TITOLO III DEL REGOLAMENTO (UE) 2019/881, "REGOLAMENTO SULLA CIBERSICUREZZA",

ATTUAZIONE NAZIONALE DEL QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

SCHEDA INFORMATIVA

SOMMARIO

1 Introduzione....2

2 Il contesto attuale in materia di sicurezza cibernetica....3

2.1 Contesto nazionale, europeo ed internazionale antecedente e successivo al Cybersecurity Act....3

2.2 Futuri sistemi europei di certificazione....5

2.3 Possibilità di introdurre sistemi europei di certificazione obbligatori....6

2.4 Nuovo contesto nazionale con l'approvazione della Legge di Delegazione Europea 2019-2020....6

3 Gli obiettivi della proposta normativa....8

3.1 Obiettivi del regolamento (UE) 2019/881....8

3.2 Criteri di delega: articolo 18 della Legge di delegazione europea 2019-2020....8

4 Le opzioni di intervento....9

4.1 Scelta di uno o più schemi di decreti legislativi....9

4.2 Rilascio dei certificati: modalità di emissione per i livelli elevato, sostanziale e di base....9

4.3 Vigilanza nazionale: collaborazione dell'autorità nazionale con altre autorità e organismi....10

4.4 Vigilanza nazionale: possibile ruolo dei laboratori privati....10

4.5 Vigilanza nazionale: potere di revoca dei certificati della NCCA....11

4.6 Certificazioni obbligatorie....12

1 Introduzione

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

Il suddetto regolamento richiede a tutti gli Stati Membri di designare una o più Autorità Nazionali di Certificazione della Cibersicurezza (National Cybersecurity Certification Authorities - NCCA) (art. 58 del regolamento (UE) 2019/881) che vigileranno sull'applicazione dello stesso a livello nazionale e coopereranno con le autorità designate dagli altri stati membri, la Commissione Europea e l'agenzia europea ENISA nella realizzazione e revisione del quadro europeo di certificazione. Alle NCCA sono assegnati alcuni poteri, tra cui il potere sanzionatorio (artt. 58.8.(f) e 65 del regolamento UE) allo scopo di far rispettare il quadro europeo di certificazione nel proprio ambito nazionale. Le NCCA avranno anche il compito di rilasciare i certificati di cibersicurezza nel caso in cui questi abbiano un livello di affidabilità elevato (art. 56.6) e in altri casi, debitamente giustificati, ove previsto esplicitamente in singoli sistemi europei di certificazione (art. 56.5a).

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.

Il MISE, con la nuova funzione di NCCA ai sensi dell'art. 58 del Regolamento (UE) 2019/881, estenderà le competenze già attribuite in materia di certificazione e vigilanza nel settore della cibersicurezza. In particolare, presso la Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica - Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DG TCSI-ISCTI) del MISE è già operativo l'Organismo di Certificazione della Sicurezza Informatica (OCSI), che sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi del DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004). Inoltre, sempre presso la DG TCSI-ISCTI opera il CVCN (Centro di valutazione e certificazione nazionale) ai sensi del decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017 per la valutazione di sicurezza delle infrastrutture critiche e strategiche nazionali ed un laboratorio (Centro di valutazione - CE.VA) per la valutazione di sicurezza informatica per l'ambito classificato. Per quanto riguarda invece le attività di vigilanza in materia di sicurezza informatica, la DG TCSI-ISCTI è autorità NIS (Direttiva (UE) 1148/2016) in vari settori, nonchè autorità competente per la sicurezza delle reti di comunicazione elettronica (Direttiva (UE) 2018/1972).

Nel seguito si illustrano per il suddetto intervento normativo:

- il contesto attuale,
- gli obiettivi della proposta normativa,
- le opzioni di intervento.

2 Il contesto attuale in materia di sicurezza cibernetica

2.1 Contesto nazionale, europeo ed internazionale antecedente e successivo al Cybersecurity Act.

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 telematici, organismi di normazione, laboratori di prova specializzati nella valutazione della cibersicurezza e agenzie governative[1] 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 in EU 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. L'IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components), quale organismo dell'IEC (International Electrotechnical Commission), esprime vari schemi di certificazione con mutuo riconoscimento internazionale per i componenti del settore elettrotecnico[2].

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 TIC, 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 nazioni UE ed EFTA[3] e per l'ambito mondiale l'accordo CCRA (Common Criteria Recognition Arrangement) che vede aderenti agenzie governative di nazioni europee ed extraeuropee[4].

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. 10[5], a cui sovraintende l'OCSI (Organismo di

[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 governativo, indipendentemente dal grado di indipendenza economico-giuridica rispetto al governo e dall'ordinamento dello stato di riferimento.

