimento di esperti esterni e laboratori di prova esterni registrati in un apposito elenco di esperti e di laboratori di prova per le attività di vigilanza

Il **comma 8** descrive le modalità di indagine ed ispezione dell'autorità per l'esercizio dei relativi poteri sui certificati e sulle dichiarazioni (UE) di conformità ai sensi dell'art. 58, par. 8 lett. a)-d). In particolare, si afferma il principio che il soggetto interessato dalle attività d'indagine deve offrire collaborazione, fornendo tutti i documenti, strumenti e informazioni necessari per le attività di indagine e che l'onere della prova della conformità dei certificati o delle dichiarazioni UE è in capo al soggetto emittitore o titolare sottoposto ad indagine.

Il **comma 9** stabilisce che il soggetto titolare del certificato o dell'emittente della dichiarazione UE di conformità sottoposto all'attività di vigilanza è tenuto a rimborsare integralmente i costi dell'Agenzia per l'utilizzo di personale interno e relativi mezzi, costi di missione e spese generali in base all'articolo 30, commi 4 e 5 della legge 234 del 2012 e successive modifiche. Altri costi, ad esempio relativi all'utilizzo di laboratori esterni di valutazione e spedizione di prodotti prelevati, sono anch'essi a carico del soggetto vigilato. I rimborsi da corrispondere per l'attività di vigilanza sono da erogare secondo le modalità dell'articolo 13.

L'**articolo 6** "Rilascio dei certificati di cybersicurezza" definisce le modalità per l'emissione dei certificati di cybersicurezza a livello nazionale per i livelli di affidabilità elevato (art. 56, paragrafo 6 del regolamento europeo) ed i livelli di affidabilità di base e sostanziale quando il rilascio per uno specifico sistema europeo di certificazione spetta ad un organismo pubblico (art. 56, paragrafo 5 del regolamento europeo), e disciplina, inoltre, le modalità con cui un sistema europeo di certificazione volontario possa essere reso obbligatorio a livello nazionale.

In particolare, il **comma 1** stabilisce che l'organismo di certificazione dell'autorità (art. 60, paragrafo 2) è l'Organismo di Certificazione della Sicurezza Informatica, detto anche OCSI, istituito con DPCM

⁴ L'organismo nazionale di accREDITamento, in base al regolamento (CE) 765/2008 ed al regolamento (UE) 2019/881, interviene nella verifica delle competenze degli organismi di valutazione della conformità. Il certificato di accREDITamento da esso emesso consente all'organismo di valutazione della conformità che ne è in possesso di operare autonomamente dall'autorità nell'emissione di certificati di livello di base e sostanziale, mentre l'attività di emissione dei certificati di livello elevato è subordinata ad una decisione dell'autorità ai sensi dell'art. 56, par. 6, lett. a) o b). Solo se previsto da uno specifico sistema di certificazione, l'operatività degli organismi di valutazione della conformità è subordinata ad una verifica supplementare o più specifica di competenze da parte dell'autorità, con la quale l'autorità autorizza l'organismo di valutazione della conformità (art. 60, par. 3) ad operare. Pertanto, salvo eccezioni, l'operatività degli organismi di valutazione della conformità per il rilascio dei certificati di affidabilità più bassa (di base e sostanziale) sarà normalmente assicurata da soggetti privati senza la supervisione diretta dell'autorità.



30 ottobre 2003 e trasferito all’Agenzia (articolo 7, comma 1, lett. e), del D.L. 14 giugno 2021, n. 82), che si può avvalere per l’emissione dei certificati di esperti esterni o laboratori di prova. Si osserva che, questi ultimi, in quanto organismi di valutazione della conformità, in base all’articolo 60, paragrafo 1 del regolamento europeo sono preliminarmente accreditati dall’organismo di accreditamento nazionale. Per poter svolgere tale attività per l’Agenzia, i laboratori di prova, già accreditati, devono essere abilitati dall’Agenzia e inseriti in un apposito elenco per le attività di rilascio dei certificati (articolo 8, comma 4). In alternativa all’emissione dei certificati da parte dell’Agenzia, la stessa può anche avvalersi di organismi di valutazione della conformità accreditati per il rilascio di certificati, in base alle modalità previste dal regolamento europeo ai sensi dell’articolo 56, paragrafo 6, lettere a) o b).

Si sottolinea che nel caso in cui l’Agenzia riservi per sé l’emissione dei certificati avvalendosi di esperti esterni o di laboratori di prova, l’Agenzia supervisiona ogni valutazione condotta da esperti o laboratori di prova e rilascia il certificato finale in caso di esito positivo della valutazione. Invece, nel caso del coinvolgimento di un organismo di valutazione della conformità ai sensi dell’articolo 56, paragrafo 6, lettere a) o b) del regolamento europeo, sarà lo stesso organismo di valutazione della conformità ad emettere il certificato, con preventiva approvazione da parte dell’Agenzia (lettera a)), o in base ad una delega generale ad emettere i certificati (lettera b)) conferita dall’Agenzia. In quest’ultimo caso, l’Agenzia potrà effettuare un audit periodico (ad esempio con cadenza annuale) sull’organismo di valutazione della conformità accreditato e dei certificati emessi a posteriori, piuttosto che verificare ogni singolo certificato prima della sua emissione.

Il **comma 2** individua le modalità di attuazione nazionali per l’articolo 56, paragrafo 5, lettere a) o b) del regolamento europeo, che individua come possibilità per alcuni sistemi europei di certificazione che sia solo un soggetto pubblico a rilasciare i certificati per il livello di base ed il livello sostanziale. Infatti, per tali livelli di certificazione, normalmente, l’emissione è effettuata, ai sensi dell’articolo 56, paragrafo 4, da un qualsiasi organismo di valutazione della conformità accreditato dall’organismo nazionale di accreditamento, senza la partecipazione dell’Agenzia.

Il comma 2 dispone che quando si applica l’eccezione di cui all’articolo 56, paragrafo 5, lettera a), decisa in sede europea per uno specifico sistema europeo di certificazione, l’autorità potrà anche avvalersi di esperti o di laboratori di prova come prospettato al comma 1. Invece, nel caso in cui si scelga altro organismo pubblico accreditato per l’emissione dei certificati (lettera b)), sarà l’Agenzia a designarla, salvo che lo specifico sistema di certificazione non disponga diversamente. Tale disposizione è volta a disciplinare a livello nazionale in modo semplice le modalità di base per la designazione dell’organismo di cui all’articolo 56, paragrafo 5, lettera b), e permette di escludere il ricorso ad un processo legislativo di rango primario.

Il **comma 3**, stabilisce che la certificazione della cybersicurezza è volontaria, salvo diversamente specificato dal diritto dell’Unione o dal diritto nazionale, ai sensi dell’articolo 56, paragrafo 2 del regolamento europeo. È possibile rendere obbligatorio un sistema di certificazione europeo esistente con regolamentazione tecnica dell’Agenzia, ai sensi del decreto legislativo del 15 dicembre 2017, n. 223, previa consultazione con i portatori di interesse. Tale disposizione recepisce il considerando (91) del regolamento europeo.

Il **comma 4**, in base all’articolo 30, commi 4 e 5 della legge 234 del 2012 e successive modifiche, pone gli oneri per il rilascio dei certificati da parte dell’Agenzia a carico del soggetto richiedente la certificazione. Le somme da corrispondere sono determinate ai sensi del successivo articolo 13 che individua le attività prestate a titolo oneroso dall’Agenzia.

L’**articolo 7** “Dichiarazioni UE di conformità”, disciplina le modalità di rilascio e gestione delle dichiarazioni UE di conformità da parte dei fabbricanti o fornitori, in accordo con l’articolo 55 del regolamento europeo.

Il **comma 1** stabilisce che i costruttori e fornitori, in conformità ai sensi dell’articolo 54, paragrafo 1, lettera e) del regolamento europeo, possono rilasciare dichiarazioni UE di conformità per dimostrare il rispetto di requisiti tecnici previsti da un sistema di certificazione per il livello di affidabilità di base.



Il **comma 2** stabilisce che il fabbricante o fornitore di prodotti TIC deve rendere disponibile all’Agenzia la dichiarazione di conformità, la relativa documentazione e le altre informazioni pertinenti. La copia di una dichiarazione UE di conformità è trasmessa all’Agenzia e ad ENISA

Il **comma 3** stabilisce l’obbligo per i fornitori o fabbricanti che rilasciano dichiarazioni UE non conformi di revisionarle o revocarle entro 30 giorni dall’accertamento di non conformità da parte dell’Agenzia dandone comunicazione all’Agenzia e all’ENISA, salvo diversa disposizione dello specifico sistema di certificazione.

Il **comma 4** stabilisce che il rilascio sulla conformità è volontario, in base all’articolo 53, paragrafo 4 del regolamento europeo e stabilisce la possibilità per l’Agenzia di rendere obbligatorie le dichiarazioni (UE) di conformità con regolamentazioni tecniche con le stesse modalità definite per i certificati obbligatori ai sensi dell’articolo 6, comma 3.

L’**articolo 8** “Accreditamento ed autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova dell’Agenzia” definisce l’assetto nazionale per le attività di valutazione delle competenze e di coinvolgimento degli organismi di valutazione della conformità nelle attività nazionali di valutazione e certificazione per l’attuazione del regolamento europeo.

Con il termine organismo di valutazione della conformità come da definizione nel regolamento europeo che riprende a sua volta la definizione nel regolamento (CE) 765/2008 si intende “*un organismo che svolge attività di valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni*”. Per le finalità specifiche del regolamento europeo, si individuano due tipologie di organismi di valutazione della conformità di maggior interesse, di cui all’articolo 3 dello schema di decreto legislativo ai punti 27 e 28:

- i *laboratori di prova*, che svolgono verifiche documentali e/o prove in base alle norme armonizzate europee ed agli standard e specifiche tecniche di riferimento ai sensi dell’articolo 54, para. 1, lett. c) del regolamento europeo per il sistema di certificazione per cui sono accreditati;
- gli *organismi di certificazione* che emettono certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli standard di riferimento ai sensi dell’articolo 54, para. 1, lett. c) del regolamento europeo per il sistema di certificazione per cui sono accreditati.

Essenzialmente i laboratori di prova effettuano le attività di valutazione di un prodotto TIC, servizio TIC o processo TIC rispetto ad una metodologia di riferimento emettendo un rapporto di prova che riporta i risultati della valutazione. Gli organismi di certificazione emettono invece un certificato per attestare, sulla base delle prove effettuate come documentate nei rapporti di prova prodotti in esito alle attività di valutazione, che un prodotto TIC, un servizio TIC o un processo TIC è conforme ad una norma armonizzata, standard o specifica tecnica.

Il **comma 1**, dispone che le attività di accreditamento e successivi aggiornamenti, a cura dell’organismo nazionale di accreditamento, in base all’articolo 60, paragrafi 1, 2 e 4 del regolamento europeo, siano comunicate all’Agenzia, in modo che questi possa notificare la Commissione Europea, ai sensi dell’articolo 61 dello stesso regolamento. Il comma prevede che tale comunicazione sia fatta anche all’ufficio unico di collegamento designato per l’Italia ai sensi dell’articolo 10, comma 3 del regolamento (UE) 2019/1020. L’ufficio unico di collegamento, istituito in seno al nuovo regolamento europeo per la vigilanza del mercato, ha la funzione di rappresentare la posizione coordinata nazionale delle autorità di vigilanza del mercato, come previsto dal comma 4 dello stesso articolo.

Il **comma 2**, stabilisce che l’Agenzia partecipa con propri rappresentanti alle deliberazioni sui certificati di accreditamento rilasciati dell’organismo nazionale di accreditamento nell’ambito del Cybersecurity Act.

Il **comma 4** stabilisce che l’Agenzia può costituire due elenchi di laboratori di prova per potersene avvalere rispettivamente nelle attività di vigilanza nazionale e nelle attività di rilascio dei certificati di cybersicurezza. Stabilisce inoltre che l’iscrizione all’elenco dei laboratori per le attività di vigilanza sia incompatibile con l’attività di valutazione o certificazione per i livelli di base e sostanziale in ambito nazionale. Tale restrizione è stabilita onde prevenire potenziali conflitti d’interesse tra l’attività di



vigilanza e l'attività di emissione dei certificati di uno stesso soggetto. Infine, rinvia, la definizione delle modalità di dettaglio per la gestione degli elenchi, ad un provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223.

Il **comma 5** qualifica le attività dell'Agenzia per l'autorizzazione degli organismi di valutazione della conformità, ove previste dallo specifico sistema di certificazione ai sensi dell'articolo 60, paragrafo 3, e l'abilitazione dei laboratori di prova quali attività svolte dall'Agenzia a titolo oneroso, da rimborsare da parte del soggetto abilitato o autorizzato in base all'articolo 13.

L'**articolo 9** "Attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza" introduce disposizioni per poter permettere all'Agenzia di realizzare riforme ed investimenti in ricerca ed innovazione, formazione e sperimentazione a livello nazionale per elevare il livello nazionale di sicurezza cibernetica.

Al **comma 1** è previsto che l'Agenzia possa realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione anche in collaborazione con università, centri di ricerca e laboratori specializzati nel campo della valutazione della sicurezza informatica anche nel contesto di attività di supporto alla standardizzazione nazionale, europea ed internazionale. Tale attività è svolta allo scopo di sviluppare competenze e contribuire al consesso europeo ai sensi dell'articolo 58, par. 9 del regolamento europeo.

Al **comma 2** si chiarisce che l'attività di ricerca e formazione è orientata anche a monitorare gli sviluppi nel campo della certificazione della sicurezza informatica, ai sensi dell'articolo 58, paragrafo 7, lettera i) del regolamento europeo e condividere buone pratiche a livello europeo con le omologhe autorità nazionali ed ENISA, ai sensi dell'articolo 58, paragrafo 9.

Al **comma 3** si individua come possibili riforme del quadro nazionale di certificazione la possibilità che l'Agenzia possa introdurre in via sperimentale nuovi sistemi di certificazione nazionali in conformità all'articolo 57 del regolamento europeo, ovvero escludendo ambiti già coperti da un sistema europeo di certificazione. Tale sistema nazionale può permettere lo sviluppo di nuovi settori per gli organismi di valutazione della conformità in vista di un successivo sistema di certificazione europeo sullo stesso campo di applicazione.

Il Capo III "Sanzioni, reclami e ricorsi giurisdizionali" raccoglie gli articoli da 10 a 12

L'**articolo 10** "Quadro sanzionatorio" introduce, come richiesto a tutti gli stati membri dall'articolo 65 del regolamento europeo, un quadro sanzionatorio per la violazione del regolamento europeo e dei sistemi europei di certificazione della cybersicurezza.

L'articolo è, inoltre, predisposto nell'esercizio del criterio delega di cui al comma 2, lettera c), del citato articolo 18 della legge di delegazione europea 2019-2020, che prevede la definizione del sistema delle sanzioni applicabili ai sensi del richiamato articolo 65 del regolamento (UE) 2019/881.

Inoltre, l'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021, prevede che l'Agenzia per la cybersicurezza nazionale assuma tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

Per la maggioranza delle sanzioni sono fatte salve le responsabilità penali qualora sia accertato un reato. Un prospetto riassuntivo delle sanzioni pecuniarie (commi 2 – 15) è riportato in Tabella 1.

Il **comma 1**, individua nell'Agenzia, conformemente all'articolo 58, par. 8, lett. f) del regolamento europeo ed anche ai sensi dell'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021, il soggetto nazionale a cui compete l'irrogazione delle sanzioni per violazione del quadro europeo di certificazione. Per l'irrogazione delle sanzioni si applica, in quanto compatibile, la disciplina della legge 24 novembre 1981, n. 689.

Il **comma 2** stabilisce una sanzione pecuniaria per l'organismo di valutazione della conformità emittente un certificato di cybersicurezza non conforme al quadro europeo di certificazione da 15.000



euro a 75.000 euro. Qualora il certificato non sia revocato direttamente dall’Agenzia e debba essere piuttosto l’organismo a revocarlo, ai sensi dell’articolo 5, comma 4, in caso di omessa revoca da parte dell’organismo si applica una ulteriore sanzione da 30.000 a 150.000 euro.

Il **comma 3** individua le sanzioni pecuniarie per il fabbricante o fornitore emittente una dichiarazione UE di conformità volontaria nel caso di accertamento di non conformità. È prevista una sanzione da 15.000 euro a 75.000 euro.

L’accertamento di non conformità comporta il successivo obbligo di revisione o di revoca della dichiarazione entro 30 giorni da parte del soggetto emittente, ai sensi dell’articolo 7, comma 3. In caso di omessa revisione o revoca sia nel caso di un sistema europeo di certificazione obbligatorio, sia nel caso di un sistema europeo di certificazione volontario, si applica inoltre una sanzione da 30.000 a 150.000 euro.

Il **comma 4** individua le sanzioni pecuniarie ed accessorie in relazione alla messa a disposizione sul mercato di un prodotto TIC o servizio TIC che richieda certificato o dichiarazione UE obbligatoria. L’obbligatorietà di un sistema di certificazione può essere disposta per l’ambito europeo o essere anticipata da un singolo stato membro. In caso di obbligatorietà di un certificato o dichiarazione UE di conformità, le violazioni del quadro europeo di certificazione rivestono maggiore gravità rispetto al caso di un regime volontario.

In particolare, in caso di messa a disposizione sul mercato senza un certificato o dichiarazione UE di conformità il fabbricante o fornitore è punito con sanzione da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC si avvale di un processo TIC privo di dichiarazione UE obbligatoria o con dichiarazione UE obbligatoria non conforme o in assenza di certificato di cybersicurezza obbligatorio.

Preso atto dell’assenza di un certificato o dichiarazione UE di conformità obbligatoria per l’immissione sul mercato o in caso di non conformità è necessario provvedere al ritiro dal mercato del prodotto o inibizione del servizio, venendo a mancare il presupposto fondamentale per l’immissione. Il **comma 5** pertanto stabilisce che, in caso di revoca o decadenza di un certificato obbligatorio, l’Agenzia dispone per il ritiro del prodotto o inibizione del servizio dal mercato a carico esclusivo del fabbricante o fornitore indicandone i tempi e le eventuali modalità.

Il **comma 6** individua per il fabbricante che non ottempera a quanto prescritto al comma 5 per il richiamo di prodotti già immessi sul mercato una sanzione amministrativa da 60.000 euro a 300.000 euro. Nel caso in cui il fabbricante emittente una dichiarazione UE di conformità non ottemperi al richiamo di prodotti dal mercato, l’Agenzia, trascorsi 6 mesi dalla scadenza fissata, può provvedere, al sequestro dei prodotti residui dal mercato, a spese del fabbricante.

Il **comma 7** individua le sanzioni per il fornitore emittente una dichiarazione UE di conformità che non ottempera a quanto prescritto al comma 5 per l’inibizione del servizio dal mercato assoggettandolo alla sanzione amministrativa da 60.000 euro a 300.000 euro.

Il **comma 8** dispone che i soggetti che, rilevando o venendo a conoscenza della presenza di vulnerabilità nel prodotto TIC, servizio TIC o processo TIC certificato o dichiarato conforme, successivamente al processo di valutazione, non notifichino o trattino tali vulnerabilità ai sensi dell’articolo 56, paragrafo 8 del regolamento europeo o ai sensi dell’articolo 54, paragrafo 1, lettera m) dello stesso regolamento siano assoggettati ad una sanzione da 60.000 euro a 300.000 di euro.

Il **comma 9** stabilisce le sanzioni da 30.000 a 150.000 euro per il fabbricante o fornitore che non ottemperi ai vari obblighi informativi stabiliti dal regolamento europeo in relazione a dichiarazioni UE di conformità emesse o certificati detenuti. Alla medesima sanzione è assoggettato il fornitore o fabbricante che non comunichi la revisione o revoca di una dichiarazione UE ai sensi dell’articolo 7, comma 3.

Il **comma 10** stabilisce sanzioni da 30.000 a 150.000 euro per l’organismo di valutazione della conformità che non ottemperi ad obblighi informativi stabiliti dal regolamento europeo in relazione ai certificati emessi.

