EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Numero di notifica : 2023/0761/ES (Spain)

REGIO DECRETO CHE APPROVA IL REGIME DI SICUREZZA NAZIONALE PER LE RETI E I SERVIZI 5G

Data di ricezione : 29/12/2023
Termine dello status quo : 02/04/2024 (closed)

Message

Messaggio 001

Comunicazione della Commissione - TRIS/(2023) 3739

Direttiva (UE) 2015/1535

Notifica: 2023/0761/ES

Notifica di un progetto di testo da parte di uno Stato membro

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta' dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.IT

1. MSG 001 IND 2023 0761 ES IT 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Telecomunicazioni

5. REGIO DECRETO CHE APPROVA IL REGIME DI SICUREZZA NAZIONALE PER LE RETI E I SERVIZI 5G

6. Reti e servizi di comunicazione elettronica 5G

Apparecchiature di telecomunicazione.

7.

8. Il regolamento consiste in una parte esplicativa, un articolo unico che approva l'ENS5G (regime di sicurezza nazionale per il 5G), due disposizioni aggiuntive e quattro disposizioni finali.
L'ENS5G da approvare è composto da 33 articoli suddivisi in otto capitoli e tre allegati.
La relazione illustra i motivi alla base dell'adozione del regolamento e degli articoli del regio decreto-legge che sono in fase di elaborazione.
L'articolo unico approva il regime di sicurezza nazionale per le reti e i servizi 5G.
La prima disposizione aggiuntiva prevede che il governo, mediante regio decreto, su proposta del ministero della Trasformazione digitale, a seguito di una relazione del Consiglio di sicurezza nazionale, riveda il regime di sicurezza nazionale per le reti e i servizi 5G quando le circostanze lo richiedono e, in ogni caso, ogni quattro anni.
La seconda disposizione aggiuntiva stabilisce che il regio decreto-legge 7/2022, del 29 marzo 2022, e l'ENS5G si applicano alle generazioni di comunicazioni elettroniche dopo la quinta generazione, mentre non vi è alcuna regolamentazione specifica per queste ultime.
La prima disposizione finale relativa al titolo di competenza stabilisce che il regio decreto e il regime da esso approvato sono emanati ai sensi dell'articolo 149, paragrafo 1, punto 21, e dell'articolo 149, paragrafo 1, punto 29, della Costituzione spagnola, che conferiscono allo Stato, rispettivamente, una competenza esclusiva in materia di sistema generale delle telecomunicazioni e in materia di pubblica sicurezza.
La seconda disposizione finale dichiara che la legge 11/2022 del 28 giugno 2022 sulle telecomunicazioni generali e i relativi regolamenti di esecuzione sono di applicazione complementare, e stabilisce che il regio decreto-legge 12/2018, del 7 settembre 2018, sulla sicurezza delle reti e dei sistemi informativi e la legge 8/2011, del 28 aprile 2011, che istituisce misure per la protezione delle infrastrutture critiche, nonché i rispettivi regolamenti di esecuzione, sono di applicazione supplementare per tutte le questioni non disciplinate da detta normativa.