[2] Esistono inoltre numerose libere associazioni private che esprimono un proprio sistema di valutazione o di certificazione basato a volte su norme internazionali, quali ad esempio il GSMA per le comunicazioni mobili, Global platform, Eurosmart. Gli ambiti sinteticamente accennati non costituiscono una trattazione completa dei settori di interesse per la valutazione e certificazione di sicurezza informatica. Il Regolamento (UE) 2019/881, con la sua futura attuazione europea e conseguente attuazione nazionale in ciascuno stato membro, potrebbe incidere su questi ambiti e su altri non menzionati introducendo norme armonizzate per vari settori di riferimento.

[3] 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.

[4] 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.

[5] Tale articolo è stato abrogato dal d.lgs. 82/2005 e sostituito dall'art. 35 comma 5 dello stesso decreto legislativo

Certificazione della Sicurezza Informatica)[6]. L'OCSI, 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 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 da parte di ENISA, e che sarà probabilmente adottato nel 2021 dalla Commissione Europea.

Il nuovo quadro di certificazione europeo introdurrà anche sistemi di certificazione della cibersicurezza per settori/contesti specifici sulla base di altri standard di riferimento ed avrà le seguenti caratteristiche principali:

- Ogni stato membro dovrà designare una o più autorità nazionali di certificazione della cibersicurezza 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 le autorità nazionali di certificazione della cibersicurezza nel cosiddetto Gruppo europeo per la certificazione della cibersicurezza (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 cibersicurezza, attesi entro il 2021, la normativa europea comincerà a produrre i primi effetti sulla normativa nazionale dei singoli Stati Membri. In particolare, 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 cibersicurezza, in base alle regole specifiche definite per ogni sistema europeo di certificazione potranno essere emessi secondo varie modalità:
    - da organismi di valutazione della conformità terzi ai sensi del Regolamento (CE) 765/2008, accreditati dall'organismo di accreditamento nazionale e, se previsto dal singolo sistema di certificazione, autorizzati ad operare dalla NCCA;
    - dalle NCCA per i certificati di livello elevato o da altri organismi di valutazione della conformità pubblici nei casi debitamente giustificati definiti nei singoli sistemi di certificazione europei via via introdotti.
- Nel contesto di alcuni sistemi di certificazione europei sarà inoltre possibile emettere dichiarazioni UE di conformità da parte del fornitore di un servizio TIC o fabbricante di un prodotto TIC, per attestare il rispetto dei requisiti di cibersicurezza per il livello di garanzia di base.

preservando le prerogative dell'organismo di certificazione nazionale.

[6] 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 "Codice dell'amministrazione digitale" (CAD), modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179.

- Le autorità nazionali di certificazione saranno responsabili a livello nazionale della vigilanza sui certificati di cibersicurezza emessi sul proprio territorio 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. Collaboreranno inoltre a livello europeo con la Commissione Europea nella elaborazione e revisione dei sistemi di certificazione già adottati in seno all'ECCG.

2.2 Futuri sistemi europei di certificazione

Con l'entrata in vigore del Regolamento, la Commissione Europea ha avviato le attività dell' ECCG (art. 62 del Regolamento (UE) 2019/881), con il compito principale di discutere l'elaborazione dei prossimi sistemi europei di certificazione della cibersicurezza. In tale contesto, la Commissione Europea ha già conferito mandato ad ENISA per l'elaborazione dei primi tre sistemi europei di certificazione della cibersicurezza:

- Certificazione della cibersicurezza basata su Common Criteria e Metodologie Comuni di Valutazione (ISO/ IEC 15408 e ISO/IEC 18045).
- Certificazione della cibersicurezza per i servizi cloud[7].
- 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'acqua[8].
- Dispositivi IoT (Internet of Thing) – Per l'ambito consumer electronics.

Potrebbero essere considerati anche gli ulteriori ambiti per i successivi sistemi di certificazione tra i seguenti:

- Processi sicuri per sviluppo e gestione del ciclo di vita di prodotti TIC.
- Semplificazioni della metodologia Common Criteria[9] per garantire tempi di valutazione definiti.
- Audit service provider
- Crittografia,
- Intelligenza artificiale

Il programma di lavoro progressivo dell'Unione per la certificazione europea della cibersicurezza (art. 47) che sarà pubblicato dalla Commissione Europea definirà i suddetti ambiti dei sistemi europei di certificazione da elaborare per il prossimo triennio 2021-2023.