Il **comma 11** punisce l'esercizio di attività quale organismo di valutazione della conformità senza autorizzazione con una sanzione pecuniaria da 120.000 euro a 600.000 euro e con una sanzione accessoria che stabilisce il divieto di rilascio di autorizzazione per tale soggetto nei successivi 3 anni dall'accertamento della violazione. Il comma distingue tuttavia un caso particolare d'infrazione più lieve, ovvero se l'autorizzazione è scaduta da meno di un anno. In tal caso la sanzione è ridotta e compresa tra 10.000 euro e 150.000 euro e non si applica la sanzione accessoria in quanto non si ricade nel caso di un soggetto che esercita abusivamente l'attività di organismo di valutazione della conformità senza esser stato mai autorizzato o non più autorizzato da diverso tempo, ma piuttosto si tratta del caso di un organismo di valutazione della conformità che verosimilmente ha ritardato il processo di rinnovo dell'accreditamento.

Il **comma 12** punisce con una sanzione pecuniaria da 90.000 a 450.000 euro, chi scientemente fornisce dati falsi o ometta informazioni necessarie durante un processo di certificazione o le attività di verifica per la vigilanza nazionale.

Il **comma 13** punisce il fabbricante o fornitore che viola le condizioni di utilizzo degli eventuali marchi o etichette previste da un sistema europeo di certificazione, con una sanzione da 30.000 a 150.000 euro.

Il **comma 14** punisce l'organismo di valutazione della conformità che non ottempera agli eventuali obblighi riguardanti la conservazione dei registri, ai sensi dell'articolo 54, paragrafo 1, lettera n) del regolamento europeo, con una sanzione amministrativa da 45.000 a 225.000 euro

Il **comma 15** prevede che l'Agenzia possa impartire ordini o intimare diffide ai soggetti che operano in contrasto al quadro europeo di certificazione. Ai soggetti che non ottemperano l'Agenzia commina una sanzione amministrativa pecuniaria da euro 200.000 ad euro 1.000.000. Per i soggetti con fatturato elevato, almeno pari a 200.000.000 di euro, si applica una sanzione amministrativa pecuniaria proporzionale al fatturato non inferiore allo 0,3 per cento e non superiore al 1,5 per cento del fatturato, restando comunque fermo il limite massimo di 5.000.000 di euro (stabilito dal criterio direttivo di cui al comma 2, lett. c) dell'articolo 18 della L. 53/2021). Come riferimento per il fatturato si assume il valore realizzato dallo stesso soggetto nell'ultimo esercizio finanziario chiuso anteriormente alla notificazione della contestazione.

Al **comma 16** si prevede che, fermo restando il limite massimo di 5.000.000 di euro per la sanzione, i valori minimi e massimi delle sanzioni pecuniarie dal comma 2 al comma 16, siano triplicati, se la violazione ha riguardato l'ambito di un sistema di certificazione destinato ad un servizio essenziale ai sensi dell'allegato II del decreto legislativo 18 maggio 2018, n. 65 e successive modificazioni o ad un servizio di comunicazione elettronica ai sensi del decreto legislativo del 1 agosto 2003, n. 259 e successive modificazioni.

Il **comma 17** prevede che i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie sono definiti con successivo provvedimento dell'Agenzia, specificando che nelle more dell'adozione del provvedimento di definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della L. 24 novembre 1981, n. 689. Tale disposizione, seppur non limitando la discrezionalità concessa alle amministrazioni di graduare le sanzioni da un livello minimo ad un massimo come previsto dalla legge 689 del 1981, dà copertura normativa ad un possibile provvedimento successivo adottato con la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, che stabilisca in modo oggettivo i criteri di graduazione delle sanzioni, una volta valutati, sulla base dell'esperienza maturata nell'irrogazione delle sanzioni, i principali aspetti da considerare.

Il **comma 18**, fermo restando il limite massimo di 5.000.000 di euro, stabilisce un criterio di rivalutazione delle sanzioni amministrative pecuniarie previste dal presente decreto ai commi, dal 2 al 14 da attuarsi ogni 5 anni con provvedimento dell'Agenzia, adottato con la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, rapportato all'indice ISTAT dei prezzi al consumo.

Il **comma 19** punisce con la sospensione o revoca dell'autorizzazione per un organismo di valutazione della conformità ad operare nel sistema europeo di certificazione ai sensi dell'articolo 60, paragrafo 3



del regolamento europeo, nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio. In caso di revoca dell'autorizzazione, il trasgressore non può ottenere nuova autorizzazione nei successivi 5 anni dal provvedimento di revoca. Il **comma 20** prevede, come stabilito dall'articolo 65 del regolamento europeo, che l'Agenzia notifichi alla Commissione Europea il quadro sanzionatorio di cui al presente articolo. Si stabilisce il termine di 60 giorni dall'entrata in vigore del presente decreto per la notifica dell'introduzione del quadro sanzionatorio e per le eventuali modifiche ugualmente si stabilisce il termine di 60 giorni dall'introduzione delle stesse modifiche per la notifica alla Commissione Europea.

Tabella 1 – Prospetto riassuntivo sanzioni pecuniarie

COMMA	TIPO VIOLAZIONE	destinatario della sanzione	Al di fuori dell'ambito NIS o TELCO		Nell'ambito NIS o TELCO	
			MINIMO	MASSIMO	MINIMO	MASSIMO
2 - prima parte	certificato non conforme	CAB	15.000	75.000	45.000	225.000
2 - seconda parte	omessa revoca certificato non conforme dopo accertamento	CAB	30.000	150.000	90.000	450.000
3 - prima parte	dichiarazione UE volontaria non conforme	Fornitore o fabbricante	15.000	75.000	45.000	225.000
3 - seconda parte	omessa revisione o revoca di dichiarazione UE non conforme dopo accertamento	Fornitore o fabbricante	30.000	150.000	90.000	450.000
4	messa a disposizione su mercato di prodotto o servizio che prevede certificato o dichiarazione obbligatoria: dichiarazione obbligatoria assente o non conforme o certificato assente	Fornitore o fabbricante	30.000	150.000	90.000	450.000
6	messa a disposizione su mercato di prodotto che prevede certificato o dichiarazione obbligatoria: mancato richiamo di prodotti	fabbricante	60.000	300.000	180.000	900.000
7	messa a disposizione su mercato di servizio che prevede certificato o dichiarazione obbligatoria: mancata inibizione servizi	Fornitore	60.000	300.000	180.000	900.000
8	mancato trattamento o notifica vulnerabilità scoperta dopo valutazione	CAB, fornitore o fabbricante	60.000	300.000	180.000	900.000
9	inottemperanze fornitore o fabbricante ad obblighi informativi	fornitore o fabbricante	30.000	150.000	90.000	450.000
10	inottemperanze CAB ad obblighi informativi	CAB	30.000	150.000	90.000	450.000
11 - prima parte	attività abusiva di CAB senza autorizzazione dalla NCCA	aspirante CAB	120.000	600.000	360.000	1.800.000
11 - seconda parte	attività abusiva di CAB senza autorizzazione dalla NCCA ma con	CAB scaduto	30.000	150.000	90.000	450.000



	autorizzazione scaduta da meno di un anno					
12	fornitura di informazioni e/o documenti falsi durante processo di certificazione o durante verifiche di vigilanza	CAB, fornitore o fabbricante	90.000	450.000	270.000	1.350.000
13	violazione condizioni utilizzo marchi o etichette	Fornitore o fabbricante	30.000	150.000	90.000	450.000
14	violazione obblighi conservazione registri	CAB	45.000	225.000	135.000	675.000
15 - prima parte	inottemperanza ad ordini e diffide del Ministero	CAB, fornitore o fabbricante	200.000	1.000.000	600.000	3.000.000
15 - seconda parte	minimo e massimo rapportati a % del fatturato se fatturato maggiore di 200.0000.0000 di euro	Verosimilmente fornitore o fabbricante di grandi dimensioni, ma teoricamente anche CAB	0,3 % del fatturato (da 600.000)	1,5 % del fatturato (da 3.000.000)	0,9 % del fatturato (da 1.800.000)	4,5 % del fatturato (5.000.000)

L'**articolo 11** "Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità", in attuazione dell'articolo 63 e dell'articolo 58, paragrafo 7, lettera f) del regolamento europeo, individua delle modalità di composizione extra-giudiziali per i contenziosi riguardanti l'emissione dei certificati e le dichiarazioni UE sollevati da parte di persone fisiche o giuridiche.

Il **comma 1** afferma il principio del diritto a presentare un reclamo da parte di una persona fisica o giuridica su un certificato di cybersicurezza all'emittente (all'Agenzia o ad altro organismo di valutazione della conformità), e su una dichiarazione UE di conformità (in questo caso all'Agenzia ai sensi dell'articolo 58, paragrafo 7, lettera f)).

Il **comma 2** individua le modalità per presentare un reclamo ad un organismo di valutazione della conformità diverso dall'Agenzia attraverso apposita procedura di reclamo stabilita dallo stesso organismo. Inoltre, stabilisce che nel caso in cui sia necessaria, per l'operatività di un organismo di valutazione della conformità in un sistema europeo di certificazione, l'autorizzazione da parte dell'Agenzia ai sensi dell'articolo 60, paragrafo 3, il reclamo inoltrato all'organismo di valutazione della conformità sarà inviato in copia anche all'Agenzia. Ciò implica che nel caso di autorizzazione il CAB dovrà includere nella procedura di reclamo da esso predisposta l'invio dei reclami in copia anche all'Agenzia.

Il **comma 3** stabilisce le modalità di invio di un reclamo all'Agenzia per i certificati emessi dall'Agenzia e per le dichiarazioni UE di conformità.

Il **comma 4** afferma, come previsto dall'articolo 63 del regolamento europeo che l'Agenzia informi il reclamante sullo stato del procedimento di esame del reclamo e sul suo esito e sulla possibilità di un ricorso giudiziario. Stabilisce inoltre la regola del silenzio rigetto con un termine di 90 giorni.

L'**articolo 12** "Ricorso all'autorità giudiziaria" descrive le modalità per i ricorsi giurisdizionali in relazione ai certificati europei di cybersicurezza.

Il **comma 1** afferma, come previsto dall'articolo 64 del regolamento europeo, il diritto ad un ricorso giudiziario da parte di una persona fisica o giuridica in relazione all'emissione o mancata emissione di un certificato di cybersicurezza o al mancato o parziale accoglimento di un reclamo ai sensi dell'articolo 10.

Il **comma 2** individua il Tribunale Amministrativo Regionale del Lazio quale organo giudiziario al quale adire ricorsi giurisdizionali contro l'Agenzia ed il Tribunale Amministrativo Regionale in cui hanno sede gli altri organismi di valutazione della conformità per i ricorsi contro tali organismi.

Il **Capo IV** “Disposizioni finanziarie” contiene i due articoli 13 e 14.

L’**articolo 13** “Destinazione dei proventi derivanti dalle attività dell’Agenzia” disciplina le modalità di gestione degli introiti derivanti dalle attività di vigilanza e di certificazione dell’Agenzia.

In particolare, il **comma 1** stabilisce che le attività di vigilanza nazionale (articolo 5, comma 1), di certificazione (articolo 6, comma 1), di autorizzazione (articolo 8, comma 3), di abilitazione dei laboratori di prova (articolo 8, comma 4) sono da rimborsare in base alla disciplina vigente per prestazioni erogate a titolo oneroso dall’Agenzia. Con Decreto del Presidente del Consiglio dei ministri di concerto con il Ministro dell’economia e delle finanze su proposta del Direttore Generale dell’Agenzia sono determinate le tariffe e modalità di riscossione.

Il **comma 2** stabilisce che le spese per l’impiego di esperti o laboratori abilitati dall’Agenzia per le attività di vigilanza di cui all’articolo 5, comma 1, sono calcolate ai sensi del comma 1.

Il **comma 3** individua le modalità di riassegnazione dal Ministero dell’economia e delle finanze all’Agenzia per gli introiti derivanti dall’irrogazione delle sanzioni di cui all’articolo 10 disponendo che siano destinati ad alimentare le attività di ricerca e formazione come stabilito dalla legge delega al criterio direttivo specifico c) di cui al comma 2 dell’articolo 18 della L. 53/2021.

L’**articolo 14** “Ulteriori disposizioni finanziarie” specifica le modalità di approvvigionamento per finanziare le spese di funzionamento dell’Agenzia ed i necessari aggiornamenti dei capitoli di spesa dell’Agenzia per le nuove attività in capo all’Agenzia discendenti dal regolamento europeo.

In particolare, in accordo con l’articolo 1, comma 2 della legge delega, il comma 1 dispone per l’utilizzo delle risorse di cui al fondo ex articolo 41-bis della L. 234/2021 come fonte di copertura per le spese fisse e continuative di cui all’articolo 4, comma 3. In particolare, per gli oneri di funzionamento di cui allo stesso comma, si individua una copertura di euro 657.500 per il 2022, euro 592.500 per l’anno 2023e per 637.500 euro dal 2024.

Il **comma 2** dispone che le spese sostenute dall’Agenzia per l’adeguamento dei sistemi informativi al Articolo 4, comma 3 debbano essere coerenti con il Piano triennale per l’informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell’articolo 1, della legge 28 dicembre 2015, n. 208 e s.m.i..

Il **comma 3** stabilisce che dall’attuazione del decreto legislativo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l’Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente, fatto salvo il ricorso al fondo 41-bis di cui al comma 1 per la copertura dei costi di cui all’articolo 4 comma 3, riguardo ai costi per l’assunzione di personale ed agli altri costi fissi e continuativi.

Il **comma 4** autorizza Il Ministro dell’economia e delle finanze ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati in attuazione degli articoli 13 e 14.

Il **Capo V** “Disposizioni finali” contiene l’articolo 15.

L’**articolo 15** “Successiva attuazione nazionale dei sistemi europei di certificazione” individua le modalità per riadattare il quadro nazionale di certificazione della sicurezza informatica definito dal presente decreto legislativo e dal provvedimento di cui all’articolo 4, comma 2, per le parti di maggior dettaglio, nel caso in cui un nuovo sistema europeo di certificazione adottato dalla Commissione europea ai sensi dell’articolo 49 del regolamento europeo non sia direttamente applicabile nel quadro vigente.

In tal caso si prevede che l’Agenzia ne possa dare attuazione semplicemente integrando o modificando il provvedimento di cui al comma 2 dell’articolo 4.

Iter di approvazione dello schema di decreto legislativo

Lo schema di decreto legislativo in oggetto verrà trasmesso, previa approvazione in preliminare deliberazione da parte del Consiglio dei Ministri, alle competenti Commissioni della Camera dei deputati e del Senato della Repubblica, per la formulazione dei relativi pareri, ai sensi dell'art. 31 della legge 24 dicembre 2012, n. 234, così come richiamato anche dall'articolo 1, comma 1, della legge 22 aprile 2021, n. 53.



TABELLA DI CONCORDANZA

(comma 2, art. 31 della L. 234/2012 e s.m.i.)

*Attuazione nazionale del Titolo III del regolamento (UE) 2019/881
delega art. 18 Legge 53/2021*

Schema di decreto legislativo per l'adeguamento della normativa nazionale alle disposizioni del Titolo III "Quadro di certificazione della cibersicurezza" del 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»).

Premessa

Di seguito si riporta la tabella di concordanza ai sensi del comma 2, art. 31 della L. 234/2012 e s.m.i.

Non trattandosi del recepimento di una direttiva europea, bensì dell'adeguamento della normativa nazionale ad un regolamento europeo, solo alcuni articoli del Titolo III richiedono adempimenti nazionali, essendo il Titolo III già entrato in vigore in tutti gli stati membri dal 28 giugno 2019 ed operativo per le molte parti.

Il Titolo III include gli articoli del regolamento dal 46 al 65 del regolamento (UE) 2019/881, che possono essere suddivisi in due gruppi:

- Articoli la cui entrata in vigore è posticipata di due anni (ai sensi dell'articolo 69, comma 2), ovvero dal 28 giugno 2021, e che richiedono esplicitamente degli adempimenti in capo agli stati membri: artt. 58, 60, 61, 63, 64 e 65.
- Articoli già entrati in vigore a partire dal 28 giugno 2019 (ai sensi dell'articolo 69, comma 1) e che riguardano primariamente gli obiettivi generali del Titolo III e le finalità e caratteristiche dei sistemi europei di certificazione della cibersicurezza, le attività da svolgersi in ambito europeo della Commissione Europea, ENISA, anche in collaborazione con gli stati membri: artt. 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 59, 62.

Gli adempimenti normativi nazionali si concentrano sul primo gruppo di articoli.

Ulteriori disposizioni del Titolo III di cui tenere conto implicitamente nella attuazione nazionale riguardano gli obblighi in capo agli organismi di valutazione della conformità, titolari di certificati europei di cybersicurezza e i fornitori di servizi ICT e i fabbricanti di prodotti ICT discendenti dal Titolo III o dai successivi sistemi di certificazione adottati dalla Commissione Europea a norma dell'art. 49. Infatti, in caso di violazione del Titolo III o delle disposizioni dei singoli sistemi europei di certificazione, tali soggetti sono destinatari di sanzioni ai sensi dell'articolo 58, par. 8, lett. f) e articolo 65. Le sanzioni possono derivare essenzialmente da:



- obblighi espressi già previsti nel Titolo III (ad es. obbligo di notifica della scoperta di vulnerabilità a carico dei titolari dei certificati europei di cybersicurezza ai sensi dell'articolo 56, paragrafo 8),
- o obblighi che saranno definiti successivamente con l'adozione dei singoli sistemi europei di certificazione in accordo con l'art. 54, comma 1.

NB: Va evidenziata tale difficoltà nel prevedere sanzioni per inottemperanza delle disposizioni specifiche dei singoli sistemi di certificazione, che saranno adottati successivamente con atto di esecuzione della Commissione Europea ai sensi dell'articolo 49, e quindi non ancora definiti.

Pertanto nel decreto legislativo, ed in particolare nell'articolo 10, sono previste delle sanzioni per violazioni delle regole specifiche dei sistemi europei di certificazione rimandando semplicemente alle regole e modalità che saranno definite successivamente alle singole lettere di cui al comma 1 dell'articolo 54 per ogni specifico sistema di certificazione.

Nella successiva tabella di concordanza (Tabella 1) si presentano per ogni articolo del Titolo III le disposizioni nazionali corrispondenti per realizzare i necessari adempimenti nazionali, ove previsti, con riferimento agli articoli specifici dello schema di decreto legislativo. Si include nella tabella anche una colonna con i riferimenti ai criteri direttivi specifici che il Governo è chiamato ad osservare ai sensi dell'articolo 18 comma 2 della legge delega, L. 53/2021.

Si fornisce anche una tabella di concordanza (Tabella 2) relativa ad articoli del Titolo I e Titolo IV richiamati dal Titolo III, tenuti anch'essi in considerazione per l'elaborazione del decreto legislativo.



Tabella 1 - Tabella di concordanza relativa agli articoli del Titolo III

Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
	<p>C.1. C.2, criteri direttivi specifici di cui alle lett. b)-d). <i>NB: il criterio direttivo specifico c.2.(a) (designazione autorità nazionale) è riformato implicitamente dall'art. 7, comma 1, lett. e) del DL 82/2021. In particolare la NCCA in Italia è stata già individuata e non è il MISE bensì l'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 5 del DL 82/2021.</i></p>	Art. 1, cc.1-2.	<p>Il c.1 dell'art. 1 definisce l'ambito del decreto legislativo riferendosi al c.1 dell'art. 18 della legge di delegazione europea 2019-2020. Il c.2, alle lett. a)-c) dell'art. 1 dettaglia l'ambito del decreto legislativo coerentemente con i criteri direttivi specifici del c.2 dell'art 18 della legge di delegazione europea 2019-2020.</p>
<p><u>Art. 46 - Quadro europeo di certificazione della cibersicurezza</u> Stabilisce gli obiettivi generali per l'istituzione di un quadro europeo di certificazione della cibersicurezza.</p>	Non sono richiesti adempimenti normativi per gli stati membri.		
<p><u>Art. 47 - Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza</u> Introduce lo URWP (Union Rolling Work Programme), il piano della Commissione Europea dei futuri sistemi europei di certificazione da elaborare ed adottarsi a norma dell'art. 49.</p>	Non sono richiesti adempimenti normativi per gli stati membri.		



