Il Presidente del Consiglio dei Ministri

VISTA la legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri;

VISTO il decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56 e successive modificazioni ed integrazioni, recante norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni;

VISTO il decreto del Presidente della Repubblica 19 febbraio 2014, n. 35, recante l'individuazione delle procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale a norma dell'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

VISTO il decreto del Presidente del Consiglio dei Ministri 6 agosto 2014, che disciplina l'attività di coordinamento della Presidenza del Consiglio dei ministri per lo svolgimento delle attività propedeutiche all'esercizio dei poteri speciali, ai sensi del decreto del Presidente della Repubblica 19 febbraio 2014, n. 35 e del decreto del Presidente della Repubblica 25 marzo 2014, n. 86;

VISTO il decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva;

VISTO il decreto del Ministro dello sviluppo economico 12 dicembre 2018 recante "Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi", pubblicato sulla Gazzetta Ufficiale, Serie Generale n. 17 del 21 gennaio 2019;

VISTO il decreto-legge 25 marzo 2019, n. 22, convertito, con modificazioni, dalla legge 20 maggio 2019, n. 41, che ha inserito, nel decreto-legge 15 marzo 2012, n. 21, l'articolo 1-*bis* in materia di "Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G";

VISTO il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

VISTO il decreto-legge 8 aprile 2020, n. 23, convertito, con modificazioni, dalla legge 5 giugno 2020, n. 40, recante misure urgenti, tra l'altro, in materia di poteri speciali nei settori strategici e, in particolare, l'articolo 16 che modifica l'articolo 1-*bis* del decreto legge 15 marzo 2012, n. 21;

VISTO il decreto del Presidente del Consiglio dei ministri 30 settembre 2019, con il quale è stato istituito il Comitato di monitoraggio per la verifica dell'ottemperanza alle prescrizioni imposte ai sensi dell'articolo 1-*bis* del decreto legge 15 marzo 2012, n. 21, in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G;

VISTA la nota del 21 maggio 2020 con la quale la società Telecom Italia S.p.a. ha notificato, ai sensi dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, la stipula con la società Huawei Technologies Italia S.r.l., in data 13 maggio 2020, di quattro contratti per l'acquisto di apparati di accesso radio, la loro manutenzione, la fornitura di licenze e di supporto specialistico alla rete mobile;

Il Presidente del Consiglio dei Ministri

VISTA la nota del Dipartimento per il coordinamento amministrativo del 25 maggio 2020, con la quale la notifica è stata trasmessa alle Amministrazioni componenti il Gruppo di coordinamento, ai sensi dell'articolo 5 del decreto del Presidente del Consiglio dei ministri 6 agosto 2014,

VISTA la nota del Dipartimento per il coordinamento amministrativo del 19 giugno 2020, con la quale, a seguito delle riunioni del Gruppo di coordinamento dell'11 e del 18 giugno 2020, è stato comunicato alla società notificante l'individuazione del Ministero dello sviluppo economico quale Amministrazione responsabile dell'istruttoria e dell'eventuale proposta per l'esercizio dei poteri speciali e, contestualmente, al fine di svolgere ulteriori approfondimenti tecnici, è stata disposta la proroga di 20 giorni del termine di conclusione del procedimento;

VISTA la nota del 26 giugno 2020 con la quale la società Telecom Italia S.p.a. è stata convocata in audizione al fine di acquisire ulteriori elementi informativi e chiarimenti sull'operazione oggetto di notifica;

VISTA la nota del 7 luglio 2020 con la quale la società Telecom Italia S.p.a. ha trasmesso documentazione integrativa,

VISTE le note del Dipartimento per il coordinamento amministrativo del 20 luglio 2020 con le quali, a seguito della riunione del Gruppo di coordinamento del 16 luglio 2020, è stato comunicato, ai sensi dell'articolo 1-*bis*, comma 3-*bis*, del decreto-legge 15 marzo 2012, n. 21, alla Società notificante e alle Amministrazioni componenti il Gruppo di coordinamento, la proroga di 20 giorni del termine di conclusione del procedimento al fine di svolgere ulteriori approfondimenti riguardanti aspetti tecnici relativi alla valutazione di possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano;

RILEVATO che Telecom Italia S.p.a. è un'azienda italiana di telecomunicazioni, che offre in Italia e all'estero servizi di telefonia fissa, mobile, pubblica e IP, nonché Internet e televisione via cavo;