È da evidenziare l'approccio ambizioso con il quale si intende affrontare in modo organico ed armonizzato a livello europeo la messa in sicurezza di settori strategici e spesso particolarmente complessi attraverso la certificazione di cibersicurezza. Da una parte si ravvisa la necessità di garantire l'immissione di prodotti TIC sicuri nel mercato unico europeo per non minare la fiducia dei consumatori e frenare di conseguenza lo sviluppo del mercato unico. Dall'altra si individua come prioritario l'obiettivo di proteggere alcuni servizi essenziali per i cittadini europei che fanno uso di TIC.

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

[8] 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.

[9] Vi interesse a sviluppare sistemi di certificazione leggeri in grado di condurre valutazioni in un tempo limitato e definito senza rinunciare agli aspetti essenziali di verifica dei prodotti a partire dall'esperienza maturata sui Common Criteria.

2.3 Possibilità di introdurre sistemi europei di certificazione obbligatori

Ulteriore sfida per alcuni futuri sistemi di certificazione europei riguarda la possibilità di passare da un regime puramente volontario ad un regime obbligatorio, prevedendo che per determinati settori di interesse pubblico per l'immissione sul mercato di prodotti e servizi TIC sia richiesta la certificazione di cibersicurezza obbligatoria. Tale requisito si potrà ottenere convertendo un sistema europeo esistente volontario già sperimentato in un sistema obbligatorio. A tal proposito si riporta il testo dell'articolo 56, par 3 in cui si ipotizza l'introduzione di sistemi europei di certificazione obbligatori per i settori riguardanti i servizi essenziali individuati nella Direttiva (UE) 2016/1148.

> *La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione e migliorare il funzionamento del mercato interno. La prima valutazione di questo genere è effettuata entro il 31 dicembre 2023 e le successive valutazioni sono effettuate almeno ogni due anni. Sulla base dei risultati di tali valutazioni, la Commissione individua i prodotti TIC, servizi TIC e processi TIC coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione.*
> *In via prioritaria la Commissione si concentra sui settori elencati all'allegato II della direttiva (UE) 2016/1148, che sono sottoposti a valutazione al più tardi due anni dopo l'adozione del primo sistema europeo di certificazione della cibersicurezza.*
> *Nel preparare la valutazione la Commissione:*
> *a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC o processi TIC e sugli utenti in termini di costi di tali misure nonché i benefici sociali o economici derivanti dal previsto aumento del livello di sicurezza per i prodotti TIC, i servizi TIC o i processi TIC in questione;*
> *b) tiene conto dell'esistenza e dell'attuazione di diritto degli Stati membri e dei paesi terzi in materia;*
> *c) procede a un processo di consultazione aperto, trasparente e inclusivo con tutti i pertinenti portatori di interesse e gli Stati membri;*
> *d) prende in considerazione le scadenze di attuazione e le misure transitorie e i periodi di transizione, in particolare con riferimento al possibile impatto delle misure sui fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC, PMI comprese;*
> *e) propone il modo più rapido ed efficace per realizzare la transizione da un sistema di certificazione volontario a uno obbligatorio.*

Se, da una parte, attraverso la certificazione obbligatoria si mira a mettere in sicurezza alcuni settori critici per i cittadini europei, dall'altra si sottolinea l'importanza di effettuare un'analisi di impatto adeguata prima di procedere al cambio di regime da volontario ad obbligatorio per un sistema di certificazione europeo.

2.4 Nuovo contesto nazionale con l'approvazione della Legge di Delegazione Europea 2019-2020

In attuazione dell'articolo 58, paragrafo 1,

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

A tal proposito, si sottolinea come il compito prioritario dell'autorità o delle autorità nazionali da designare sia il compito di vigilanza sull'applicazione del regolamento per il territorio nazionale.
Inoltre, a ciascuna autorità è richiesto di cooperare strettamente con le autorità nazionali competenti per gli altri stati membri, la Commissione Europea ed ENISA (art. 58 par. 6, art. 58 par. 7 lett. g), art. 58 par. 9, art. 59, art. 62).
In aggiunta, la NCCA ha il compito di irrogare sanzioni applicabili in caso di violazione del Titolo III del regolamento e di violazione dei sistemi europei di certificazione della cibersicurezza (art. 65, art. 58 par. 8 lett. f)).
A tali compiti si aggiunge, per la NCCA, quello del rilascio in via esclusiva dei certificati di cibersicurezza per i livelli di affidabilità elevati (art. 56, par. 6) e quando stabilito per lo specifico sistema di certificazione anche per i livelli di base e sostanziale (art. 56, par. 5, lett. a).