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
<p><u>Art. 48 - Richiesta di un sistema europeo di certificazione della cibersicurezza</u></p> <p>Stabilisce come e da parte di chi in sede europea può essere richiesta ad ENISA l'elaborazione di un sistema europeo di certificazione.</p>	Non sono richiesti adempimenti normativi per gli stati membri.		
<p><u>Art. 49 - Preparazione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza</u></p> <p>Stabilisce le modalità di richiesta, elaborazione, adozione e revisione di un sistema europeo di certificazione in sede europea.</p>	Non sono richiesti adempimenti normativi per gli stati membri.		
<p><u>Art. 50 - Sito web sui sistemi europei di certificazione della cibersicurezza</u></p> <p>Istituisce un sito web di ENISA che raccoglie le informazioni sui sistemi europei di certificazione, i certificati e le dichiarazioni UE (emessi, non più validi, scaduti, revocati) ed i riferimenti ai sistemi europei nazionali eventualmente abrogati da un sistema europeo di certificazione ai sensi dell'articolo 57.</p>		Art.7, c.3.	<p>Nel Titolo III non è previsto un obbligo esplicito per fornitori di servizi ICT o fabbricanti di prodotti ICT di notificare la revoca o revisione di una dichiarazione UE di conformità. Tuttavia, la revoca o revisione di una dichiarazione UE di conformità si rende necessaria in caso risulti non conforme in esito alla attività di vigilanza delle NCCA.</p> <p>Qualora una dichiarazione UE risultasse non conforme in esito all'attività di vigilanza dell'Agenzia, l'art. 7, c.3, introduce l'obbligo nazionale di revisione o revoca della stessa entro 30 giorni e contestuale notifica all'Agenzia e ad ENISA (per permettere l'aggiornamento del sito web di ENISA con le informazioni corrette sulle dichiarazioni UE di conformità valide nell'UE)</p>
<p><u>Art. 51 - Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza</u></p> <p>Elenca gli obiettivi generali di un sistema di certificazione.</p>	Non sono richiesti adempimenti normativi per gli stati membri.		
<p><u>Art. 52 - Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza</u></p>	Non sono richiesti adempimenti normativi per gli stati membri.		



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
Definisce i tre livelli di affidabilità che i certificati rilasciati in un sistema europeo di certificazione possono avere (di base, sostanziale ed elevato) in termini di obiettivi generali ed azioni di valutazione minime richieste per ciascun livello.			
<p><u>Art. 53 - Autovalutazione della conformità, par. 1-2</u></p> <p>Descrive l'autovalutazione di conformità che può essere prevista in alcuni sistemi di certificazione per il livello di base. La possibilità di emissione di dichiarazioni UE di conformità e le conseguenti responsabilità sono poste in capo a fornitori e fabbricanti.</p>		<p>Art. 7, c. 1.</p> <p>Art. 7, c. 3.</p> <p>Art. 10, c. 3.</p>	<p>L'art. 7, c. 1 riprende le disposizioni dell'art. 53, par. 1-2 del regolamento.</p> <p>L'art. 7, c. 3, introduce l'obbligo nazionale per un fornitore di servizi ICT o fabbricante di prodotti ICT emittente una dichiarazione UE di conformità che risulti non conforme di revisionarla o revocarla entro 30 giorni notificando l'Agenzia ed ENISA (per permettere l'aggiornamento del sito web di ENISA)</p> <p>L'art. 10 c. 3 stabilisce sanzioni pecuniarie in caso di accertamento di dichiarazione UE di conformità volontaria non conforme emessa ai sensi dell'art. 53 del regolamento ed in caso di violazione dell'art. 7, c.3.</p>
<p><u>Art. 53 - Autovalutazione della conformità, par. 3</u></p> <p>Descrive gli obblighi informativi in capo a fornitori e fabbricanti emittenti di dichiarazioni UE.</p>		<p>Art. 7, c. 2.</p> <p>Art. 10, c. 9.</p>	<p>L'art. 7, c. 2 riprende le disposizioni dell'art. 53, par. 3 del regolamento.</p> <p>L'art. 10, c. 9 stabilisce sanzioni pecuniarie in caso di inottemperanza agli obblighi informativi di cui all'articolo 53 del regolamento.</p>
<p><u>Art. 53 - Autovalutazione della conformità, par. 4</u></p> <p>Stabilisce che le dichiarazioni UE di conformità sono emesse in un regime volontario salvo norma europea o nazionale che ne preveda l'obbligatorietà.</p>		<p>Art. 7, c. 4.</p> <p>Art. 10, cc. 4-7.</p>	<p>L'art. 7, c. 4 stabilisce le modalità per rendere obbligatoria una dichiarazioni UE di conformità per l'immissione sul mercato nazionale di prodotti o servizi TIC.</p> <p>L'art. 10, ai cc. 4-7 stabilisce sanzioni pecuniarie ed accessorie in caso di accertamento di non conformità di certificati europei di cybersicurezza o dichiarazioni UE di conformità obbligatorie.</p>
<p><u>Art. 53 - Autovalutazione della conformità, par. 5</u></p>	Non sono richiesti adempimenti normativi per gli stati membri.		



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
Stabilisce il mutuo riconoscimento delle dichiarazioni UE di conformità in tutta l'Unione			
<p><u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. a)-e)</u></p> <p>Individuano varie proprietà generali di un sistema europeo di certificazione (ambito, finalità, standard di riferimento, livelli di affidabilità, eventuale permesso ad effettuare autovalutazioni in luogo di valutazioni di terze parti) di un sistema europeo di certificazione da specificare per ogni sistema europeo di certificazione adottato a norma dell'art. 49.</p>		Art. 10, cc. 2, 3 e 4.	Una dichiarazione UE di conformità o certificato di cibersicurezza potrebbe essere emessa/o con modalità che non rispettano i requisiti generali stabiliti all'art. 54, par. 1, lett. a)-e) del regolamento. In tal caso si applica una sanzione di carattere generale ai sensi dell'art. 10, cc. 2-4 per non conformità del certificato.
<p><u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. f)</u></p> <p>Individua gli eventuali requisiti più specifici o supplementari rispetto all'elenco di cui all'allegato del regolamento che gli organismi di valutazione della conformità devono soddisfare per poter operare in uno schema di certificazione specifico, per l'autorizzazione ad operare nel sistema di certificazione ad opera dell'NCCA (art. 60, c. 3).</p>		Art. 10, c. 11.	L'art. 10, c. 11 sanziona l'attività di organismo della conformità esercitata senza autorizzazione da parte dell'autorità nazionale ai sensi dell'art. 60, par. 3 del regolamento, laddove siano identificati requisiti più specifici o addizionali ai sensi dell'art. 54, par. 1, lett. f), rispetto a quanto richiesto per l'accreditamento (Allegato al reg. (UE) 2019/881).
<p><u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. g)</u></p> <p>Individua i metodi di valutazione specifici da dettagliare per ogni sistema europeo di certificazione</p>		Art. 10, cc. 2, 3 e 4.	Una dichiarazione UE di conformità o certificato di cibersicurezza potrebbe essere emessa/o con modalità che non rispettino i requisiti stabiliti all'art. 54, par. 1, lett. g) del regolamento. In tal caso si applica una sanzione ai sensi dell'art. 10, cc. 2-4 per non conformità del certificato.
<p><u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. h)</u></p> <p>Individua le informazioni che il richiedente di una dichiarazione deve fornire o mettere a disposizione durante il processo di certificazione, da dettagliare per ogni sistema europeo di certificazione. L'obbligo di fornire informazioni</p>		Art. 10, c. 12.	L'art. 10, c. 12 punisce con sanzioni pecuniarie chi fornisce informazioni false o ometta informazioni necessarie durante un processo di certificazione.



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
nell'ambito di un processo di certificazioni è stabilito anche all'art. 56, c. 7.			
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. i)</u> Individua le eventuali modalità di utilizzo di marchi ed etichette da dettagliare per ogni sistema europeo di certificazione.		Art. 10, c. 13.	L'art. 10, c. 13 sanziona l'utilizzo improprio di eventuali marchi o etichette.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. j)-k)</u> Individua le modalità per assicurare la validità nel tempo di certificati con verifiche successive al rilascio del certificato da dettagliare per ogni sistema europeo di certificazione.		Art. 10, c. 2.	Tra le varie non conformità dei certificati rilevabili nell'attività di vigilanza vi può essere la mancata osservanza delle regole di controllo e mantenimento del certificato stabilite ai sensi dell'art. 54, par. 1, lett. j) - k) del regolamento. Tale non conformità è sanzionabile ai sensi dell'art. 10, c. 2.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. l)</u> Individua le regole per gestire le conseguenze di una dichiarazione UE di conformità o certificato di cybersicurezza non conforme, da dettagliare per ogni sistema europeo di certificazione.		Art. 10, cc. 2-3. Art. 5, cc. 4-5.	Le regole e conseguenze stabilite ai sensi dell'art. 54, par. 1, lett. l) regolamento potrebbero prevedere adempimenti in capo agli organismi di valutazione della conformità, ai titolari dei certificati europei di cybersicurezza, a fornitori di servizi ICT o fabbricanti di prodotti ICT. In caso di inosservanza a tali obblighi si applicano le sanzioni generali di cui all'art 10, cc. 2-7. L'art. 5, cc.4-5 del decreto legislativo individua delle modalità di revoca dei certificati, in quanto compatibili con le specifiche disposizioni dei sistemi europei di certificazione, in particolare ai sensi dell'art. 54, par. 1, lett. l) del regolamento.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. m)</u> Individua le regole per segnalare e trattare le vulnerabilità nei prodotti TIC, servizi TIC e processi TIC non rilevate in fase di valutazione , da dettagliare per ogni sistema europeo		Art. 10, c. 8.	L'art. 10, c. 8 sanziona il mancato trattamento o notifica di vulnerabilità riscontrate dopo il processo di valutazione in base a quanto stabilito per lo specifico sistema di certificazione ai sensi dell'art. 54, par. 1, lett. m) del regolamento.



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
di certificazione. Si applica sia ai certificati e sia alle dichiarazioni UE di conformità. L'obbligo di notifica delle vulnerabilità per i certificati, a carico dei titolari dei certificati , è stabilito anche dall'art. 56, c. 8.			
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. n)</u> Individua le eventuali regole di conservazione dei registri da parte degli organismi di valutazione della conformità.		Art. 10, c. 14	L'art. 10, c. 14 sanziona l'inosservanza delle eventuali regole definite nel sistema di certificazione europeo della cibersicurezza per la conservazione dei registri da parte degli organismi di valutazione della conformità.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. o)</u> Individua gli eventuali sistemi europei di certificazione nazionali esistenti che coprono lo stesso ambito del sistema europeo di certificazione. La norma permette identificare tali sistemi da abrogare ai sensi dell'art. 57 del regolamento per la pubblicazione sul sito web di ENISA ai sensi dell'art. 50.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. p)</u> Individua il contenuto ed il formato di un certificato o dichiarazione UE da definire per ogni sistema di certificazione.		Art. 10, cc. 2, 3 e 4.	Il mancato rispetto di forma e/o contenuto del certificato o dichiarazione UE di conformità è sanzionabile ai sensi dell'art. 10, cc. 2-3.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. q)</u> Individua obblighi informativi a carico di fornitori o fabbricanti emittenti di dichiarazioni UE di conformità, riprendendo il relativo testo dell'articolo 53, par. 3, da definire per ogni sistema di certificazione.		Art. 10, c. 9.	Il mancato rispetto degli obblighi informativi in capo a fabbricanti di prodotti ICT o fornitori di servizi ICT emittenti di dichiarazioni UE è sanzionato ai sensi dell'art. 10, c. 9.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. r)</u>	Non sono richiesti adempimenti normativi per gli stati membri.		



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
Individua il periodo massimo di validità di un certificato, da definire per ogni sistema di certificazione.			
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. s)</u> Individua obblighi informativi a carico degli organismi di valutazione della conformità emittenti certificati, da definire per ogni sistema di certificazione.		Art. 10, c. 10.	Il mancato rispetto degli obblighi informativi in capo agli organismi di valutazione della conformità emittenti di certificati di cybersicurezza è sanzionato ai sensi dell'art. 10, c. 10.
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. t)</u> Individua le eventuali condizione per il mutuo riconoscimento dei certificati con i paesi terzi, da definire per ogni sistema di certificazione.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. u)</u> Individua le regole per l'eventuale valutazione inter pares tra organismi di valutazione della conformità o degli organismi di certificazione dell'autorità (art. 60, c. 2) operanti a livello di affidabilità elevato, da definire eventualmente nell'ambito dei sistemi di certificazione che includono il livello elevato di affidabilità.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 54 - Elementi dei sistemi europei di certificazione della cibersicurezza, par. 1, lett. v)</u> Individua il formato e le procedure da rispettare per fornire o aggiornare le informazioni supplementari ai sensi dell'articolo 55		Art. 10, c. 9.	Il mancato rispetto degli obblighi informativi in capo a fabbricanti di prodotti ICT o fornitori di servizi ICT emittenti di dichiarazioni UE è sanzionato ai sensi dell'art. 10, c. 9.
<u>Art. 55 - Informazioni supplementari sulla cibersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati</u> Specifica un elenco di informazioni da rendere pubbliche ed in formato elettronico per tutte le certificazioni e dichiarazioni UE emesse da parte dei rispettivi titolari. Tali		Art. 10, c. 9.	Il mancato rispetto degli obblighi informativi in capo a fabbricanti o fornitori emittenti di dichiarazioni UE è sanzionato ai sensi dell'art. 10, c. 9. La fornitura ed aggiornamento delle informazioni supplementari ai sensi dell'art. 55 del regolamento



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
informazioni sono accessibili dal sito web di ENISA (art. 50) tramite appositi link ipertestuali per ogni certificato e dichiarazione UE emesso.			sono a carico dei fornitori di servizi ICT e fabbricanti di prodotti ICT.
<u>Art. 56 – Certificazione della cibersicurezza, paragrafo 1</u> Si sancisce il principio di presunzione di conformità dei prodotti certificati a requisiti tecnici stabiliti per un sistema di certificazione.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 56 – Certificazione della cibersicurezza, paragrafo 2</u> Si stabilisce che i sistemi di certificazione europei siano di base volontari ma che possano essere resi obbligatori con norma europea o nazionale.		Art. 6, c. 3.	L'art. 6, c. 3 individua le modalità per rendere obbligatorio per l'ambito nazionale un sistema europeo di certificazione volontario.
<u>Art. 56 – Certificazione della cibersicurezza, paragrafi 3-4</u> Si prospetta la possibilità di rendere obbligatori in ambito europeo i sistemi di certificazione che interessano i servizi essenziali di cui alla Direttiva NIS (Allegato II della Direttiva (UE) 1148/2016). Il rilascio dei certificati di livello di base e sostanziale può avvenire da parte di un qualunque organismo di valutazione della conformità ai sensi dell'art. 60.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 56 - Certificazione della cibersicurezza, paragrafi 5-6</u> Si individuano le possibili modalità di rilascio dei certificati: - di livello di base e sostanziale quando l'emissione è riservata ad un organismo pubblico per espressa disposizione dello specifico sistema di certificazione (paragrafo 5) - e di livello elevato che prevede il controllo da parte della NCCA dell'emissione dei certificati (paragrafo 6) potendo mantenere per sé questo ruolo o potendolo delegare ad organismi di valutazione della conformità terzi.	C. 2, criterio direttivo specifico di cui alle lett. b)	Art. 6, cc.1-2. Art. 8, c. 4.	L'art. 6 ai cc. 1-2 stabilisce le modalità di emissione dei certificati di livello elevato (art. 56, par. 6 del regolamento) e di base/sostanziale quando sono affidate ad un altro organismo pubblico (art. 56, par. 5, let. b) del regolamento) in attuazione del criterio direttivo specifico di cui all'art. 18, c.2, lett. b) della L. 53/2021. L'art. 8, c. 4 stabilisce un processo di verifica, denominato abilitazione, per gli esperti ed i laboratori di prova che vogliono operare per conto dell'Agenzia nelle attività di rilascio dei certificati. Si prevede la costituzione di un elenco di esperti e di laboratori di



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
			prova abilitati per coadiuvare l'Agenzia nelle attività di rilascio dei certificati.
<u>Art. 56 - Certificazione della cibersicurezza, par. 7</u> Introduce obblighi informativi da parte di chi richiede una certificazione (par. 7)		Art. 10, c. 12.	L'art. 10, c. 12 punisce con sanzioni pecuniarie chi fornisce informazioni false durante un processo di certificazione o omette informazioni necessarie per la certificazione.
<u>Art. 56 - Certificazione della cibersicurezza, par. 8</u> Introduce obblighi di notifica da parte di chi viene a conoscenza di una vulnerabilità successivamente alla conclusione dell'attività di valutazione (par. 8)		Art. 10, c. 8.	L'art. 10, c. 8 punisce la mancata notifica di una vulnerabilità da parte del titolare del certificato successivamente alla conclusione delle attività di valutazione.
<u>Art. 57 - Sistemi e certificati nazionali di certificazione della cibersicurezza</u> Introduce disposizioni per l'armonizzazione dei sistemi di certificazione a livello europeo, in particolare, abrogando i sistemi nazionali in sovrapposizione con nuovi sistemi europei e ponendo il divieto per gli stati membri di introdurre sistemi nazionali in sovrapposizione con sistemi europei già esistenti.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par.1-3</u> Si richiede ad ogni stato membro di designare una o più autorità nazionali di certificazione della cibersicurezza, assegnandola ad uno o più entità nazionali o di altro stato membro (parr. 1-2), che siano indipendenti dai soggetti vigilati (par. 3).	C.2, criterio direttivo specifico di cui alle lett. a) <i>NB: il criterio direttivo specifico c.2.(a) (designazione autorità nazionale) è riformato implicitamente dall'art. 7, comma 1, lett. e) del DL 82/2021.</i>	Art. 4, c.1.	In attuazione del criterio direttivo specifico di cui all'art. 18, c.2, lett. a) e successivo DL 14 giugno 2021, n. 82, il c.1 dell'art. 4 del decreto legislativo individua l'Agenzia come unica autorità nazionale di certificazione della cibersicurezza in Italia. Non essendo l'Agenzia un operatore del mercato, con interessi nel mercato, si ritengono soddisfatti i requisiti d'indipendenza organizzativa, finanziaria, giuridica e decisionale rispetto ai soggetti su cui vigila, ovvero gli organismi di valutazione della conformità, i fornitori di servizi TIC ed i fabbricanti di prodotti TIC.
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 4</u>	C.2, criterio direttivo specifico di cui alla	Art. 4, c. 2.	Il c. 2 dell'art. 4 individua le funzioni principali dell'autorità (vigilanza nazionale, rilascio dei



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
<p>Stabilisce che le funzioni di rilascio dei certificati (art. 56, par. 5(a) e 6) siano rigorosamente separate, dalle attività di vigilanza (art.58, par. 7, lett. a)-e)) e svolte indipendentemente le une dalle altre.</p>	lett. b)		<p>certificati, autorizzazione/abilitazione degli organismi di valutazione della conformità) e stabilisce la necessità di prevedere la separazione organizzativa tra vigilanza nazionale e rilascio dei certificati. Rinvia a provvedimento dell'Agenzia per la definizione di dettaglio (ai sensi dell'art. 5, comma 3 del DPCM 223/2021) che stabilisca le due funzioni in Divisioni distinte dell'Agenzia.</p> <p>L'art. 15 prevede un possibile aggiornamento del provvedimento dell'Agenzia (ai sensi art. 5, comma 3 del DPCM 223/2021), laddove a seguito dell'adozione di un nuovo sistema europeo di certificazione da parte della Commissione Europea, questo non sia immediatamente operativo a livello nazionale.</p>
<p><u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 5</u></p> <p>Il paragrafo 5 dispone che siano assegnate risorse adeguate alle autorità per l'esercizio dei poteri ed esecuzione dei loro compiti.</p>		<p>Art. 4, c. 3 Art. 14, c. 1</p>	<p>L'art. 4, c. 3 individua le risorse necessarie per garantire l'operatività dell'Agenzia in termini di spese fisse e continuative di funzionamento da finanziare.</p> <p>L'art. 14, c.1 individua le modalità di finanziamento delle risorse fisse e continuative per l'operatività dell'Agenzia di cui all'art. 4, c. 3, attraverso corrispondente riduzione del fondo 41-bis ex L. 234/2012.</p>
<p><u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 6</u></p> <p>Evidenzia l'opportunità che le autorità nazionali partecipino attivamente all'ECCG (art. 62).</p>		Art. 4, c.2.	<p>Il c.2 dell'art. 4 stabilisce che l'autorità parteciperà con proprio personale all'attività dell'ECCG (art. 62 del regolamento) e del Comitato (art. 66 del regolamento) per assicurare continuità del supporto tecnico nel processo di adozione dei sistemi europei di certificazione (artt. 49 e 66 del regolamento).</p>
<p><u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 7, lett. a)-e)</u></p> <p>Stabilisce le funzioni di vigilanza delle autorità nazionali sui certificati (lett. a)) e le dichiarazioni UE di conformità (lett. b)) ed i principali soggetti su cui vigilare e con cui</p>	c. 2, criterio direttivo specifico di cui alle lett. b)	<p>Art. 5, cc.1, 2-3, 7, 8 e 9 Art. 13, c. 1-3. Art. 8, c. 4.</p>	<p>In attuazione del criterio direttivo specifico di cui alla lett. b), c. 1, art. 18 L. 53/2021,</p> <ul style="list-style-type: none"> il c.1 dell'art. 5 delinea gli aspetti principali dell'attività di vigilanza nazionale.