La terza disposizione finale sullo sviluppo normativo consente al responsabile del ministero della Trasformazione digitale di sviluppare le disposizioni del presente regio decreto e del regime da esso approvato, e di modificare per mezzo di ordinanza i contenuti degli allegati in funzione dell'evoluzione del progresso tecnologico, dell'approvazione di nuovi standard tecnici e sistemi di certificazione per le apparecchiature di telecomunicazione e i prodotti connessi, nonché dello sviluppo di diverse configurazioni e parametri tecnici delle reti e dei servizi 5G e delle future generazioni di comunicazioni elettroniche.
La quarta disposizione finale prevede che il regolamento entri in vigore il giorno successivo alla pubblicazione nella "Gazzetta ufficiale dello Stato".
Per quanto riguarda il contenuto dell'ENS5G approvato:
l'articolo 1 stabilisce che il regolamento è emanato in attuazione del regio decreto legge 7/2022 del 29 marzo 2022, in particolare in applicazione del capo IV.
L'articolo 2 fa riferimento agli obiettivi del regolamento, che sono già stati analizzati.
L'articolo 3 stabilisce che si utilizzano le definizioni di cui al regio decreto-legge 7/2022, del 29 marzo 2022, alla legge 11/2022 del 28 giugno 2022 sulle telecomunicazioni generali e al codice europeo delle comunicazioni elettroniche.
L'articolo 4 stabilisce che il regolamento si applica agli operatori 5G, ai fornitori 5G e agli utenti aziendali 5G che hanno il diritto di utilizzare il dominio radio pubblico per installare, dispiegare o gestire una rete privata 5G o per fornire servizi 5G per scopi professionali o di autofornitura.
L'articolo 5 individua gli elementi, le infrastrutture e le risorse minimi che costituiscono una rete di comunicazione elettronica 5G, facendo riferimento all'allegato I per la loro descrizione dettagliata. Definisce inoltre gli elementi critici di una rete 5G, che deve essere ubicata, di norma, nel territorio nazionale (comprese eventuali eccezioni).
L'articolo 6 fa riferimento al trattamento globale della sicurezza in conformità della legislazione internazionale, comunitaria e nazionale approvata o che può essere approvata, imponendo alle parti obbligate di effettuare, mediante un metodo olistico, un'analisi delle vulnerabilità, delle minacce e dei rischi che li riguardano in quanto agenti economici e delle varie componenti, nonché una gestione adeguata e completa di tali rischi mediante l'uso di tecniche e misure appropriate per conseguire la loro mitigazione o eliminazione e conseguire l'obiettivo finale di un uso e un funzionamento sicuri di reti e servizi 5G.

