RACCOMANDAZIONI

RACCOMANDAZIONE (UE) 2019/534 DELLA COMMISSIONE

del 26 marzo 2019

Cibersicurezza delle reti 5G

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) La Commissione ha riconosciuto come il dispiegamento della 5ª generazione (5G) delle tecnologie di rete costituisca un fattore abilitante fondamentale per lo sviluppo dei servizi digitali del futuro nonché una priorità per la strategia per il mercato unico digitale. La Commissione ha adottato il piano d'azione per il 5G al fine di garantire che l'Unione disponga delle infrastrutture di connettività necessarie per la sua trasformazione digitale dal 2020 ([1]).

(2) Le reti 5G si baseranno sull'attuale 4ª generazione (4G) delle tecnologie di rete, fornendo nuove capacità di servizio e diventando l'infrastruttura centrale nonché il fattore abilitante per un'ampia parte dell'economia dell'Unione. Una volta lanciate, le reti 5G costituiranno la struttura portante di una vasta gamma di servizi essenziali per il funzionamento del mercato interno e per il mantenimento e la gestione di funzioni economiche e sociali vitali, quali l'energia, i trasporti, i servizi bancari e sanitari e i sistemi di controllo industriale. Anche l'organizzazione dei processi democratici, quali le elezioni, si baserà sempre di più sulle infrastrutture digitali e sulle reti 5G.

(3) Poiché molti servizi essenziali dipendono dalle reti 5G, le conseguenze di malfunzionamenti sistemici e diffusi sarebbero particolarmente gravi. Pertanto garantire la cibersicurezza delle reti 5G è una questione di importanza strategica per l'Unione, in un momento in cui gli attacchi informatici sono più numerosi e sofisticati che mai.

(4) Date la natura interconnessa e transnazionale delle infrastrutture alla base dell'ecosistema digitale e la natura transfrontaliera delle minacce in questione, eventuali vulnerabilità e/o incidenti di cibersicurezza significativi riguardanti le reti 5G che si verificano in uno Stato membro inciderebbero sull'Unione nel suo complesso. Per questo motivo è opportuno prevedere misure che siano alla base di un elevato livello comune di cibersicurezza delle reti 5G.

(5) Gli Stati membri hanno confermato la necessità di un'azione a livello di Unione. Secondo quanto riportato nelle conclusioni del 21 marzo 2019, il Consiglio europeo attende con interesse la raccomandazione della Commissione su un approccio concertato in materia di sicurezza delle reti 5G ([2]).

(6) Garantire la sovranità europea dovrebbe essere un obiettivo fondamentale, nel pieno rispetto dei valori europei di apertura e tolleranza ([3]). Anche gli investimenti esteri nei settori strategici, l'acquisizione di beni, tecnologie e infrastrutture critici nell'Unione e la fornitura di apparecchiature fondamentali possono mettere a rischio la sicurezza dell'Unione.

(7) La cibersicurezza delle reti 5G riveste un'importanza fondamentale per garantire l'autonomia strategica dell'Unione, come riconosciuto nella comunicazione congiunta «UE-Cina – Una prospettiva strategica» ([4]).

(8) Anche nella risoluzione del Parlamento europeo sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione si invita la Commissione e gli Stati membri ad agire a livello di Unione ([5]).

(9) La presente raccomandazione affronta i rischi di cibersicurezza nelle reti 5G presentando orientamenti sulle opportune misure di analisi e gestione dei rischi a livello nazionale, sullo sviluppo di una valutazione dei rischi coordinata a livello europeo e sulla definizione di un processo per lo sviluppo di un insieme di strumenti comuni volti a garantire la migliore gestione dei rischi.

(10) Le reti di comunicazione elettronica sono protette da un solido quadro legislativo dell'Unione.

([1]) COM(2016) 588 final.
([2]) Conclusioni del Consiglio europeo del 21 e 22 marzo 2019.
([3]) Stato dell'Unione 2018 – L'ora della sovranità europea, 12 settembre 2018.
([4]) JOIN(2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//IT.