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
collaborare.			<ul style="list-style-type: none"> • i cc. 2, 3, 8, 9 e 10 individuano le modalità specifiche dell'attività di vigilanza. <p>L'articolo 13, cc. 1-3 stabilisce le modalità di rimborso e di riassegnazione degli introiti derivanti dalle attività di vigilanza e dalle relative sanzioni. Per quest'ultime si stabilisce che siano destinate ad alimentare le attività di ricerca e formazione come stabilito dalla L. 53/2021 al criterio direttivo specifico c).</p> <p>L'art. 8, c. 4 stabilisce un processo di verifica, denominato abilitazione, per gli esperti ed i laboratori di prova che vogliano operare per conto dell'autorità nazionale nelle attività di vigilanza. Si prevede la costituzione di un elenco di esperti e di laboratori di prova abilitati per coadiuvare l'Agenzia nelle attività di vigilanza.</p>
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, parr. 7, lett. f)</u> Assegna all'autorità la funzione di trattamento dei reclami sui certificati di livello elevato e sulle dichiarazioni UE di conformità.		Art. 11, cc.3-4	I reclami per i certificati emessi dall'autorità nazionale e per le dichiarazioni UE di conformità sono trattati all'art. 11, cc. 3 e 4.
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, parr. 7, lett. g)</u> Individua tra i compiti delle autorità l'adempimento annuale d'invio di una relazione sulle attività di vigilanza.	Non sono richiesti adempimenti normativi per gli stati membri.		
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, parr. 7, lett. h)</u> Si stabilisce la cooperazione delle autorità nazionali con altre autorità.		Art. 5, c. 2.	L'art. 5, c. 2 afferma il principio di cooperazione con le altre autorità europee, in aggiunta alle autorità competenti del mercato con cui è già prevista cooperazione ai sensi dell'art. 58, par. 7, lett. a) del regolamento.
<u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 7, lett. i)</u>	C.2, criterio direttivo specifico di cui alle	Art. 9, c.1.	L'art. 9 sull'attività di ricerca, sperimentazione e formazione nel campo della certificazione della



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
Si assegna all'autorità il compito di monitorare gli sviluppi della certificazione di cibersicurezza	lett. c).	Art. 13, c.3.	cibersicurezza. Gli introiti delle sanzioni, come previsto dal successivo art. 13, c.3, in attuazione del criterio direttivo specifico di cui alla lett. c) saranno utilizzati per finanziare ricerca e formazione.
<p><u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 8</u></p> <p>Si individuano i poteri minimi che ciascuna autorità nazionale può esercitare nelle attività di vigilanza.</p>	C.2, criterio direttivo specifico di cui alla lett. d).	Art. 5, cc. 3-6.	L'art. 5, comma 3 riassume i poteri dell'autorità previsti all'articolo 58, par. 8 del regolamento europeo. In attuazione del criterio direttivo specifico d) della legge di delegazione europea 2019-2020, i cc. 4-6 dell'art. 5 disciplinano i casi di revoca, che estendono i poteri di revoca dell'autorità in quanto compatibili con le disposizioni dei sistemi europei di certificazione ed in particolare dell'art. 54, par. 1, lett. l) del regolamento. In particolare, l'Agenzia oltre a revocare certificati di livello elevato ove necessario come già previsto dal regolamento, potrà revocare certificati di livello di base o sostanziale emessi da altri organismi di valutazione della conformità in alcuni casi particolarmente critici.
<p><u>Art. 58 - Autorità nazionali di certificazione della cibersicurezza, par. 9</u></p> <p>Si stabilisce la cooperazione tra le autorità nazionali europee e la Commissione Europea nello scambio di buone pratiche nel campo della certificazione della cibersicurezza.</p>	C.2, criterio direttivo specifico di cui alle lett. c)	Art. 9 Art. 13, c.3	L'art. 9, sull'attività di ricerca, sperimentazione e formazione, stabilisce la possibilità di realizzare progetti di sviluppo software e di ricerca anche per lo scambio di buone pratiche con le altre autorità e la Commissione Europea. L'Agenzia può anche sperimentare l'introduzione di nuovi sistemi di certificazione nazionale. Gli introiti delle sanzioni, come previsto dal successivo art. 13, c. 3, in attuazione del criterio direttivo specifico di cui alla lett. c) saranno utilizzati per finanziare l'attività di ricerca e formazione.
<p><u>Art. 59 - Valutazione inter pares</u></p> <p>Disciplina le modalità per effettuare valutazioni inter pares</p>	Non sono richiesti adempimenti normativi per gli stati membri.		



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
in ambito europeo tra le autorità nazionali europee, con la presenza di ENISA ed il coinvolgimento dell'ECCG.			
<p><u>Art. 60 - Organismi di valutazione della conformità</u></p> <p>Si stabilisce che gli organismi di valutazione della conformità debbano essere accreditati ai sensi del regolamento (CE) 765/2008 dall'organismo nazionale di accreditamento (ONA) (par. 1), compreso l'organismo di certificazione dell'autorità nazionale (art. 60, par. 2). L'ONA avrà anche il compito di limitare, sospendere o revocare il certificato di accreditamento (art. 60, par. 4). Gli organismi di valutazione della conformità saranno anche autorizzati (art. 60, c.3) dall'autorità nazionale di accreditamento di certificazione della cybersicurezza, quando il sistema europeo di certificazione lo prevede, essendo necessario verificare requisiti supplementari o più specifici ai sensi dell'art. 54, par. 1, lett. f).</p>		Art. 8, cc 4 e 5.	<p>L'art 8, c. 3 individua il processo di autorizzazione da parte dell'Agenzia sui CAB ai sensi dell'art. 60, par. 3 del regolamento.</p> <p>L'art. 8, c. 5 stabilisce per le attività di autorizzazione dell'autorità ai sensi dell'art. 60, par.3 del regolamento le modalità di rimborso, rimandando all'art. 13.</p>
<p><u>Art. 61 – Notifica</u></p> <p>Si stabilisce che l'autorità nazionale di certificazione della cibersicurezza notifica gli organismi di valutazione della conformità accreditati ed ogni successivo aggiornamento in termini di sospensione, limitazione e revoca dell'accreditamento o autorizzazione.</p>		Art. 8, c.1	Il c. 1 dell'art. 8 stabilisce che l'organismo di accreditamento nazionale deve aggiornare regolarmente l'Agenzia e l'ufficio di collegamento nazionale ai sensi del regolamento UE 2019/1020 sugli accreditamenti degli organismi di valutazione della conformità e successive limitazioni, sospensioni e revoche del certificato di accreditamento affinché l'autorità nazionale possa notificare tali variazioni alla Commissione Europea.
<p><u>Art. 62 - Gruppo europeo per la certificazione della cibersicurezza</u></p> <p>Istituisce l'ECCG come comitato tecnico consultivo della Commissione Europea e di ENISA ai sensi del regolamento (UE) 2019/881, definendone la composizione ed i compiti principali.</p>		Art. 4, c.2.	Il c.2 dell'art. 4 stabilisce che l'autorità parteciperà con proprio personale all'attività dell'ECCG (art. 62 del regolamento) e del Comitato (art. 66 del regolamento) per assicurare continuità del supporto tecnico nel processo di adozione dei sistemi europei di certificazione (artt. 49 e 66 del regolamento).
<u>Art. 63 – Diritto di presentare un reclamo</u>		Art. 11	L'art. 11 disciplina le modalità di presentazione e



Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 - Quadro di Certificazione della Cibersicurezza	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di attuazione	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
Disciplina le modalità di presentazione e trattamento di un reclamo su un certificato di cibersicurezza.			trattamento di un reclamo su un certificato o una dichiarazione UE di conformità.
<u>Art. 64 – Diritto a un ricorso giurisdizionale effettivo</u> Disciplina le modalità di presentazione di ricorso giurisdizionale su reclamo presentato o un certificato di cibersicurezza.		Art. 12	L'art. 12, disciplina a le modalità di presentazione di un ricorso giurisdizionale su un certificato o una dichiarazione UE di conformità.
<u>Art. 65 – Sanzioni</u> Stabilisce per gli stati membri il compito di introdurre nell'ordinamento nazionale un quadro sanzionatorio adeguato per rendere possibile il rispetto del Titolo III del regolamento (UE) 2019/881 e dei successivi sistemi europei di certificazione.	C. 2, criterio direttivo specifico di cui alle lett. c)	Art. 10.	L'art. 10 introduce sanzioni pecuniarie da un minimo di 15.000 ad un massimo di 5.000.000 di euro e sanzioni accessorie, per il rispetto degli obblighi stabiliti dal regolamento e successivi sistemi di certificazione.

Tabella 2 – Tabella di concordanza relativa agli articoli del Titolo I e IV richiamati dal Titolo III

<u>Articolo ed eventuale paragrafo del Titolo III del regolamento (UE) 2019/881 – Quadro di Certificazione della Cibersicurezza</u>	Disposizioni dell'articolo 18 della legge di delegazione europea 2019-2020	Articolo ed eventuale comma del decreto legislativo di adeguamento	Note riguardo agli articoli corrispondenti dello schema di decreto legislativo
<u>Art. 1 – Oggetto e ambito di applicazione, paragrafo 2</u> Definisce l'ambito di applicazione del regolamento (UE) 2019/881.		Art. 1, c.3.	L'esclusione delle attività di cui all'art. 1, par. 2 del regolamento è ripresa nell'art. 1 c. 3 del decreto legislativo per delineare l'ambito del decreto legislativo, che in particolare "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."
<u>Art. 2 – Definizioni</u> Introduce le principali definizioni utilizzate nel regolamento		Art. 3.	L'art. 3 del decreto legislativo introduce le definizioni utilizzate dal decreto legislativo e fa riferimento in buona parte alle definizioni già introdotte dal



(UE) 2019/881.			regolamento.
<u>Art. 66 – procedura di comitato</u> Definisce la procedura di comitato ai sensi del regolamento (UE) n. 182/2011, per l'adozione dei sistemi europei di certificazione (art. 49, par. 7) con atti di esecuzione della Commissione europea.		Art. 4, c.2.	Il c.2 dell'art. 4 stabilisce che l'autorità parteciperà con proprio personale all'attività dell'ECCG (art. 62 del regolamento) e del Comitato (art. 66 del regolamento) per assicurare continuità del supporto tecnico nel processo di adozione dei sistemi europei di certificazione (artt. 49 e 66 del regolamento).



Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del Titolo III “Quadro di certificazione della cibersicurezza” del 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»).

RELAZIONE TECNICA

Il presente decreto è predisposto nell’esercizio della delega contenuta nell’articolo 18 della legge 22 aprile 2021, n. 53 – legge di delegazione europea 2019-2020 e contiene disposizioni per il completo adeguamento dell’ordinamento interno alle disposizioni del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all’ENISA, l’Agenzia dell’Unione europea per la cybersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell’informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza) (di seguito Regolamento).

In particolare, lo schema di decreto ha la finalità di:

a) designare l’Agenzia per la cybersicurezza nazionale (di seguito Agenzia) quale autorità competente ai sensi del paragrafo 1 dell’articolo 58 del Regolamento;

b) individuare l’organizzazione e le modalità per lo svolgimento dei compiti e l’esercizio dei poteri dell’Agenzia, previsti dall’articolo 58 e dall’articolo 56, paragrafi 5 e 6, del Regolamento;

c) definire il sistema delle sanzioni applicabili ai sensi dell’articolo 65 del Regolamento, prevedendo che gli introiti derivanti dall’irrogazione delle sanzioni siano versati all’entrata del bilancio dello Stato per essere riassegnati ad apposito capitolo dello stato di previsione dell’Agenzia per finalità di ricerca e formazione in materia di certificazione della cibersicurezza. L’articolo 18, comma 2, lettera c), della citata legge di delega n. 53 del 2021, in deroga ai limiti previsti dall’articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234, stabilisce che le sanzioni amministrative pecuniarie non devono essere inferiori nel minimo a 15.000 euro e non devono essere superiori nel massimo a 5.000.000 di euro;

d) prevedere, in conformità all’articolo 58, paragrafi 7 e 8, del Regolamento, il potere dell’Agenzia di revocare i certificati rilasciati ai sensi dell’articolo 56, paragrafi 4 e 5, lettera b), emessi sul territorio nazionale, salvo diverse disposizioni dei singoli sistemi europei di certificazione adottati ai sensi dell’articolo 49 del Regolamento.

Di seguito si fornisce una illustrazione dettagliata degli articoli del decreto.

L’**articolo 1** prevede la definizione dell’organizzazione dell’autorità nazionale di certificazione della cybersicurezza in Italia, le relative modalità di cooperazione con le altre autorità pubbliche nazionali ed europee e con l’Organismo di accreditamento, nonché la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

Si rappresenta che l’autorità nazionale di certificazione della cybersicurezza, di cui all’articolo 58, paragrafo 1, del Regolamento, per l’Italia è l’Agenzia per la cybersicurezza nazionale, di cui all’articolo 5 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, designata in tale qualità dall’articolo 7, comma 1, lettera e), del medesimo decreto-legge.



L'articolo 1, limitandosi a definire l'oggetto e l'ambito di applicazione dello schema di decreto legislativo, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 2** prevede che il trattamento dei dati personali in applicazione del presente decreto sia effettuato ai sensi del regolamento (UE) 2016/679 e del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni.

La norma ha la unica finalità di specificare la normativa di riferimento per il trattamento dei dati personali e, dunque, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 3** contiene le definizioni adottate ai fini del presente decreto. Stante la sua finalità, la norma non comporta nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 4**, al **comma 1**, specifica che l'Agenzia per la cybersicurezza nazionale, ai sensi degli articoli 7, comma 1, lettera e), e 16, comma 12, lettera b), del citato decreto-legge n. 82 del 2021, è l'autorità nazionale di certificazione della cybersicurezza, ai sensi dell'articolo 58, paragrafo 1 del Regolamento.

Con il **comma 2** si stabilisce che l'organizzazione e le procedure per lo svolgimento dei compiti dell'Agenzia quale autorità nazionale di certificazione della cybersicurezza, nonché la definizione delle modalità applicative delle attività di cui al presente Capo I ed all'articolo 11, saranno individuate con un provvedimento dell'Agenzia, adottato ai sensi dell'articolo 5, comma 3, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223.

Inoltre, il **comma 2**, stabilisce che l'Agenzia partecipa alle attività internazionali dell'ECCG e del comitato ai sensi degli articoli 62 e 66 del Regolamento con proprio personale.

Il **comma 3** attribuisce all'Agenzia la dotazione finanziaria necessaria per lo svolgimento dei compiti per la realizzazione e la gestione dei sistemi informativi, la formazione del personale tecnico ed amministrativo, la ricerca e l'innovazione, la realizzazione e l'aggiornamento di laboratori interni, l'abilitazione di laboratori di prova ed esperti, l'autorizzazione di organismi di valutazione della conformità, la vigilanza, l'accreditamento, il rinnovo e l'estensione dell'organismo di certificazione della sicurezza informatica (OCSI), le missioni nazionali ed internazionali e le spese generali.

I limiti per la copertura dei predetti oneri per le spese di funzionamento dell'Agenzia sono indicati dall'articolo 14 dello schema di decreto e sono stimati in complessivi euro 657.500 per il 2022, euro 592.500 per l'anno 2023 e per euro 637.500 dal 2024.

Considerato che l'individuazione dell'autorità nazionale di certificazione della cybersicurezza e l'attribuzione alla stessa di adeguate risorse costituisce adempimento di obblighi europei e che, a tal fine, è stata conferita una delega al Governo con l'articolo 18 della citata legge n. 53 del 2021, alla copertura delle spese relative al predetto adeguamento si farà fronte facendo ricorso al fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234, come previsto dall'articolo 1 della medesima legge n. 53 del 2021.

In tabella è sintetizzata tale stima complessiva con riferimento al triennio 2022-2024;

Elementi per stima costi attività dell'autorità di certificazione per triennio 2022-2024	artt. Reg. (UE) 881/2019	2022	2023	2024
Missioni internazionali Commissione Europea, ENISA	47.4, 48.2, 49.2, 49.5-6, 58.6, 58.7(g)-(h), 58.9, 59, 62	15	25	35
Costi missioni internazionali (€)		22.500 €	37.500 €	52.500 €



Costi di accreditamento dell'organismo di certificazione (€)	60.2	15.000 €	5.000 €	5.000 €
Costi di ricerca, formazione e cooperazione internazionale (€)	56.5(a), 56.6, 58.7(i), 58.9	500.000 €	500.000 €	500.000 €
Costi di avvio e spese generali (€)		120.000 €	50.000 €	80.000 €
Totale costi (€)		657.500,00 €	592.500,00 €	637.500,00 €

In merito, si specifica quanto segue:

- **stima dei costi di missione:** con riferimento alle missioni nazionali ed internazionali si rendono necessarie tipicamente due tipologie di missioni:

- **Missioni nazionali** nell'ambito dell'attività di vigilanza dell'agenzia presso le sedi dei soggetti vigilati di cui all'articolo 58, par. 8 del Reg. UE 2019/881;
- **Missioni internazionali** nell'ambito delle attività di cooperazione internazionale con la Commissione europea, ENISA, le altre autorità nazionali di certificazione della cybersicurezza europee o organismi omologhi da paesi terzi.

Per quanto riguarda le **missioni nazionali** dell'Autorità, esse deriverebbero dallo svolgimento di:

- funzioni di supporto e sostegno che ACN assicurerà ad Accredia ai fini del monitoraggio e della vigilanza delle attività degli organismi di valutazione della conformità (vds. Articolo 58, paragrafo 7, lettera c), del regolamento (UE) 2019/881);
- indagini presso le sedi degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza (vds. Articolo 58, paragrafo 8, lettera d), del regolamento (UE) 2019/881).

Con riferimento ai predetti casi, non si prevedono ulteriori oneri a carico della finanza pubblica poiché, nelle more che gli schemi di certificazione in corso di predisposizione trovino effettiva diffusione, essi si configurano come attività a supporto di soggetti terzi (Accredia), che ne detengono la titolarità, o come funzioni che potranno comunque trovare copertura finanziaria nelle dotazioni ordinarie dell'Agenzia, integrandosi efficientemente nei regolari programmi di ispezione.

La configurazione tipica di una **missione internazionale** a seconda delle necessità richiede l'impiego di uno o due delegati per la partecipazione ad incontri internazionali, in particolare se la partecipazione prevede lo svolgimento di più sessioni tecniche in parallelo.

Per la determinazione della stima di 1.500 euro per ciascuna missione internazionale è pertanto stata presa a riferimento una trasferta a Bruxelles della durata di due giorni (con due pernottamenti) di uno/due dipendenti appartenenti all'Area manageriale e alte professionalità inquadrati nel segmento professionale "Consigliere".