RILEVATO che Huawei Technologies Italia S.r.l. è una società controllata dal gruppo Huawei Technologies Co. (di diritto cinese), impegnata nello sviluppo, produzione e commercializzazione di prodotti, di sistemi e di soluzioni di rete e telecomunicazioni;

VISTA la nota del 31 luglio 2020 con la quale la società Telecom Italia S.p.a. ha comunicato di mantenere la società Nokia S.p.a. quale proprio fornitore dei nodi di rete nella regione Friuli-Venezia Giulia;

TENUTO CONTO che il Gruppo di coordinamento, nella riunione del 4 agosto 2020, ha preso atto della citata nota della società Telecom Italia S.p.a. del 31 luglio 2020;

VISTA la relazione istruttoria del 31 luglio 2020, con la quale il Ministero dello sviluppo economico, a seguito della riunione del Gruppo di coordinamento del 28 luglio 2020, ha proposto di esercitare i poteri speciali nella forma di imposizione di specifiche prescrizioni all'operazione, ai sensi dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, al fine di ridurre a livelli accettabili il rischio derivante dall'utilizzo dei componenti oggetto di notifica, secondo modalità che possono avere rilevanza per il sistema di difesa e sicurezza nazionale;

TENUTO CONTO che, come evidenziato nella citata istruttoria, per far sì che l'operatore di telecomunicazioni sostenga gli oneri derivanti dalle prescrizioni nei soli casi in cui sussistano effettivi rischi per il sistema di difesa e sicurezza nazionale è necessario che lo stesso svolga un

ruolo attivo nell'individuazione dei predetti casi, utilizzando a tal fine tutte le informazioni e conoscenze rilevanti in suo possesso;

CONSIDERATO che, per i componenti oggetto di notifica, i casi in cui sussistano effettivi rischi per il sistema di difesa e sicurezza nazionale possono variare durante il ciclo di vita dei componenti stessi;

RITENUTO necessario attivare un processo di monitoraggio delle eventuali variazioni rispetto a quanto già dichiarato dalla Società notificante;

RITENUTO di condividere le risultanze della citata relazione istruttoria;

RITENUTO necessario, al fine di garantire una corretta gestione della sicurezza nei processi rilevanti ai fini del decreto-legge 15 marzo 2012, n. 21, esercitare i poteri speciali ai sensi dell'articolo 1-*bis* del citato decreto e dell'articolo 6, comma 3, del decreto del Presidente della Repubblica 19 febbraio 2014, n. 35, mediante l'imposizione di specifiche prescrizioni;

VISTA la conforme deliberazione del Consiglio dei ministri adottata nella riunione del 7 agosto 2020, sulla proposta del Ministero dello sviluppo economico;

DECRETA

ART. 1

(PRESCRIZIONI)

1. Ai sensi e per gli effetti dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, si dispone l'imposizione delle seguenti specifiche prescrizioni nei confronti di Telecom Italia S.p.a.:

a) coinvolgere la funzione aziendale Security nei processi di *governance*, con particolare riferimento a tutti i processi decisionali afferenti ad attività ritenute rilevanti ex art. 1-*bis* del decreto-legge 15 marzo 2012, n. 21;

b) comunicare tempestivamente al Comitato di monitoraggio aggiornamenti circa il numero di utenti serviti dai componenti oggetto di notifica;

c) eseguire una nuova notifica:

   1) nel caso in cui mutino le caratteristiche delle componenti oggetto di notifica, a seguito di modifiche strutturali (sia in termini architetturali e di interconnessione tra i sistemi, che di aggiornamenti *software*) e a livello di configurazione che, secondo le valutazioni del rischio condotte dall'operatore, siano rilevanti rispetto all'ambito di applicazione dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21;

   2) allorquando verrà individuata l'esatta collocazione geografica di tali componenti, comunicando le coordinate geografiche e le altre informazioni necessarie per delimitarne la portata (quali frequenze utilizzate, *azimuth*, raggio, ecc.) e fornendo una trasposizione su carta geografica comprensiva delle coperture spaziali offerte dai singoli nodi;

d) avvalendosi della funzione aziendale Security, eseguire la progettazione e gestione della sicurezza relativa a componenti 5G tenendo conto delle indicazioni fornite dal 5G *Infrastructure Public Private Partnership* (5G PPP, Progetto 5G-Ensure);

e) fornire evidenza delle modalità seguite nella selezione dei fornitori, sulla base di precisi indicatori di qualità, che ne consentano la valutazione del livello di sicurezza intrinseco ai processi di produzione, di *delivery* e di gestione del ciclo di vita dei prodotti (*Supply Chain Security*). Le predette valutazioni possono essere effettuate dal notificante anche sulla base di documentazione, acquisita presso il fornitore o rilasciata da enti di certificazione terzi rispetto ad esso, che attesti il rispetto di standard internazionali di qualità e sicurezza;

f) garantire adeguate misure di controllo dell'accesso ai sistemi di gestione della rete a tutti i livelli (accesso radio, trasporto e *Core Network*), adottando – fatti salvi documentati limiti tecnici delle piattaforme in uso o eventuali vincoli derivanti dal rispetto di specifiche di interoperabilità definite da soggetti di riferimento nel contesto 5G – sistemi di *Authentication, Authorization and Accounting* (AAA) centralizzati, meccanismi di autenticazione a due fattori, di cui uno preferibilmente biometrico, e soluzioni di *Privileged Access Management* (PAM);

g) integrare i contratti notificati con clausole che prevedano, a pena di risoluzione espressa ai sensi dell'articolo 1456 del codice civile, che la Società possa:

   1) effettuare, anche tramite terzi, processi di verifica e di controllo del codice sorgente e dei disegni *hardware* degli apparati;

   2) comunicare tempestivamente i relativi risultati al Comitato di monitoraggio;

   3) mettere a disposizione, ove richiesto, i suddetti codici sorgente e disegni *hardware* dei componenti oggetto di notifica al Comitato di monitoraggio, nonché mettere a disposizione supporto nella verifica della loro corrispondenza con le implementazioni dei componenti stessi;

h) integrare i contratti con clausole che prevedano, a pena di risoluzione espressa ai sensi dell'articolo 1456 del codice civile, che:

   1) i fornitori e la Società si obblighino a non comunicare ad autorità governative estere o, comunque, a terzi dati e informazioni comunque acquisiti in relazione all'operazione notificata, salvo preventivo assenso del Comitato di monitoraggio;

   2) i fornitori si obblighino a informare tempestivamente la Società notificante nei casi in cui sussistano ragionevoli indicazioni circa l'inadempimento all'obbligo di non comunicazione di cui al punto che precede ovvero nel caso in cui autorità governative estere o, comunque, terzi siano venuti a conoscenza di dati e informazioni comunque acquisiti in relazione all'operazione notificata;

i) comunicare al Comitato di monitoraggio qualsiasi informazione di cui siano venuti a conoscenza con riferimento agli obblighi derivanti dalle clausole contrattuali di cui alla lettera h);

j) avvalersi delle clausole risolutive espresse di cui alle lettere g) e h) in caso di inadempimento agli obblighi in esse descritti.

k) al fine di avviare un processo di diversificazione dei fornitori e promuovere in tal modo la resilienza complessiva delle infrastrutture di rete 5G, elaborare un piano di diversificazione

   1) "orizzontale", che valuti la sostenibilità di una strategia finalizzata all'impiego di soluzioni di produttori differenti all'interno delle diverse tipologie di componenti dell'infrastruttura di rete (accesso radio, trasporto e *Core Network*).

   2) "verticale", che valuti la sostenibilità di adottare soluzioni di fornitori diversi per gli strati *hardware*, di virtualizzazione e applicativo di ciascuna componente dell'infrastruttura di rete (accesso radio, trasporto e *Core Network*). Tale piano, redatto anche con riferimento alle misure stabilite nel *toolbox* UE del 29 gennaio 2020 (SM05 e SM06), dovrà essere inviato in occasione della trasmissione della relazione di ottemperanza al Comitato di monitoraggio;

l) istituire e mantenere aggiornato il registro del personale che detiene il ruolo di amministratore degli apparati notificati, da esibire, su richiesta, agli organi di controllo;

m) far eseguire a parte terza e competente, riconosciuta dal Comitato di monitoraggio, con frequenza almeno annuale, la valutazione delle vulnerabilità di sistemi oggetto di notifica. L'esito di tali *assessment* di sicurezza sarà partecipato al Comitato di monitoraggio in occasione delle comunicazioni periodiche dirette al predetto organismo;

n) effettuare test e verifiche di sicurezza con cadenza almeno semestrale sui dispositivi a protezione dei collegamenti *backhauling* (*security gateway* e simili), da effettuarsi in esito a valutazioni di rischio e in aderenza agli standard e alle *best practice* di riferimento, e segnalare al Comitato di monitoraggio eventuali criticità riscontrate;

o) condurre le attività di *Operation and Maintenance* sotto la supervisione della funzione aziendale Security, escludendo interventi da remoto di terze parti - anche tramite collegamento VPN - al di fuori del *Network Operation Center* (NOC) della società e prevedendo, per le procedure di aggiornamento, una fase di validazione dei pacchetti software propedeutica al loro rilascio sui sistemi in esercizio. Nei soli casi in cui, per far fronte a malfunzionamenti di carattere straordinario, che richiedano, in via inderogabile, un intervento da parte del fornitore, è ammesso, in via eccezionale, l'intervento da remoto, alle condizioni e con le modalità specificate nell'Allegato 1, che costituisce parte integrante del presente decreto.

ART. 2

(MONITORAGGIO DELLE PRESCRIZIONI IMPOSTE)

1. Il Comitato di cui al decreto del Presidente del Consiglio dei ministri 30 settembre 2019 cura il monitoraggio e la verifica del rispetto delle prescrizioni imposte con il presente decreto, ai sensi dell'articolo 7 del decreto del Presidente della Repubblica 19 febbraio 2014, n. 35.

2. Telecom Italia S.p.a. è tenuta a inviare alla Presidenza del Consiglio dei ministri, entro il termine di 60 (sessanta) giorni dalla data del presente decreto e, successivamente, con cadenza semestrale, una relazione con la quale sono comunicate le misure adottate ai fini del rispetto delle prescrizioni di cui all'articolo 1 e, comunque, a comunicare tempestivamente al Comitato di monitoraggio di cui al comma 1, qualsiasi determinazione societaria o aziendale rilevante in relazione alle predette prescrizioni.

Il Presidente del Consiglio dei Ministri

3. Il Comitato:

a) verifica, sulla base della relazione prevista dall'articolo 2, comma 2, l'ottemperanza alle prescrizioni imposte con il presente decreto;

b) può richiedere, anche direttamente all'impresa, ogni altra informazione, ivi inclusi dati e notizie, utili all'attività di monitoraggio ai sensi dell'articolo 7, comma 3, del decreto del Presidente della Repubblica 19 febbraio 2014, n. 35.

4. Il Comitato informa tempestivamente il Gruppo di coordinamento, di cui all'articolo 3 del decreto del Presidente del Consiglio dei ministri 6 agosto 2014, sugli esiti delle attività di monitoraggio, anche al fine di valutare, in caso di violazione delle prescrizioni di cui all'articolo 1, la revoca del presente decreto ovvero l'esercizio di ulteriori poteri speciali tra quelli previsti dall'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21.

ART. 3

(SANZIONI)

1. In caso di inadempimento o violazione delle prescrizioni imposte dal presente decreto si applicano le disposizioni di cui all'articolo 1 del decreto-legge 15 marzo 2012, n. 21.

Ai sensi degli articoli 1 e 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito dalla legge 11 maggio 2012, n. 56, ed ai sensi dell'articolo 3, comma 1, lett. *a)*, della legge 14 gennaio 1994, n. 20, il presente decreto è inviato ai competenti organi di controllo.

Roma, 7 agosto 2020

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

IL MINISTRO DELLO SVILUPPO ECONOMICO

ALLEGATO 1

Accesso da remoto per assistenza tecnica di terzo livello

(Condizioni e misure di sicurezza)

Fermo restando il principio generale per cui gli interventi da remoto da parte di terzi non sono permessi al di fuori del NOC, si può derogare a tale prescrizione esclusivamente alle seguenti condizioni:

1) l'intervento da remoto è l'unica via percorribile, in tempi compatibili con i livelli di servizio che il notificante è tenuto a garantire ai propri clienti, per la risoluzione di problemi tecnici che richiedano un intervento del fornitore di carattere straordinario, urgente e non pianificabile, ossia quelli che siano trattabili esclusivamente dai centri di ricerca e sviluppo di prodotto del fornitore;

2) prima di consentire l'accesso a personale del fornitore in sede extra-europea, il notificante deve verificare se l'intervento da remoto può essere eseguito da personale del fornitore presente presso sedi nazionali o, in second'ordine, europee;

3) l'accesso da remoto deve prevedere almeno un doppio livello di autenticazione:

   a) il primo, mediante autenticazione a due fattori, per consentire l'accesso a un concentratore VPN;

   b) il secondo, mediante credenziali per l'accesso al sistema oggetto d'intervento;

4) le credenziali per l'autenticazione devono avere validità temporanea ridotta al minimo indispensabile e comunque non superiore alle 12 ore;