(11) Il quadro dell'Unione nel settore delle comunicazioni elettroniche ([6]) promuove la concorrenza, il mercato interno e gli interessi degli utenti finali e con il codice europeo delle comunicazioni elettroniche ([7]) persegue un ulteriore obiettivo in materia di connettività, articolato in termini di risultati: ampio accesso alla connettività fissa e mobile ad altissima capacità e diffusione della stessa per tutti i cittadini e le imprese dell'Unione, tutelando nel contempo gli interessi dei cittadini. La direttiva 2002/21/CE impone agli Stati membri di garantire il mantenimento dell'integrità e della sicurezza delle reti di comunicazione pubbliche e di assicurare che le imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico adottino adeguate misure di natura tecnica e organizzativa per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi. Essa prevede inoltre che le competenti autorità nazionali di regolamentazione abbiano la facoltà di impartire istruzioni vincolanti al fine di garantire il rispetto di tali obblighi.

(12) La direttiva 2002/20/CE del Parlamento europeo e del Consiglio ([8]) consente inoltre agli Stati membri di vincolare l'autorizzazione generale a condizioni relative alla sicurezza delle reti pubbliche contro l'accesso non autorizzato, al fine di tutelare la riservatezza delle comunicazioni conformemente alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([9]).

(13) Per sostenere l'attuazione di tali obblighi, l'Unione ha istituito una serie di organismi di cooperazione. L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), la Commissione, gli Stati membri e le autorità nazionali di regolamentazione hanno elaborato orientamenti tecnici per le autorità nazionali di regolamentazione in materia di notifica degli incidenti, misure di sicurezza, minacce e risorse ([10]). Il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([11]) («il gruppo di cooperazione») riunisce le autorità competenti al fine di sostenere e facilitare la cooperazione, in particolare fornendo orientamenti strategici per le attività della rete dei gruppi di intervento per la sicurezza informatica in caso di incidente, che agevola la cooperazione operativa a livello tecnico.

(14) Il futuro quadro europeo di certificazione della cibersicurezza ([12]) dovrebbe fornire uno strumento di sostegno essenziale per promuovere livelli coerenti di sicurezza. Esso dovrebbe consentire lo sviluppo di sistemi di certificazione della cibersicurezza per rispondere alle esigenze degli utenti di apparecchiature e software legati al 5G. L'importanza fondamentale di tali infrastrutture dovrebbe far sì che lo sviluppo dei pertinenti sistemi europei di certificazione della cibersicurezza per i prodotti, i servizi o i processi delle tecnologie dell'informazione e della comunicazione usati per le reti 5G sia considerato una priorità immediata. Gli Stati membri e gli operatori del mercato dovrebbero impegnarsi attivamente nello sviluppo di tali sistemi di certificazione, anche fornendo sostegno per la definizione di profili di protezione specifici per le reti 5G.

(15) In assenza di una legislazione armonizzata dell'Unione, gli Stati membri possono specificare, mediante regolamenti tecnici nazionali adottati in conformità alla legislazione dell'Unione, che un sistema europeo di certificazione della cibersicurezza dovrebbe essere obbligatorio. Gli Stati membri ricorrono inoltre ai sistemi europei di certificazione della cibersicurezza nel contesto degli appalti pubblici e della direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([13]) e potrebbero sostenere lo sviluppo di meccanismi di assistenza, quale un polo di assistenza, per l'acquisto di soluzioni di cibersicurezza da parte di acquirenti pubblici.

(16) Nel garantire la sicurezza delle reti 5G è fondamentale un livello elevato di protezione dei dati e della vita privata. Sono state inoltre definite norme a livello di Unione che garantiscono la sicurezza del trattamento dei dati personali, anche nelle comunicazioni elettroniche. Il regolamento generale sulla protezione dei dati ([14]) sancisce l'obbligo di trattare i dati personali in modo da garantirne la sicurezza, anche al fine di prevenire l'accesso non

([6]) Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU L 108 del 24.4.2002, pag. 33) e le direttive specifiche.

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

([8]) Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni) (GU L 108 del 24.4.2002, pag. 21).