L'importo è stato determinato sulla base delle previsioni di cui all'art. 111 del Regolamento del Personale dell'Agenzia, in base al quale, per le missioni all'estero, al personale inviato in missione competono:

- la fruizione dei servizi di viaggio (sono stati considerati i biglietti aereo di andata e ritorno Roma-Bruxelles);



- il rimborso di ulteriori spese di viaggio (sono stati considerati i servizi taxi abitazione-aeroporto-Hotel);
- la fruizione dei servizi di alloggio messi a disposizione dall'Agenzia (sono stati considerati n. 2 pernottamenti in Hotel a Bruxelles);
- la diaria per i giorni di espletamento dell'incarico;
- **stima dei costi di accreditamento:** in base all'art. 60.2 del Regolamento (UE) 2019/881, l'organismo di certificazione dell'autorità dovrà essere accreditato dall'organismo nazionale di accreditamento (Reg. CE 765/2008 - Accredia per l'Italia) per ogni nuovo sistema di certificazione. Considerando per il primo accreditamento una stima di euro 15.000 IVA inclusa e 5.000 euro IVA inclusa per ogni anno successivo per spese di mantenimento/estensione dell'accREDITAMENTO di accREDITAMENTO, gli oneri per gli anni 2022, 2023, 2024 ammontano, rispettivamente, ad euro 15.000, 5.000 e 5.000;
- **stima dei costi di ricerca e formazione:** per sostenere le attività di ricerca per sviluppare nuove metodologie di valutazione, linee guida, strumenti e conoscenze, si ipotizza un investimento costante di euro 500.000 per ogni anno da impiegare per finanziare progetti di ricerca e borse di studio, in collaborazione con enti universitari e di ricerca;
- **stima delle spese generali e di avvio:** premesso che le capacità tecniche del Servizio Certificazione e Vigilanza potranno trarre beneficio anche da altre iniziative di investimento assunte in ambito Perimetro, appare cauto stimare, per il solo anno 2022, una spesa un tantum di euro 100.000 euro per l'allestimento di spazi e locali. Per l'acquisto di postazioni informatiche e per la manutenzione si stimano per gli anni 2022, 2023 e 2024 rispettivamente euro 20.000, euro 50.000 ed euro 80.000. Pertanto, le spese generali e di avvio per il triennio ammontano rispettivamente a euro 120.000, euro 50.000 ed euro 80.000.

Tra i costi operativi che l'Agenzia dovrà sostenere ai sensi dell'**articolo 4, comma 3**, si individuano i costi di accreditamento per l'organismo di certificazione dell'autorità, che ai sensi dell'articolo 60, paragrafo 2 del Regolamento, dovrà essere fatto per l'organismo nazionale di accreditamento. Ai sensi dell'articolo 8, comma 3, dello schema di decreto, dal momento che l'Agenzia presterà assistenza all'organismo nazionale di accreditamento nel monitoraggio degli organismi di valutazione della conformità accreditati, ai sensi dell'articolo 58, paragrafo 7, lett. c) del Regolamento, il compenso ricevuto per tale attività di assistenza da parte dell'organismo nazionale di accreditamento potrà compensare in tutto o in parte i costi di accreditamento per l'organismo di certificazione dell'autorità da rimborsare all'organismo nazionale di accreditamento.

L'**articolo 5** stabilisce le modalità di realizzazione dell'attività di vigilanza del mercato in ambito nazionale.

In particolare, il **comma 1** stabilisce che, ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, con riferimento ai certificati di cybersicurezza ed alle dichiarazioni UE di conformità emessi nel territorio dello Stato, ai sensi dell'articolo 58, paragrafo 7, lettere *a*) e *b*), del Regolamento, l'Agenzia vigila sui fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8, del Regolamento.

Inoltre, l'Agenzia, ai sensi dell'articolo 58, paragrafo 7, lettere *c*), *d*) ed *e*), del Regolamento:

a) fatto salvo l'articolo 60, paragrafo 3, assiste e sostiene attivamente l'Organismo di AccREDITAMENTO nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del Regolamento;

b) monitora e vigila sulle attività degli organismi di valutazione della conformità pubblici di cui all'articolo 56, paragrafo 5, lettera *b*), del Regolamento;

c) ove previsto dal sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera *f*), del Regolamento, autorizza gli organismi di valutazione della conformità a norma dell'articolo 60,



paragrafo 3, del Regolamento, e limita, sospende o revoca l'autorizzazione esistente qualora violino le prescrizioni del Regolamento, dandone notizia all'Organismo di Accreditamento.

Ai sensi del **comma 2**, l'Agenzia, nello svolgimento delle predette attività di vigilanza, opera anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità di vigilanza degli altri Stati membri ai sensi dell'articolo 58, paragrafo 7, lettere *a)* e *h)*, del Regolamento. L'Agenzia esegue l'attività di vigilanza di cui al comma 1 anche in collaborazione con le Forze dell'ordine.

Tali disposizioni rivestono carattere ordinamentale e non comportano nuovi o maggiori oneri a carico della finanza pubblica. Con particolare riguardo alla possibile collaborazione con le Forze dell'ordine, tale forma di avvalimento, già prevista dall'articolo 5, comma 5, del decreto-legge n. 82 del 2021, per l'assolvimento dei compiti istituzionali dell'Agenzia, troverà concreta disciplina nelle convenzioni ivi previste e verrà svolta nell'ambito delle risorse già assegnate all'Agenzia e alle stesse Forze dell'ordine, non comportando nuovi o maggiori oneri a carico della finanza pubblica.

Il **comma 3**, stabilisce che l'Agenzia, nell'attività di vigilanza nazionale, può effettuare indagini ed audit nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cybersicurezza e degli emittenti delle dichiarazioni di conformità UE, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza. Inoltre, l'Agenzia può irrogare le sanzioni pecuniarie ed accessorie previste all'articolo 10 dello schema di decreto. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

Nei successivi **commi 4 e 5** sono dettate disposizioni in tema di revoca dei certificati europei di cybersicurezza

Il **comma 6** disciplina l'ipotesi di accertamento dell'emissione di un certificato non conforme rilasciato ai sensi dell'articolo 56, paragrafi 4, 5 lettera *b)*, o 6, lettere *a)* e *b)*, del Regolamento, in esito alle attività di vigilanza di competenza dell'Agenzia. **Stabilisce, inoltre**, che le modalità di sostegno ed assistenza dell'Agenzia all'Organismo di accreditamento per l'attività di vigilanza di competenza, siano disciplinate da apposita convenzione o protocollo di intesa fra gli stessi.

Ai sensi del **comma 7**, l'Agenzia, per le prove tecniche nell'ambito delle attività di vigilanza, può effettuare valutazioni di sicurezza informatica anche attraverso esperti esterni o laboratori di prova abilitati dall'Agenzia, ai sensi dell'articolo 8, comma 4, dello schema di decreto, e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

Il **comma 8** prevede in capo agli organismi di valutazione della conformità, ai titolari dei certificati europei di cybersicurezza ed agli emittenti delle dichiarazioni di conformità, un obbligo, durante l'attività di vigilanza a cui sono sottoposti, di cooperazione con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi.

Il **comma 9** stabilisce che gli oneri derivanti dall'applicazione dei commi 3, 7 e 8 per i controlli effettuati dall'Agenzia e relativi in particolare all'impiego del personale in forza all'Agenzia, della strumentazione utilizzata nelle prove e dei materiali di consumo e per le missioni e spese generali, siano a carico dell'organismo di valutazione della conformità, del titolare del certificato o dell'emittente della dichiarazione UE di conformità sottoposto all'attività di vigilanza, come previsto dall'articolo 30, commi 4 e 5, della legge 24 dicembre 2012, n. 234. Nel caso in cui l'attività di vigilanza includa ulteriori spese, tra cui l'utilizzo di laboratori di prova esterni ed eventuali spese di trasporto per prodotti prelevati o sequestrati da sottoporre a verifica, le ulteriori spese sono ugualmente a carico del soggetto sottoposto all'attività di vigilanza. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

L'**articolo 6** contiene disposizioni relative al rilascio dei certificati di cybersicurezza con livello di affidabilità elevato (**comma 1**) e al rilascio dei certificati con livello di affidabilità sostanziale o di base (**comma 2**), stabilendo al **comma 3** che la certificazione della cybersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 56, paragrafo 2 del Regolamento.



Il **comma 4**, prevede che gli oneri derivanti dall'applicazione dei commi 1 e 2 per il rilascio dei certificati da parte dell'Agenzia siano a carico del soggetto richiedente la certificazione, come previsto dall'articolo 30, commi 4 e 5 della legge n. 234 del 2012. Per la determinazione e la corresponsione delle somme di cui al presente comma si fa rinvio all'articolo 13 del presente decreto.

L'**articolo 7** regola l'ipotesi di dichiarazioni UE di conformità rilasciate nel caso di sistemi di certificazione in cui sia autorizzata l'autovalutazione di conformità ai sensi dell'articolo 54, par. 1, lett. e) del Regolamento. In tale ipotesi, i fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema.

L'**articolo 8** detta norme relative all'accreditamento e all'autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia.

In particolare, il **comma 1**, stabilisce l'obbligo, in capo all'Organismo di accreditamento, di comunicare all'Agenzia e all'ufficio unico di collegamento, designato per l'Italia ai sensi dell'articolo 10, par. 3, del regolamento (UE) 2019/1020, ogni aggiornamento relativo agli organismi di valutazione della conformità accreditati in merito nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento per la successiva notifica da parte dell'Agenzia alla Commissione europea.

Il **comma 2**, stabilisce che l'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'Organismo di accreditamento, mentre, il **comma 3** stabilisce che, nel caso in cui un sistema europeo di certificazione stabilisca requisiti specifici o supplementari, solo gli organismi di valutazione della conformità che soddisfano i predetti requisiti sono autorizzati dall'Agenzia a svolgere i compiti previsti dal sistema europeo di certificazione.

Il **comma 4** prevede la costituzione, l'aggiornamento e la pubblicità di un elenco di esperti e un elenco di laboratori di prova abilitati dall'Agenzia ad operare, rispettivamente, ai sensi dell'articolo 5, comma 8 ed ai sensi dell'articolo 6, comma 1, dello schema di decreto, a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia. Tali elenchi, sono costituiti con provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223. Gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati di cui all'articolo 5, comma 8, dello schema di decreto, non possono effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale ai sensi dell'art. 56, paragrafo 4, o paragrafo 5(b), del Regolamento, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati. Le modalità per l'abilitazione e l'eventuale rinnovo, l'inserimento, la sospensione e la cancellazione di esperti e laboratori di prova dai suddetti elenchi, sono individuate con provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del richiamato regolamento adottato con DPCM n. 223 del 2021.

Il **comma 5** stabilisce che, ai sensi dell'articolo 30, commi 4 e 5 della legge n. 234 del 2012, gli oneri derivanti dall'abilitazione di cui al comma 3, le spese per le eventuali attività di autorizzazione di cui all'articolo 8, comma 3, dello schema di decreto, e gli eventuali successivi aggiornamenti sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

L'**articolo 9** contiene disposizioni in materia di attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza, prevedendo che l'Agenzia possa realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale con il fine di elevare il livello nazionale di cybersicurezza.



Tale disposizione riveste carattere ordinamentale e non comporta nuovi o maggiori oneri a carico della finanza pubblica. A tal proposito, si rappresenta che la realizzazione di progetti di ricerca è già prevista dall'articolo 7, comma 1, lettera *r*), del decreto-legge n. 82 del 2021, che dispone che l'Agenzia, perseguendo obiettivi di eccellenza, supporti negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca, nonché del sistema produttivo nazionale, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e che possa promuovere, sviluppare e finanziare specifici progetti e iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. Tali funzioni, pertanto, verranno svolte nell'ambito delle risorse, di cui all'articolo 18 del decreto-legge n. 82 del 2021, già assegnate all'Agenzia.

L'**articolo 10** definisce il sistema delle sanzioni applicabili per la violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, ai sensi dell'articolo 58, paragrafo 8, lettera *f*), e dell'articolo 65 del Regolamento.

Come anticipato in premessa, l'articolo 18, comma 2, lettera *c*), della legge di delega n. 53 del 2021, in deroga ai limiti previsti dall'articolo 32, comma 1, lettera *d*), della legge 24 dicembre 2012, n. 234, stabilisce che le sanzioni amministrative pecuniarie non devono essere inferiori nel minimo a 15.000 euro e non devono essere superiori nel massimo a 5.000.000 di euro. Al riguardo, il **comma 17** dell'articolo 10 dello schema di decreto prevede che con successivo provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del DPCM 9 dicembre 2021, n. 223, saranno definiti i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie previste dal presente decreto. Nelle more dell'adozione del provvedimento di definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della L. 24 novembre 1981, n. 689.

Ai sensi dell'articolo 18, comma 2, lettera *c*), della legge n. 53 del 2021 e dell'articolo 7, comma 1, lettera *e*), del decreto-legge n. 82 del 2021, l'Agenzia, in caso di violazione dei predetti obblighi può irrogare sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. La predetta attività sanzionatoria genera introiti per l'Agenzia che saranno riutilizzati per costituire una dotazione variabile per le attività di ricerca e formazione.

Il comma 3 del presente articolo 10 non comporta nuovi o maggiori oneri per la finanza pubblica in quanto trattasi di sanzioni di nuova istituzione.

Infatti, si ritiene utile rappresentare che l'articolo 21 del decreto legislativo 18 maggio 2018, n. 65 detta l'apparato sanzionatorio per la violazione degli obblighi previsti dalla direttiva (UE) 2016/1148; ai sensi dell'articolo 7, comma 1, lettera *d*), del D.L. n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale è individuata quale autorità nazionale competente NIS (art. 8, par. 1 della direttiva (UE) 2016/1148) ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto legislativo n. 65 del 2018.

Il regolamento (UE) 2019/881, invece - oggetto del presente schema di decreto legislativo - prevede, all'articolo 58, par. 7, lettera *f*), tra le funzioni delle autorità nazionali di certificazione della cybersicurezza, quella di *“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”*.

Nella sua qualità di autorità nazionale di certificazione della cybersicurezza, l'Agenzia svolge la predetta funzione.

Gli ambiti previsti dai citati atti europei (direttiva (UE) 2016/1148 e regolamento (UE) 2019/881) sono diversi e prevedono obblighi distinti, pertanto, le attività svolte dall'Agenzia in tali ambiti sono distinte e non sussiste, dunque, sovrapposizione tra le sanzioni previste dall'articolo 10 del presente schema di decreto legislativo e l'articolo 21 del decreto legislativo n. 65/2018.



Ciò risulta, peraltro, evidente dalle fattispecie di sanzioni di cui all'articolo 21 del d.lgs n. 65 del 2018, che prevedono inosservanza di obblighi riguardanti l'adozione di misure di sicurezza o notifica di incidenti in capo a fornitori di servizi essenziali o servizi digitali, mentre l'articolo 10 del presente schema di decreto legislativo prevede obblighi in capo a diversi soggetti riguardanti la gestione dei certificati europei di cybersicurezza e le dichiarazioni UE di conformità associate a prodotti, servizi e processi TIC.

Le sanzioni introdotte con il presente schema di decreto legislativo costituiscono, dunque, nuove sanzioni – non precedentemente irrogate – per inosservanza degli obblighi introdotti dal regolamento (UE) 2019/881, successivo alla direttiva (UE) 2016/1148, e che investe un ambito distinto rispetto all'ambito trattato dalla direttiva.

L'**articolo 11** contiene disposizioni in materia di reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità.

La disposizione ha carattere ordinamentale e, pertanto, non comportano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 12** descrive le modalità per i ricorsi giurisdizionali in relazione ai certificati europei di cybersicurezza.

La disposizione ha carattere ordinamentale e, pertanto, non comportano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 13** contiene disposizioni relative alla destinazione dei proventi derivanti dall'attività dell'Agenzia.

Il **comma 1**, in tal senso, stabilisce che le attività di vigilanza (art. 58.7 del Regolamento e articolo 5 dello schema di decreto), di certificazione (art. 56.5.(a) e art. 56.6) del Regolamento e articolo 6, comma 1 dello schema di decreto) e di autorizzazione ed abilitazione di esperti, di laboratori di prova, ed organismi di valutazione della conformità (art. 60.3 del Regolamento e articolo 8 dello schema di decreto) sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi. I relativi proventi sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione degli appositi capitoli dell'Agenzia.

Con decreto del Presidente del Consiglio dei ministri sono determinate le tariffe e modalità di riscossione.

Il **comma 2** stabilisce che le spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza di cui all'articolo 5, comma 1, dello schema di decreto, sono calcolate ai sensi del comma 1.

Il **comma 3**, infine, stabilisce che gli introiti derivanti dalle sanzioni pecuniarie di cui all'articolo 10 dello schema di decreto, sono versati ad apposito capitolo del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione dei capitoli del bilancio dell'Agenzia destinati alle attività e ai progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione concernenti la certificazione della cybersicurezza di prodotti TIC, servizi TIC e processi TIC di cui all'articolo 9, comma 1.

L'**articolo 14**, posto che gli introiti previsti all'articolo 13 non sono sufficienti per garantire l'operatività dell'Agenzia, stabilisce che agli oneri per le attività che la stessa dovrà svolgere nell'esercizio dei suoi compiti in ambito nazionale di certificazione della cybersicurezza, individuate all'articolo 4, comma 3, e stimati in complessivi euro 657.500 per il 2022, euro 592.500 per l'anno 2023 e per euro 637.500 dal 2024, si farà fronte facendo ricorso al fondo per il recepimento della normativa europea di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234, come previsto dall'articolo 1 della medesima legge n. 53 del 2021.



Ciò, in considerazione del fatto che l'individuazione dell'autorità nazionale di certificazione della cybersicurezza, e l'attribuzione alla stessa di adeguate risorse, costituisce adempimento di obblighi europei e che, a tal fine, è stata conferita una delega al Governo con l'articolo 18 della citata legge n. 53 del 2021.

Il **comma 2** stabilisce che le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi all'articolo 4, comma 3, sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1, della legge 28 dicembre 2015, n. 208 e successive modificazioni.

Il **comma 3** dispone che dall'attuazione del presente decreto, ad esclusione dall'articolo 4, comma 3, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

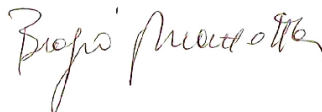
Ai sensi del **comma 4**, il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati in attuazione del presente articolo e dell'articolo 13.

L'**articolo 15** stabilisce che ai nuovi sistemi europei di certificazione, che sono adottati dalla Commissione europea ai sensi dell'articolo 49, paragrafo 7, del Regolamento, e che non siano autonomamente applicabili nel quadro di certificazione nazionale vigente, sia data attuazione modificando o integrando il provvedimento di cui all'articolo 4, comma 2, in ogni aspetto operativo necessario per dare piena attuazione al nuovo sistema europeo di certificazione.

L'articolo contiene disposizioni di carattere ordinamentale e, pertanto, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

La verifica della presente relazione tecnica, effettuata ai sensi dell'art. 17 comma 3, della Legge 31 dicembre 2009, n. 196 ha avuto esito **positivo** negativo

06/05/2022 Il Ragioniere Generale dello Stato
Firmato digitalmente *Biagio Mazzotta*



ANALISI TECNICO-NORMATIVA

Decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del Titolo III, Quadro di certificazione della cibersicurezza, del 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»)

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) **Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.**

Obiettivo della proposta normativa è l'attuazione delle disposizioni non direttamente operative a livello nazionale del Titolo III del regolamento (UE) 2019/881, relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, entrato in vigore il 27 giugno 2019. In particolare, è necessario dare attuazione al regolamento (UE) 2019/881 in tutte le sue parti non direttamente operative con la sua entrata in vigore, avvenuta il 27 giugno 2019.

Il principale adempimento richiesto agli Stati Membri è l'istituzione di una o più autorità nazionali di certificazione della cibersicurezza per la vigilanza nazionale e la cooperazione europea ai sensi del suddetto regolamento (art. 58), operativa nel gruppo di certificazione europeo (art. 62), con capacità sanzionatoria (art. 65), con compiti accessori di emissione dei certificati per i casi particolari previsti dal regolamento (art. 56, par. 5 lett. a), par. 6). L'altro principale adempimento da realizzarsi a livello nazionale è l'introduzione di un quadro sanzionatorio (art. 65), per permettere all'autorità nazionale di far rispettare le disposizioni del regolamento e dei successivi sistemi europei di certificazione (art. 54), che saranno adottati dalla Commissione Europea con atti di esecuzione successivi (art. 49) con cui saranno definite le modalità di certificazione armonizzate nell'UE in ambiti specifici (ad es. servizi cloud, reti 5G, automazione industriale).