Con l'articolo 18 della Legge n. 53 del 22 aprile 2021, si individua il MISE quale NCCA in Italia. Tale scelta è operata coerentemente con i compiti già individuati per il MISE in materia di vigilanza della cibersicurezza (d.lgs. 18 maggio 2018 n. 65 art. 7 par. 1 lett. a), DM 12 dicembre 2018 del Ministro dello Sviluppo Economico) e certificazione della cibersicurezza (d.lgs. n. 82/2005 e smi art. 35, par. 5, DPCM 30 ottobre 2003[10]).

In particolare, con riferimento al DPCM 30 ottobre 2003 si individua presso l'ex Ministero delle Comunicazioni, oggi confluito nel MISE, l'Organismo di Certificazione della Sicurezza informatica (OCSI), che si avvale di una rete di laboratori di prova da esso accreditati per la certificazione della cibersicurezza in base allo standard Common Criteria. Tale organismo, come discusso in sezione 2, partecipa agli accordi di mutuo riconoscimento europeo SOG-IS MRA ed internazionale CCRA. In particolare, il SOG-IS MRA rappresenta di fatto un primo sistema europeo di certificazione, che anche se non discendente da normativa europea, realizza già il mutuo riconoscimento dei certificati di cibersicurezza tra alcuni degli stati membri su base volontaria. Per tale motivo è in corso la trasposizione delle attività del SOG-IS nel primo sistema europeo di certificazione ai sensi del regolamento (UE) 2019/881. Le modalità operative dell'OCSI saranno quindi adeguate in base al suddetto sistema europeo di certificazione, che sarà adottato dalla Commissione Europea, probabilmente entro il 2021. Alcuni aspetti oggetto di modifica potranno ad esempio essere le modalità di emissione dei certificati, le modalità per assicurare nel tempo il mantenimento delle garanzie ottenute dei certificati ed il mutuo riconoscimento europeo. Il nuovo sistema condizionerà anche il mutuo riconoscimento dei certificati in ambito internazionale, ed in particolare in seno al CCRA, dove potranno rendersi necessarie delle modifiche per rendere possibile la coesistenza del CCRA e del nuovo sistema europeo di certificazione europeo per i Common Criteria garantendo il mutuo riconoscimento.

Con l'adozione di ulteriori sistemi europei di certificazione, come prospettato in sezione 3, l'organismo di certificazione presso il Ministero dello Sviluppo Economico, dovrà occuparsi anche degli altri contesti di certificazione da questi regolati e certificare in base anche ad altri standard di riferimento.

[10] DPCM del 30 ottobre 2003, Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10. (pubblicato sulla GU n. 98 del 27-04-2004)

3 Gli obiettivi della proposta normativa

3.1 Obiettivi del regolamento (UE) 2019/881

La presente proposta normativa ha come obiettivo primario l'attuazione del quadro nazionale di certificazione della cibersicurezza 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 cibersicurezza 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 cibersicurezza nell'Unione con beneficio per cittadini ed imprese, incrementando la fiducia dei consumatori in prodotti TIC e servizi TIC. La certificazione di sicurezza informatica può inoltre offrire uno strumento per proteggere servizi essenziali per cittadini ed imprese dimostrando la conformità di misure di sicurezza a standard riconosciuti.

3.2 Criteri di delega: articolo 18 della Legge di delegazione europea 2019-2020

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 disposizione del Titolo III del Regolamento (UE) 2019/881, non immediatamente operative, adeguando il quadro nazionale di certificazione della cibersicurezza vigente.

Nell'attuazione, il Governo osserverà i seguenti princìpi e 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 del Ministero dello sviluppo economico per finalità di ricerca e formazione in materia di certificazione della cibersicurezza; 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.*

4 Le opzioni di intervento

Il Regolamento (UE) 2019/881, in quanto norma europea con effetto diretto sulla normativa nazionale, senza necessità di recepimento, ha già definito le principali modalità di funzionamento del nuovo quadro nazionale di certificazione della cibersicurezza che dovrà operare con modalità armonizzate a livello europeo. Alcuni di questi, come già commentato, richiedono però preliminarmente un'attuazione nazionale, quali la designazione dell'autorità nazionale e del quadro sanzionatorio.

L'articolo 18 della Legge di delegazione europea 2019-2020 ha inoltre individuato tale autorità nel Ministero dello sviluppo economico stabilito alcuni criteri direttivi specifici, che costituiscono il mandato conferito al Governo.

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 ed individuando per ciascuna una opzione di riferimento che sarà oggetto di consultazione.

4.1 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.