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

([10]) https://resilience.enisa.europa.eu/article-13.

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

([12]) Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione («regolamento sulla cibersicurezza») [COM(2017) 477 final - 2017/0225 (COD)].

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

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

autorizzato ai dati personali o agli strumenti di trattamento dei dati e l'utilizzo non autorizzato degli stessi. La direttiva relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche stabilisce norme specifiche in materia di protezione della riservatezza delle comunicazioni e delle apparecchiature terminali degli utenti finali. Essa impone inoltre ai fornitori dei servizi l'obbligo di adottare misure tecniche e organizzative appropriate per salvaguardare la sicurezza dei servizi da essi offerti.

(17) L'Unione ha inoltre adottato uno strumento che proteggerà le infrastrutture e le tecnologie critiche, quali quelle utilizzate nelle comunicazioni, consentendo agli Stati membri di controllare gli investimenti esteri diretti per motivi di sicurezza o di ordine pubblico e creando un meccanismo di cooperazione tramite il quale gli Stati membri e la Commissione saranno in grado di scambiare informazioni e manifestare preoccupazione in merito a investimenti specifici ([15]).

(18) Gli Stati membri e gli operatori stanno attualmente adottando importanti misure preparatorie volte a consentire il lancio su larga scala delle reti 5G. Diversi Stati membri hanno espresso preoccupazione riguardo ai potenziali rischi di sicurezza relativi alle reti 5G nell'ambito dell'esecuzione di procedure per la concessione di diritti d'uso di bande di frequenza radio designate per le reti 5G ([16]) e stanno studiando misure per affrontare tali rischi.

(19) Per affrontare i rischi di cibersicurezza nelle reti 5G si dovrebbe tener conto dei fattori sia tecnici che di altro tipo. I fattori tecnici possono includere le vulnerabilità di cibersicurezza che possono essere sfruttate per l'accesso non autorizzato alle informazioni (ciberspionaggio, per motivi tanto economici quanto politici) o per altri scopi dolosi (attacchi informatici volti a distruggere sistemi e dati o a provocarne il malfunzionamento). Aspetti importanti di cui tenere conto dovrebbero essere la necessità di proteggere le reti nel corso del loro intero ciclo di vita e la necessità di considerare tutte le pertinenti apparecchiature, anche nelle fasi di progettazione, sviluppo, appalto, diffusione, funzionamento e manutenzione delle reti 5G.

(20) Altri fattori possono includere requisiti normativi o di altro tipo imposti ai fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione. Una valutazione dell'importanza di tali fattori dovrebbe tener conto, tra l'altro, del rischio generale di influenza da parte di un paese terzo, in particolare in relazione al suo modello di governance, all'assenza di accordi di cooperazione sulla sicurezza o di disposizioni analoghe, quali le decisioni di adeguatezza, tra l'Unione e il paese terzo interessato per quanto riguarda la protezione dei dati, e dovrebbe esaminare se tale paese sia parte di accordi multilaterali, internazionali o bilaterali in materia di cibersicurezza, lotta alla criminalità informatica o protezione dei dati.

(21) Dovrebbe essere effettuata e completata una valutazione dei rischi a livello nazionale, come passo importante verso lo sviluppo di un approccio dell'Unione in materia di cibersicurezza delle reti 5G. Ciò aiuterebbe gli Stati membri ad adeguare le misure nazionali in materia di requisiti di sicurezza e di gestione dei rischi alla luce di tale valutazione.

(22) È opportuno sviluppare un coordinamento per garantire l'efficacia delle misure volte ad affrontare tali minacce di cibersicurezza, misure che sono essenziali per il corretto funzionamento del mercato interno e per la protezione dei dati personali e della vita privata.