L'articolo 7 sottolinea che l'analisi e la gestione dei rischi sono una parte essenziale del processo di sicurezza e dovrebbero costituire un'attività continua e costantemente aggiornata.
L'articolo 8 si riferisce al monitoraggio continuo e alla rivalutazione periodica.
L'articolo 9 stabilisce che l'analisi dei rischi a livello nazionale figura nell'allegato II ed è stata effettuata tenendo conto di vari elementi quali le informazioni raccolte presso le parti obbligate, l'esame delle vulnerabilità legate alla catena di approvvigionamento delle reti e dei servizi 5G, la valutazione del grado di dipendenza dei fornitori, il rischio di interruzione dell'approvvigionamento a causa di circostanze economiche, societarie o commerciali che incidono sui fornitori o la valutazione dell'efficacia delle misure di sicurezza applicate.
L'articolo 10 sulla gestione del rischio a livello nazionale stabilisce che i criteri, i requisiti, le condizioni e i termini per le parti obbligate al fine di progettare e attuare tecniche e misure di attenuazione del rischio sono quelli stabiliti nell'allegato III.
L'articolo 11 elabora le disposizioni dell'articolo 14 del regio decreto legge 7/2022 del 29 marzo 2022 per quanto riguarda la procedura e gli aspetti che devono essere valutati dal Consiglio dei ministri per la classificazione dei fornitori come ad alto rischio e gli elementi da prendere in considerazione al momento di ordinare l'eventuale sostituzione delle apparecchiature, dei prodotti e dei servizi forniti da tali fornitori. Allo stesso modo, in conformità con le disposizioni del citato regio decreto legge, si precisa che i fornitori ad alto rischio le cui apparecchiature di telecomunicazione, hardware, software o servizi accessori sono utilizzati unicamente ed esclusivamente nelle reti private 5G o per la fornitura di servizi 5G nell'ambito dell'autofornitura sono classificati come fornitori a medio rischio.
L'articolo 12 relativo alla determinazione dei luoghi in cui non possono essere installate apparecchiature di fornitori classificati come ad alto rischio stabilisce che il Consiglio di sicurezza nazionale, a seguito di una relazione del ministero della Trasformazione digitale, può determinare i luoghi, le aree e i centri in cui non possono essere installate attrezzature di fornitori classificati come ad alto rischio. Per l'installazione, la modifica o l'adattamento di stazioni radio che forniscono la copertura a tali luoghi, aree e centri, gli operatori 5G devono richiedere l'autorizzazione al ministero della Trasformazione digitale.
L'articolo 13 impone agli operatori 5G di elaborare una strategia di diversificazione della catena di approvvigionamento e di disporre di apparecchiature di trasmissione nella rete di accesso fornite da almeno due fornitori diversi. Esso prevede inoltre criteri che devono essere presi in considerazione dal Consiglio dei ministri per decidere se sia possibile mantenere un unico fornitore qualora il numero di fornitori sia ridotto a seguito di fusioni. Inoltre stabilisce le ipotesi e la procedura con cui il ministero della Trasformazione digitale può modificare la strategia di diversificazione della catena di approvvigionamento di un operatore 5G.
L'articolo 14 si concentra sull'analisi dei rischi che gli operatori 5G devono effettuare in relazione a tutti gli elementi, le infrastrutture e le risorse della rete di cui all'allegato I, elenca i fattori da prendere in considerazione e obbliga gli operatori a raccogliere dai loro fornitori le pratiche e le misure di sicurezza adottate nei prodotti e servizi che hanno fornito loro e a includere una priorità e una gerarchia dei rischi in base a determinati parametri che sono anch'essi elencati. Gli operatori 5G devono presentare un'analisi dei rischi entro il 1º ottobre 2024 e successivamente ogni due anni.
L'articolo 15 sull'analisi dei rischi da parte dei fornitori 5G richiede l'analisi dei rischi delle apparecchiature di telecomunicazione, dell'hardware e del software e dei servizi accessori connessi al funzionamento o alla gestione delle reti 5G o alla fornitura di servizi 5G, nonché la fornitura di tali analisi al ministero su richiesta. Nel caso di fornitori classificati come ad alto rischio o a rischio medio, l'analisi è presentata entro sei mesi a decorrere da tale classificazione e successivamente ogni due anni.
L'articolo 16 sull'analisi dei rischi da parte degli utenti aziendali 5G prevede che l'analisi del rischio sia fornita al ministero della Trasformazione digitale, quando tali utenti sono tenuti a farlo.
L'articolo 17 consente al ministero della Trasformazione digitale di raccogliere dalle parti obbligate le informazioni necessarie per l'analisi dei rischi e classifica la mancata comunicazione di tali informazioni entro 15 giorni lavorativi come infrazione grave. Le informazioni sono considerate riservate e non possono essere utilizzate per scopi diversi dall'adempimento degli obiettivi e degli obblighi stabiliti nel regio decreto-legge 7/2022, del 29 marzo 2022, nell'ENS5G e negli atti emanati in attuazione di entrambe le disposizioni.
L'articolo 18 enuncia il dovere generale di tutte le parti obbligate di gestire i rischi per la sicurezza.
L'articolo 19 si concentra sulla gestione della sicurezza da parte degli operatori 5G, sull'obbligo di elencare tutti gli operatori (ad esempio l'adozione di piani e misure di emergenza, il rispetto delle norme europee o delle specifiche tecniche e i sistemi di certificazione, il fatto di sottoporsi a un audit di sicurezza a proprie spese o di imporre ai propri