L'articolo 18 della Legge 22 aprile 2021, n. 53, "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020", conferisce al Governo il mandato di predisporre uno o più decreti legislativi per l'adeguamento del quadro nazionale di certificazione della cibersicurezza al Titolo III regolamento (UE) 2019/881. La presente proposta normativa si pone come obiettivo la realizzazione della suddetta delega attraverso un singolo decreto legislativo, che prevede l'Agenzia della cybersicurezza nazionale di cui all'art. 5 del decreto legge 14 giugno 2021, n.82, il ruolo di autorità competente ai sensi dell'art. 58 del reg. UE 2019/881, come previsto dall'articolo 7, lett. e) dello stesso decreto, introduce un quadro sanzionatorio e definisce gli ulteriori aspetti necessari per l'adeguamento della normativa nazionale alle esigenze del Titolo III del regolamento UE 2019/881.

2) **Analisi del quadro normativo nazionale.**

Il quadro nazionale di certificazione della cibersicurezza s'inserisce nel più ampio contesto europeo ed internazionale di seguito descritto, sul quale il regolamento UE 2019/881 inciderà con l'adozione dei primi sistemi europei di certificazione della cibersicurezza, adottati dalla Commissione Europea (Art. 49 del reg. UE 2019/881), da realizzare in tutti gli stati membri in base a nuove regole armonizzate.

In particolare, lo scenario attuale europeo e internazionale della certificazione della cibersicurezza prima dell'entrata in vigore del regolamento, vede già impegnati diversi soggetti quali produttori/utilizzatori di prodotti TIC e fornitori di servizi TIC, laboratori di prova specializzati nella valutazione della cibersicurezza, organismi di normazione e agenzie governative¹ con il ruolo prevalente di organismi di certificazione. Non tutti i paesi europei e mondiali sono dotati di un organismo di certificazione della cibersicurezza governativo. L'attività di certificazione della cibersicurezza per alcuni contesti è demandata anche ad organismi di valutazione della conformità per lo più privati ai sensi del Regolamento (CE) 765/2008. Inoltre, gli standard di riferimento per la certificazione della cibersicurezza sono molteplici e si focalizzano sulla certificazione di prodotti (ad es. ISO/IEC 15408), di sistemi di gestione (ad es. ISO/IEC 27001), di servizi TIC e di processi TIC.

Per quanto riguarda il contesto attuale delle certificazioni a supervisione governativa, il mutuo riconoscimento tra organismi di certificazione governativi non discende da norme europee o da trattati internazionali, bensì da accordi volontari di mutuo riconoscimento tra agenzie governative. In particolare, con riferimento allo standard ISO/IEC 15408 per la certificazione di prodotti, detto anche "Common Criteria", è operativo per l'ambito europeo l'accordo SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement) con adesioni da parte di alcune agenzie governative di nazioni UE ed EFTA² e per l'ambito mondiale l'accordo CCRA (Common Criteria Recognition Arrangement) che vede aderenti alcune agenzie governative di nazioni europee ed extraeuropee³.

A livello nazionale, il DPCM del 30 ottobre 2003 ha istituito presso l'ex Ministero delle Comunicazioni, oggi confluito nel MISE, lo Schema Nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, in attuazione dell'art. 10, comma 1, del Decreto Legislativo del 23 febbraio 2002, n. 10⁴. Le competenze dell'OCSI sono state successivamente trasferite alla costituenda Agenzia per la cybersicurezza nazionale, ai sensi

1 Con il termine agenzia governativa s'intende in senso generale qualsiasi ente della pubblica amministrazione centrale o da essa delegato per l'attività di organismo nazionale di certificazione della sicurezza informatica, indipendentemente dal grado di indipendenza economico-giuridica rispetto al governo e dall'ordinamento dello stato di riferimento.

2 Nazioni aderenti al SOG-IS MRA: Austria, Belgio, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Italia, Paesi Bassi, Lussemburgo, Norvegia, Polonia, Slovacchia, Spagna, Svezia, Regno Unito. Maggiori informazioni disponibili sul portale web <https://www.sogis.eu>.

3 Nazioni aderenti al CCRA: Australia, Canada, Francia, Germania, India, Italia, Giappone, Malesia, Paesi Bassi, Nuova Zelanda, Norvegia, Repubblica di Corea del Sud, Singapore, Spagna, Svezia, Turchia, Stati Uniti, Austria, Repubblica Ceca, Danimarca, Etiopia, Finlandia, Grecia, Ungheria, Indonesia, Israele, Pakistan, Polonia, Qatar, Slovacchia, Regno Unito. Maggiori informazioni disponibili sul portale web <https://www.commoncriteriaportal.org>.



dell'articolo 7, comma 1, lettera e) del DL 14 giugno 2021, n. 82.

L'OCSI⁵, attualmente operativo presso la DG TCSI-ISCTI del MISE, ha aderito ad entrambi gli accordi SOG-IS MRA e CCRA ed i certificati da esso emessi sono mutuamente riconosciuti dalle agenzie governative che partecipano ai suddetti accordi rispettivamente in Europa e nel mondo. Il nuovo quadro di certificazione europeo introdotto dal regolamento (UE) 2019/881 riformerà il mutuo riconoscimento europeo attualmente realizzato dal SOG-IS MRA ed avrà un impatto anche sull'accordo CCRA a livello mondiale. In particolare, le attività del SOG-IS migreranno nel primo sistema di certificazione europeo ai sensi dell'art 49 del Regolamento (UE) 2019/881, basato sullo standard ISO/IEC 15408 e attualmente in corso di elaborazione da parte di ENISA, che sarà probabilmente adottato nel 2022 dalla Commissione Europea.

L' OCSI è inoltre designato, ai sensi dell'art. 35 comma 5 del d.lgs. 82/2005 e successive modificazioni, quale organismo di accertamento della conformità per dispositivi di firma e sigilli qualificati ai sensi dell'allegato II del Regolamento eIDAS (regolamento (UE) 2014/910). Per tale attività l'OCSI, sulla base di una certificazione Common Criteria conseguita con lo stesso OCSI o altro organismo di certificazione omologo nell'UE, attesta la conformità di un dispositivo di firma o sigillo qualificato in base ai suddetti requisiti.

3) ***Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.***

Il nuovo quadro di certificazione europeo introdurrà una molteplicità di sistemi di certificazione della cibersicurezza e comporterà i seguenti effetti principali sul quadro nazionale di certificazione della cibersicurezza in Italia, una volta completamente attuato dalla presente proposta normativa:

- L'Agenzia per la cybersicurezza nazionale (ACN) sarà designata autorità competente ai sensi dell'articolo 58 del regolamento UE 2019/881 (NCCA).
- I certificati di sicurezza informatica in Italia, come negli altri stati membri, in base alle regole specifiche definite per ogni sistema europeo di certificazione potranno essere emessi
 - o dalla NCCA, in quanto autorità, ai sensi dell'art. 58 del regolamento UE 2019/881,
 - o da organismi di valutazione della conformità terzi ai sensi del Regolamento CE 2008/765, accreditati dall'organismo di accreditamento nazionale per i livelli di

4 Tale articolo è stato abrogato dal d.lgs. 82/2005 e sostituito dall'art. 35 comma 5 dello stesso decreto legislativo preservando le prerogative dell'organismo di certificazione nazionale.

5 L'OCSI è anche l'organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014 sull'identità digitale eIDAS (Electronic IDentification, Authentication and Signature) e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica qualificata o di un sigillo elettronico qualificato ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento eIDAS, in base al comma 5 dell'articolo 35 del decreto legislativo 7 marzo 2005, n. 82, recante ^a Codice dell'amministrazione digitale^o (CAD), modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179.

affidabilità di base e sostanziale;

- Per alcuni sistemi di certificazione, i fornitori e fabbricanti di prodotti TIC e servizi TIC potranno emettere delle dichiarazioni UE di conformità per il livello di affidabilità di base, in sostituzione delle certificazioni rilasciate da organismi di valutazione della conformità terzi.
- La ACN sarà responsabile a livello nazionale della vigilanza sui certificati di sicurezza informatica emessi in Italia ed in generale sulle attività degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità
 - Sarà introdotto un quadro sanzionatorio nazionale attraverso il quale la ACN potrà far rispettare le disposizioni del regolamento europeo e dei successivi sistemi europei di certificazione.

4) ***Analisi della compatibilità dell'intervento con i principi costituzionali.***

Il provvedimento non presenta profili d'incompatibilità con i principi costituzionali essendo finalizzato all'attuazione di un regolamento europeo che va reso operativo. Le misure previste nel decreto legislativo realizzano i criteri direttivi generali e specifici dell'articolo 18 della Legge 22 aprile 2021, n. 53.

5) ***Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.***

Non si rilevano problemi di compatibilità dell'intervento con le competenze e le funzioni delle regioni, sia ordinarie sia a statuto speciale, nonché degli enti locali.

6) ***Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.***

Il regolamento (UE) 2019/881 indirizza il mercato unico dell'Unione Europea e si inserisce quindi tra le materie a competenza concorrente tra l'Unione e gli Stati Membri. L'attuazione, in base alle modalità previste dalla presente proposta, non presenta criticità rispetto al dettato costituzionale.

7) ***Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.***

La proposta normativa va realizzata necessariamente con decreto legislativo su proposta del Governo in attuazione alla delega già conferite per legge ai sensi dell'art. 18 della Legge 22 aprile 2021, n. 53.

8) ***Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.***

Non risultano iniziative concernenti analoga materia all'esame del Parlamento in quanto la presente proposta normativa è l'unica finalizzata per la realizzazione della delega ex articolo 18



della Legge 22 aprile 2021, n.53, la cui competenza prevalente è affidata all'Agenzia per la cybersicurezza nazionale di cui all'art. 5 del decreto legge 14 giugno 2021, n.82.

9) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.***

Non risultano pendenti giudizi di costituzionalità nella stessa materia, che è stata regolata nell'Unione Europea per la prima volta con il regolamento (UE) 2019/881, entrato in vigore il 28 giugno 2019.

PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

1) ***Analisi della compatibilità dell'intervento con l'ordinamento comunitario.***

La proposta normativa ha come obiettivo l'attuazione di un regolamento europeo tramite misure di adeguamento dell'ordinamento nazionale. E' pertanto pienamente compatibile.

2) ***Verifica dell'esistenza di procedure di infrazione da parte della Commissione Europea sul medesimo o analogo oggetto.***

Non si è a conoscenza di procedure d'infrazione riguardanti la materia regolata. La materia della certificazione della sicurezza informatica è stata toccata da normativa europea solo limitatamente al settore delle firme e sigilli elettronici nell'ambito del regolamento eIDAS, regolamento (UE) 2014/910, che è stato pienamente attuato con successiva riforma del Codice dell'Amministrazione Digitale, d.lgs. 82/2005 ed successive modificazioni. In tale ambito l'accertamento di conformità di un dispositivo di firma o sigillo qualificato avviene attraverso preliminare certificazione del dispositivo in base allo standard Common Criteria (ISO/IEC 15408).

3) ***Analisi della compatibilità dell'intervento con gli obblighi internazionali***

La proposta normativa si pone come obiettivo la piena attuazione del regolamento (UE) 2019/881.

4) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia delle Comunità Europee sul medesimo o analogo oggetto.***

Non risulta vi siano giudizi pendenti dinanzi alla CGUE nelle medesime o analoghe materie oggetto del decreto.

5) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.***

Non risulta vi siano giudizi pendenti dinanzi alla CEDU nelle medesime o analoghe materie oggetto del decreto.

6) ***Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione Europea.***

Il decreto legislativo da attuazione al regolamento (UE) 2019/881 e quindi attraverso disposizioni di dettaglio univoche per tutti gli stati membri.



PARTE III. ELEMENTI DI QUALITA' SISTEMATICA E REDAZIONALE DEL TESTO

1) ***Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.***

La proposta normativa richiama per la maggior parte le definizioni già disponibili nelle principali norme di riferimento che comprendono:

- Il regolamento UE 2019/881 (Cybersecurity act)
- Il regolamento UE 2012/1025 (gli organismi di normazione europei)
- Il regolamento CE 765/2008 (vigilanza del mercato per l'Unione)

A tali definizioni si aggiungono alcune definizioni necessarie per specifiche esigenze di scrittura del decreto legislativo, coerenti con quelle già presenti nella normativa comunitaria sopra citata.

2) ***Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni ed integrazioni subite dai medesimi.***

È stata verificata la correttezza dei riferimenti normativi contenuti nel provvedimento.

3) ***Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.***

Non si è ancora fatto ricorso alla tecnica della novella legislativa in quanto la proposta normativa è finalizzata ad introdurre un primo decreto legislativo sulla materia trattata, che potrà essere successivamente emendato da future norme di rango primario per esigenze nazionali o necessari futuri adeguamenti a modifiche dell'ordinamento europeo che potranno verificarsi in futuro.

4) ***Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.***

Le norme contenute nel decreto legislativo non comportano effetti abrogativi impliciti.

5) ***Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.***

Non si individuano nella presente proposta normativa tali fattispecie.

6) ***Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.***

Non risultano aperte deleghe sulle medesime materie. L'unica delega da realizzare riguarda l'articolo 18 della Legge 22 aprile 2021, n. 53.

7) ***Indicazione degli eventuali atti successivi attuativi; verifica della congruenza dei termini previsti per la loro adozione.***

Successivamente all'entrata in vigore del presente decreto legislativo è previsto un provvedimento dell'Agenzia per la cybersicurezza nazionale per definire l'organizzazione dell'autorità nazionale di certificazione della cybersicurezza in Italia.

- 8) ***Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.***

Non si ravvisa la necessità di commissionare analisi statistiche per il presente decreto legislativo.



RELAZIONE AIR

(Ai sensi dell'Allegato 2 della direttiva del PCM del 16 febbraio 2018)

Provvedimento: *Schema di decreto legislativo, recante “Adeguamento della normativa nazionale alle disposizioni del Titolo III, Quadro di certificazione della cibersicurezza, del 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»)».*

Amministrazione competente: Ministero dello sviluppo economico

Referente AIR dell’amministrazione competente: Ufficio Legislativo

SINTESI DELL’AIR E PRINCIPALI CONCLUSIONI

1. CONTESTO E PROBLEMI DA AFFRONTARE

1.1 I sistemi di certificazione nazionali esistenti, gli accordi di mutuo riconoscimento ed il contesto nazionale

Attualmente, il mutuo riconoscimento dei certificati di sicurezza cibernetica emessi da organismi di certificazione governativi non discende da norme europee o da trattati internazionali vincolanti, bensì da accordi volontari di mutuo riconoscimento tra agenzie governative sulla base di sistemi di certificazione della cybersicurezza nazionali stabiliti nei rispettivi paesi.

In particolare, con riferimento allo standard ISO/IEC 15408 per la certificazione di prodotti TIC (Tecnologie dell’Informazione e della Comunicazione), detto anche “Common Criteria”, è operativo per l’ambito europeo l’accordo SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement) con la partecipazione di alcune agenzie governative di paesi UE ed EFTA¹; mentre per l’ambito mondiale, con riferimento allo stesso standard, l’accordo CCRA (Common Criteria Recognition Arrangement) che vede aderenti agenzie governative di nazioni europee ed extraeuropee².

A livello nazionale, il DPCM del 30 ottobre 2003 ha istituito presso l’ex Ministero delle Comunicazioni, oggi confluito nel MISE, lo Schema Nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell’informazione, in attuazione dell’art. 10, comma 1, del Decreto Legislativo del 23 febbraio 2002, n. 10³ ed a cui sovrintende l’OCSI (Organismo di Certificazione della Sicurezza Informatica)⁴. Per effetto dell’articolo 7 del DL 14 giugno 2021, n. 82, le competenze dell’OCSI sono state trasferite dal Ministero dello sviluppo economico all’Agenzia per la cybersicurezza nazionale istituita ai sensi dell’articolo 5 dello stesso decreto. L’OCSI ha aderito ad entrambi gli accordi SOG-IS MRA e CCRA ed i certificati da esso emessi sono

1 Nazioni aderenti: Austria, Belgio, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Italia, Paesi Bassi, Lussemburgo, Norvegia, Polonia, Slovacchia, Spagna, Svezia, Regno Unito. Maggiori informazioni disponibili sul portale web <https://www.sogis.eu>.

2 Nazioni aderenti: Australia, Canada, Francia, Germania, India, Italia, Giappone, Malesia, Paesi Bassi, Nuova Zelanda, Norvegia, Repubblica di Corea del Sud, Singapore, Spagna, Svezia, Turchia, Stati Uniti, Austria, Repubblica Ceca, Danimarca, Etiopia, Finlandia, Grecia, Ungheria, Indonesia, Israele, Pakistan, Polonia, Qatar, Slovacchia, Regno Unito. Maggiori informazioni disponibili sul portale web <https://www.commoncriteriaportal.org>.

3 Tale articolo è stato abrogato dal d.lgs. 82/2005 e sostituito dall’art. 35 comma 5 dello stesso decreto legislativo preservando le prerogative dell’organismo di certificazione nazionale.

mutuamente riconosciuti dalle agenzie governative che partecipano ai suddetti accordi rispettivamente in Europa e nel mondo.

1.2 Il nuovo quadro europeo di certificazione della cybersicurezza ed i suoi effetti

Il Titolo III del Regolamento (UE) 2019/881, detto “regolamento sulla cybersicurezza” (in inglese noto come “Cybersecurity Act”), pubblicato il 7 giugno 2019 nella Gazzetta Ufficiale dell’Unione Europea ed entrato in vigore il 28 giugno 2019, introduce nell’Unione Europea un quadro di certificazione della cybersicurezza armonizzato per superare la frammentazione attuale del mercato interno dei certificati di cybersicurezza e rendere maggiormente affidabili per il consumatore i prodotti e i servizi che utilizzano tecnologie dell’informazione e della comunicazione (TIC), realizzando un mutuo riconoscimento dei certificati di cybersicurezza tra tutti gli stati membri a beneficio del mercato unico dell’UE.

In particolare, ai sensi dell’articolo 49 del suddetto regolamento, la Commissione Europea con successivi atti di esecuzione introdurrà regole armonizzate per la certificazione di prodotti ICT, servizi ICT e processi ICT in specifici ambiti (ad es. servizi cloud, reti 5G, sistemi di automazione industriale, Internet delle cose), che abrogheranno eventuali sistemi nazionali esistenti nell’Unione Europea negli ambiti di intervento degli stessi. In particolare, ai sensi dell’articolo 57 del suddetto regolamento, laddove esistano dei sistemi nazionali di certificazione della cybersicurezza nell’Unione Europea, che per ambito si dovessero sovrapporre ad un sistema europeo di certificazione adottato della Commissione Europea ai sensi del regolamento, questi saranno abrogati e gli stati membri dovranno astenersi dall’introduzione di nuovi sistemi nazionali di certificazione nello stesso ambito coperto da un sistema europeo di certificazione esistente.

Più in generale, il nuovo quadro europeo di certificazione della cybersicurezza avrà i seguenti effetti principali negli stati membri:

- In base all’articolo 58 del “Cybersecurity Act”, ogni stato membro dovrà designare una o più autorità nazionali di certificazione della cybersicurezza nel proprio territorio o delegare altra o altre autorità esistenti al di fuori del proprio territorio.
- Entrato in vigore il regolamento europeo, a far data dal 28 giugno 2019, la Commissione Europea, con il supporto tecnico di ENISA ed il coinvolgimento degli stati membri, attraverso consultazione con i rappresentanti nazionali nel cosiddetto Gruppo europeo per la certificazione della cybersicurezza (European Cybersecurity Certification Group – ECCG) (art. 62 del regolamento UE 2019/881), adotterà tramite atti di esecuzione nuovi sistemi di certificazione europei per specifici settori tecnologici e/o di mercato determinando per ciascuno le modalità di gestione a livello europeo in forma armonizzata (art. 54 del Regolamento (UE) 2019/881).
- Con l’introduzione dei primi sistemi europei di certificazione della cybersicurezza, attesi entro il 2022, la normativa europea comincerà a produrre i primi effetti reali sulla normativa nazionale dei singoli Stati Membri. In particolare, come anzidetto i sistemi di certificazione nazionali esistenti eventualmente concorrenti ed in sovrapposizione con i sistemi europei di certificazione che saranno via via introdotti, cesseranno di esistere con l’entrata in vigore di questi ultimi ai sensi dell’art. 57 del Regolamento (UE) 2019/881, allo scopo di ridurre la frammentazione del mercato interno UE.
- I certificati di cybersicurezza, in base alle regole specifiche definite per ogni sistema europeo di certificazione potranno essere emessi secondo varie modalità a seconda del livello di

4 L’OCSE è anche l’organismo designato, ai sensi del comma 1 dell’articolo 30 del Regolamento (UE) n. 910/2014 sull’identità digitale – eIDAS (Electronic IDentification, Authentication and Signature) e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l’accertamento della conformità di un dispositivo per la creazione di una firma elettronica qualificata o di un sigillo elettronico qualificato ai requisiti di sicurezza espressi nell’Allegato II al suddetto Regolamento eIDAS, in base al comma 5 dell’articolo 35 del decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell’amministrazione digitale” (CAD), modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179.

affidabilità (art. 52 del regolamento UE 2019/881:

- o salvo eccezioni debitamente giustificate e stabilite in sede europea, per i livelli di certificazione di base e sostanziale, da organismi di valutazione della conformità di terze parti ai sensi del regolamento (CE) 765/2008, accreditati dagli organismi di accreditamento nazionali e, se previsto da uno specifico sistema di certificazione, autorizzati ad operare dalle NCCA;
 - o dalle NCCA per il livello elevato o da altri organismi di valutazione della conformità da esse delegate in base alle scelte nazionali.
- Nel contesto di alcuni sistemi di certificazione europei sarà inoltre possibile emettere dichiarazioni UE di conformità direttamente da parte del fornitore di un servizio TIC o fabbricante di un prodotto TIC, per attestare il rispetto dei requisiti di cibersecurity di un prodotto ICT, un servizio ICT o processo ICT, limitatamente, però, al livello di affidabilità di base.
 - Le autorità nazionali di certificazione saranno responsabili a livello nazionale della vigilanza sui certificati di cibersecurity e sulle dichiarazioni UE di conformità emessi sul proprio territorio (*vigilanza oggettiva* – art. 58, par. 7, lett. a) e b)) ed in generale sulle attività degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersecurity e degli emittenti di dichiarazioni UE di conformità (*vigilanza soggettiva* – art. 58, par. 8).
 - Le autorità nazionali di certificazione collaboreranno inoltre a livello europeo con la Commissione Europea, ENISA e le autorità degli altri stati membri nella elaborazione e revisione dei sistemi di certificazione già adottati in seno all'ECCG.

In tale contesto, la Commissione Europea ha già conferito mandato ad ENISA per l'elaborazione dei primi tre sistemi europei di certificazione della cibersecurity:

- Certificazione della cibersecurity basata su Common Criteria e Metodologie Comuni di Valutazione (ISO/ IEC 15408 e ISO/IEC 18045).
- I servizi cloud⁵.
- Reti 5G.

Sono inoltre in corso di valutazione, come candidati per i prossimi sistemi europei di certificazione, i seguenti ambiti:

- Componenti del settore IACS – Industrial automation control systems, con un impatto in ambiti quali il settore energetico, settore trasporti e distribuzione dell'acqua⁶.
- Dispositivi IoT (Internet of Thing) – per l'ambito consumer electronics.

Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersecurity (art. 47) che sarà pubblicato dalla Commissione Europea definirà gli ambiti dei sistemi europei di certificazione da elaborare per il prossimo triennio 2022-2024.

1.3 Gli effetti del regolamento sul quadro nazionale di certificazione della cibersecurity

L'art. 18 della Legge n. 53 del 22 aprile 2021, "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020.", delega il Governo ad adottare, entro dodici mesi dalla data di entrata in vigore della legge, uno o più decreti legislativi per l'adeguamento della normativa nazionale al Titolo III del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, designando il Ministero dello Sviluppo Economico (MISE) quale NCCA per l'Italia. Con successivo decreto legge 14 giugno 2021, n. 82, ai sensi dell'art. 7, comma 1, lettera e) le competenze del Ministero dello sviluppo economico quale NCCA sono trasferite alla costituenda Agenzia per la cibersecurity nazionale.

⁵ Il sistema ha come obiettivo principale dare attuazione al libero flusso dei dati nell'ambito dell'UE con un approccio sicuro.

⁶ Un sistema europeo di certificazione dei componenti IACS è oggetto di studio da parte della Commissione europea da diversi anni. Per maggiori informazioni si può consultare il sito del progetto ERNACIP IACS della Commissione Europea DG JRC - <https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs>.

Il nuovo quadro di certificazione europeo introdotto dal regolamento (UE) 2019/881 riformerà il mutuo riconoscimento europeo attualmente realizzato dal SOG-IS MRA, esistente su base volontaria tra agenzia governative, ed avrà un impatto anche sull'accordo CCRA a livello mondiale. In particolare, le attività del SOG-IS migreranno nel primo sistema di certificazione europeo ai sensi dell'art 49 del Regolamento (UE) 2019/881, attualmente in corso di elaborazione, e che sarà probabilmente adottato nel 2022 dalla Commissione Europea.

Ad entrambi gli accordi partecipa, l'OCSI, l'organismo nazionale di certificazione che sarà riformato in conseguenza dell'adozione del primo sistema europeo di certificazione, dedicato alle certificazioni di prodotti ICT basati sui Common Criteria.

2. OBIETTIVI DELL'INTERVENTO E RELATIVI INDICATORI

2.1 Obiettivi generali e specifici

L'obiettivo primario è l'attuazione del quadro nazionale di certificazione della cibersecurity ai sensi del Regolamento (UE) 2019/881. Gli obiettivi generali della proposta normativa sono gli stessi obiettivi generali del suddetto regolamento che mira a realizzare un quadro europeo con regole armonizzate di certificazione della cibersecurity adottate da tutti gli stati membri, a beneficio del mercato unico dell'Unione ed in grado di realizzare il mutuo riconoscimento in tutta l'Unione dei certificati emessi nel territorio di un qualsiasi stato membro. Ciò permetterà di elevare il livello generale della cibersecurity nell'Unione con beneficio per cittadini ed imprese, incrementando la fiducia dei consumatori in prodotti TIC e servizi TIC. La certificazione di sicurezza cibernetica può inoltre offrire uno strumento per proteggere servizi essenziali per cittadini ed imprese dimostrando la conformità di misure di sicurezza a standard riconosciuti.

In attuazione del disposto di cui all'art. 18 della Legge di delegazione europea 2019-2020, il Governo elaborerà una proposta normativa consistente in un solo decreto legislativo con lo scopo di attuare a livello nazionale le disposizioni del Titolo III del Regolamento (UE) 2019/881, non immediatamente operative, adeguando il quadro nazionale di certificazione della cibersecurity vigente. Nell'attuazione, il Governo osserverà i seguenti principi e criteri direttivi specifici:

- a) designare l'Agenzia per la cybersecurity nazionale quale autorità competente ai sensi del paragrafo 1 dell'articolo 58 del regolamento (UE) 2019/881;
- b) individuare l'organizzazione e le modalità per lo svolgimento dei compiti e l'esercizio dei poteri dell'autorità di cui alla lettera a), attribuiti ai sensi dell'articolo 58 e dell'articolo 56, paragrafi 5 e 6, del regolamento (UE) 2019/881;
- c) definire il sistema delle sanzioni applicabili ai sensi dell'articolo 65 del regolamento (UE) 2019/881, prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati ad apposito capitolo dello stato di previsione del Ministero dello sviluppo economico per finalità di ricerca e formazione in materia di certificazione della cibersecurity; le sanzioni amministrative pecuniarie non devono essere inferiori nel minimo a 15.000 euro e non devono essere superiori nel massimo a 5.000.000 di euro;
- d) prevedere, in conformità all'articolo 58, paragrafi 7 e 8, del regolamento (UE) 2019/881, il potere dell'autorità di cui alla lettera a) di revocare i certificati rilasciati ai sensi dell'articolo 56, paragrafi 4 e 5, lettera b), emessi sul territorio nazionale, salvo diverse disposizioni dei singoli sistemi europei di certificazione adottati ai sensi dell'articolo 49 di detto regolamento.

Con riferimento ai suddetti criteri di delega, si osserva che l'entrata in vigore del Decreto Legge 14 giugno 2021, n. 82, convertito con Legge 4 agosto 2021, n. 109, che ha comportato i seguenti effetti principali:

- Con l'articolo 7, comma 1, lett. e) del decreto legge, la nuova Agenzia per la cibersecurity nazionale (ACN) assume la funzione di Autorità nazionale di certificazione della cibersecurity ai sensi dell'articolo 58 del regolamento europeo. Pertanto il criterio di delega

a) è abrogato implicitamente in quanto la designazione della NCCA in Italia è già avvenuta ed è stata destinata all'ACN.

- In base all'art. 16, comma 12, lettera b) del decreto legge “ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale”. Pertanto la destinazione finale degli introiti delle sanzioni di cui al criterio di delega c) non è più il Ministero dello sviluppo economico, bensì l'ACN.

2.2 Indicatori e valori di riferimento

Gli effetti del Cybersecurity act e della successiva attuazione nazionale attraverso il decreto legislativo ai sensi dell'articolo 18 della L. 53/2021 potranno essere valutati in termini di sviluppo del mercato delle certificazioni di cybersicurezza ed utilizzo di prodotti TIC e servizi certificati TIC ed aumento della consapevolezza dei problemi di cybersecurity da parte di cittadini, imprese e pubblica amministrazione.

In particolare come indicatore quantitativo per lo sviluppo del mercato delle certificazioni potrà essere valutato:

- Il *numero di certificati disponibili sul mercato per prodotti TIC, processi TIC e servizi TIC* con riferimento ai principali standard di riferimento per la cybersecurity.

A tal riguardo possiamo considerare, oltre al già citato standard ISO/IEC 15408 per la certificazione dei prodotti, anche il ben noto ISO/IEC 27001 per la certificazione dei sistemi di gestione della sicurezza delle informazioni e lo standard emergente l'ISA/IEC 62443 per l'automazione industriale. Con l'introduzione di nuovi sistemi europei di certificazione è prevedibile l'adozione di ulteriori standard di cybersecurity nella normativa europea e contestuale aumento dei certificati di cybersicurezza disponibili sul mercato.

Per quanto riguarda le certificazioni Common Criteria, sono disponibili statistiche nazionali su certificati emessi dal sito dell'Organismo di Certificazione della Sicurezza Informatica dell'*ordine di una settantina*⁷, per prodotti di elevato profilo e con certificazione riconosciuta internazionalmente a livello degli accordi CCRA e SOG-IS MRA.

Per quanto riguarda invece le certificazioni ISO 27001 dal sito di ACCREDIA risultano disponibili sul mercato italiano a fine settembre 2021 *circa 1700 certificati*⁸. Tali numeri potranno aumentare man mano che prenderanno piede ulteriori standard in attuazione del quadro europeo in corso di implementazione con l'adozione di nuovi sistemi europei di certificazione della cybersicurezza. L'incremento potrà essere facilitato da azioni di sensibilizzazione e di sostegno agli investimenti in certificazioni di cybersicurezza a favore di imprese e pubbliche amministrazione.

Per misurare invece il livello di consapevolezza e di effettivo utilizzo delle certificazioni potranno essere valutate statistiche sul

- Numero di prodotti certificati acquistati da cittadini, imprese e pubbliche amministrazione
- Numero di servizi certificati offerti da fornitori di servizi TIC

Potrà inoltre essere osservata l'inclusione in bandi per forniture di beni e servizi da parte della pubblica amministrazione o di gestori di pubblici servizi o di servizi essenziali (ad es. energia, trasporti, acqua potabile, sistema bancario) facenti uso di tecnologie ICT di della certificazione di cybersicurezza, come requisito minimo di accesso o come elemento da valutare positivamente nell'attribuzione del punteggio finale per l'aggiudicazione della fornitura. Dall'utilizzo dei sistemi europei di certificazione nei suddetti bandi potrà valutarsi la reale applicazione del quadro europeo di certificazione nel contesto nazionale da u punto di vista qualitativo.

⁷ <https://ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati>

⁸ https://services.accredia.it/ppsearch/accredia_stats_reserved_2.jsp?ID_LINK=1755&area=310

3. OPZIONI DI INTERVENTO E VALUTAZIONE PRELIMINARE

Il Regolamento (UE) 2019/881, in quanto norma europea con effetto diretto sulla normativa nazionale, senza necessità di recepimento, ha definito la maggior parte l'assetto dei quadri nazionali di certificazione della cybersicurezza. Richiede tuttavia l'adeguamento degli stessi attraverso alcune riforme. Tra queste vi è l'istituzione dell'autorità nazionale di certificazione della cybersicurezza e l'introduzione di un quadro sanzionatorio.

L'articolo 18 della Legge di delegazione europea 2019-2020 ha individuato inizialmente tale autorità nel Ministero dello sviluppo economico e stabilito alcuni criteri direttivi specifici, che costituiscono il mandato conferito al Governo. Il DL 14 giugno 2021, n.82, ha successivamente trasferito le competenze della NCCA in Italia all'Agenzia per la cybersicurezza nazionale (ACN) ai sensi dell'articolo 5 dello stesso decreto.

Nel seguito sono pertanto individuate e discusse alcune aree libere, non già fissate dal regolamento europeo e dalla legge delega, sulle quali è possibile operare scelte per l'attuazione nazionale coerentemente con il mandato ricevuto dal Governo, evidenziando eventuali criticità per ciascuna di esse.

3.1 Scelta di uno o più schemi di decreti legislativi

Ai sensi dell'articolo 18 della Legge di delegazione europea 2019-2020 il Governo è chiamato ad elaborare uno più schemi di decreti legislativi per l'attuazione nazionale del Titolo III del Regolamento (UE) 2019/881.

3.2 Rilascio dei certificati: modalità di emissione per i livelli elevato, sostanziale e di base

Per ogni sistema di certificazione che sarà adottato dalla Commissione Europea, ai sensi dell'articolo 56, parr. 5-6 del regolamento (UE) 2019/881, dovranno essere effettuate delle scelte nazionali per le modalità operative dell'attività di emissione dei certificati. In particolare, il regolamento UE 2019/881, relativamente a tale aspetto individua le seguenti possibilità:

- **CERTIFICATI DI LIVELLO ELEVATO:** L'art. 56, par. 6 prevede che il rilascio del certificato avvenga ad opera dell'autorità nazionale di certificazione oppure da parte di un altro organismo di valutazione della conformità in base alle seguenti due possibili opzioni:
 - a) con approvazione preventiva dell'autorità nazionale di certificazione della cybersicurezza di ogni singolo certificato europeo di cybersicurezza da effettuarsi prima dell'emissione da parte dell'organismo di valutazione della conformità individuato dall'autorità;
 - b) sulla base di una delega generale a rilasciare tali certificati europei di cybersicurezza conferita dall'autorità all'organismo di valutazione della conformità.
- **CERTIFICATI DI LIVELLO DI BASE E SOSTANZIALE:** Per quanto riguarda i livelli di certificazione più bassi, ovvero il livello di base e sostanziale, di norma qualsiasi organismo di valutazione della conformità accreditato dall'organismo nazionale di accreditamento (art. 56 par. 4) potrà rilasciare i certificati, salvo che lo specifico sistema europeo di certificazione non disponga che debba essere solo un soggetto pubblico a rilasciare i certificati (art. 56 par. 5). In tal caso, a rilasciare i certificati potrà essere l'autorità nazionale (art. 56 par. 5 lett. a)) o altro organismo di valutazione della conformità pubblico (art. 56 par. 5 lett. b)).

Di conseguenza per l'emissione dei certificati il Cybersecurity Act conferisce all'autorità un controllo pieno per i certificati di livello elevato. L'autorità può essenzialmente decidere se operare autonomamente o avvalersi di organismi di valutazione della conformità esterni riservandosi controlli preventivi o a posteriori sul loro operato. Nel caso invece dei certificati di livello di base o sostanziale, l'emissione dei certificati è affidata di norma ad un qualsiasi organismo di valutazione della conformità accreditato, salvo che nel contesto di uno specifico sistema di certificazione si stabilisca di affidare tale compito ad un soggetto pubblico, potendo tale soggetto essere la stessa autorità.

Si ravvisa quindi nell'ambito dell'emissione dei certificati un effettivo spazio per effettuare scelte nazionali specialmente per quanto riguarda l'emissione dei certificati di livello elevato, che l'autorità potrebbe riservare per se o ad altro organismo di valutazione della conformità.

3.3 Vigilanza nazionale: collaborazione dell'autorità nazionale con altre autorità e organismi

Tra i compiti dell'autorità nazionale di certificazione della cibersicurezza si individuano

- le collaborazioni con altre autorità di vigilanza del mercato competenti (art. 58, par. 7, lett. a))
- attività di sostegno e assistenza all'organismo di valutazione di accreditamento nazionale (art. 58, par. 7, lett. c))
- cooperazione con altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche (art. 58, par. 7, lett. h))

Per ciascun ambito è possibile operare delle scelte nazionali allo scopo di rendere la collaborazione con tali soggetti efficiente ed efficace rafforzando le attività di vigilanza nazionale.

3.4 Vigilanza nazionale: possibile ruolo dei laboratori privati

L'attività di vigilanza nazionale richiederà la verifica delle certificazioni e delle dichiarazioni UE di conformità (ove permesse da uno specifico sistema di certificazione) di cibersicurezza emesse dai soggetti diversi dall'NCCA.

In particolare ai sensi dell'articolo 58, par. 7, lett. a)-b), 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;

In tale contesto la NCCA, come già sperimentato nel rilascio delle certificazioni Common Criteria dell'OCSI ai sensi del DPCM 30 ottobre 2003, potrà avvalersi di laboratori privati di valutazione per effettuare prove su prodotti ICT certificati e prelevati dal mercato nel contesto della vigilanza nazionale. Nel prevedere il ruolo di laboratori privati abilitati per le attività di vigilanza da parte della NCCA bisognerà tuttavia prevenire potenziali conflitti di interesse rispetto a possibili attività concorrenti di vigilanza ed emissione dei certificati effettuabili nello stesso ambito dai medesimi laboratori. In particolare, va evitato che un laboratorio di prova possa essere coinvolto dalla NCCA nella attività di vigilanza di un settore nel quale è anche organismo di valutazione della conformità accreditato per l'emissione dei certificati o laboratorio di prova per un organismo di certificazione. Un tale conflitto potrebbe nascere in particolare rispetto alle emissioni dei certificati di livello di base e sostanziale nel quale la NCCA non eserciterà un controllo dell'emissione dei certificati (salvo che non sussista per lo specifico sistema di certificazione l'eccezione ex art. 56.5.(a) del regolamento).

3.5 Vigilanza nazionale: potere di revoca dei certificati della NCCA

L'art. 58, par. 8 del Regolamento individua i poteri minimi esercitabili dalle NCCA stabilite nei vari paesi europei:

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 cibersecurity 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 audit, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersecurity 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 cibersecurity e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersecurity;
- d) ottenere accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersecurity 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 cibersecurity rilasciati dalle autorità nazionali di certificazione della cibersecurity o i certificati europei di cibersecurity 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 cibersecurity;
- 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.

Nella L. 53/2021, attraverso il criterio direttivo specifico dell'articolo 18, comma 2, lettera d), è assegnato alla NCCA in Italia il potere aggiuntivo di

revoca di certificati emessi da organismi di valutazione della conformità diversi dalla NCCA per i livelli di affidabilità di base e sostanziale (art. 56, par. 4, 5(b)) in aggiunta al potere di revoca per i certificati di livello elevato (art. 56, par. 6) di cui le NCCA già dispongono ed individuato alla lettera suddetta e).

Pertanto se la disposizione di cui all'articolo 58, par. 8, lett. e) già conferisce all'autorità il potere di revoca dei certificati di livello elevato, con il suddetto criterio di delega specifico, tale potere è esteso anche al livello di base e sostanziale. In attuazione del criterio di delega vanno quindi stabilite le casistiche di revoca.

3.6 Certificazioni obbligatorie

Per alcuni sistemi di certificazione, già adottati, la Commissione Europea potrebbe valutare l'opportunità di un cambio di regime da puramente volontario ad un regime obbligatorio. Vale a dire un certificato di cibersecurity o una dichiarazione UE di conformità diverrebbero requisiti essenziali per l'immissione di un prodotto ICT o servizio ICT sul mercato.

Inoltre, i singoli stati membri potrebbero decidere autonomamente di rendere un sistema europeo di certificazione da volontario ad obbligatorio. In particolare, ai sensi dell'articolo 56, paragrafo 2 del Cybersecurity Act:

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

Di conseguenza la scelta di mantenere un sistema di certificazione puramente volontario oppure renderlo obbligatorio è effettuabile non solo a livello europeo ma anche a livello nazionale. Si pone pertanto la questione generale di come individuare eventuali sistemi europei di certificazione da rendere obbligatori e con quali modalità effettuare un tale cambio di regime.

4. COMPARAZIONE DELLE OPZIONI E MOTIVAZIONE DELL'OPZIONE PREFERITA

4.1 Impatti economici, sociali ed ambientali per categoria di destinatari

Da un punto di vista del mercato interno dell'UE, l'attuazione del regolamento (UE) 2019/881 dovrebbe favorire l'utilizzo delle certificazioni di cybersicurezza e lo sviluppo del mercato ad esse associato da più punti di vista.

Come sottolineato nella sezione 1, allo stato attuale solo alcuni paesi europei dispongono di un organismo di certificazione governativo in seno al SOG-IS per la certificazione di prodotti ICT. Inoltre, nell'ambito della certificazione di processi e servizi sono accreditati a livello europeo ai sensi del regolamento (CE) 765/2008 diversi organismi di valutazione della conformità, per lo più privati. Il nuovo quadro di certificazione europeo porterà ad un'armonizzazione della certificazione della sicurezza informatica nell'UE, garantendo il mutuo riconoscimento dei certificati emessi in qualsiasi Stato Membro e degli ambiti ben definiti per la partecipazione degli organismi di certificazione governativi e commerciali. La diffusione della certificazione della sicurezza informatica portata avanti dai molteplici attori coinvolti, imprese, laboratori di prova, agenzie governative dovrebbe aumentare il grado di consapevolezza dei consumatori sulla sicurezza informatica dei prodotti ICT acquistati, portando una quota consistente a preferire prodotti certificati sicuri, rispetto ad altri prodotti non certificati a basso costo.

La diffusione della certificazione di sicurezza informatica, che ai sensi del regolamento (EU) 2019/881 sarà, di base, di tipo volontario per non incidere negativamente sul mercato dei prodotti e servizi ICT, potrà richiedere per alcuni settori critici, come l'ambito dei servizi erogati dagli operatori di servizi essenziali previsti nell'allegato II della Direttiva NIS, la direttiva (UE) 2016/1148, l'obbligatorietà. L'obbligatorietà della certificazione potrà essere stabilita sia con norma europea e sia con norma nazionale con l'intervento della stessa autorità nazionale.

Pertanto, nel breve termine è possibile attendersi per il consumatore un effetto positivo, in termini di aumento della consapevolezza sulla sicurezza informatica e richiesta di prodotti e servizi certificati, anche a tutela della riservatezza dei propri dati personali e per contrastare possibili frodi informatiche. Sempre nel breve termine dovrebbero proporsi sul mercato aziende fornitrici di prodotti certificati per raccogliere la nuova domanda posta dai consumatori e svilupparsi al contempo l'indotto di organismi di valutazione della conformità privati per la valutazione e certificazione dei prodotti TIC, processi TIC e servizi TIC. Tale tendenza dovrebbe portare nel breve termine ad un'iniziale tendenza di aumento del livello di sicurezza cibernetica del mercato europeo e nazionale.

In una fase successiva, attraverso l'introduzione della certificazione obbligatoria per alcuni settori fondamentali, sarà possibile mettere in sicurezza i servizi essenziali di pubblica utilità. Tuttavia, bisognerà prestare attenzione ad effettuare una transizione graduale, sia perché il mercato degli organismi di valutazione della conformità non sarà in grado di raccogliere da subito l'improvvisa domanda aumentata di prodotti e servizi certificati, sia perché la certificazione obbligatoria avrà un effetto di aumento dei prezzi generalizzata per prodotti TIC e servizi TIC a danno del consumatore.

E' in tale ambito che le scelte del regolatore nazionale o europeo dovranno misurarsi, bilanciando le esigenze di messa in sicurezza dei settori più critici e di contenimento dei prezzi del mercato di prodotti TIC e servizi TIC. Sarà quindi importante confrontarsi con i portatori di interesse principali tra cui i consumatori, le aziende produttrici, i laboratori di prova e gli organismi di valutazione della conformità per individuare lo scenario nazionale da realizzare che meglio tenga conto delle esigenze di tutti gli attori.

Con riferimento ai potenziali destinatari, si evidenzia la possibilità di una loro individuazione sulla base dei documenti di consultazione in allegato. In particolare, si individuano i potenziali destinatari negli Organismi di normazione nazionale UNINFO – CEI, in Accredia in qualità di organismo di accreditamento, nei laboratori OCSI in qualità di organismi di valutazione della conformità (attualmente individuabili in 10 unità, evidenziando tuttavia la possibilità di un loro incremento anche in ragione del subentrare di parametri eurounitari da cui consegue un eventuale obbligo di

certificazione), nelle fabbricanti di prodotti informatici e nelle imprese che forniscano servizi TIC, cioè gli operatori di telecomunicazione nazionale.

4.2 Impatti specifici

4.2.1 Sviluppo del mercato

Per quanto riguarda le PMI è da attendersi una scarsa propensione ad abbracciare il mercato dei prodotti e servizi certificati in ragione dei costi aumentati, anche in attesa di verificarne l'effettivo sviluppo a livello europeo e nazionale. Fanno eccezione quelle PMI che concentrando conoscenze nel settore della sicurezza informatica, come ad esempio i laboratori di prova privati, affiancandosi alle grandi aziende, maggiormente orientate ad investire nelle TIC, potrebbero beneficiare del nuovo mercato di prodotti e servizi certificati. Ulteriore eccezione riguarda i prodotti certificati a "livello base", per i quali, come previsto dal regolamento, attraverso una autovalutazione o modalità di certificazione semplificata con costi contenuti, potranno acquisire un valore aggiunto rispetto ai prodotti e servizi non certificati.

Un obiettivo del Governo potrebbe essere quello di assicurare un livello di sicurezza minimo nei prodotti e servizi commerciali per aumentare la sicurezza del mercato nazionale incentivando le PMI ad effettuare certificazioni anche di "livello base".

Va inoltre considerato che, rispetto alla concorrenza internazionale, la sicurezza informatica di prodotti e servizi diventa sempre di più un fattore determinante, e quindi il quadro di certificazione europea potrebbe fornire all'UE un vantaggio competitivo. Inoltre un sostegno specifico nazionale permetterebbe uno sviluppo delle esportazioni nazionali in ambito internazionale.

4.2.2 Oneri informativi

Per quanto riguarda gli oneri informativi, le aziende produttrici e fornitrici di servizi che intenderanno avvalersi delle autodichiarazioni di conformità in un regime volontario, dovranno rendere disponibili tutte le informazioni necessarie sui prodotti e servizi autovalutati in termini di dichiarazioni UE emesse e revocate e le informazioni addizionali obbligatorie da rendere disponibile per l'utente ai sensi del regolamento europeo. Tali informazioni saranno raccolte e rese pubbliche attraverso il sito web dedicato dell'agenzia ENISA e potenzialmente anche dal sito web dell'autorità nazionale di certificazione della sicurezza cibernetica. Ugualmente gli organismi di valutazione della conformità, in relazione ai certificati emessi, modificati e revocati saranno sottoposti ad analoghi oneri informativi attraverso i quali i consumatori e le aziende fruitrici di prodotti e servizi TIC certificati potranno avere un quadro aggiornato dei certificati validi emessi nell'UE.

Nella presente proposta normativa non sono previsti ulteriori obblighi informativi o incrementi del livello di regolazione minima già previsto dal regolamento (UE) 2019/881.

4.3 Motivazione dell'opzione preferita

La Tabella 1 mostra le scelte effettuate in ogni area d'intervento descritta in sezione 3 e che costituiscono nel complesso l'opzione complessiva selezionata.

Tali opzioni sono state sottoposte a consultazione pubblica dal Ministero dello sviluppo economico terminata il 6 giugno 2021, prima del trasferimento delle competenze della NCCA alla costituenda

Agenzia per la cybersicurezza nazionale ai sensi del DL 14 giugno 2021, n.82. Per maggiori dettagli si veda sezione successiva dedicata alla consultazione.

Tabella 1 – Le opzioni di riferimento e le scelte effettuate

Area di intervento	Scelta effettuata	Motivazione della scelta	Consenso riscontrato durante la consultazione pubblica ⁹
Scelta di uno o più schemi di decreti legislativi	Si sceglie di attuare la delega art. 18 della L. 53/2021 con un singolo decreto legislativo.	Non si ravvisano motivi particolari per prevedere più di uno schema di decreto legislativo. Si propone per semplicità di attuare con un singolo decreto legislativo la delega complessiva di cui all'articolo 18 della Legge di delegazione europea 2019-2020 per rendere completamente operativo a livello nazionale il regolamento (UE) 2019/881, fatti salvi atti di esecuzione della Commissione Europea che dovessero essere adottati successivamente ai sensi del regolamento (UE) 2019/881.	Dai questionari inviati risulta un consenso unanime sulla posizione del Ministero dello sviluppo economico.
Rilascio dei certificati: modalità di emissione per i livelli elevato, sostanziale e di base	In seno alla proposta di decreto legislativo si ritiene di lasciare aperta ogni possibilità per l'emissione dei certificati prevedendo possibili collaborazioni pubblico-privato che potranno coinvolgere l'NCCA, i laboratori di prova e gli altri organismi di valutazione della conformità pubblici e privati accreditati dall'organismo nazionale di accreditamento. Saranno eventualmente operate scelte specifiche sulla base delle esigenze del singolo sistema di certificazione che sarà adottato, ove necessario.	Le scelte riguardo all'emissione dei certificati potranno essere fatte per ogni sistema europeo di certificazione che sarà adottato dalla Commissione Europea sulla base delle esigenze specifiche del sistema di certificazione.	La posizione del Ministero dello sviluppo economico è sostenuta nei contributi ricevuti.
Vigilanza nazionale: collaborazione e dell'autorità nazionale con altre autorità e organismi	La proposta normativa tratterà alcuni principi generali di cooperazione della NCCA con le altre autorità competenti e l'organismo nazionale di accreditamento.	Le effettive modalità di collaborazione potranno essere oggetto di accordi successivi tra le autorità/organismi o di	La posizione del Ministero dello sviluppo economico raccoglie il consenso unanime dei partecipanti.

⁹ Si veda sezione successiva su consultazione pubblica effettuata.

5. MODALITÀ DI ATTUAZIONE E MONITORAGGIO

5.1 Attuazione

L'Agenzia per la cybersicurezza nazionale (ACN) è il soggetto primariamente responsabile per l'attuazione della proposta normativa. La stessa come chiarito nelle precedenti sezioni mira ad attuare a livello nazionale il Titolo III del regolamento (UE) 2019/881, che introduce nell'Unione Europea un quadro di certificazione della sicurezza cibernetica armonizzato, che ha lo scopo di ridurre la frammentazione interna del mercato delle certificazioni di sicurezza cibernetica, elevando il livello di sicurezza di prodotti, servizi e processi TIC, a beneficio di imprese e consumatori dell'Unione e realizzando un mutuo riconoscimento in tutta l'Unione dei certificati emessi nei singoli stati membri.

Da un punto di vista giuridico, con il presente decreto legislativo si tratterà la cornice generale del quadro nazionale di certificazione della sicurezza cibernetica, che prevede in particolare:

- l'istituzione della autorità nazionale ai sensi dell'articolo 58,
- l'introduzione di un quadro sanzionatorio nazionale per il rispetto del regolamento europeo e dei successivi sistemi europei di certificazione adottati dalla Commissione Europea con atti di esecuzione.

Sarà inoltre oggetto del decreto legislativo, come previsto dal criterio direttivo specifico di cui alla lettera b), comma 2 dell'art. 18 della L. 53/2021, l'organizzazione dell'autorità nazionale. Tale organizzazione dovrà definire gli aspetti essenziali di organizzazione ed in particolare assicurare la separazione ed indipendenza tra le funzioni di vigilanza (art. 58 del reg. (UE) 2019/881) e di emissione dei certificati (art. 56, par. 5(a) e par. 6 del reg. (UE) 2019/881) da parte dell'autorità nazionale.

Essendo il quadro europeo di certificazione in evoluzione e prevedendo in particolare l'introduzione di nuovi sistemi europei di certificazione adottati dalla Commissione Europea con atti di esecuzione, il quadro nazionale dovrà essere aggiornato, con successivi provvedimenti dell'Agenzia, per poter rendere applicabili ove necessario i nuovi sistemi europei di certificazione non ancora operativi.

In sintesi,

- l'attuazione del quadro nazionale di certificazione tramite il presente decreto legislativo sarà responsabilità dell'ACN,
- la definizione del quadro sarà condivisa dal Governo, e troverà una soluzione attraverso il confronto con il Parlamento.
- L'operatività del quadro nazionale per gli specifici sistemi europei di certificazione sarà assicurata dall'ACN con l'emanazione di provvedimenti successivi per l'attuazione dei singoli sistemi europei di certificazione ove necessario.

5.2 Monitoraggio

Potrà costituirsi un tavolo con i principali portatori di interesse nazionali per tale monitoraggio, che comprenderà:

- associazioni di imprese
- associazioni dei consumatori
- l'organismo nazionale di accreditamento
- gli enti nazionali di normazione nel settore delle TIC
- gli organismi di valutazione della conformità accreditati

- università e centri di ricerca

Nell'ambito di tale attività sarà possibile monitorare gli sviluppi del mercato nazionale delle certificazioni e formulare proposte di revisione della disciplina nazionale ed eventuali proposte di promozione ed incentivazione del settore.

CONSULTAZIONI SVOLTE NEL CORSO DELL'AIR

Per l'elaborazione del decreto legislativo si sono svolte due tipologie di consultazione a cura del Ministero dello sviluppo economico:

- una consultazione pubblica svoltasi dal 6 maggio 2021 al 6 giugno 2021,
- una consultazione mirata con l'organismo nazionale di accreditamento, ritenuto il principale portatore di interesse degli effetti del regolamento europeo e del decreto legislativo, e con il quale l'autorità nazionale dovrà collaborare strettamente.

Risultati della consultazione pubblica

La consultazione pubblica si è svolta attraverso il sito istituzione del Ministero dello sviluppo economico della DG TCSI-ISCTI (<https://atc.mise.gov.it>) sul quale è stata preparata una pagina di consultazione con le informazioni essenziali sulla consultazione ed alcuni documenti di riferimento:

- intervallo previsto per l'invio di contributi: 6 maggio 2021 - 6 giugno 2021,
- descrizione del contesto normativo, finalità dell'intervento e possibili opzioni: attraverso una apposita scheda informativa predisposta per la consultazione,
- modalità di raccolta dei contributi: attraverso un questionario strutturato da compilare in formato digitale e da reinviare firmato ad un indirizzo di posta elettronica dedicato (consultazione.CSA@mise.gov.it)
- pubblicazione degli atti: sul sito dedicato alla consultazione sono stati pubblicati i contributi ricevuti la cui pubblicazione è stata autorizzata ed un documento di sintesi.

Al momento dell'avvio della consultazione, la stessa è stata segnalata con PEC della DG TCSI-ISCTI ad un certo numero di soggetti nazionali identificati come portatori di interesse per l'attuazione nazionale del Cybersecurity Act [COM_CONS_PUB1]. La pubblicazione della consultazione è stata inoltre segnalata al DAGL con PEC separata [COM_CONS_PUB2].

In seno alla consultazione pubblica è stato richiesto di commentare attraverso il questionario le opzioni di riferimento riportate in Tabella 1. In particolare, i contributi ricevuti a commento della proposta del Ministero dello sviluppo economico sono sintetizzati nell'ultima colonna della stessa tabella.

Le opzioni di riferimento proposte dal Ministero dello sviluppo economico sono state accolte nel complesso dai partecipanti alla consultazione. L'unico punto su cui si sono riscontrate opinioni

divergenti ha riguardato la previsione di misure per il controllo del conflitto di interesse dei laboratori privati esterni utilizzabili dall'autorità nazionale nelle attività di vigilanza. Il Ministero dello sviluppo economico ha proposto come misura unica di controllo del conflitto di interesse l'obbligo di astensione per i laboratori di prova utilizzati nella attività di vigilanza dal Ministero dalle attività di emissione dei certificati. La misura è stata ritenuta da alcuni necessaria, da altri eccessivamente stringente e poco efficace. Visto che non si è manifestata una posizione chiaramente contraria alla misura di astensione proposta dal Ministero, si è ritenuto di mantenerla immodificata per l'elaborazione del decreto legislativo. Tale misura permette di distinguere chiaramente il ruolo di un laboratorio nel contesto dei certificati di livello sostanziale e di base. In tale ambito un laboratorio di prova occorre che scelga

- se vuole operare come organismo di certificazione autonomamente dalla NCCA, selezionando in particolare il mercato delle certificazioni di livello di base e sostanziale, ed essere soggetto alla relativa attività di vigilanza
- o partecipare come soggetto attivo nello stesso ambito per conto dell'autorità nelle attività di vigilanza.

Maggiori dettagli sono disponibili nel documento di sintesi [DOC-SIN]. Sono allegati anche la scheda informativa [SCH-INF] ed il questionario utilizzato nella consultazione [QUEST]

Tali documenti assieme ai contributi forniti dai portatori d'interesse, la cui pubblicazione è stata autorizzata, sono disponibili sulla pagina pubblica dedicata alla consultazione:

<https://atc.mise.gov.it/index.php/eventi/971-consultazione-pubblica-sull-attuazione-nazionale-del-titolo-iii-del-regolamento-ue-2019-881-quadro-di-certificazione-della-sicurezza-cibernetica>

Risultati della consultazione mirata

Attraverso il confronto diretto con l'organismo nazionale di accreditamento, successivamente alla conclusione della consultazione pubblica, il Ministero dello sviluppo economico ha potuto raccogliere proposte di emendati alla bozza di decreto legislativo in preparazione sui seguenti punti:

- sorveglianza nazionale degli organismi di valutazione della conformità in cooperazione con l'organismo di accreditamento (art. 58, par. 7, lett. c))
- modalità di rilascio dei certificati da parte dell'autorità ed accreditamento dell'organismo di certificazione in seno all'autorità (art. 60, parr. 1-2 del reg. (UE) 2019/881)
- coordinamento dell'autorità e dell'organismo di accreditamento nazionale nelle attività di accreditamento (Art. 60. 1 del reg. (UE) 2019/881) e di autorizzazione (art. 60.3 e art. 54, par. 1.(f) del reg. (UE) 2019/881)
- reclami e ricorsi giurisdizionali nei confronti degli organismi di valutazione della conformità (art. 63 e art. 64 del reg. (UE) 2019/881)

Si fornisce in allegato un prospetto [PRSP_ACCREDIA] con il testo originario proposto dal Ministero dello sviluppo economico, le proposte di emendamento formulate dall'organismo nazionale di accreditamento e le proposte di emendamento accolte dal Ministero dello sviluppo economico nella formulazione finale, che hanno portato ad un aggiornamento dell'attuale bozza di decreto legislativo per la successiva attività di revisione in concertazione con i ministeri interessati.

PERCORSO DI VALUTAZIONE

Il coordinamento della redazione della proposta d'intervento normativo è stata curata dalla Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI-ISCTI).

La proposta di decreto legislativo è stata elaborata dalla Divisione II della DGTCSI-ISCTI, competente nel Ministero dello sviluppo economico per l'implementazione nazionale del Cybersecurity Act, ai sensi del Decreto ministeriale 14 gennaio 2020.

Il testo proposto, preceduto dalla consultazione pubblica e mirata con l'organismo nazionale di accreditamento, è stato successivamente revisionato con la collaborazione dell'Ufficio Legislativo del Ministero dello sviluppo economico e condiviso internamente con la Direzione generale per il mercato, la concorrenza, la tutela del consumatore e la normativa tecnica (DGMCTCNT).

LISTA DOCUMENTI ALLEGATI

In allegato alla presente relazione sono forniti i seguenti documenti:

[COM_CONS_PUB1] Comunicazione di avvio della consultazione pubblica ai portatori di interesse.

[COM_CONS_PUB2] Comunicazione al DAGL dell'avvio della consultazione pubblica

[DOC-SIN] Documento di sintesi dei risultati della consultazione pubblica

[SCH-INF] Scheda informativa per i partecipanti alla consultazione

[QUEST] Questionario per i partecipanti alla consultazione

[PRSP_ACCREDIA] Sintesi della consultazione mirata con l'organismo nazionale di accreditamento