Opzione di riferimento*: Non ravvisandosi 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.*

4.2 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, par. 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 cibersicurezza di ogni singolo certificato europeo di cibersicurezza da effettuarsi prima dell'emissione da parte di un organismo di valutazione della conformità individuato dall'autorità;*
> *b) o sulla base di una delega generale a rilasciare tali certificati europei di cibersicurezza conferita dall'autorità ad un 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 lo specifico sistema di certificazione 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, che tuttavia non può essere totalmente indipendente dallo specifico sistema di certificazione, specialmente per quanto riguarda l'emissione dei certificati di livello di base e sostanziale.

***Opzione di riferimento**: Dal momento che le scelte riguardo all'emissione dei certificati potranno essere fatte per ogni sistema europeo di certificazione che sarà adottato dalla Commissione Europea, 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.*

4.3 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.

***Opzione di riferimento**: La proposta normativa traccerà 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/organismo di accreditamento nazionale.*

4.4 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 sicurezza informatica emesse dai soggetti diversi dall'NCCA, ai sensi dell'articolo 58, paragrafo 7, lettere a) e 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).

***Opzione di riferimento**: La NCCA costituirà due elenchi distinti nei quali saranno inseriti rispettivamente i laboratori privati da essa abilitati per le attività di certificazione e per le attività di vigilanza nazionale della NCCA. Per quanto riguarda il secondo elenco sarà necessario prevedere per i soggetti iscritti l'astensione da qualsiasi attività di emissione dei certificati o di valutazione di sicurezza informatica nell'ambito vigilato.*

4.5 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 cibersicurezza e agli emittenti di dichiarazioni UE di conformità di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;*
> *b) condurre indagini, sotto forma di audit, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità allo scopo di verificarne l'osservanza del presente titolo;*
> *c) adottare misure appropriate, nel rispetto del diritto nazionale, per accertare che gli organismi di*

valutazione della conformità, i titolari di certificati europei di cibersicurezza e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;
d) ottenere accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersicurezza al fine di svolgere indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;
e) revocare, conformemente al diritto nazionale, i certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o i certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, qualora tali certificati non siano conformi al presente regola mento o a un sistema europeo di certificazione della cibersicurezza;
f) irrogare sanzioni conformemente al diritto nazionale, a norma dell'articolo 65, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.

Nella Legge di Delegazione Europea 2019-2020, 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) conferisce all'autorità il potere di revoca dei certificati di livello elevato, con il suddetto criterio di delega specifico è esteso anche al livello di base e sostanziale. In attuazione del criterio di delega vanno quindi stabilite le casistiche di revoca.

***Opzione di riferimento**: Per quanto riguarda i certificati di livello elevato, ove fossero confermate delle non conformità l'NCCA effettuerà la revoca del certificato. Invece per l'ambito dei certificati di livello di base e sostanziale la revoca del certificato sarà effettuata dalla NCCA qualora a fronte dell'accertamento da parte della stessa di certificati non conformi, l'organismo di conformità emittente, non provveda alla riconduzione a conformità del certificato. Il certificato sarà revocato in eventuali altre situazioni particolarmente critiche, ad esempio 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 della Direttiva (UE) 2016/1148,*
- *o servizio di comunicazione elettronica ai sensi della Direttiva (UE) 2018/1972,*
- *o alla salute o all'incolumità personale.*

Sarà inoltre effettuata la revoca di un certificato di livello di base o sostanziale se previsto espressamente dallo specifico sistema europeo di certificazione.

4.6 Certificazioni obbligatorie

Come evidenziato nella sezione 3, 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. Inoltre, i singoli stati membri potrebbero decidere autonomamente di rendere un sistema europeo di certificazione volontario in obbligatorio. In particolare, ai sensi dell'articolo 56, paragrafo 2 del Cybersecurity Act:

La certificazione della cibersicurezza 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.

Opzione di riferimento*: La scelta di operare un cambio di regime di un sistema di certificazione da volontario ad obbligatorio sarà effettuata direttamente dall'autorità nazionale. Tale scelta potrebbe essere motivata dalla tutela di particolari interessi pubblici e sarà preceduta da una consultazione con i portatori di interesse. Infatti, se da una parte l'attività di certificazione dei prodotti TIC, servizi TIC e processi TIC conferisce un livello maggiore di affidabilità ai prodotti commercializzati e servizi erogati, dall'altro potrebbe comportare maggiori costi a carico dei fabbricanti/fornitori ed utilizzatori di prodotti TIC e servizi TIC, che siano cittadini, imprese o pubbliche amministrazioni. Inoltre, una certificazione obbligatoria in un determinato settore impegnerebbe maggiormente il sistema di vigilanza nazionale che dovrebbe monitorare un numero considerevolmente maggiore di emissioni di certificati rispetto ai numeri di un sistema volontario.*