fornitori di rispettare le norme di sicurezza) e sugli obblighi aggiuntivi per gli operatori che possiedono o gestiscono elementi critici di una rete pubblica 5G (come i divieti sull'uso di apparecchiature provenienti da fornitori ad alto rischio in elementi di rete critici o in determinati luoghi, aree e centri). Gli operatori 5G devono presentare al ministero della Trasformazione digitale una descrizione delle misure tecniche e organizzative concepite e attuate per gestire e mitigare i rischi entro il 1º ottobre 2024 e successivamente ogni due anni. Inoltre gli operatori 5G che possiedono o gestiscono elementi critici di una rete pubblica 5G devono presentare al ministero della Trasformazione digitale una strategia di diversificazione della catena di approvvigionamento entro il 1º ottobre 2024 e successivamente ogni volta che ciò è soggetto a modifiche. Le informazioni sullo stato di attuazione di tale strategia devono essere presentate entro il 1º ottobre di ogni anno.
L'articolo 20 sulla gestione della sicurezza da parte dei fornitori 5G contiene un elenco di obblighi, tra cui lo svolgimento di un audit di sicurezza delle loro apparecchiature, prodotti e servizi, la fornitura di informazioni su eventuali interferenze da parte di terzi nella progettazione, il funzionamento e la gestione delle loro attrezzature, prodotti e servizi, e la collaborazione con gli operatori 5G e gli utenti aziendali 5G fornendo informazioni e certificando la conformità alle norme e alle certificazioni. I fornitori 5G devono redigere una relazione sulle misure tecniche e organizzative progettate e attuate per gestire e mitigare i rischi e fornire tale relazione al ministero su richiesta. Nel caso di fornitori classificati come ad alto rischio o a rischio medio, la relazione è presentata entro sei mesi a decorrere da tale classificazione e successivamente ogni due anni.
L'articolo 21 sulla gestione della sicurezza da parte degli utenti aziendali 5G stabilisce che questi ultimi non possono utilizzare negli elementi critici di rete apparecchiature di telecomunicazione, sistemi di trasmissione, apparecchiature di commutazione o instradamento e altre risorse, che consentono il trasporto di segnali, hardware, software o servizi accessori da fornitori classificati come rischio medio. Inoltre gli utenti devono fornire al ministero della Trasformazione digitale, su richiesta, una descrizione delle misure tecniche e organizzative progettate e attuate per gestire e mitigare i rischi.
L'articolo 22 sulla gestione della sicurezza da parte delle pubbliche amministrazioni stabilisce che, per motivi di sicurezza nazionale, nell'installazione, nel dispiegamento e nella gestione di reti 5G, pubbliche o private, o nella fornitura di servizi 5G, disponibili al pubblico o per l'autofornitura, le amministrazioni pubbliche non possono utilizzare apparecchiature, prodotti e servizi forniti da fornitori ad alto rischio o a medio rischio.
L'articolo 23 stabilisce che, nel rispetto degli obblighi previsti dai precedenti articoli, le parti obbligate tengono conto e applicano quanto stabilito dal regio decreto-legge 7/2022, del 29 marzo 2022, dall'ENS5G e dagli atti emanati in attuazione di entrambe le disposizioni.
L'articolo 24 consente al ministero della Trasformazione digitale di raccogliere dalle parti obbligate le informazioni necessarie per la gestione del rischio e classifica la mancata comunicazione di tali informazioni entro 15 giorni lavorativi come infrazione grave. Le informazioni sono considerate riservate e non possono essere utilizzate per scopi diversi dall'adempimento degli obiettivi e degli obblighi stabiliti nel regio decreto-legge 7/2022, del 29 marzo 2022, nell'ENS5G e negli atti emanati in attuazione di entrambe le disposizioni.
L'articolo 25 stabilisce che tutte le parti obbligate, nonché le amministrazioni pubbliche, i fabbricanti, gli importatori, i distributori e coloro che immettono sul mercato e vendono apparecchiature terminali e dispositivi per connettersi a una rete 5G e per essere in grado di fornire servizi 5G, devono cooperare e trasmettere le informazioni necessarie per la modifica e l'attuazione dell'ENS5G.
L'articolo 26 stabilisce che, per mezzo di ordinanza del capo del ministero della Trasformazione digitale, l'uso di un'apparecchiatura, di un sistema, di un programma o di un servizio specifico può essere subordinato alla previa certificazione ai sensi del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sulla cibersicurezza, o nell’ambito di regimi di certificazione e norme tecniche per la certificazione di apparecchiature e prodotti 5G chE possono essere approvati a livello europeo o internazionale.
L'articolo 27 stabilisce che il regolamento si applica fatte salve le normative in materia di investimenti esteri e concorrenza.
L'articolo 28 relativo alle apparecchiature terminali stabilisce che la fabbricazione, l'importazione, la distribuzione, l'immissione sul mercato e la vendita di apparecchiature terminali e dispositivi per connettersi a una rete 5G e per essere in grado di fornire servizi 5G sono subordinati al rispetto dei requisiti di sicurezza per i prodotti digitali e dei requisiti essenziali applicabili in materia di cibersicurezza, adottati conformemente alla legislazione europea, in particolare per quanto riguarda la protezione dei dati personali, la vita privata e la protezione contro le frodi.
L'articolo 29 fa riferimento alla cooperazione internazionale che deve essere sviluppata dal ministero della