(23) Le valutazioni nazionali dei rischi dovrebbero costituire la base per una valutazione dei rischi coordinata a livello di Unione, costituita da una mappatura del panorama delle minacce e da una revisione congiunta condotta dagli Stati membri, con il sostegno della Commissione e in collaborazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

(24) Tenendo conto delle valutazioni dei rischi a livello nazionale e di Unione, il gruppo di cooperazione dovrebbe istituire un insieme di strumenti che identifichino i tipi di rischi di cibersicurezza e le possibili misure di attenuazione dei rischi in settori quali la certificazione, le prove e i controlli degli accessi. Tale insieme di strumenti dovrebbe inoltre identificare eventuali misure specifiche adeguate per far fronte ai rischi individuati da uno o più Stati membri. Il gruppo di cooperazione dovrebbe avvalersi del sostegno dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), di Europol, dell'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e del Centro dell'UE di situazione e intelligence. Tale insieme di strumenti dovrebbe orientare la Commissione in merito allo sviluppo di requisiti minimi comuni a ulteriore garanzia di un elevato livello di cibersicurezza delle reti 5G in tutta l'Unione.

(25) Nell'adottare misure volte ad affrontare i rischi di cibersicurezza si dovrebbe prendere in considerazione la promozione della cibersicurezza mediante la selezione di fornitori diversi al momento della costruzione di ogni singola rete.

([15]) Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione (GU L 79I1 del 21.3.2019, pag. 1).

([16]) La procedura d'asta per almeno una banda di frequenze è prevista per il 2019 in 11 Stati membri: Austria, Belgio, Francia, Germania, Grecia, Irlanda, Lituania, Paesi Bassi, Portogallo, Repubblica ceca, Ungheria. Altre sei aste sono previste per il 2020: Spagna, Malta, Lituania (frequenze diverse), Slovacchia, Polonia, Regno Unito. *Fonte:* http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) La presente raccomandazione lascia impregiudicate le competenze degli Stati membri per quanto riguarda le attività relative alla sicurezza pubblica, alla difesa, alla sicurezza nazionale e alle attività dello Stato in materia di diritto penale, compreso il diritto degli Stati membri di escludere determinati fornitori dai loro mercati per motivi di sicurezza nazionale,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

I. **OBIETTIVI**

(1) Al fine di sostenere lo sviluppo di un approccio dell'Unione volto a garantire la cibersicurezza delle reti 5G, la presente raccomandazione individua le azioni che dovrebbero essere adottate per consentire:

a) agli Stati membri di valutare i rischi di cibersicurezza che interessano le reti 5G a livello nazionale e adottare le necessarie misure di sicurezza;

b) agli Stati membri e alle istituzioni, alle agenzie e ad altri organismi pertinenti dell'Unione di elaborare congiuntamente una valutazione dei rischi coordinata a livello di Unione basata sulla valutazione nazionale dei rischi;

c) al gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 (gruppo di cooperazione) di individuare un'eventuale serie comune di misure da adottare per attenuare i rischi di cibersicurezza relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare le reti 5G.

II. **DEFINIZIONI**

(2) Ai fini della presente raccomandazione, si intende per:

a) «reti 5G»: un insieme di tutti gli elementi pertinenti delle infrastrutture di rete per le tecnologie delle comunicazioni mobili e senza fili utilizzati per la connettività e per servizi a valore aggiunto con caratteristiche di prestazione avanzate, quali capacità e velocità di trasmissione dei dati molto elevate, comunicazioni a bassa latenza, affidabilità ultra-elevata o capacità di supportare un numero elevato di dispositivi connessi. Tale insieme può includere elementi di rete tradizionali basati sulle precedenti generazioni di tecnologie delle comunicazioni mobili e senza fili, come il 4G o il 3G. Le reti 5G dovrebbero essere intese in modo da includere tutte le parti pertinenti della rete;

b) «infrastrutture alla base dell'ecosistema digitale»: le infrastrutture utilizzate per consentire la digitalizzazione in un'ampia gamma di applicazioni critiche nell'economia e nella società.

III. **AZIONE SU SCALA NAZIONALE**

(3) Entro il 30 giugno 2019 gli Stati membri dovrebbero effettuare una valutazione dei rischi dell'infrastruttura della rete 5G, anche identificando gli elementi più sensibili in relazione ai quali le violazioni della sicurezza avrebbero un impatto negativo significativo. Entro la stessa data gli Stati membri dovrebbero altresì rivedere i requisiti di sicurezza e i metodi di gestione dei rischi applicabili a livello nazionale, al fine di tenere conto delle minacce di cibersicurezza che possono derivare da: i) fattori tecnici, quali le caratteristiche tecniche specifiche delle reti 5G, e ii) altri fattori, come il quadro giuridico e politico cui possono essere soggetti i fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione in paesi terzi.

(4) Sulla base di tale valutazione e revisione nazionale dei rischi e tenendo conto delle azioni coordinate in corso a livello di Unione, gli Stati membri dovrebbero:

a) aggiornare i requisiti di sicurezza e i metodi di gestione dei rischi applicati alle reti 5G;

b) aggiornare i pertinenti obblighi imposti alle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico a norma degli articoli 13 *bis* e 13 *ter* della direttiva 2002/21/CE;

c) vincolare a condizioni l'autorizzazione generale riguardante la sicurezza delle reti pubbliche contro l'accesso non autorizzato e chiedere alle imprese che parteciperanno alle prossime procedure per la concessione di diritti d'uso delle frequenze radio nelle bande 5G di assumersi impegni per quanto riguarda la conformità ai requisiti di sicurezza per le reti a norma della direttiva 2002/20/CE;

d) applicare altre misure preventive volte ad attenuare i potenziali rischi di cibersicurezza.

(5) Le misure di cui al punto 4 dovrebbero includere maggiori obblighi per fornitori e operatori al fine di garantire la sicurezza di parti sensibili delle reti, nonché obblighi, se del caso, quali quelli di fornire alle autorità nazionali competenti informazioni pertinenti sulle modifiche previste delle reti di comunicazione elettronica, e requisiti volti a garantire che specifici componenti e sistemi informatici siano sottoposti a prove preliminari da parte di laboratori nazionali di audit/certificazione per motivi di sicurezza e integrità.

(6) Due o più Stati membri dovrebbero effettuare revisioni congiunte di sicurezza, utilizzando e condividendo le adeguate strutture e competenze tecniche relative alle infrastrutture alla base dell'ecosistema digitale e delle reti 5G, ad esempio quando la stessa impresa utilizza o costruisce un'infrastruttura di rete in più di uno Stato membro o laddove le configurazioni di rete siano molto simili. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA), Europol e l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) dovrebbero dare la priorità alle richieste di sostegno da parte degli Stati membri in questo settore. I risultati di tali revisioni dovrebbero essere trasmessi al gruppo di cooperazione e alla rete dei gruppi di intervento per la sicurezza informatica in caso di incidente.

IV. **AZIONE COORDINATA A LIVELLO DI UNIONE**

(7) Al fine di sviluppare un approccio comune per affrontare i rischi di cibersicurezza per quanto riguarda le reti 5G, gli Stati membri dovrebbero cominciare ad operare nell'ambito di un apposito flusso di lavoro nell'ambito del gruppo di cooperazione entro il 30 aprile 2019. Gli Stati membri dovrebbero invitare le autorità competenti a partecipare, se del caso, ai lavori del gruppo di cooperazione.

Valutazione dei rischi coordinata a livello europeo

(8) Gli Stati membri dovrebbero scambiarsi informazioni sia tra di essi sia con gli organismi pertinenti dell'Unione al fine di sviluppare una consapevolezza comune dei rischi di cibersicurezza esistenti e potenziali associati alle reti 5G.

(9) Gli Stati membri dovrebbero trasmettere le valutazioni nazionali dei rischi alla Commissione e all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) entro il 15 luglio 2019.

(10) L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrebbe completare una mappatura specifica del panorama delle minacce per le reti 5G. Il gruppo di cooperazione e la rete di gruppi di intervento per la sicurezza informatica in caso di incidente, istituiti a norma della direttiva (UE) 2016/1148, dovrebbero sostenere questo processo.

(11) Tenendo conto di tutti questi elementi, ed entro il 1º ottobre 2019, gli Stati membri, con il sostegno della Commissione e insieme all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), dovrebbero completare una revisione congiunta dell'esposizione a livello di Unione ai rischi relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare delle reti 5G.

(12) Tale revisione congiunta dovrebbe dare la priorità a un'analisi dei rischi applicabile agli elementi particolarmente sensibili o vulnerabili inclusi negli elementi fondamentali delle reti 5G, ai centri di gestione e manutenzione, nonché agli elementi della rete di accesso 5G utilizzati per le applicazioni industriali.

(13) In una seconda fase, tale revisione congiunta dovrebbe essere estesa ad altri elementi strategici della catena del valore digitale.

Un insieme di strumenti comuni a livello di Unione per affrontare i rischi

(14) I lavori del gruppo di cooperazione dovrebbero individuare le migliori pratiche applicate a livello nazionale del tipo previsto al punto 4. Sulla base di tali migliori pratiche nazionali, entro il 31 dicembre 2019 dovrebbe essere concordato un insieme di possibili misure di gestione dei rischi adeguate, efficaci e proporzionate al fine di attenuare i rischi di cibersicurezza individuati a livello nazionale e di Unione, che orienterà la Commissione nello sviluppo di requisiti minimi comuni a ulteriore garanzia di un elevato livello di cibersicurezza delle reti 5G in tutta l'Unione.

(15) Tale insieme di strumenti dovrebbe comprendere:

a) un inventario dei tipi di rischi di sicurezza che possono incidere sulla cibersicurezza delle reti 5G (ad esempio rischio relativo alla catena di approvvigionamento, rischio di vulnerabilità del software, rischio relativo al controllo degli accessi, rischi derivanti dal quadro giuridico e politico cui possono essere soggetti i fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione in paesi terzi); e

b) una serie di possibili misure di attenuazione (ad esempio, certificazione da parte di terzi per hardware, software o servizi, prove o controlli di conformità ufficiali per hardware e software, processi volti a garantire l'esistenza e l'applicazione del controllo degli accessi e che identifichino prodotti, servizi o fornitori considerati potenzialmente non sicuri ecc.). Tali misure dovrebbero riguardare tutti i tipi di rischi di sicurezza individuati in uno o più Stati membri in seguito alla valutazione dei rischi.

(16) Una volta sviluppati i sistemi europei di certificazione della cibersicurezza pertinenti per le reti 5G, gli Stati membri dovrebbero adottare, in conformità al diritto dell'Unione, regolamenti tecnici nazionali che prevedano la certificazione obbligatoria dei prodotti, dei servizi o dei sistemi delle tecnologie dell'informazione e della comunicazione contemplati da tali sistemi.

(17) Gli Stati membri, insieme alla Commissione, dovrebbero individuare le condizioni riguardanti la sicurezza delle reti pubbliche contro l'accesso non autorizzato alle quali vincolare l'autorizzazione generale, e i requisiti di sicurezza delle reti al fine di chiedere alle imprese che parteciperanno alle prossime procedure per la concessione di diritti d'uso dello spettro nelle bande 5G di assumersi impegni a norma della direttiva 2002/20/CE. Questi ultimi dovrebbero riflettersi, ove possibile, nelle misure di cui al punto 4, lettera c).

(18) Gli Stati membri dovrebbero cooperare con la Commissione al fine di sviluppare requisiti di sicurezza specifici che potrebbero applicarsi nel contesto degli appalti pubblici relativi alle reti 5G. Tali requisiti dovrebbero includere requisiti obbligatori per l'attuazione di sistemi di certificazione della cibersicurezza negli appalti pubblici, nella misura in cui tali sistemi non sono ancora vincolanti per tutti i fornitori e gli operatori.

V. **RIESAME**

(19) Gli Stati membri dovrebbero cooperare con la Commissione per valutare gli effetti della presente raccomandazione entro il 1º ottobre 2020, al fine di determinare modi opportuni di procedere. Tale valutazione dovrebbe tenere conto dei risultati della valutazione dei rischi coordinata a livello di Unione e dell'insieme di strumenti dell'Unione.

Fatto a Strasburgo, il 26 marzo 2019

Per la Commissione
Julian KING
Membro della Commissione