5) le *policy* di autorizzazione devono consentire accesso limitato ai soli componenti oggetto di intervento;

6) l'accesso da remoto deve essere monitorato tramite piattaforme di *Privileged Access Management* (PAM), con tracciamento puntuale delle operazioni svolte, con registrazione dei comandi eseguiti, degli *output* ricevuti e/o registrazione video della sessione remota, inclusi gli eventuali dati scaricati dai sistemi o in essi caricati, compresi eventuali aggiornamenti *software*;

7) l'effettuazione di ciascun accesso remoto deve trarre origine da una richiesta di supporto di carattere straordinario e urgente, adeguatamente motivata ed autorizzata da soggetto appartenente ad un'unità organizzativa differente da quella richiedente (preferibilmente con l'intervento della funzione aziendale Security), e registrata in un sistema di *ticketing*. Dall'esame del sistema di *ticketing* deve essere possibile ricostruire a posteriori l'intero processo di *escalation*, comprensivo delle attivazioni dei livelli di supporto intermedi. In caso di necessità, più accessi remoti potranno essere associati alla medesima richiesta di supporto straordinario e urgente;

8) l'intervento da remoto deve essere supervisionato in tempo reale da un dipendente del notificante in grado di comprendere le attività effettuate e di interrompere la connessione remota in qualunque momento.

9) ciascun accesso remoto deve essere rendicontato in un apposito registro, in formato digitale, in cui vanno riportate almeno le seguenti informazioni:

   a) [EXT_NAME] Generalità del soggetto che interviene da remoto
   b) [EXT_COMP+ Società di appartenenza dell'operatore remoto
   c) [TS_START] Data e ora di inizio attività
   d) [TS_STOP] Data e ora di fine attività
   e) [SYS] Sistema oggetto di intervento
   f) [VPN_SRC_IP] Indirizzo IP utilizzato dal soggetto operante da remoto per stabilire il tunnel VPN
   g) [USR_1LIV] Username impiegato sul primo livello di autenticazione (VPN)
   h) [USR_2LIV] Username impiegato sul secondo livello di autenticazione
   i) [DESCR] Sommaria descrizione delle attività svolte
   j) [LOGREF] Riferimento utile a reperire le informazioni di tracciamento registrate durante l'accesso da remoto
   k) [SUPERV+ Generalità del dipendente del notificante che supervisiona l'attività eseguita da remoto
   l) [TICKET ID+ Riferimento al ticket aperto per l'intervento di carattere straordinario e urgente
   m) [APPR_BY] Generalità del funzionario o dirigente del notificante che ha autorizzato l'intervento
   n) [REPORT] Denominazione del report descrittivo dell'intervento, di cui al punto 11), lett. b)
   o) [HASH REPORT] Hash (SHA-256) del report di cui al punto precedente;

10) i dati registrati dal concentratore VPN di cui al punto 3) e dal sistema PAM di cui al punto 6), i *log* del sistema di *ticketing* di cui al punto 7) e quelli del registro digitale degli accessi da remoto di cui al punto 9) devono possedere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richiesti; i predetti dati ed informazioni di tracciamento devono essere conservati per almeno 12 mesi e messi a disposizione, su richiesta, degli Organi di controllo;

11) ogni 3 mesi il notificante invia al Comitato di monitoraggio un estratto del predetto registro contenente:

   a) i record degli interventi di carattere straordinario e urgente eseguiti nel trimestre di riferimento, secondo il tracciato identificato al punto 9);
   b) un report descrittivo di ciascun intervento di carattere straordinario e urgente richiesto e di quelli autorizzati, debitamente sottoscritto dal responsabile della funzione incaricata del rilascio delle autorizzazioni, che

attesti la correttezza e la completezza di quanto dichiarato nonché la sussistenza di tutte le condizioni previste per l'attivazione dell'accesso remoto. Il report deve contenere anche le informazioni relative alle fasi iniziali del processo (interventi di primo e secondo livello).

c) un'attestazione da parte della funzione Security aziendale circa la completezza della documentazione trasmessa in merito agli accessi da remoto richiesti ed autorizzati;

d) Tale report periodico dovrà essere firmato digitalmente e inviato per Posta Elettronica Certificata al Comitato di monitoraggio. In ragione della potenziale delicatezza delle informazioni ivi presenti, potranno essere concordate modalità di invio sicuro di tale documentazione (ad es., mediante l'impiego di meccanismi di cifratura dei contenuti).