Trasformazione digitale, in particolare a livello dell'Unione europea.
L'articolo 30 fa riferimento alla competenza del ministero della Trasformazione digitale per l'attuazione dell'ENS5G. Il ministero dovrebbe coordinarsi con gli altri organismi responsabili della cibersicurezza e delle infrastrutture critiche per garantire un'attuazione coerente dell'ENS5G.
L'articolo 31 suddivide i poteri di attuazione dell'ENS5G che corrispondono al ministero della Trasformazione digitale, tra cui, ad esempio, lo sviluppo, la specificazione e i dettagli del contenuto dell'ENS5G, lo svolgimento di audit per verificare e controllare il rispetto degli obblighi imposti e la concessione di aiuti pubblici.
L'articolo 32 attribuisce al ministero della Trasformazione digitale tutti i poteri della funzione di ispezione.
L'articolo 33 sul sistema sanzionatorio fa riferimento alle disposizioni degli articoli 30 e 31 del regio decreto-legge 7/2022, del 29 marzo 2022.
L'allegato I descrive gli elementi, le infrastrutture e le risorse che costituiscono una rete 5G.
L'allegato II contiene l'analisi dei rischi a livello nazionale.
L'allegato III definisce la gestione del rischio a livello nazionale.

9. Le comunicazioni mobili di quinta generazione o 5G rappresentano un nuovo paradigma di comunicazione elettronica con un grande potenziale di trasformazione a beneficio della società e dell'economia, in quanto offrono la possibilità di incorporare nuove funzionalità che avranno un grande impatto, come il network computing, e consentono la creazione di reti virtuali, l'offerta di una bassa latenza e la fornitura di servizi dall'elevato valore aggiunto in settori quali la medicina, i trasporti e l'energia.
Pertanto, sia l'Unione europea che la Spagna stanno promuovendo il rapido dispiegamento delle reti 5G e l'attuazione di progetti che dimostrano la loro utilità per diversi settori attraverso la fornitura di servizi 5G.
Le reti e i servizi 5G hanno vantaggi di sicurezza comparativi rispetto alle generazioni precedenti. Tuttavia, essi presentano anche rischi specifici derivanti, ad esempio, dalla loro architettura di rete più complessa, aperta e disaggregata, dalla loro capacità di trasportare enormi volumi di informazioni e di consentire l'interazione simultanea di più persone e cose. La loro interconnessione con altre reti e la natura transnazionale di molte minacce hanno un impatto sulla loro sicurezza, e il prevedibile uso diffuso di tali reti per funzioni economiche e sociali essenziali aumenterà l'impatto potenziale degli incidenti di sicurezza subiti.
Questi nuovi rischi specifici per la sicurezza delle comunicazioni mobili 5G sono stati affrontati in termini normativi con il regio decreto-legge 7/2022, del 29 marzo 2022, sui requisiti per garantire la sicurezza delle reti e dei servizi di comunicazione elettronica di quinta generazione, che integra pienamente la raccomandazione (UE) 2019/534 della Commissione europea, del 26 marzo 2019, sulla cibersicurezza delle reti 5G, nonché le raccomandazioni che la comunicazione della Commissione europea del 29 gennaio 2020 sul dispiegamento sicuro del 5G nell'UE - Attuazione del pacchetto di strumenti dell'UE (COM/2020/50 final) ha fornito agli Stati membri per quanto riguarda l'uso di tale pacchetto di strumenti.
Il regio decreto-legge 7/2022, del 29 marzo 2022, prevede il suo sviluppo normativo attraverso il regime di sicurezza nazionale per le reti e i servizi 5G (ENS5G).
Ai sensi dell'articolo 5, paragrafo 3, del suddetto regio decreto legge, l'ENS5G effettua un trattamento globale della sicurezza delle reti e dei servizi 5G, tenendo conto dei contributi alla portata di ciascun agente della catena del valore 5G, nonché dei regolamenti, delle raccomandazioni e degli standard tecnici dell'Unione europea, dell'Unione internazionale delle telecomunicazioni (ITU) e di altre organizzazioni internazionali, al fine di garantire l'obiettivo finale dell'uso e del funzionamento sicuri delle reti e dei servizi 5G in Spagna.
Da parte sua, l'articolo 20 del regio decreto legge stabilisce che, al fine di garantire il funzionamento continuo e sicuro della rete e dei servizi 5G, l'ENS5G effettua un'analisi dei rischi a livello nazionale sulla sicurezza delle reti e dei servizi 5G e individua, specifica e sviluppa misure per attenuare e gestire i rischi analizzati.
Infine, ai sensi dell'articolo 21 del regio decreto legge, l'ENS5G è approvato dal governo, con regio decreto, su proposta del ministero della Trasformazione digitale, a seguito di una relazione del Consiglio di sicurezza nazionale.
Il presente regolamento approva l'ENS5G, sviluppando le disposizioni del regio decreto legge 7/2022, del 29 marzo 2022, sui requisiti per garantire la sicurezza delle reti e dei servizi di comunicazione elettronica di quinta generazione.

10. Riferimenti ai testi di base:

11. No

12.

13. No

14. No

15. Sì

16.
Aspetto OTC: No

Aspetto SPS: No

****
Commissione europea
Punto di contatto Direttiva (UE) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu