RAPPORTO

Alla luce del nuovo ecosistema di sicurezza e del Libro bianco dell'Unione europea sulle sovvenzioni dei paesi terzi, analisi dei rischi e delle minacce alle infrastrutture di comunicazione strategiche nazionali, europee e atlantiche derivanti dalla decisione del governo italiano di consentire alla società cinese Huawei di fornire componenti della rete 5G a Telecom Italia S.p.A.

Maurizio Mensi

Indice

Premessa

Oggetto della presente disamina sono le implicazioni relative alla circostanza che alla società cinese Huawei è stato consentito di fornire componenti tecnologici a Telecom Italia S.p.A. (di seguito TIM) destinati ad integrare la rete 5G di quest'ultima.

Ciò in conseguenza del decreto con cui la Presidenza del Consiglio dei Ministri (d.P.C.M) in data 7 agosto 2020, in esercizio dei poteri di *Golden Power* previsti dal decreto-legge 15 marzo 2012, n. 21, convertito in legge n. 56 del 2012[1], ha autorizzato l'operazione relativa all'acquisto di apparati di accesso radio, la loro manutenzione e la fornitura di licenze e di supporto specialistico alla rete mobile, subordinandola ad una serie di prescrizioni in capo a TIM, soggetto acquirente[2].

Il citato decreto non è stato pubblicato in Gazzetta Ufficiale, cosicché le osservazioni e le valutazioni che seguono si basano sul contenuto dello stesso riportato da alcuni organi di stampa.

1. LA DECISIONE TIM-HUAWEI

1.1. Principali aspetti

I soggetti coinvolti nell'operazione sono: Telecom Italia S.p.A., società italiana di telecomunicazioni che offre in Italia e all'estero servizi di telefonia fissa, mobile, pubblica, e IP, nonché internet e televisione via cavo, e Huawei Technologies Italia s.r.l., società controllata dal gruppo Huawei Technologies Co (di diritto cinese) impegnata nello sviluppo, produzione e commercializzazione di prodotti, sistemi e soluzioni di rete e telecomunicazioni.

La definizione di rete 5G si ricava dalla raccomandazione UE del 26 marzo 2019[3]. Si tratta dell'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

[1] L'articolo 1 bis del decreto legge 15 marzo 2012 n. 21 convertito, con modificazioni, dalla legge 11 maggio 2012 n. 56, qualifica tutti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, da chiunque forniti, come "*attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*" abilitando il governo a fare uso dei poteri previsti dalla disciplina sul *Golden Power* per fronteggiare i rischi di un uso improprio dei dati "*con implicazioni sulla sicurezza nazionale*".

[2] Ai fini della verifica in ordine alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico, il decreto-legge 15 marzo 2012, n. 21 prevede, in caso di minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale (articoli 1 e 1-bis), nonché per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti (articolo 2), la facoltà per il Governo di esercitare con apposito d.P.C.M. i poteri speciali previsti dalla norma (potere di veto, opposizione all'acquisto, imposizione di prescrizioni). Il provvedimento prevede, in caso di imposizione di specifiche prescrizioni e condizioni, che sia effettuata un'attività di monitoraggio, che può essere svolta dall'amministrazione competente per materia o da un Comitato di monitoraggio appositamente costituito. Il d.P.C.M. dispone infine l'applicazione di sanzioni amministrative pecuniarie in caso di inottemperanza alle prescrizioni e condizioni imposte.

[3] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, Cybersicurezza delle reti 5G, in GU L 88 del 29 marzo 2019.

mobili e senza fili, come il 4G o il 3G. Le reti 5G[4] dovrebbero essere intese in modo da includere tutte le parti pertinenti della rete.

In sostanza, la decisione adottata con d.P.C.M. in seguito alla notifica[5] effettuata da TIM ai sensi della legge 11 maggio 2012 n. 56, all'esito dell'istruttoria svolta dal Ministero dello sviluppo economico, consente al fornitore cinese di integrare propri apparati nella rete 5G del principale operatore di telecomunicazioni italiano, al quale sono imposte una serie di prescrizioni. La gestione di tale articolato sistema è affidata allo stesso operatore, con un ruolo rilevante in capo alla sua funzione *Security,* preposta a compiti di progettazione e gestione della sicurezza oltre alla vigilanza sulle attività di *operation and maintenance*.

La verifica demandata a TIM è di tipo dinamico; il che comporta che non solo debbono essere comunicati al Comitato di monitoraggio[6] gli aggiornamenti circa il numero di utenti serviti dai componenti oggetto della notifica, ma si rende necessaria una nuova notifica nel caso in cui mutino le caratteristiche dei componenti per effetto di modifiche strutturali o di configurazione.

Di qui la necessità di effettuare una costante e aggiornata valutazione del rischio.

La decisione impone inoltre la necessità di dimostrare che la procedura di selezione dei vari fornitori si sia svolta sulla base di precisi indicatori di qualità inerenti al livello di sicurezza più appropriato per i processi di produzione, di *delivery* e di gestione del ciclo di vita dei prodotti. Tale valutazione può essere effettuata da TIM anche sulla base della documentazione resa da fornitore o della certificazione di appositi enti, alla stregua degli standard internazionali di qualità e sicurezza.

Un elemento centrale è la diversificazione dei fornitori, sia di carattere "orizzontale", con soluzioni di produttori differenti all'interno delle diverse tipologie di componenti dell'infrastruttura di rete, sia "verticale", con fornitori diversi per gli strati *hardware*, di virtualizzazione e applicativo di ciascuna componente dell'infrastruttura di rete. Ciò dovrà costituire parte integrante della relazione che TIM è tenuta ad inviare al Comitato di monitoraggio al fine di dimostrare l'ottemperanza alle varie prescrizioni.

Una specifica previsione del d.P.C.M. impone ai fornitori e alle società di obbligarsi a non comunicare ad autorità governative estere o comunque a terzi dati e informazioni comunque acquisiti in relazione all'operazione notificata. Il riferimento sottinteso è alla previsione contenute nella legge sulla sicurezza nazionale cinese del 2016, che impone ai cittadini e alle società cinesi di collaborare con i servizi di sicurezza statale per raccogliere informazioni senza rivelare tale collaborazione. Prevede in particolare che: "*qualsiasi organizzazione e cittadino, in conformità alla legge, sostiene, fornisce assistenza, collabora con il lavoro*

[4] A fine maggio 2020, i servizi su rete 5G erano attivi in 12 Stati membri: Austria (3 operatori), Belgio (1), Finlandia (3), Germania (2), Ungheria (1), Irlanda (2), Italia (2), Lettonia (3), Paesi Bassi (1), Romania (3), Spagna (1) e Svezia (3).

[5] E' l'impresa che acquisisce i beni e servizi legati alla tecnologia 5G (in questo caso TIM), e non il contraente extra UE, a dover notificare la conclusione del contratto alla Presidenza del Consiglio dei ministri; le società che acquisiscono tali beni e servizi, infatti, oltre a fornire la descrizione degli elementi tecnici del contratto, possono altresì fornire informazioni sull'impatto che l'operazione notificata ha sulle attività strategiche dell'impresa stessa.

[6] Istituito con d.P.C.M. del 30 settembre 2019, il Comitato ha il compito di verificare l'ottemperanza delle misure adottate ai fini del rispetto delle prescrizioni imposte nei confronti di tutte le società notificanti in materia di tecnologia 5G. I suoi componenti sono designati con decreto del Segretario generale della Presidenza del Consiglio dei Ministri.

dell'intelligence nazionale e mantiene il segreto su qualsiasi operazione dell'intelligence nazionale di cui sia a conoscenza".

La decisione prevede che siano effettuati annualmente, ad opera di soggetti terzi, all'uopo incaricati, una valutazione delle vulnerabilità dei sistemi oggetti di notifica, il cui esito dovrà essere comunicato al comitato di monitoraggio, oltre ad una serie di test e verifiche di sicurezza semestrali sui dispositivi a protezione dei collegamenti *backhauling* (rete di accesso).

Una particolare enfasi è attribuita ai profili contrattuali. Il decreto impone infatti di integrare lo strumento negoziale (i vari contratti notificati) con clausole che prevedano espressamente la risoluzione in caso di inadempimento di una serie di specifici obblighi indicati nella decisione, ai sensi dell'articolo 1456[7] del codice civile.

1.2. Il suo contenuto

In dettaglio, ai sensi del citato d.P.C.M. è stato imposto a TIM di osservare le seguenti prescrizioni (contenute all'articolo 1):

a) coinvolgere la sua funzione aziendale *Security* nei processi di *governance*, con particolare riferimento a tutti i processi decisionali afferenti ad attività ritenute rilevanti ai sensi delle norme sul *Golden Power*;

b) circa il numero di utenti serviti dai componenti oggetto della notifica del contratto;

c) dovrà altresì eseguire una nuova notifica sia nel caso in cui mutino le caratteristiche delle componenti già oggetto di notifica, in seguito a modifiche strutturali (in termini di architettura e di interconnessione tra sistemi oltre che di aggiornamento *software*) e a livello di configurazione che secondo le valutazioni del rischio condotte dalla stessa TIM siano rilevanti rispetto all'ambito di applicazione dell'articolo 1 bis del decreto legge 15 marzo 2012 n. 2, sia nel caso in cui sia individuata l'esatta collazione geografica di tali componenti, comunicando le coordinate geografiche e le altre informazioni necessarie per delimitare la portata e fornendo una trasposizione su carta geografica comprensive delle coperture spaziali offerte dai singoli nodi;

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

e) fornire evidenza della 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. Le predette valutazioni possono essere effettuate da TIM anche sulla base di documentazione, acquisita presso il fornitore o rilasciata da enti di certificazione terzi rispetto a 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 adottando, fatti salvi documentati limiti tecnici delle piattaforme in uso, sistemi di *Authentication, Authorization and Accounting* centralizzati, meccanismi di autenticazione a

[7] Art. 1456. Clausola risolutiva espressa. "*I contraenti possono convenire espressamente che il contratto si risolva nel caso che una determinata obbligazione non sia adempiuta secondo le modalità stabilite. In questo caso, la risoluzione si verifica di diritto quando la parte interessata dichiara all'altra che intende valersi della clausola risolutiva".*

due fattori, di cui uno probabilmente 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 TIM possa effettuare anche tramite terzi processi di verifica e di controllo del codice sorgente e dei disegni *hardware* degli apparati, comunicare tempestivamente i relativi risultati al Comitato di monitoraggio, mettere a disposizione, ove richiesto, i suddetti codici sorgente e disegni *hardware* dei componenti oggetti di notifica al Comitato di monitoraggio, nonché mettere a disposizione supporto nella verifica della loro corrispondenza con le implementazioni dei componenti stessi;

h) integrare il contratto con clausole che prevedano, a pena di risoluzione espressa ai sensi dell'articolo 1456 del codice civile, che i fornitori e le 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 accesso al Comitato di monitoraggio. I fornitori devono altresì obbligarsi a informare tempestivamente TIM nei casi in cui sussistano ragionevoli indicazioni circa l'inadempimento all'obbligo di non comunicazione ad autorità governative estere o comunque a terzi o 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 predette clausole contrattuali;

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 "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 e "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. Tale piano, redatto anche con riferimento alle misure stabilite nel *Toolbox* Ue del 29 gennaio 2020 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 appalti 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 oggetti di notifica. L'esito di tali *assessment* di sicurezza dovrà essere comunicato al comitato di monitoraggio in occasione delle comunicazioni periodiche dirette al predetto organismo;

n) effettuare test e verifica di sicurezza con cadenza almeno semestrale sui dispositivi a protezione dei collegamenti *backhauling*, da effettuarsi in esito di valutazioni di rischio e in aderenza agli standard e alle *best practices* di riferimento, e segnalare a comitato di monitoraggio eventuali criticità riscontrate;

o) condurre le attività di *operation and maintenance* sotto la supervisione della funzione aziendale *Security*, escludendo interventi da remoti di terze parti - anche tramite collegamento WPN - 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 funzionamenti 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 decreto.

Il comitato di cui al decreto del Presidente del Consiglio dei Ministri 30 settembre 2019 ha il compito di curare il monitoraggio e la verifica del rispetto delle prescrizioni imposte con il presente decreto, ex articolo 7 del decreto del Presidente della Repubblica 19 febbraio 2014, n. 35 (così prevede l'articolo 2 della decisione in esame).

TIM è tenuta a inviare alla Presidenza del Consiglio dei Ministri entro il termine di 60 giorni dalla data del decreto in esame e successivamente, con cadenza semestrale, una relazione con la quale sono comunicate le misure adottate ai fini del rispetto delle prescrizioni previste e comunque a comunicare tempestivamente al citato comitato di monitoraggio qualsiasi determinazione societaria o aziendale rilevante in relazione alle predette prescrizioni.

A sua volta il comitato deve verificare, sulla base della relazione inviata da TIM l'ottemperanza alle prescrizioni imposte con il decreto e 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.

Il comitato è altresì tenuto a informare 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 alle 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.

Il decreto prevede anche delle sanzioni (articolo 3) in caso di inadempimento o violazione delle prescrizioni imposte dallo stesso In tal caso si applicano le disposizioni di cui all'articolo 1 del decreto legge 15 marzo 2012, n. 21.

1.3. La Relazione al Parlamento in tema di poteri speciali

Come emerge dalla Relazione al Parlamento "*concernente l'attività svolta sulla base dei 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*" comunicata alla Presidenza del Consiglio dei Ministri il 22 giugno 2020, con riferimento alle reti di telecomunicazione elettronica a banda larga con tecnologia 5G (ex art. 1-bis del d. l. n. 21 del 2012), nel corso del 2019 sono state effettuate complessivamente n. 14 notifiche. Tutti i procedimenti avviati si sono conclusi con la imposizione di specifiche prescrizioni (nessuno si è tradotto in un divieto) e in cinque casi (indicati qui di seguito) l'accordo oggetto dell'istruttoria ha riguardato società cinesi.

A. WIND TRE S.p.A.
   Oggetto: accordi aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G.
   La società Wind Tre S.p.A. ha inviato un'informativa relativa ad accordi stipulati dalla società notificante con la società cinese Huawei, aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G. Nello specifico, il contratto consente di acquistare da Huawei

apparecchiature e servizi per lo sviluppo della rete di trasporto ottica e IP di collegamento fra la rete di accesso e la rete core.
Con d.P.C.M. 5 settembre 2019 sono stati esercitati i poteri speciali nella forma di imposizione di specifiche prescrizioni.

B. FASTWEB S.p.A.
Oggetto: acquisto dalla società ZTE Corporation degli apparati relativi alle componenti radio per la realizzazione dell'ultima tratta della rete 5G FWA.
La notifica della società Fastweb S.p.a. riguarda l'acquisto dalla società ZTE Corporation degli apparati relativi alle componenti radio per la realizzazione dell'ultima tratta della rete 5G FWA (*Fixed Wireless Access*), in particolare: il servizio di progettazione della rete radio, l'acquisto e la configurazione delle antenne trasmittenti che saranno dislocate sul territorio, il servizio di manutenzione delle stesse e il *tool* di supervisione della componente radio, allo scopo di monitorare performance ed affidabilità della rete.
Con d.P.C.M. 5 settembre 2019 sono stati esercitati i poteri speciali nella forma di imposizione di prescrizioni.

C. WIND TRE S.p.A.
Oggetto: accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G con le società ZTE Italia S.r.l. e ZTE Corporation.
L'operazione notificata da Wind Tre S.p.a. è inerente all'acquisto dalle società ZTE Italia S.r.l. e ZTE Corporation (di seguito "ZTE Italia" e "ZTE Corp.") di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti la tecnologia 5G.
Con d.P.C.M. 10 ottobre 2019 sono stati esercitati i poteri speciali nella forma di imposizione di specifiche prescrizioni.

D. GO INTERNET S.p.A.
Oggetto: Contratto di acquisto di n. 200 unità di "Ran Equipment" prodotti e forniti da ZTE Corporation.
La società Go Internet S.p.a. ha notificato l'informativa riguardante la sottoscrizione di un accordo di acquisto di 200 unità di "Ran Equipment" prodotti e forniti da ZTE, ossia di materiali e di componenti hardware, oltre che dei loro rispettivi software.
Con d.P.C.M. 15 ottobre 2019 sono state imposte prescrizioni all'impresa notificante.

E. FASTWEB S.p.A.
Oggetto: acquisto di apparati di accesso radio per la realizzazione dell'ultima tratta della rete 5G FWA e di CPE 5G Huawei, da collegare a una core network Ericsson.
Con d.P.C.M. 5 marzo 2020 sono state imposte prescrizioni all'impresa notificante.

2. INQUADRAMENTO GIURIDICO

2.1. Il *Golden Power*

Come rilevato, l'articolo 1 bis del decreto legge n. 22/2019[8] del 25 marzo 2019, convertito in legge n. 41/2019, base giuridica della decisione, qualifica tutti i servizi di comunicazione

[8] Decreto-legge 25 marzo 2019, n. 22, Misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea, convertito con modificazioni dalla legge 20 maggio 2019, n. 41, in G.U. 24 maggio 2019, n. 120.

elettronica a banda larga basati sulla tecnologia 5G, da chiunque forniti, come "*attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*"[9]. Alla luce di tale previsione il governo è abilitato a utilizzare i poteri previsti dalla disciplina sul *Golden Power* per fronteggiare i rischi di un uso improprio dei dati "*con implicazioni sulla sicurezza nazionale*"[10].

In concreto, l'impresa che stipula, a qualsiasi titolo, contratti o accordi aventi ad oggetto l'acquisizione di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti relative ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, ovvero acquisisca, a qualsiasi titolo, componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea, deve pertanto presentare una notifica ai sensi della normativa sul *Golden Power*[11]. Così è avvenuto nel caso in esame, con il d.P.C.M. del 7 agosto 2020.

---

[9] L'articolo 1-bis ha lo scopo di garantire la protezione delle reti e dei servizi di comunicazione elettronica a banda larga, basati sulla tecnologia 5G, dai rischi derivanti dal coinvolgimento in tali attività di imprese con sede in Stati non facenti parte dell'Unione europea.

[10] Il novellato decreto-legge prevede dunque poteri molto incisivi in ambito di tecnologia 5G, in linea con la raccomandazione (UE) 2019/534 del 26 marzo 2019, adottata dalla Commissione europea, avente ad oggetto la "Cybersicurezza" delle reti 5G. Tale raccomandazione ha evidenziato che "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 e stanno studiando misure per affrontare tali rischi" (considerato 18).

[11] Quella relativa al *Golden Power* è una disciplina che è stata oggetto di diverse revisioni nel corso degli anni. Fino a qualche anno fa lo Stato aveva la possibilità di opporsi all'acquisizione di partecipazione rilevanti di qualsiasi tipo, anche intra-UE, per mezzo di apposite previsioni inserite negli statuti delle principali società di diritto italiano, ai sensi del decreto legge n. 332/1994, convertito in legge n. 474/1994, relativo alle società controllate direttamente o indirettamente dallo Stato operanti nei settori di difesa, trasporti, telecomunicazioni, fonti di energia e negli altri pubblici servizi. Il decreto-legge 31 maggio 1994, n. 332, recante norme per l'accelerazione delle procedure di dismissione di partecipazioni dello Stato e degli enti pubblici in società per azioni, convertito, con modificazioni, dalla legge 30 luglio 1994, n. 474: stabiliva che "*Tra le società controllate direttamente o indirettamente dallo Stato operanti nel settore della difesa, dei trasporti, delle telecomunicazioni, delle fonti di energia, e degli altri pubblici servizi, sono individuate con decreto del Presidente del Consiglio dei ministri* […] *quelle nei cui statuti, prima di ogni atto che determini la perdita del controllo, deve essere introdotta con deliberazione dell'assemblea straordinaria una clausola che attribuisca al Ministro dell'economia e delle finanze la titolarità di uno o più dei seguenti poteri speciali da esercitare di intesa con il Ministro delle attività produttive* […]".
Era la cosiddetta *Golden Share*, che abilitava il governo a facoltà di dettare specifiche condizioni all'acquisito di partecipazioni, porre il veto all'adozione di determinate delibere societarie e opporsi all'acquisto di partecipazioni, entrata nel mirino di Bruxelles a causa della sua contrarietà al diritto europeo. Tale normativa - come di seguito evidenziato - è stata successivamente modificata con il decreto legge 15 marzo 2012, n. 21, convertito in legge n. 56/2012, con cui il legislatore nazionale ha ridisegnato l'istituto trasformandolo in *Golden Power*. Con il decreto legge n. 21/2012 il legislatore ha recepito le censure sollevate dalla Commissione europea e aderito alle sue indicazioni, determinando il 15 febbraio 201 l'archiviazione della procedura di infrazione da parte della Commissione europea, che ha ritenuto la nuova disciplina italiana compatibile con il Trattato sul funzionamento dell'Unione europea.
La disciplina relativa ai poteri speciali del Governo non riguarda peraltro solo il nostro paese e si ricollega infatti agli istituti della *Golden Share* inglese e dell'*Action spécifique* francese*,* oggetto di censure sollevate dalla Commissione europea e di una pronuncia di condanna da parte della Corte di giustizia UE. La disciplina della *Golden share* è stata oggetto della procedura d'infrazione n. 2009/2255, in quanto ritenuta lesiva della libertà di stabilimento e della libertà di circolazione dei capitali garantite dal trattato sul funzionamento dell'Unione europea. Nell'ambito di tale procedura di infrazione, la Commissione europea, il 24 novembre 2012, aveva deciso di deferire il governo italiano alla Corte, ex articolo 258 TFUE. La Commissione europea aveva infatti rilevato che l'esercizio di tali poteri dovesse essere effettuato senza discriminazioni e ammesso qualora si

Come rilevato, alla stregua di tale previsione innovativa è stato esteso al 5G l'ombrello protettivo del *Golden Power,* che non si applica più soltanto ai mutamenti proprietari (come avveniva in precedenza) bensì anche a questioni eminentemente operative, come per esempio l'acquisto di apparati per accendere la rete 5G. vengono infatti ricompresi nell'ambito oggettivo di applicazione diverse fattispecie legate alla nuova tecnologia, come gli appalti e le forniture commerciali di beni o servizi relativi alla progettazione, realizzazione, manutenzione e gestione delle reti.

E' confermata l'applicabilità dei veti normativi ai soggetti extra-UE e viene fornita una definizione ampia di "*soggetto esterno all'Unione europea*" in chiave anti elusiva. Ciò avviene ad opera del comma 3 del citato articolo 1-bis e riguarda, oltre alle persone fisiche e giuridiche stabilite fuori dello spazio economico europeo (soggetti esterni in senso stretto), quelle in esso stabilite ma controllate direttamente o indirettamente da soggetti esterni, nonché quelle che siano stabilite in Europa al fine di eludere l'applicazione della disciplina in argomento.

E' prevista la valutazione del Comitato interministeriale incardinato presso la Presidenza del Consiglio di tutte le acquisizioni di componenti ad alta intensità tecnologica funzionali alla realizzazione o alla gestione del 5G. Sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano.

2.2. La legge n. 56 del 2012

E' il decreto-legge 15 marzo 2012, n. 21, convertito con legge 11 maggio 2012, n. 56, a definire l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio da parte del governo dei poteri speciali nei settori della difesa e della sicurezza nazionale, nonché di taluni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni[12].

In sostanza, ai sensi di tale previsione il governo ha la facoltà di porre il veto rispetto all'adozione di determinate delibere, atti e operazioni delle imprese che gestiscono attività strategiche in specifici settori, di dettare impegni e condizioni in caso di acquisito di partecipazioni in tali imprese, ovvero di opporsi all'acquisto delle medesime partecipazioni. Si tratta di un potere di intervento rilevante, che attiene alla *governance* di società operanti in settori considerati strategici e finalizzato alla tutela degli *asset* definiti di prioritaria importanza per il paese.

---

fondasse su "*criteri obiettivi, stabili e resi pubblici*" e giustificato da "*motivi imperiosi di interesse generale*". In tal senso, con la legge n. 56/2012 il legislatore nazionale, anche mediante il rinvio a fonti di rango secondario ha ridefinito l'istituto, in linea con quanto indicato nella comunicazione della Commissione del 19 luglio 1997, relativa ad alcuni aspetti giuridici attinenti agli investimenti intracomunitari (in GU n. C 220 del 19 luglio 1997). Con due provvedimenti, il d.P.R. 19 febbraio 2014, n. 35, in materia di poteri speciali nei settori della difesa e della sicurezza nazionale e il d.P.R. 25 marzo 2014, n. 86 che disciplina i poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni, sono stati definiti gli ambiti soggettivi e oggettivi di applicazione della norma primaria, così come la tipologia, le condizioni e le procedure per l'esercizio dei relativi poteri speciali. Proprio tale comunicazione conteneva quegli indirizzi in base ai quali era stata avviata la procedura di infrazione nei confronti del nostro Paese e che aveva ad oggetto le disposizioni della legge n. 474/1994. Peraltro, analoghe procedure di infrazione hanno riguardato anche il Belgio, Germania, Regno Unito, Portogallo, Francia e Spagna.

[12] A differenza della legge n. 474/1994, la nuova disciplina estende la possibilità di esercitare i poteri speciali nei confronti di tutte le società, pubbliche o private che svolgono attività considerate di rilevanza strategica e non più soltanto rispetto alle società privatizzate o in mano pubblica (art. 1).

L'impresa che opera nei settori in questione è tenuta a notificare alla Presidenza del Consiglio dei ministri un'informativa completa circa la delibera o l'atto da adottare ai fini dell'eventuale esercizio del potere di veto, la cui proposta è affidata al Ministero dello sviluppo economico. L'inosservanza degli obblighi di notifica o l'inadempimento di impegni e condizioni derivanti dall'esercizio dei poteri sono puniti con specifiche sanzioni amministrative pecuniarie.

Quest è ciò che è avvenuto nel caso in esame.

Alla disciplina di fonte secondaria (decreti del Presidente del Consiglio dei Ministri) è invece affidata la individuazione delle attività per le quali potranno essere attivati i poteri speciali, la individuazione della tipologia di atti o operazioni infragruppo esclusi dall'ambito operativo della nuova disciplina, il concreto esercizio dei poteri speciali e l'individuazione di ulteriori disposizioni attuative. Tali poteri riguardano i settori della difesa e della sicurezza nazionale nonché taluni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti, delle comunicazioni.

Con il d.P.R. n. 35/2014[13] per i settori della difesa e della sicurezza nazionale ed il d.P.R. n. 86/2014 per i settori di energia, trasporti e comunicazioni sono stati definiti gli ambiti soggettivi e oggettivi di applicazione della legge n. 56/2012, così come la tipologia, le condizioni e le procedure per l'esercizio dei relativi poteri speciali.

Con il d.P.C.M. 6 agosto 2014 sono state delineate le attività di coordinamento della Presidenza del Consiglio dei Ministri finalizzate all'esercizio dei poteri speciali, con un Gruppo di coordinamento interministeriale del quale fanno parte rappresentanti della Presidenza e componenti designati dai ministeri interessati. Il Dipartimento per il coordinamento amministrativo è l'ufficio responsabile delle attività di coordinamento, delle attività propedeutiche all'esercizio dei poteri speciali e delle relative attività istruttorie.

Gli obblighi di notifica sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa nazionale ed europea di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti e per l'operatività dei servizi pubblici essenziali. Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Per le violazioni è prevista la sanzione della nullità degli atti.

[13] In particolare il decreto del Presidente della Repubblica 19 febbraio 2014, n. 35, regolamento per 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 (in GU Serie Generale n.66 del 20 marzo 2014), ha stabilito le procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale, mentre con il d.P.C.M. 6 giugno 2014, n. 108, regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, a norma dell'articolo 1, comma 1, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56 (in GU Serie Generale n.176 del 31 luglio 2014), è stato adottato il regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Quest'ultimo comprende le norme che individuano le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, ivi incluse le attività strategiche chiave, di competenza sia del Ministero dell'interno sia del Ministero della difesa.

I due regolamenti citati sono entrati in vigore il 7 giugno 2014. Si tratta del d.P.R. 25 marzo 2014, n. 85[14], il regolamento per l'individuazione degli attivi di rilevanza strategica" e del già citato d.P.R. 25 marzo 2014, n. 86[15], relativo all'individuazione delle procedure per l'attivazione dei poteri speciali.

Con il decreto legge n. 148 del 2017[16] è stata modificata ed estesa la disciplina dell'esercizio dei poteri speciali del Governo con riferimento alla *governance* di società considerate strategiche, ampliando anche i settori ai quali i poteri speciali risultano applicabili. E' stata anche prevista la sanzione amministrativa pecuniaria ove siano violati gli obblighi di notifica e esteso l'esercizio dei poteri speciali applicabili nei settori dell'energia, dei trasporti e delle comunicazioni anche al settore della cosiddetta alta intensità tecnologica.

La normativa ha inoltre individuato il criterio a cui il governo deve attenersi nell'esercizio dei poteri speciali, con riferimento a quelle operazioni di acquisto da parte di soggetti extra UE di società che detengono attivi strategici nel settore energetico, dei trasporti e delle comunicazioni, ove l'acquisto di partecipazioni determini l'insediamento stabile dell'acquirente. In tali ipotesi il governo deve valutare, oltre alla minaccia di grave pregiudizio agli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, anche il pericolo per la sicurezza o per l'ordine pubblico[17].

L'articolo 3-bis del decreto-legge 15 marzo 2012, n. 21 prevede che il Presidente del Consiglio dei ministri trasmetta alle Camere una Relazione sull'attività svolta in materia di poteri speciali sugli assetti societari di rilevanza strategica nei settori della difesa e della sicurezza nazionale, della tecnologia 5G e dell'energia, dei trasporti e delle comunicazioni, sulla base dei poteri attribuiti e sui risultati conseguiti. La Relazione è stata trasmessa alle Camere il 22 giugno 2020 e riguarda l'attività svolta dal 1° gennaio 2019 al 31 dicembre 2019.

---

[14] Decreto del Presidente della Repubblica 25 marzo 2014, n. 85, Regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2, comma 1, del decreto-legge 15 marzo 2012, n. 21, in GU Serie Generale n.129 del 6 giugno 2014.

[15] Decreto del Presidente della Repubblica 25 marzo 2014, n. 86, Regolamento per l'individuazione delle procedure per l'attivazione dei poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2, comma 9, del decreto-legge 15 marzo 2012, n. 21, in GU Serie Generale n.129 del 6 giugno 2014.

[16] Decreto-legge 16 ottobre 2017, n. 148, Disposizioni urgenti in materia finanziaria e per esigenze indifferibili, convertito con modificazioni dalla L. 4 dicembre 2017, n. 172, in G.U. 5 dicembre 2017, n. 284.

[17] Oltre alla disciplina del *Golden Power*, altri interventi normativi hanno perseguito analoghi obiettivi di tutela delle società operanti in settori giudicati strategici per l'economia nazionale. In particolare, sono stati previsti diritti speciali in capo all'azionista pubblico nella disciplina codicistica delle società; a ciò si aggiunge la legge 23 dicembre 2005, n. 266 (legge finanziaria 2006), in GU Serie Generale n.302 del 29 dicembre 2005 - Suppl. Ordinario n. 211, che ha introdotto nell'ordinamento italiano la cd. *Poison pill* (pillola avvelenata) che consente, in caso di offerta pubblica di acquisto ostile riguardante società partecipate dalla mano pubblica, di deliberare un aumento di capitale, grazie al quale l'azionista pubblico potrebbe accrescere la propria quota di partecipazione vanificando il tentativo di scalata non concordata. Con il medesimo obiettivo di salvaguardare le società d'interesse nazionale, l'articolo 7 del decreto-legge 31 marzo 2011, n. 34, Disposizioni urgenti in favore della cultura, in materia di incroci tra settori della stampa e della televisione, di razionalizzazione dello spettro radioelettrico, di moratoria nucleare, di partecipazioni della Cassa depositi e prestiti, nonché per gli enti del Servizio sanitario nazionale della regione Abruzzo, convertito con modificazioni dalla L. 26 maggio 2011, n. 75 (in GU 27 maggio 2011, n. 122) ha autorizzato la Cassa Depositi e Prestiti ad assumere partecipazioni in società di rilevante interesse nazionale. In particolare, sono state definite "*di rilevante interesse nazionale*" le società di capitali operanti nei settori della difesa, della sicurezza, delle infrastrutture, dei trasporti, delle comunicazioni, dell'energia, delle assicurazioni e dell'intermediazione finanziaria, della ricerca e dell'innovazione ad alto contenuto tecnologico e dei pubblici servizi.

2.3. Aspetti procedurali. La notifica e il comitato di monitoraggio

In seguito alla conversione del decreto-legge 25 marzo 2019, n. 22, che ha esteso l'esercizio dei poteri speciali alle reti di telecomunicazione elettronica a banda larga con tecnologia 5G, diverse società operanti nel settore delle telecomunicazioni hanno proceduto ad effettuare notifiche ai sensi della normativa sul *Golden Power*. Le informative inviate hanno riguardato la sottoscrizione dei contratti e degli accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea.

Al fine di curare l'istruttoria delle predette notifiche ed in ragione della peculiarità della specifica materia trattata, è stato informalmente costituito un "tavolo tecnico" che ha affiancato il Gruppo di coordinamento durante le audizioni delle Società notificanti e ha altresì collaborato con l'amministrazione competente nella fase istruttoria del procedimento e nell'individuazione delle prescrizioni adottate[18].

Al termine dell'istruttoria è stato deciso di esercitare, nei confronti di dette società, i poteri speciali nella forma di imposizione di specifiche prescrizioni, al fine di ridurre a livelli accettabili il rischio relativo alle criticità associate all'utilizzo dei componenti oggetto di notifica secondo modalità che possono avere rilevanza per il sistema di difesa e sicurezza nazionale.

L'estrema tecnicità della materia trattata e la necessità di individuare gli eventuali elementi indicanti la presenza di fattori di vulnerabilità, che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, ha reso indispensabile l'attivazione di un processo di monitoraggio, la cui gestione è stata affidata ad un apposito Comitato, istituito con d.P.C.M. del 30 settembre 2019 e i cui componenti sono stati designati con decreto del Segretario generale della Presidenza del Consiglio dei ministri.

A differenza di quanto previsto per le società TIM e Vivendi con il d.P.C.M. del 16 ottobre 2017, il Comitato in materia di tecnologia a banda larga 5G è competente a verificare l'ottemperanza delle misure adottate ai fini del rispetto delle prescrizioni imposte nei confronti di tutte le società notificanti in materia di tecnologia 5G, anche successivamente alla data di costituzione del Comitato stesso.

Tale Comitato valuta altresì le determinazioni aziendali rilevanti relative alle prescrizioni imposte e può richiedere direttamente alle imprese ulteriori informazioni utili all'attività di monitoraggio. Possono inoltre essere chiamati, a supporto dei lavori del Comitato ed al fine di potenziarne le capacità di analisi, altri rappresentanti delle pubbliche amministrazioni, nonché di altre autorità o di soggetti pubblici competenti nella specifica materia.

Il citato Comitato è composto da un rappresentante della Presidenza del Consiglio dei ministri, in veste di coordinatore, coadiuvato dai rappresentanti dei Ministeri competenti per materia e da un membro del Dipartimento delle informazioni per la sicurezza.

2.4. La possibilità di intervenire sui contratti già conclusi

[18] Cfr. Relazione al Parlamento "*concernente l'attività svolta sulla base dei 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*" comunicata alla Presidenza del Consiglio dei Ministri il 22 giugno 2020.

Il decreto-legge 21 settembre 2019, n. 105[19], convertito in legge n. 133 del 2019 sul perimetro di sicurezza nazionale cibernetica[20] ha esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici, coordinandolo con l'attuazione del regolamento 2019/452 in materia di controllo degli investimenti esteri diretti[21].

In particolare l'articolo 3[22] raccorda le previsioni della legge sul perimetro di sicurezza nazionale cibernetica con quelle relative ai poteri speciali in tema di 5G. Si prevede che le norme della legge citata si applichino ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica anche per i contratti o gli accordi, ove conclusi con soggetti esterni all'Unione europea, relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

La legge prolunga da 15 a 45 giorni il termine, decorrente dalla notifica da parte dell'impresa della informativa dell'operazione di acquisto avviata nei confronti di aziende italiane, per l'esercizio dei poteri speciali da parte del governo.

L'articolo 4-bis ha invece esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori strategici, coordinandolo con l'attuazione del regolamento (UE) 2019/452 sul controllo degli investimenti esteri. Ha inoltre apportato, da un lato, significativi cambiamenti sulle procedure di esercizio dei poteri speciali; dall'altro, ha integrato la disciplina in tema di esercizio dei poteri speciali inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G. Tale previsione estende infatti il termine per l'esercizio dei poteri speciali da parte del Governo, con l'indicazione di

[19] Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, in G.U. 20 novembre 2019, n. 272.

[20] Ha l'obiettivo di assicurare la sicurezza di reti, sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza del paese. L'individuazione dei soggetti inclusi nel perimetro è demandata ad un decreto del Presidente del Consiglio dei Ministri, adottato su proposta del CISR. E' affidato ad un regolamento, da adottarsi entro 10 mesi dalla data di entrata in vigore della legge di conversione, la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici.

[21] Il decreto-legge 21 settembre 2019, n. 105 (convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019) ha istituito il c.d. "perimetro di sicurezza nazionale cibernetica", che prevede la predisposizione di sistemi volti a garantire il massimo livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche. Il citato decreto ha altresì apportato importanti modifiche alla normativa in materia di poteri speciali.

[22] Articolo 3, Disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5G. […] "3. *Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui all'articolo 1, comma 6, le condizioni e le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei ministri, adottati ai sensi dell'articolo 1 -bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, in data anteriore alla data di entrata in vigore del medesimo regolamento, qualora attinenti alle reti, ai sistemi informativi e ai servizi informatici inseriti negli elenchi di cui all'articolo 1, comma 2, lettera b) , del presente decreto, possono essere modificate o integrate, con la procedura di cui al comma 2, del presente articolo, se, a seguito della valutazione svolta da parte dei centri di valutazione di cui all'articolo 1, comma 6, lettera a) , emergono elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, con misure aggiuntive necessarie al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal presente decreto, anche prescrivendo la sostituzione di apparati o prodotti, ove indispensabile al fine di risolvere le vulnerabilità accertate"*.

ulteriori elementi informativi che devono essere resi dalle imprese detentrici degli asset strategici; viene ampliato l'oggetto di alcuni poteri speciali e sono modificati e integrati gli obblighi di notifica finalizzati all'esercizio dei poteri speciali.

Introduce poi una disciplina transitoria, con la possibilità di modificare o integrare con misure aggiuntive le condizioni e le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei ministri (e adottati sulla base della normativa sui poteri speciali in data anteriore alla data di entrata in vigore del medesimo regolamento), qualora attinenti alle reti, ai sistemi informativi e ai servizi informatici inseriti negli elenchi dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

Qualora infatti emergano, in seguito alle valutazioni svolte dai centri di valutazione previsti dalla stessa legge n. 133 del 2019, elementi che indicano fattori di vulnerabilità suscettibili di compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, possono essere disposte misure aggiuntive anche prescrivendo, qualora indispensabile al fine di risolvere le vulnerabilità accertate, la sostituzione di apparati e di prodotti[23].

Si tratta di una previsione importante, che consente al governo di intervenire con riferimento ai contratti già conclusi, addirittura ordinando alle imprese la sostituzione degli apparati e prodotti non sicuri. La possibilità di fare uso di tale strumento è tuttavia consentita solo qualora si tratti di misura indispensabile.

Tale ipotesi non è peraltro esclusa nel caso in esame. Ai sensi del d.P.C.M. del 7 agosto 2020, come rilevato, TIM è stata autorizzata a dare attuazione ai contratti di fornitura in questione con Huawei, condizionatamente al rispetto di alcune specifiche prescrizioni. Tuttavia nulla esclude che, in seguito all'accertamento di fattori di vulnerabilità, una volta esperiti infruttuosamente i rimedi previsti dalla stessa decisione, possano applicarsi le rigorose previsioni di cui all'articolo 3, comma 3, della legge n. 11/2019, con l'ordine di sostituzione dei prodotti non sicuri ed i relativi oneri a carico della società.

In sostanza, la disciplina dei poteri speciali relativa al 5G è stata leggermente rivista così da rendere il procedimento sostanzialmente simmetrico a quello previsto per i settori della difesa e della sicurezza nazionale: ridefinito il concetto di "soggetto esterno all'Unione europea", sono stati precisati i criteri per determinare se un investimento estero sia suscettibile di incidere sulla sicurezza o sull'ordine pubblico e sottoposta all'obbligo di notifica l'acquisizione a qualsiasi titolo (in luogo del solo acquisto) di beni o servizi relativi alle reti 5G, qualora posti in essere con soggetti esterni all'Unione europea. Sono state inoltre introdotte ulteriori circostanze che il Governo può tenere in considerazione per l'esercizio dei poteri speciali, nel caso in cui l'acquirente di partecipazioni rilevanti sia un soggetto esterno all'Unione europea.

2.5. Il *Golden Power* "allargato"

Risulta importante, anche per esigenza di completezza, evidenziare che l'obiettivo di proteggere il sistema economico nazionale indebolito dall'emergenza Covid-19 e tutelare i

[23] E' inoltre disciplinata l'ipotesi di intervento di emergenza in casi di rischio grave o di crisi di natura cibernetica. Si prevede infatti che il Presidente del Consiglio, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR), possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati. Entro 30 giorni, il Presidente del Consiglio è tenuto ad informare il Comitato parlamentare per la sicurezza della Repubblica delle misure disposte.

suoi *asset* pregiati ha indotto il governo a integrare, con l'art. 15 del decreto legge "Liquidità" n. 23 dell'8 aprile 2020[24], le norme vigenti in tema di *Golden Power*.

La previsione normativa, simile a quella adottata da Germania e Spagna, benché contenuta in un solo articolo, risulta tecnicamente complessa e articolata.

Raccogliendo le indicazioni del Copasir (Comitato parlamentare per la sicurezza della Repubblica) in data 25 marzo 2020 e sulla scia delle linee guida di cui alla raccomandazione della Commissione europea del 25 marzo 2019, il governo con tale intervento in sostanza ha anticipato la valutazione prevista dal regolamento europeo 2019/452 sul controllo degli investimenti esteri (applicabile dall'11 ottobre scorso), con la possibilità di adottare misure restrittive a protezione di sicurezza e ordine pubblico.

Allarga infatti l'ombrello protettivo del *Golden Power*, finora limitato a difesa e sicurezza nazionale, energia, trasporti e comunicazioni, ai settori riguardati dal citato regolamento europeo, attribuendo al governo un potere rilevante e dalle delicate implicazioni, ancorché per un periodo limitato (fino al 31 dicembre 2020).

Le disposizioni contenute nel decreto legge non incidono tuttavia sulla supervisione già assicurata al governo sul 5G in virtù della legge n. 41/2019 e della legge sul perimetro di sicurezza n. 133/2019. In tal senso i contratti e gli accordi relativi all'acquisizione di beni e servizi relativi alla progettazione, realizzazione, manutenzione e gestione della rete 5G continuano pertanto riguardati dalle citate previsioni normative; tuttavia le operazioni societarie relative al 5G possono rientrare nel raggio d'azione della nuova previsione.

Il tempo di risposta del comitato *Golden Power* è di 45 giorni, salvo le proroghe previste; per le operazioni relative alla rete 5G (i contratti e gli accordi citati) si applica invece il termine di 30 giorni.

Come rilevato, il decreto legge estende gli obblighi relativi al *Golden Power* a beni e rapporti nei settori riguardati dal regolamento europeo. Si applica pertanto alle infrastrutture critiche, siano esse fisiche o virtuali, tra cui l'energia, i trasporti, l'acqua, la salute, le comunicazioni, i media, il trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie, e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture, tecnologie critiche e prodotti a duplice uso, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cybersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie. Sono riguardati anche la sicurezza dell'approvvigionamento di fattori produttivi critici, tra cui l'energia e le materie prime, nonché la sicurezza alimentare, l'accesso a informazioni sensibili, compresi i dati personali, o la capacità di controllare tali informazioni, la libertà e pluralismo dei media. Tutti i settori citati assumono pertanto rilevanza strategica e in essi operano un vasto numero di società, ivi comprese molte PMI.

Le nuove norme sul *Golden Power* previste dal decreto legge si applicano ai soggetti UE solo nel caso in cui l'acquisto di partecipazione sia rilevante e determini l'insediamento stabile dell'acquirente in ragione dell'assunzione di controllo della società. È previsto invece l'obbligo di notifica, da parte di un soggetto esterno all'UE, di un acquisto di partecipazioni

24 Decreto-legge 8 aprile 2020, n. 23, Misure urgenti in materia di accesso al credito e di adempimenti fiscali per le imprese, di poteri speciali nei settori strategici, nonché interventi in materia di salute e lavoro, di proroga di termini amministrativi e processuali, in GU n. 94 dell'8 aprile 2020.

che attribuiscono una quota dei diritti di voto o di capitale superiore al 10% e il valore complessivo dell'investimento è pari o superiore a 1 milione di euro.

In base alle nuove disposizioni il governo ha la possibilità di intervenire d'ufficio anche senza notifica. Lo Stato si riserva infatti di intervenire d'ufficio qualora venga a conoscenza di operazioni poste in essere fino al 31 dicembre 2020, a prescindere dal fatto che la notifica sia avvenuta o meno. In tal caso si applica il termine di 45 giorni e l'eventuale decisione di divieto sarà adottata con decreto del Presidente del Consiglio dei Ministri. La Presidenza del Consiglio dei Ministri e la società non hanno l'obbligo di dare comunicazione al pubblico dell'operazione ai sensi del testo unico della finanza. E' peraltro previsto che in presenza di disposizioni specifiche inerenti ad altri settori, volte a garantire la tutela degli stessi interessi essenziali dello Stato perseguiti dalle norme sul *Golden Power*, si applichino le prime in quanto "*lex specialis*".

L'obbligo di notifica dell'acquisto di partecipazioni finanziarie in tutti i settori ivi riguardati si applica sino al momento in cui, con decreto, il Presidente del Consiglio dei Ministri indicherà i beni e i rapporti di rilevanza strategica per l'interesse nazionale ulteriori rispetto a quelli già individuati nei settori di difesa e sicurezza nazionale, energia, trasporti e comunicazioni. Tutte le altre misure previste, relative per esempio a delibere, atti o operazioni che modificano la titolarità, il controllo o la disponibilità degli attivi delle società, hanno invece come scadenza il 31 dicembre 2020, compreso il potere di intervento d'ufficio del governo.

2.6. La funzione *Security* di TIM

La decisione del 7 agosto 2020 affida alla funzione *Security* di TIM un importante ruolo nella gestione di varie attività inerenti alle prescrizioni oltre che per la vigilanza sulle attività di *operation and maintenance*.

Questo induce a richiamare alla memoria l'operazione di partecipazione della società Vivendi s.a. in TIM S.p.A. che nel 2017 che ha indotto il governo ad esercitare i poteri di *Golden power*.

In quel caso con d.P.C.M. del 16 ottobre 2017 sono state imposte specifiche prescrizioni e condizioni nei confronti sia di Vivendi sia di Telecom Italia, comprese le due controllate Sparkle S.p.A. e Telsy Elettronica e Telecomunicazioni S.p.A., in quanto società titolari delle attività di rilevanza strategica per la difesa e la sicurezza nazionale.

Tra le prescrizioni previste alcune hanno riguardato il mantenimento stabile sul territorio nazionale delle funzioni di gestione e sicurezza di reti, servizi e forniture che supportano attività "strategiche", altre sono volte a garantire la continuità delle funzioni connesse alle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale.

Sono state, inoltre, previste condizioni volte ad assicurare assetti organizzativi dedicati alle attività aziendali rilevanti per la sicurezza nazionale, prevedendone la piena autonomia sia sotto il profilo economico-finanziario sia di gestione del personale, attraverso l'assegnazione di una dotazione di risorse umane, finanziarie e strumentali idonee a garantirne l'indipendenza.

Di qui la creazione in Telecom Italia S.p.A. di una cosiddetta "organizzazione di sicurezza" (*Security*), ovvero una funzione aziendale autonoma e indipendente dal vertice societario, volta a garantire l'attuazione delle prescrizioni governative. Si tratta della stessa funzione a cui la decisione del 7 agosto 2020 affida gran parte della complessa e delicata serie di incombenze previste.

3. LA DIMENSIONE STRATEGICA E OPERATIVA

3.1. Sicurezza nazionale e sovranità europea

Le delicate implicazioni insite nella decisione del governo italiano del 7 agosto 2020 di consentire a Huawei di fornire componenti della rete 5G di TIM emergono solo se si consideri che le vulnerabilità della rete 5G potrebbero essere sfruttate per compromettere sistemi e infrastrutture vitali, con il rischio di danni devastanti, spionaggio o furti di dati su vasta scala. Questo è tanto più preoccupante se si considera che gli stessi processi democratici, così come le consultazioni elettorali, sono basati sempre più sulle infrastrutture digitali.

Pertanto garantire la cybersicurezza delle reti 5G è questione di importanza strategica per l'Unione europea, in una fase in cui gli attacchi informatici sono sempre più numerosi e sofisticati. Date la natura interconnessa e transnazionale delle infrastrutture che sono alla base dell'ecosistema digitale e il carattere transfrontaliero delle minacce, eventuali vulnerabilità o incidenti riguardanti le reti 5G che si verificano in uno Stato membro sono destinate a incidere sull'Unione nel suo complesso.

Sono in gioco, insomma, oltre alla sicurezza di sistemi e apparati tecnologici, la stessa sovranità europea a cui sono strettamente collegati quegli stessi "*valori di apertura e tolleranza*" che fanno parte del patrimonio culturale del vecchio continente. In tal senso la sicurezza delle reti 5G è essenziale per assicurare l'autonomia strategica dell'UE, come riconosciuto nella Comunicazione congiunta "*UE-Cina – Una prospettiva strategica*" del 12 marzo 2019[25].

Sicurezza nazionale, sovranità, autonomia strategica europea: sono infatti questi i concetti da qualche tempo al centro dello sforzo dispiegato da Stati nazionali e istituzioni europee.

In concreto, si tratta non solo di approntare adeguati strumenti di difesa rispetto all'aggressiva strategia posta in essere dal governo cinese e dalle sue principali imprese, Huawei e ZTE, sempre più presenti nel mercato europeo e con un ruolo crescente nello sviluppo della tecnologia e nel dispiegamento delle reti 5G[26], ma di verifificare se nel caso in esame, per esempio, essi siano stati correttamente utilizzati e utilizzabili. Peraltro le predette società cinesi hanno già partecipato con successo alle gare svolte e collaborano con quasi tutti i principali operatori di telecomunicazioni a livello nazionale ed europeo.

Occorre considerare che, dal punto di vista strategico, la contesa con la Cina, che ha nel 5G il suo punto focale, è stata qualificata nei termini di un vero e proprio "scontro di civiltà" dal Dipartimento di Stato USA (così J. Gehrke sul *Washington Examiner* il 30 aprile 2019). Si tratta in effetti di una competizione con una civiltà e un'ideologia molto diversa da quella con la quale sinora gli Stati Uniti si sono confrontati. Il regime di Pechino, a differenza del regime sovietico (e delle stesse teorie marxiste), non è figlio della filosofia e della cultura

[25] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio UE-Cina – Una prospettiva strategica, del 12 marzo 2019 JOIN(2019) 5 final

[26] Dopo una prima fase che ha visto la prevalenza degli Stati Uniti, da qualche anno sono cresciute in modo rilevante le aziende cinesi (Huawei, ZTE), che hanno oggi un ruolo rilevante nella tecnologia per la realizzazione delle reti 5G a livello internazionale. Huawei in particolare ha notevolmente potenziato la sua presenza commerciale nel nostro Paese ed oggi è uno dei principali attori per la realizzazione della rete 5G. Contrariamente a quanto avviene per le imprese occidentali, le aziende cinesi, pur formalmente indipendenti dal potere governativo, sono strettamente collegate alle istituzioni del loro Paese, anche in virtù di un peculiare contesto normativo.

occidentale. Ecco perché si è reso necessario ridefinire la strategia di sicurezza nazionale considerando che Russia e Cina che non sono equivalenti, in quanto quest'ultima rappresenta un concorrente non solo sul piano economico ma anche su quello ideologico e la contesa in corso è molto diversa dalla quella che ha guidato la strategia americana di contenimento dell'Unione sovietica durante la guerra fredda.

In tel senso la sfida principale per l'UE oggi è piuttosto di aggiornare e ridefinire il proprio quadro giuridico per consentire agli Stati membri di competere, dotarsi di un *governance* che valorizzi le competenze nazionali per costruire una sovranità europea basata su quella dei singoli paesi che abbia fra i suoi obiettivi e presupposti lo sviluppo e l'indipendenza tecnologica. In concreto questo significa, far leva sul suo già collaudato ed efficace assetto regolamentare e confermare il proprio impegno in sintonia con l'alleanza transatlantica e gli sforzi NATO[27].

Al riguardo finora la risposta più convincente è stata quella sul piano regolamentare, in particolare con due interventi normativi, a distanza di pochi giorni l'uno dall'altro. Si tratta *in primis* del regolamento (UE) 2019/452 del 19 marzo 2019 entrato in vigore il 10 aprile che istituisce un sistema di controllo degli investimenti diretti esteri in Europa, in aree e attività strategiche**,** per proteggere sicurezza e ordine pubblico. A ciò si aggiunge la raccomandazione (UE) 2019/534 del 26 marzo, che affronta il tema della sicurezza delle reti di quinta generazione (il 5G).

Integra tale quadro normativo anche il codice europeo delle comunicazioni elettroniche, di cui alla direttiva 1972 del 2018[28], il cui termine di trasposizione nei vari Stati membri scade il 21 dicembre 2020. Il suo Titolo V (gli articoli 40 e 41) è dedicato alla sicurezza, con poteri rilevanti affidati alle autorità competenti che al riguardo avranno la possibilità di impartire agli operatori istruzioni vincolanti e attivare in taluni casi un raccordo con i gruppi di intervento per la sicurezza informatica («CSIRT») ai sensi della direttiva NIS.

Certo, sono pur sempre gli Stati membri ad essere responsabili della sicurezza nazionale (lo stabilisce l'articolo 4, par. 2, TEU e ne fa cenno il considerato 16 del regolamento 2016/679), ma l'Unione europea ritiene, a ragione, di dover dispiegare un intervento sui profili di cybersicurezza, a protezione di reti, sistemi e dati a tutela dello stesso mercato interno. Ciò in considerazione del carattere sovranazionale delle minacce e della circostanza che dispone di strumenti, strutture e risorse che le consentono di agire con più efficacia rispetto ai singoli Stati per proteggere un sistema di scambi ormai basato sul digitale e sul commercio elettronico.

E' la natura interconnessa delle infrastrutture digitali a giustificare un'azione volta a fornire incentivi e sostegno agli Stati membri perché sviluppino e mantengano capacità nazionali di

[27] Risale al 19 marzo 2019 il rapporto "*Huawei, 5G, and China as a Security Threat*", elaborato dal NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) che evidenzia i fattori che hanno consentito a Huawei di affermarsi quale società leader: la politica nazionale cinese di superiorità tecnologica e il quadro giuridico di riferimento. Il rapporto rileva come le reti 5G siano destinate a costituire il sistema nervoso digitale delle società contemporanee ed evidenzia le delicate implicazioni strategiche insite nella scelta, da parte di paesi e imprese europee, di privilegiare l'interlocutore cinese, considerata l'aggressiva strategia di politica industriale di quel governo messa in atto anche mediante lo strumento della partnership pubblico-privata. Il rapporto indica che la rete può essere utilizzata anche per le comunicazioni critiche e, a prescindere dalle vulnerabilità tecnologiche, la scelta di affidarsi alla tecnologia fornita da un solo fornitore può creare un vincolo difficilmente rescindibile, in grado di compromettere l'autonomia di un paese e la sua stessa sovranità digitale.

[28] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche, in GU L 321/36 del 17 dicembre 2018.

cybersicurezza in stretto raccordo fra loro e con le istituzioni europee. Di qui la necessità di una strategia integrata, a livello nazionale ed europeo, con un approccio basato sulla valutazione dei rischi piuttosto che su misure di mitigazione successive.

Al centro dell'attenzione dell'UE sono soprattutto la Cina e l'aggressiva strategia delle sue arrembanti imprese. Gli stessi capi di Stato e di governo UE nel Consiglio del 22 marzo 2019 avevano sollecitato la Commissione europea ad agire con un "*approccio concertato*" in materia di sicurezza delle reti 5G, necessario per salvaguardare la già citata '"autonomia strategica"dell'Unione, obiettivo individuato nella stessa comunicazione congiunta "*EU-China, a Strategic Outlook*" del 12 marzo dello stesso anno.

Queste le ragioni per le quali nel nostro paese il Copasir, nella sua *Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale,* in data 11 dicembre 2019, aveva manifestato preoccupazione circa l'ingresso delle aziende cinesi nelle attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G; "*conseguentemente, oltre a ritenere necessario un innalzamento degli standard di sicurezza idonei per accedere alla implementazione di tali infrastrutture* [si] *dovrebbe valutare anche l'ipotesi, ove necessario per tutelare la sicurezza nazionale, di escludere le predette aziende dalla attività di fornitura di tecnologia per le reti 5G*". Il Copasir prosegue rilevando che "*le pur significative esigenze commerciali e di mercato, che assumono un ruolo fondamentale in una economia aperta, non possono prevalere su quelle che attengono alla sicurezza nazionale, ove queste siano messe in pericolo*".

Il 16 maggio 2019 il Dipartimento del Commercio USA, per motivi di sicurezza nazionale, ha inserito Huawei in una "*Black-Entity List*", introducendo divieto per Huawei di acquistare tecnologia statunitense se non previa autorizzazione, nonché di vendere e installare i propri prodotti sul territorio americano. A gennaio dello stesso anno il Dipartimento di Giustizia USA aveva contestato a Huawei 23 reati, relativi a furto di proprietà intellettuale, ostruzione della giustizia e frodi legate all'inosservanza delle sanzioni contro l'Iran. Ma già dal 2012 gli Stati Uniti avevano vietato alle proprie aziende di utilizzare apparecchiature di rete Huawei, società che in seguito all'inserimento nella "*Security Entity List*" è stata esclusa da tutte le reti di comunicazione. Nel frattempo, una legge del 2018 aveva vietato l'acquisto e l'uso di prodotti di telecomunicazioni e sorveglianza di una serie di società cinesi. Nel mirino, insieme a Hytera Communications Corporation, Hangzhou Hikvision, e Dahua Technology, soprattutto ZTE (di proprietà statale) e Huawei, sospettate di costituire un potenziale veicolo di spionaggio.

Non si tratta pertanto di fronteggiare soltanto i rischi per la sicurezza di reti e sistemi o per la raccolta e il trasferimento indebito di informazioni critiche, ma anche di rafforzare gli strumenti di controllo degli investimenti e delle esportazioni mediante una verifica di sicurezza nazionale. Così è avvenuto negli Stati Uniti nel 2018, allorché è stata aggiornata la legislazione sul controllo delle esportazioni e degli investimenti con l'*Export Control Reform Act* (ECRA) e l'*External Investment Risk Review Modernization Act* (FIRRMA), divenuti legge il 13 agosto dello stesso anno.

3.2. Il regolamento europeo sul controllo degli investimenti diretti esteri

Il regolamento europeo 452 del 19 marzo 2019[29], entrato in vigore l'8 aprile 2019 e in applicazione dall'11 ottobre 2020, prevede un sistema di controllo degli investimenti diretti esteri in Europa nei beni, nelle tecnologie e nelle infrastrutture critiche, al fine di proteggere sicurezza e ordine pubblico.

Il predetto strumento normativo non disciplina direttamente l'operazione oggetto del d.P.C.M. 7 agosto 2020, purtuttavia merita di essere menzionato in quanto tassello essenziale del quadro legislativo UE a protezione del suo sistema economico e infrastrutturale.

Si tratta di una serie di regole per il monitoraggio e la cooperazione tra Stati membri e Commissione europea che hanno ad oggetto la condivisione delle informazioni, la notifica di alcune fattispecie, la elaborazione di pareri e requisiti minimi per i meccanismi nazionali di verifica. Obiettivo del regolamento è creare un quadro procedurale di coordinamento per gli Stati che già dispongono di un meccanismo di controllo o che intendono adottarne uno e assicurare che tale meccanismo soddisfi alcuni requisiti (indicati dall'art. 3, quali la possibilità di ricorso contro la decisione, il principio di non discriminazione, ecc.).

Riguarda in sostanza gli investimenti esteri diretti (di seguito IED) provenienti da paesi terzi, ossia quegli investimenti "*che stabiliscono o mantengono legami durevoli e diretti tra investitori di paesi terzi, compresi le entità statali, e le imprese che esercitano un'attività economica in uno Stato membro*"[30]. Il regolamento si applica a tutti i settori dell'economia e non è soggetto ad alcuna soglia. La necessità di controllare un'operazione è infatti indipendente dal valore dell'operazione stessa; per esempio le *start-up* possono avere un valore relativamente limitato ma rivestire importanza strategica in settori quali la ricerca o la tecnologia.

E' previsto l'obbligo per uno Stato di notificare alla Commissione e agli altri Stati gli investimenti esteri diretti che siano oggetto di controllo fornendo una serie di informazioni (indicate all'art. 9); un altro Stato può formulare osservazioni a quello che sta effettuando la verifica se ritiene che l'investimento diretto estero possa incidere su sicurezza o ordine pubblico (art. 6, par. 1). In tal caso la Commissione europea può adottare un parere destinato allo Stato che effettua il controllo se ritiene che un investimento diretto estero possa avere incidenza su più paesi. Infine, un'acquisizione estera che possa incidere su progetti o programmi di interesse per l'Unione è soggetta a un esame più approfondito da parte della Commissione, i cui pareri devono essere presi nella massima considerazione dagli Stati membri. È quanto avverrebbe nel caso, per esempio, di investimenti esteri nelle imprese europee beneficiarie di finanziamenti a titolo di Orizon 2020, il programma di ricerca e innovazione dell'UE. Insomma, la Commissione può rivolgere allo Stato membro in cui ha luogo l'investimento pareri con i quali sono raccomandate azioni specifiche, in particolare qualora vi sia il rischio che l'investimento incida su progetti e programmi di interesse per l'Unione[31].

Come rilevato, si tratta di linee guida e indicazioni operative per l'esame degli investimenti esteri; lo Stato membro mantiene pertanto il potere di valutarli e decidere autonomamente, essendo responsabile della propria sicurezza nazionale, ai sensi dell'art. 4, par. 2, del trattato

[29] 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, in GU L 73 del 21 marzo 2019.
[30] Cfr. il considerando 9 del regolamento.
[31] Cfr. G. NAPOLITANO, *Il Regolamento sul controllo degli investimenti esteri diretti: alla ricerca di una sovranità europea nell'arena economica globale*, in *Rivista della regolazione dei mercati*, n. 1, 2019.

sull'Unione europea (TUE) e ha il diritto di proteggerla, come previsto dall'art. 346 del trattato sul funzionamento dell'Unione europea (TFUE). Il regolamento infatti fa espressamente salva la competenza esclusiva degli Stati membri in tema di sicurezza nazionale e il loro diritto di tutelare i propri interessi essenziali (art. 1).

Gli Stati membri sono dunque liberi di mantenere, modificare o adottare specifici meccanismi di controllo degli investimenti diretti esteri nel loro territorio per motivi di sicurezza o di ordine pubblico, che debbono tuttavia essere notificati alla Commissione europea (art. 3).

Nel determinare se un investimento diretto estero incida sulla sicurezza o sull'ordine pubblico, gli Stati membri e la Commissione europea possono prendere in considerazione i suoi effetti potenziali su: infrastrutture critiche, tra cui energia, trasporti, comunicazione, archiviazione dati, infrastruttura spaziali o finanziarie, infrastrutture sensibili; tecnologie critiche, tra cui intelligenza artificiale, robotica, semiconduttori, cybersicurezza, tecnologia spaziale o nucleare; sicurezza dell'approvvigionamento di fattori produttivi critici; accesso a informazioni sensibili o capacità di controllare informazioni sensibili (art. 4, par. 1). Tra i criteri da considerare ai fini di tale valutazione vi è anche la circostanza che l'investitore estero sia un soggetto controllato dal governo di un paese terzo, direttamente o indirettamente, anche attraverso l'assetto proprietario o consistenti finanziamenti, sia già stato coinvolto in attività che incidono sulla sicurezza o sull'ordine pubblico in uno Stato membro o che vi sia un serio rischio che l'investitore straniero svolga attività illegali o criminali (art. 4, par. 2).

Gli Stati membri e la Commissione possono "*tenere conto di tutti i fattori pertinenti, compresi gli effetti sulle infrastrutture critiche, sulle tecnologie, comprese le tecnologie abilitanti fondamentali, e sui fattori produttivi che sono essenziali per la sicurezza o il mantenimento dell'ordine pubblico la cui perturbazione, disfunzione, perdita o distruzione avrebbe un impatto significativo in uno Stato membro o nell'Unione*"[32]. Tra gli elementi di cui tenere conto in sede di controllo di un investimento estero, il regolamento fa esplicito riferimento ai rischi per le infrastrutture sanitarie e quelle relative alla fornitura di elementi chiave; nel mercato interno europeo i rischi posti da un investimento non si fermano necessariamente alle frontiere dello Stato membro in cui l'investimento viene effettuato.

Per questo motivo il regolamento non prevede solo la possibilità che la Commissione emetta un parere in merito a un investimento specifico: anche gli Stati membri diversi da quello in cui ha luogo l'investimento possono interloquire chiedendo informazioni e formulando osservazioni.

Il 25 marzo 2020 la Commissione europea ha pubblicato una comunicazione contenente orientamenti volti a coordinare l'approccio dell'UE al controllo degli investimenti[33] alla luce della crisi COVID-19 e proteggere le risorse e le tecnologie critiche dell'UE da potenziali acquisizioni e investimenti ostili da parte di società non UE[34].

[32] Cfr. il considerando 13 del regolamento.

[33] Commissione europea, Comunicazione della Commissione, Orientamenti agli Stati membri per quanto riguarda gli investimenti esteri diretti e la libera circolazione dei capitali provenienti da paesi terzi, nonché la protezione delle attività strategiche europee, in vista dell'applicazione del regolamento (UE) 2019/452, in GU C 99 del 26 marzo 2020.

[34] Comunicazione della Commissione, *Orientamenti agli Stati membri per quanto riguarda gli investimenti esteri diretti e la libera circolazione dei capitali provenienti da paesi terzi, nonché la protezione delle attività*

In tali linee guida, la Commissione osserva che "*Nel contesto dell'emergenza da COVID-19, potrebbe aggravarsi il rischio che si verifichino tentativi di acquisizione, tramite investimenti diretti esteri, di aziende della filiera dell'assistenza sanitaria (ad esempio per la fabbricazione di dispositivi medici o di protezione) o di settori correlati, quale quello degli istituti di ricerca (ad esempio per lo sviluppo di vaccini). Occorre vigilare per garantire che gli IED non abbiano effetti negativi sulla capacità dell'UE di soddisfare le esigenze sanitarie dei suoi cittadini*".

In generale, le Linee guida cercano, almeno in parte, di anticipare l'applicazione del Regolamento 2019/452 evidenziando il suo campo di applicazione e illustrando il ruolo dello screening degli IDE in caso di emergenza sanitaria pubblica.

A tal fine la Commissione europea invita gli Stati membri ad avvalersi appieno, sin da ora, dei meccanismi di controllo degli investimenti previsti dal regolamento (operativo dall'11 ottobre 2020) per tenere conto dei rischi per le infrastrutture sanitarie critiche e per l'approvvigionamento di materiali. Raccomanda altresì di istituire un siffatto sistema a quegli Stati membri che attualmente non ne dispongono avvalendosi, nel frattempo, di tutti gli altri meccanismi disponibili. Ciò per far fronte ai casi in cui l'acquisizione o il controllo di una determinata impresa, infrastruttura o tecnologia comporti un rischio per la sicurezza o l'ordine pubblico nell'UE.

Si tratta infatti di scongiurare il rischio che l'attuale crisi sanitaria comporti la vendita di *asset* preziosi da parte degli operatori industriali e commerciali europei, comprese le PMI, ad un prezzo inferiore a quello reale. Nella comunicazione la Commissione ricorda agli Stati membri le interdipendenze esistenti in un mercato integrato come quello europeo e li invita a chiedere se del caso assistenza tecnica e a coordinarsi fra loro. Meccanismi nazionali di controllo sono già peraltro in vigore in 14 Stati membri[35].

Le Linee guida evidenziano che, oltre al controllo degli investimenti, gli Stati membri possono detenere diritti speciali in talune imprese, come nel caso dei poteri di "*Golden power*", di cio alla legge n. 56/2012. In alcuni casi tali diritti possono consentire allo Stato di fissare limiti a determinati tipi di investimento nelle società interessate o bloccarli. Come le altre restrizioni alla circolazione dei capitali, ai sensi dell'art. 63 TFUE (che prevede la libera circolazione dei capitali non solo all'interno dell'UE, ma anche con i paesi terzi), tuttavia esse devono essere necessarie e proporzionate al conseguimento di un legittimo obiettivo di ordine pubblico.

Nel caso di "acquisti predatori" di attività strategiche da parte di investitori esteri (per esempio volti a limitare l'approvvigionamento sul mercato UE di un determinato bene o servizio), l'eccezione più rilevante è quella relativa all'ordine pubblico o alla pubblica sicurezza di cui all'articolo 65 TFUE. Ciò potrebbe giustificare, per esempio, l'adozione di misure restrittive atte a garantire la sicurezza dell'approvvigionamento (per esempio nel settore dell'energia) o la fornitura di servizi pubblici essenziali. Questo nel caso in cui le misure meno restrittive (come quelle che impongono obblighi di servizio pubblico a tutte le società che operano in determinati settori) siano insufficienti ad affrontare in modo adeguato tale minaccia, che rischia di compromettere gli interessi fondamentali della collettività. La sanità pubblica è stata peraltro riconosciuta dalla Corte di giustizia dell'Unione europea come un motivo imperativo di interesse generale[36].

---

strategiche europee, in vista dell'applicazione del regolamento (UE) 2019/452 (2020/C 99 I/01), in GU C 99 del 26 marzo 2020.

[35]La lista è indicata in http://trade.ec.europa.eu/doclib/html/157946.htm

[36] Causa C-531/06, Commissione/Italia, punto 51.

I motivi imperativi di interesse generale riconosciuti dalla Corte di giustizia in relazione ad altre libertà sancite dal trattato includono peraltro anche la protezione dei consumatori, la salvaguardia dell'equilibrio finanziario del sistema di sicurezza sociale e il conseguimento degli obiettivi di politica sociale, che potrebbero entrare in gioco in situazioni di emergenza.

Nel caso di investimenti esteri provenienti da paesi terzi in società aventi quotazioni al di sotto del loro valore reale o intrinseco, è consentito adottare restrizioni, tenendo conto dell'impatto effettivo o potenziale di tali investimenti sugli interessi pubblici coinvolti. Nella valutazione delle ragioni e della proporzionalità di tali misure, le restrizioni ai movimenti di capitali in provenienza di paesi terzi debbono valutarsi, dal punto di vista giuridico, in modo diverso rispetto alle restrizioni che riguardano i movimenti di capitali all'interno dell'UE. Il che significa che per le restrizioni applicate a operazioni che coinvolgono paesi terzi possono essere considerati ulteriori motivi di giustificazione rispetto a quelli previsti dal trattato per le operazioni intra UE.

Nel caso in cui un investimento estero abbia luogo prima dell'entrata in vigore del regolamento, vale a dire l'11 ottobre 2020, ma non sia sottoposto a un processo di verifica nazionale, il regolamento prevede che la Commissione e gli Stati membri diversi da quello in cui l'investimento viene effettuato possano fornire commenti e pareri *ex post* a partire dall'11 ottobre 2020 ed entro 15 mesi dal completamento dell'investimento estero.

Tali pareri possono portare al divieto dell'investimento da parte dello Stato membro dell'UE in cui l'investimento è stato effettuato o, in alternativa, all'adozione delle "*misure di attenuazione necessarie*" a discrezione dello Stato membro, nel rispetto della propria normativa.

La Commissione incoraggia gli Stati membri a esaminare attentamente le acquisizioni che non sono qualificabili come investimenti diretti esteri e che non rientrano nel campo di applicazione del regolamento (art. 2, par. 1) in base alle norme sulla libera circolazione dei capitali che consentono, ai sensi della giurisprudenza europea, l'applicazione di restrizioni qualora necessarie e proporzionate per raggiungere un legittimo obiettivo di ordine pubblico.

In tali casi è consentito far riferimento a motivi di "*ordine pubblico,* […] *sicurezza pubblica e* […] *salute pubblica*", tuttavia qualora tali obiettivi possano essere perseguiti con altri mezzi meno restrittivi (per esempio, misure regolamentari che impongono obblighi di servizio pubblico) allora una restrizione all'investimento straniero specifico potrebbe essere considerata sproporzionata.

Alcuni paesi dell'UE hanno modificato il proprio sistema di controllo degli investimenti esteri anche prima della pubblicazione delle linee guida della Commissione europea. Per esempio, la Spagna ha adottato misure piuttosto severe nel contesto dell'epidemia COVID-19 per proteggere la propria economia nazionale sospendendo alcune previsioni in tema di infrastrutture e tecnologie critiche per gli investitori provenienti da paesi extra UE ed EFTA. Ciò ha fatto seguito alle misure adottate in Australia, ove è stato previsto che tutti gli investimenti stranieri soggetti al *Foreign Acquisitions and Takeovers Act* 1975 siano sottoposti ad autorizzazione preventiva indipendentemente dal loro valore o dal tipo di investitore.

Gli Stati Uniti hanno istituito, già a partire dal 1975, un Comitato sugli investimenti esteri denominato CFIUS (*Committee on Foreign Investment in the United States*), che si occupa di analizzare le implicazioni per la sicurezza nazionale degli investimenti stranieri negli USA. Con

la legge sulla modernizzazione della revisione dei rischi per gli investimenti esteri del 2018 (*Foreign Investment Risk Review Modernization Act* – FIRRMA), è stato ulteriormente rafforzato il ruolo del CFIUS, in quanto è stata introdotta l'obbligatorietà del controllo del Comitato sulle transazioni che direttamente o indirettamente comportino l'acquisizione, da parte di un Governo straniero, di un "interesse sostanziale" (*substantial interest*) in società statunitensi che controllano infrastrutture o tecnologie di rilevanza critica per il paese.

Ancje la Cina, con la legge sugli investimenti esteri del 15 marzo 2019 (*Foreign Investment Law* - FIL), ha rimodellato integralmente la disciplina dell'accesso, promozione, protezione e gestione degli investimenti esteri nel suo territorio.

In Germania, nel 2017 e nel 2018, è stata aggiornata la disciplina in materia di controllo degli investimenti esteri con l'ampliamento del raggio d'azione dello *screening* governativo. Sono infatti soggette a controllo anche le acquisizioni o le partecipazioni in società tedesche da parte di investitori stranieri, non europei, indipendentemente dal settore in cui opera la società target o l'investitore. Inoltre, la nuova normativa ha abbassato dal 25% al 10 % la soglia di rilevanza che, in caso di acquisizione da parte di un soggetto extraeuropeo, fa scattare il potere d'intervento dello Stato.

La Gran Bretagna in data 11 giugno 2018 ha adottato un decreto per modificare le soglie dell'*Enterprise Act*, che stabilisce le circostanze in cui un'acquisizione o una concentrazione, riguardante settori specifici che hanno maggiori probabilità di avere implicazioni per la sicurezza nazionale, può essere deferita all'Autorità per la concorrenza e i mercati (CMA) per motivi di interesse pubblico. A seguito della novella normativa, il Governo britannico può ora intervenire in un'acquisizione se il fatturato annuale della società acquisita è pari a 1 milione di sterline (la precedente soglia era fissata a 70 milioni di sterline).

In Francia il decreto del 29 novembre 2018 ha ulteriormente esteso l'elenco dei settori strategici sui quali il governo francese può intervenire, al fine di tutelare anche i settori legati alle nuove tecnologie.

Come emerge da quanto precede, le varie legislazioni nazionali hanno, sostanzialmente: a) esteso l'ambito dei settori critici e strategici in cui l'investimento richiede l'intervento del Governo; b) abbassato le soglie di investimento che fanno scattare l'obbligo di notifica (compresi gli investimenti di minoranza); c) ampliato l'elenco degli interessi pubblici tutelati (dalle preoccupazioni puramente di sicurezza nazionale a questioni economiche, tecnologiche e di protezione dei dati personali più ampie); d) prolungato i termini del procedimento di esercizio dei poteri speciali; e) rafforzato i poteri speciali di prescrizione e inibizione delle autorità pubbliche[37].

Come già rilevato, il nostro paese ha previsto sin dal 2012 uno specifico meccanismo di controllo mediante le disposizioni in materia di poteri speciali dello Stato (il cosiddetto *Golden Power*, di cui al decreto-legge 21/2012 convertito in legge 56/2012), previsto per i settori di difesa e sicurezza nazionale, energia, trasporti e comunicazioni. Le norme di cui all'art. 15 del decreto legge "*Liquidità*" n. 23 dell'8 aprile 2020, convertito in legge 5 giugno 2020, n.40, hanno esteso tale sistema di controllo ai settori riguardati dal regolamento europeo 452, anticipando la valutazione richiesta da quest'ultimo.

[37] Cfr. Relazione al Parlamento "*concernente l'attività svolta sulla base dei 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*" comunicata alla Presidenza del Consiglio dei Ministri il 22 giugno 2020

In conclusione, lo scenario conseguente all'entrata in vigore del regolamento (UE) 2019/452 e l'evoluzione della disciplina nazionale a seguito delle modifiche operate al decreto-legge n. 21 del 2012, mettono in evidenza due aspetti fondamentali: da un lato, è stato delineato un maggiore coordinamento a livello europeo in tema di protezione dei settori strategici, mediante l'introduzione di forme di cooperazione e collaborazione tra i governi nazionali degli Stati membri e la Commissione europea, previste dall'articolo 6 e seguenti dello stesso regolamento; dall'altro lato, sono stati ampliati e rafforzati gli strumenti di controllo sia in materia di investimenti esteri che in materia di sicurezza cibernetica relativa alle reti di telecomunicazione in tecnologia 5G.

Peraltro occorre segnalare che il regolamento non è l'unico strumento previsto per controllare gli investimenti stranieri. Infatti sia la direttiva 2014/24/EU[38] in tema di appalti sia quella 2002/21/CE[39] in tema di comunicazioni elettroniche, che riguarda le reti e l'assegnazione delle frequenze (compreso il 5G), consentono agli Stati membri di adottare le misure necessarie per assicurare la protezione dei propri interessi nazionali, l'incolumità e la sicurezza pubblica. Lo stesso articolo XXI del WTO/GATT[40] prevede che uno Stato parte dell'accordo possa prendere le misure più appropriate per proteggere la sicurezza dei propri interessi essenziali.

3.3. La raccomandazione sulla cybersicurezza delle reti 5G

Come già indicato, in tema di cybersicurezza delle reti 5G è la raccomandazione della Commissione europea del 26 marzo 2019[41]a fornire concrete e specifiche indicazioni, sul piano tecnico e regolamentare.

In particolare, per affrontare i rischi di cybersecurity nelle reti 5G il documento evidenzia la necessità di considerare, in primo luogo, fattori tecnici, come le vulnerabilità che possono essere sfruttate per l'accesso non autorizzato alle informazioni (cyberspionaggio, per motivi economici o politici) o per altri scopi dolosi (attacchi informatici volti a distruggere sistemi e dati o a provocarne il malfunzionamento) oppure la necessità di proteggere le reti durante il loro ciclo di vita e considerare le apparecchiature nelle fasi di progettazione, sviluppo, appalto, diffusione, funzionamento e manutenzione delle reti 5G.

Inoltre, occorre prendere in considerazione altri elementi, quali i profili di carattere strategico e regolamentare, come i requisiti normativi imposti ai fornitori di apparecchiature di comunicazione. E' necessario infatti tener conto del rischio di influenza da parte di un paese terzo quale la Cina in relazione al suo modello di *governance*, l'assenza di accordi di cooperazione sulla sicurezza o di una decisione di adeguatezza europea in tema di protezione dei dati, verificando altresì se il Paese in questione sia parte di accordi in materia di cybersicurezza, lotta alla criminalità informatica o protezione dei dati.

Al fine di sostenere lo sviluppo di un approccio dell'Unione volto a garantire la cybersicurezza delle reti 5G, la raccomandazione in esame affida a vari soggetti istituzionali il compito di svolgere specifiche azioni al fine di consentire agli Stati membri di valutare i rischi di che

[38] 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, in GU L 94 del 28 marzo 2014.

[39] 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), in GU L 108/3 del 24 aprile 2002.

[40] Article XXI, Security exceptions, https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf

[41] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, Cybersicurezza delle reti 5G, in GU L 88 del 29 marzo 2019.

interessano le reti 5G a livello nazionale e adottare le necessarie misure di sicurezza. E' demandato poi alle istituzioni, alle agenzie e ad altri organismi dell'Unione di elaborare congiuntamente agli Stati membri una valutazione dei rischi coordinata a livello di Unione basata sulla valutazione nazionale dei rischi. Infine, il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 (NIS) ha il compito di individuare un'eventuale serie comune di misure da adottare per le infrastrutture che sono a base dell'ecosistema digitale, in particolare le reti 5G.

La raccomandazione prevedeva che entro il 30 giugno 2019 gli Stati membri svolgessero una valutazione sui rischi per le reti 5G a livello nazionale e adottassero le misure necessarie, compreso l'aggiornamento dei requisiti di sicurezza. Si tratta di adempimenti necessari anche ai sensi delle direttive in tema di comunicazioni elettroniche del 2002, aggiornate nel 2009, secondo cui sono le stesse reti a dover garantire "*il mantenimento dell'integrità e della sicurezza"* e un "*livello elevato di protezione dei dati personali*" come confermato dal regolamento europeo 2016/679.

Di qui l'onere in capo a TIM, *in primis*, di garantire la sicurezza della propria rete.

Tale aspetto emerge chiaramente dalla decisione del 7 agosto 2020. E' l'operatore a dover farsi carico di una serie di verifiche preventive e monitoraggio e comunicare tempestivamente gli aggiornamenti al Comitato di monitoraggio della Presidenza del Consiglio dei Ministri.

La valutazione di ogni paese sui rischi del 5G avrebbe poi dovuto essere trasmessa, entro il 15 luglio, alla Commissione e all'ENISA affinché gli stessi Stati, insieme alle istituzioni UE, alle agenzie e agli altri organismi potessero poi effettuare quella congiunta a livello europeo, da completarsi entro il 1° ottobre 2019 (in realtà ciò è avvenuto il 9 ottobre)[42]. La

[42] *Relazione sulla valutazione coordinata a livello di UE dei rischi per la cybersicurezza delle reti di quinta generazione* (5G) del 9 ottobre 2019. Il documento, predisposto dal Gruppo di cooperazione istituito dalla direttiva NIS, è volto a garantire un elevato livello di cybersicurezza delle reti 5G in tutta l'UE. Si basa sui risultati delle valutazioni nazionali dei rischi per la cybersicurezza effettuate da tutti gli Stati membri dell'UE e individua le minacce più rilevanti e i principali autori di tali minacce, le risorse più sensibili e le principali vulnerabilità, nonché diversi rischi strategici. La relazione, in particolare, sottolinea i potenziali scenari di rischio connessi alla realizzazione delle nuove reti: maggiore esposizione agli attacchi e aumento del numero dei potenziali punti di accesso per gli autori di tali attacchi. Dato che le reti 5G si basano sempre più su *software*, stanno assumendo importanza i rischi legati a gravi lacune a livello di sicurezza, come quelle derivanti da processi inadeguati di sviluppo del *software* da parte dei fornitori. Ciò potrebbe anche consentire agli autori delle minacce di inserire malevolmente *backdoor* più difficilmente individuabili nei prodotti. A ciò si aggiungono la maggiore sensibilità di alcune apparecchiature e funzioni di rete, quali le stazioni base o le principali funzioni di gestione tecnica delle reti; la maggiore esposizione ai rischi legati alla dipendenza degli operatori di reti mobili dai fornitori, che aumenterà anche il numero dei percorsi di attacco sfruttabili dagli autori delle minacce (ivi compresi gli stati non membri dell'UE) ed esacerberà la potenziale gravità dell'impatto di tali attacchi. Inoltre, l'aumento dei rischi derivanti da una forte dipendenza da un unico fornitore, che accresce l'esposizione al rischio derivante da un'eventuale interruzione dell'approvvigionamento dovuta, per esempio, a un insuccesso commerciale e alle sue conseguenze. Tale dipendenza aumenta inoltre il potenziale impatto delle debolezze o delle vulnerabilità nonché la possibilità che queste vengano sfruttate dagli autori di minacce, in particolare quando la dipendenza riguarda un fornitore che presenta un elevato grado di rischio. Infine vi è il rischio legato allo sviluppo delle minacce alla disponibilità e all'integrità delle reti, che diventeranno importanti problemi in materia di sicurezza, in aggiunta alle minacce alla riservatezza e alla tutela della privacy. La conversione delle reti 5G nella colonna portante di numerose applicazioni informatiche critiche farà sì che l'integrità e la disponibilità di tali reti diventino rilevanti problemi di sicurezza nazionale e una sfida di primo piano per la sicurezza a livello di UE. A fronte di tali rilevanti scenari di rischio, la relazione considera necessario rafforzare il paradigma di sicurezza, e a tal fine richiede un riesame dell'attuale quadro politico e di sicurezza applicabile al settore e al suo ecosistema, ed impone agli Stati membri di adottare le necessarie misure di attenuazione.

raccomandazione prevede che in seguito il Gruppo di Cooperazione istituito ai sensi della direttiva NIS avrebbe dovuto individuare, entro il 31 dicembre, gli strumenti atti a identificare i rischi e le possibili misure di mitigazione, tra i quali la certificazione, le prove e i controlli degli accessi (il *Toolbox*).

Tale insieme di strumenti – secondo la raccomandazione – sono volti ad orientare la Commissione nello sviluppo di requisiti minimi comuni, a ulteriore garanzia di un elevato livello di cybersicurezza delle reti 5G in tutta l'Unione. Si può trattare di impegni stringenti per le imprese che partecipano alle gare per l'assegnazione dei diritti d'uso delle frequenze, specifici requisiti per le procedure di appalto così come la conformità agli schemi di certificazione di *hardware, software* o servizi.

La necessità di rispettare i rigorosi parametri e standard di resilienza, sicurezza e *compliance* previsti dalle norme e dalle certificazioni nazionali (da aggiornare e integrare costantemente per tener conto dell'evoluzione delle minacce) è infatti essenziale. Ciò dovrebbe riguardare non solo gli apparati, le piattaforme e i servizi di rete ma lo stesso processo relativo alle diverse fasi di realizzazione della rete 5, compresi i contratti già in essere relativi alle forniture e ai servizi 5G.

In tal senso hanno un ruolo fondamentale gli schemi di certificazione europei (volontari, ma destinati in futuro a divenire obbligatori) elaborati da ENISA secondo quanto previsto dal *Cybersecurity Act*[43], approvato dal Parlamento europeo il 12 marzo 2019, che costituiscono gli elementi portanti del futuro mercato continentale della cybersicurezza.

La sicurezza delle reti è destinata ad essere rafforzata altresì dalla trasposizione del codice europeo delle comunicazioni elettroniche, la direttiva 1972 del 2018[44], il cui termine scade il 21 dicembre 2020. Il suo Titolo V è dedicato alla sicurezza (articoli 40 e 41) e affida fra l'altro poteri rilevanti alle autorità competenti, che al riguardo avranno la possibilità di impartire agli operatori istruzioni vincolanti e attivare in taluni casi un raccordo con i gruppi di intervento per la sicurezza informatica («CSIRT») ai sensi della direttiva NIS. Si tratta dunque di un ulteriore, importante tassello del mosaico a tutela della sicurezza di reti e servizi.

3.4. Il *Toolbox* (la "cassetta degli attrezzi")

Come previsto dalla raccomandazione, il gruppo di cooperazione istituito dalla direttiva NIS ha approvato il 29 gennaio 2020 la "cassetta degli attrezzi" (*Toolbox*) per il 5G[45], cioè le misure di mitigazione per affrontare i rischi di sicurezza legati alle reti di quinta generazione che Stati membri da applicare entro il 30 aprile.

Si tratta di un elemento essenziale, espressamente citato dalla decisione del 7 agosto 2020, con l'obiettivo di delineare un approccio coordinato basato su una serie comune di misure,

---

Così il Copasir nella sua *Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale* dell'11 dicembre 2019.

[43] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013, in GU L 151 del 7 giugno 2019.

[44] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche in GU L 321 del 17 dicembre 2018.

[45] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE, Bruxelles, 29 gennaio 2020 COM(2020) 50 final.

volte a mitigare i principali rischi di cybersicurezza delle reti 5G identificati nella relazione sulla valutazione dei rischi dell'UE del 9 ottobre 2019. Ha altresì il compito di assistere gli Stati membri nella selezione e definizione delle priorità delle misure che dovrebbero far parte dei piani nazionali ed europei di mitigazione del rischio.

Sono gli operatori come TIM ad essere responsabili dell'attuazione sicura del 5G, ma spetta agli Stati membri la tutela della sicurezza nazionale.

La sicurezza della rete peraltro ha una rilevanza strategica che travalica i confini nazionali: riguarda il mercato unico e incide sulla stessa sovranità tecnologica dell'UE, a sua volta collegata alla competitività economica e al suo ruolo sul piano geopolitico. Dal *Toolbox* emerge che i rischi strategici non possono essere mitigati solo con misure tecniche; in questi casi occorre una risposta politica e normativa, soprattutto quando un determinato fornitore (è il caso di Huawei, peraltro mai citato nel documento) è soggetto a possibili interferenze di un governo straniero (es. la legge sulla cybersicurezza del 2016[46]).

Pur mettendo in conto valutazioni differenziate a livello nazionale, l'obiettivo del *Toolbox* è quello di evitare che gli Stati procedano in ordine sparso. Di qui l'indicazione di un approccio metodologico comune e un armamentario condiviso. Al riguardo la Commissione si impegna a far uso di tutti gli strumenti di cui dispone per garantire la sicurezza dell'infrastruttura e dell'intera "*supply chain"* del 5G: le regole in tema di cyber sicurezza e telecomunicazioni (contenute nel Codice europeo delle comunicazioni elettroniche), il coordinamento in tema di standardizzazione e certificazione (il *Cybersecurity Act*); la verifica degli investimenti diretti esteri (il regolamento 2019/452); gli strumenti di difesa commerciale (le misure *antidumping*); le regole in tema di concorrenza e appalti pubblici; gli stessi programmi di finanziamento UE (*Connecting Europe Facility Digital*).

Con un delicato esercizio di equilibrismo, l'Unione europea cerca di mantenersi equidistante tra Stati Uniti e Cina, raccomandando alle autorità di regolamentazione nazionali di applicare le restrizioni ritenute più opportune per proteggere le parti centrali delle reti (le più vulnerabili alla pirateria informatica e allo spionaggio) e adottare misure adeguate nei confronti dei fornitori considerati "ad alto rischio".

Al riguardo gli Stati membri sono invitati a garantire la diversità dei fornitori e adottare una strategia "*multi-vendor*", come già avviene per il 4G. Di qui l'idea di fissare un tetto (*cap)* alla presenza di un fornitore sulla rete, come in un primo tempo aveva fatto per esempio il Regno Unito, annunciando quello del 35%.

Secondo il *Toolbox* tutti i fornitori "ad alto rischio" (Huawei e ZTE) dovrebbero essere sottoposti a condizioni o esclusi dalle parti sensibili della rete per mitigare il rischio di interferenze statali. Non si tratta solo delle funzioni *core*, ma anche della rete di accesso, come già emerso nel documento di valutazione del rischio a livello UE del 9 ottobre 2019.

Nel documento viene altresì confutata la distinzione tra centro e periferia (*core* ed *edge*) dei sistemi 5G, che si ritiene sia destinata ad evolvere in fretta con il passaggio dal 5G non autonomo (*non standalone*, essenzialmente un 4G potenziato) al 5G autonomo. Una transizione che sposterà molti dati alla periferia della rete e aprirà la strada a una maggiore virtualizzazione delle operazioni, con un'accentuata dipendenza dall'architettura software

[46] La *Cyber Security Law of the People's Republic of China*, adottata il 7 novembre 2016 ed entrata in vigore il 1° giugno 2017.

della rete e il rischio, per esempio, che un fornitore possa introdurre vulnerabilità mediante gli aggiornamenti.

Le indicazioni della Commissione europea sono chiare: ogni Stato membro dovrebbe elaborare un piano per ridurre progressivamente la dipendenza da fornitori ad altro rischio, mentre si procede al potenziamento dell'infrastruttura. Sono raccomandate esclusioni e restrizioni all'interno dei normali cicli di sostituzione degli apparati, con un periodo di transizione volto a mitigare l'impatto economico della sostituzione dei prodotti cinesi.

Per ciascuna delle nove aree di rischio identificate nella relazione sulla valutazione coordinata dei rischi a livello europeo del 9 ottobre 2019, la cassetta degli attrezzi identifica e fornisce piani di mitigazione del rischio, che comprendono possibili combinazioni di misure strategiche e tecniche, insieme ad adeguate azioni di supporto per mitigare i possibili rischi.

In particolare, gli Stati membri sono invitati a rafforzare i requisiti di sicurezza per gli operatori di rete mobile (per esempio, in tema di accesso, norme sulla sicurezza del funzionamento e del monitoraggio, limitazioni sull'esternalizzazione di specifiche funzioni, ecc.). Dovrebbero altresì valutare il profilo di rischio dei fornitori e quindi applicare restrizioni mirate per quelli considerati ad alto rischio, compresa l'esclusione, qualora necessarie per mitigare i rischi per gli *asset* critici e sensibili.

Per esempio, nella procedura di aggiudicazione di un appalto la normativa vigente affida alla stazione appaltante il compito di indicare, nei documenti di gara, sia il criterio di aggiudicazione sia, nel caso dell'offerta economicamente più vantaggiosa, gli elementi da prendere in considerazione (indicati a titolo esemplificativo al par. 6 dell'art. 95 del d.lgs. n. 50/2016[47], il codice appalti).

In tal caso è essenziale che fra tali elementi sia annoverato quello della sicurezza, soprattutto quando si tratta di beni ad alto contenuto tecnologico, come nel caso degli apparati 5G.

Al riguardo le Linee Guida n. 2 dell'ANAC (Autorità nazionale anticorruzione) relative all'offerta economicamente più vantaggiosa (approvate il 21 settembre 2016 e aggiornate il 2 maggio 2018) indicano che nella valutazione delle offerte possono essere valutati profili di carattere soggettivo qualora consentano di "*apprezzare meglio il contenuto e l'affidabilità dell'offerta o di valorizzare caratteristiche dell'offerta ritenute particolarmente meritevoli*"; in ogni caso, esse devono riguardare "*aspetti che incidono in maniera diretta sulla qualità della prestazione*". Il che significa, per l'amministrazione, poter valutare l'adeguatezza dell'offerta tenendo conto di una pluralità di elementi (da indicare peraltro necessariamente nei documenti di gara, a garanzia della tenuta giuridica della scelta finale), compresi quelli inerenti la sicurezza della fornitura e del servizio in questione, di cui fanno parte le caratteristiche soggettive dell'eventuale contraente.

Il tema della sicurezza dei beni e dei servizi informativi è rilevante soprattutto per le forniture tecnologiche. Come rilevato, la sicurezza dei vari elementi destinati ad integrare i sistemi informativi è strettamente connessa alla verifica della qualità e dell'affidabilità degli

[47] Decreto legislativo 18 aprile 2016, n. 50, Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture, in GU Serie Generale n.91 del 19-04-2016 - Suppl. Ordinario n. 10.

operatori economici aggiudicatari, a tutela e garanzia dei dati e dei diritti dei cittadini oltre che della stessa sicurezza nazionale[48].

La stessa Commissione europea, nella raccomandazione del 26 marzo 2019, così come nel *Toolbox* in esame, ha evidenziato l'importanza di procedure di appalto che consentano la valutazione dell'adeguatezza delle offerte in base agli elementi tecnici e ai requisiti normativo-regolamentari degli operatori coinvolti nelle gare, così da verificare le caratteristiche dei singoli fornitori e non compromettere la sicurezza della "*supply chain*".

La stessa valutazione coordinata del rischio dell'UE sulla sicurezza informatica di cui al rapporto del 9 ottobre 2019, evidenzia la necessità di considerare, in sede di gara, il profilo di rischio dei singoli fornitori, da valutarsi in base a fattori quali la possibilità che lo stesso sia soggetto a interferenze di un paese extra UE (pt. 2.36). Naturalmente tale valutazione dovrebbe essere condotta unicamente per motivi di sicurezza e in base a criteri oggettivi.

Tale aspetto è espressamente considerato nella decisione del 7 agosto 2020, tuttavia non fino al punto di indurre il governo ad apporre il veto all'operazione, preferendo condizionarla al rispetto di alcune precise condizioni.

Peraltro la normativa vigente in tema di comunicazioni elettroniche (art. 13 bis della direttiva 2002/21) impone agli Stati membri di garantire che gli operatori di telecomunicazioni assicurino l'integrità delle loro reti e quindi la continuità della fornitura dei servizi. Così stabilisce anche il codice europeo delle comunicazioni elettroniche (la direttiva 2018/1972) al fine ad evitare minacce alla riservatezza, alla disponibilità e all'integrità delle risorse.

Il *Toolbox* segnala altresì la necessità che ciascun operatore disponga di una strategia *multi-vendor* per evitare o limitare la dipendenza da un unico fornitore, garantire un adeguato equilibrio dei fornitori a livello nazionale ed evitare la dipendenza dai fornitori considerati alto rischio, così da consentire l'interoperabilità delle apparecchiature.

Le misure strategiche considerate nel *Toolbox* riguardano anche il rafforzamento dei poteri regolatori delle autorità di controllo, specifiche azioni per affrontare i rischi relativi a vulnerabilità non tecniche (ad esempio il rischio di interferenza da parte di uno Stato non UE o attori sostenuti dallo Stato), per valutare il profilo di rischio dei fornitori e promuovere iniziative volte a sostenere lo sviluppo di fornitori 5G affidabili e diversificati[49].

Consapevole della delicatezza e rilevanza di tale aspetto, la decisione del 7 agosto 2020 impone a TIM di integrare il contratto con clausole che prevedano, a pena di risoluzione espressa ai sensi dell'articolo 1456 del codice civile, che i fornitori e le società si obblighino a non comunicare ad autorità governative estere o comunque a terzi dati e informazioni

[48] Meritevoli di menzione le conclusioni del Consiglio UE *Trasporti, telecomunicazioni ed energia,* svoltosi il 3 e 4 dicembre 2019 e la Dichiarazione di Londra approvata dal Vertice dei Capi di Stato e di Governo della NATO, anch'esso svoltosi il 3 e il 4 dicembre 2019. Il Consiglio della UE, sul tema dei rischi connessi alle reti 5G, evidenzia la necessità di considerare fra i fattori di rischio per la sicurezza non solo i profili attinenti la tecnologia ma altresì quelli derivanti da fattori extra-tecnici e collegati alle politiche e ai sistemi legali vigenti nei paesi terzi, con i quali vengano instaurati rapporti per la fornitura di servizi e prodotti. Nella Dichiarazione di Londra i paesi NATO si impegnano, tra l'altro, a garantire la sicurezza delle comunicazioni, anche con riferimento alle reti 5G, rilevando l'esigenza di poter fare affidamento su sistemi informatici sicuri e resilienti.

[49] Il *Toolbox* prevede che la Commissione inviti gli Stati membri ad adottare misure adeguate entro il 30 aprile 2020 e il gruppo di cooperazione NIS a preparare una relazione dello stato di attuazione delle misure in ogni Stato membro chiave entro il 30 giugno. Infine, entro il 10 ottobre 2020, gli Stati membri, in collaborazione con la Commissione, sono tenuti a valutare gli effetti della raccomandazione della Commissione del 26 marzo 2019 ai fini di ulteriori azioni.

comunque acquisiti in relazione all'operazione notificata, salvo preventivo accesso al Comitato di monitoraggio.

Insomma, l'avvento del 5G mette in luce la complessa natura delle sfide tecnologiche e politiche che gli Stati membri devono affrontare e continueranno ad affrontare nei prossimi decenni. Al riguardo la Commissione europea ha dimostrato che una maggiore cooperazione in materia non è solo utile, ma necessaria per la sicurezza informatica e la sovranità tecnologica dell'Europa. La cybersicurezza è per definizione difficile da affrontare a livello nazionale ma diventa meno costosa e più efficace se il campionario delle misure o se le procedure e gli schemi di certificazione sono elaborati a Bruxelles.

Come evidenziato da Mathieu Duchâtel e François Godement nel blog dell'*Institut Montaigne* il 30 gennaio 2020, l'approccio relativo alla mitigazione del rischio, in contrapposizione all'esclusione *tout court* dei venditori ad alto rischio, implica un costante e costoso adattamento degli strumenti operativi, con una sorta di scommessa sulle future capacità della cybersicurezza europea.

A ciò si aggiunge un ulteriore, rilevante aspetto di carattere strategico, in un contesto geopolitico in cui si fronteggiano Stati Uniti e Cina: la "cassetta degli attrezzi", che consente agli Stati membri di scegliere il fornitore per le proprie reti 5G tenendo conto non solo degli elementi tecnici ma anche di quelli normativi e regolamentari, offre a questi ultimi la possibilità di rafforzare il legame con gli Stati Uniti e l'Alleanza Atlantica difendendo la propria sicurezza.

4. LA RETE 5G E I PROFILI DI RISCHIO

"*Guardando al quadro generale, riteniamo che le questioni di sicurezza 5G debbano essere affrontate in anticipo. Fare le scelte giuste all'inizio della sua applicazione è molto più facile che cercare di correggere gli errori una volta che la costruzione e l'operatività della rete sia stata avviata. Inoltre, le decisioni che hanno un impatto sulla sicurezza del 5G devono essere prese tenendo presente il lungo termine, senza concentrarsi troppo su considerazioni a breve termine*", così il presidente della FCC degli Stati Uniti Ajit Pai.

Negli ultimi anni, le architetture di rete stanno sempre più evolvendo verso tecnologie *Software-defined networking* (SDN), basate su un approccio in ottica *cloud computing*. Tale evoluzione tecnologica rende quindi necessario far convergere gli aspetti di sicurezza delle reti con concetti un tempo tipici del mondo IT, come per esempio il *cloud computing*.

4.1. L'analisi del rischio

Per un'efficace gestione della sicurezza delle reti, l'applicazione dei controlli e delle misure di sicurezza deve essere necessariamente basata su processi di *Risk Management*, che permettano di identificare e gestire vulnerabilità, minacce e le necessarie contromisure. A tal fine, oltre ai vari *framework* di sicurezza previsti, altre metodologie rilevanti da tenere in considerazione sono quelle di valutazione del rischio, tra cui le principali sono:

- CRAMM (*CCTA Risk Analysis and Management Method*) - Metodologia sviluppata dall'organizzazione governativa britannica CCTA (*Central Communication and Telecommunication Agency*), che riguarda tutte le fasi del processo di *Risk Management* attraverso l'utilizzo di una specifica strumentazione;

- FAIR (*Factor Analysis of Information Risk*) - Metodologia di analisi del rischio quantitativa sviluppata dal FAIR Institute, che fornisce una tassonomia dei fattori che contribuiscono al rischio e indica come gli stessi si influenzano tra loro;

- EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*) - Metodologia sviluppata dall'Agenzia nazionale per la sicurezza dei sistemi d'informazione (ANSSI) della Francia, che prevede un approccio che parte dal livello più alto e scende fino alle funzioni aziendali e tecniche, esaminando possibili scenari di rischio;
- NIST *Risk Management Framework* - Framework sviluppato dal NIST che definisce un processo strutturato che integra le attività di sicurezza delle informazioni e di gestione dei rischi nel ciclo di vita dei sistemi informatici.

In assenza di consolidati standard internazionali in materia di sicurezza e di regole applicate in modo omogeneo a livello europeo, talune iniziative hanno avuto limitata efficacia.

Se per esempio un paese non garantisce adeguate misure di sicurezza a protezione delle proprie reti, con la conseguenza di creare vulnerabilità, queste potrebbero diffondersi alle reti connesse di altri paesi, anche se gli stessi applicano misure di sicurezza avanzate. Questa situazione ha riguardato anche gli operatori di telecomunicazioni che operano all'interno dell'UE e che dispongono di una delle più rilevanti reti di infrastrutture strategiche.

L'attività di protezione preventiva di reti e servizi di comunicazione ha l'obiettivo di tutelare sistemi e asset tecnologici mediante l'analisi del rischio e l'applicazione di contromisure anche sulla base di una valutazione dei possibili eventi dannosi, verificandone poi la corretta esecuzione.

A loro volta le attività di analisi del rischio sono finalizzate a classificare gli asset tecnologici, identificare le vulnerabilità presenti rispetto ai controlli e requisiti di sicurezza necessari, definire ed attuare le contromisure necessarie in base alle vulnerabilità riscontrate e alle potenziali minacce rivolte allo specifico asset, anche tetendo conto delle informazioni raccolte tramite l'attività di *Threat Intelligence*.

Peraltro le analisi del rischio dovrebbero essere sempre affiancate anche da una valutazione di impatto, come la *Business Impact Analysis* (BIA) o il *Data Protection Impact Assessment* (DPIA) introdotto dal regolamento UE 2019/679, utili per delinere le conseguenze che potrebbe avere sull'organizzazione il verificarsi di una minaccia, in termini di compromissione dei processi operativi, danni di immagine o perdite economiche.

Le valutazioni d'impatto forniscono informazioni importanti anche per la definizione degli investimenti necessari per aumentare il livello di protezione preventiva dell'organizzazione. Partendo dai risultati delle analisi del rischio sugli asset di interesse e sulla base dei potenziali impatti stimati, possono infatti effettuarsi analisi costi/benefici per valutare se investire risorse per porre in essere interventi di adeguamento, oppure assumere il rischio o valutare differenti modalità operative.

Il costante aumento degli asset tecnologici da proteggere, la complessità architetturale che gli scenari di virtualizzazione e convergenza introducono così come l'incremento della superficie e dei potenziali vettori di attacco inducono necessariamente a dotarsi di strumenti di analisi preventiva automatizzata attraverso il *machine learning* e le applicazioni dell'intelligenza artificiale.

L'evoluzione tecnologica delle reti di comunicazione 5G induce una convergenza tra concetti tipici del mondo IT, come il *cloud computing*, la virtualizzazione e gli standard di comunicazione, con quelli tipici delle reti trasmissive.

4.2. La sicurezza

Fono a qualche tempo fa la sicurezza si concentrava solo nelle fasi finali del ciclo di vita del *software*. Tuttavia questo modello non risultava efficace in quanto una volta rilevate vulnerabilità gravi, spesso era impossibile avviare efficaci piani di azione, in quanto era necessario riprogettare e avviare attività di sviluppo software complesse, spesso dispendiose.

Successivamente sono stati introdotti i requisiti di sicurezza, il NIST *Cyber Security Framework* (simile al Framework nazionale di cybersecurity), il *cloud controls matrix version* 3.0 per gli ambienti cloud, per poi giungere al modello "*Security by Design*". Di qui l'esigenza di definire un "processo di sviluppo" nel quale la sicurezza sia presente in ogni fase (il concetto di DevSecOps).

L'evoluzione di tale scenario tecnologico rende necessario definire un framework specifico di cybersicurezza per le reti di nuova generazione, che integri quegli aspetti di sicurezza che fino a qualche tempo fa erano specifici del mondo IT.

4.3. La valutazione coordinata UE dei rischi

La relazione della Commissione europea del 9 ottobre 2019, risultato della raccomandazione del 26 marzo 2019, individua diversi importanti aspetti per la sicurezza delle reti 5G.

Tali sfide sono soprattutto legate a innovazioni chiave nella tecnologia di quinta generazione (in particolare la rilevanza del software e l'ampia gamma di applicazioni e servizi resi possibili dal 5G), al ruolo dei fornitori nella realizzazione e nell'uso delle reti e al grado di dipendenza da singoli fornitori.

In particolare, l'introduzione delle reti 5G avrà come effetto una maggiore esposizione agli attacchi e un aumento del numero dei potenziali punti di accesso. Dato che le reti 5G si basano sempre più sul *software*, stanno assumendo importanza i rischi legati a lacune a livello di sicurezza, come quelle derivanti da inadeguati processi di sviluppo del software da parte dei singoli fornitori. Ciò potrebbe anche consentire agli autori delle minacce di inserire nei prodotti *backdoor* malevoli difficilmente individuabili. Inoltre a causa delle nuove funzionalità e dell'architettura delle reti 5G, alcune componenti tecniche e funzioni di rete diventano più sensibili, come le stazioni base o le principali funzioni di gestione delle stesse. A ciò si aggiunga che una maggiore esposizione ai rischi legati alla dipendenza degli operatori di reti mobili dai fornitori aumenterà anche le possibilità di attacco per gli autori delle minacce con conseguenze più gravi. Tra i vari autori possibili, i paesi extra UE o i soggetti sostenuti da governi sono ritenuti i più pericolosi e potenzialmente più inclini ad attaccare le reti 5G.

In tale quadro di maggiore esposizione ad attacchi, il profilo di rischio dei singoli fornitori assumerà un particolare rilievo, compresa la possibilità che il fornitore subisca interferenze da parte del proprio governo. Inoltre emerge il profilo di rischio derivante da una forte dipendenza dai fornitori: questo aumenta l'esposizione al rischio derivante da un'eventuale interruzione dell'approvvigionamento. Tale dipendenza aumenta inoltre il potenziale impatto delle debolezze o delle vulnerabilità nonché la possibilità che le stesse siano sfruttate dagli autori delle minacce, in particolare quando la dipendenza riguarda un fornitore che presenta un elevato profilo di rischio.

In tal senso le minacce alla disponibilità e all'integrità delle reti sono destinate a comportare problemi di sicurezza: oltre alle minacce alla riservatezza e alla tutela della privacy, la circostanza che le reti 5G diventino colonna portante di numerose applicazioni informatiche

critiche farà sì che l'integrità e la disponibilità di tali reti assumano rilevanza per la sicurezza nazionale e diventino una sfida di primo piano per la sicurezza a livello di UE.

Tutte queste sfide creano un nuovo paradigma di sicurezza che richiede un riesame dell'attuale quadro politico e di sicurezza applicabile al settore e al suo ecosistema ed impone agli Stati membri di adottare le necessarie misure di attenuazione.

In particolare, i cambiamenti tecnologici introdotti dal 5G aumentano la superficie di attacco complessiva e il numero di potenziali punti di ingresso per gli aggressori. Il miglioramento delle funzionalità ai margini della rete e un'architettura meno centralizzata rispetto alle precedenti generazioni di reti mobili comporta che alcune funzioni delle reti principali possono essere integrate in altre parti delle reti rendendo più sensibili le apparecchiature corrispondenti (per esempio le stazioni di base). L'aumento della parte di *software* nelle apparecchiature 5G ha come conseguenza un aumento dei rischi legati ai processi di sviluppo e aggiornamento del *software*, crea nuovi rischi in termini di possibili errori di configurazione e attribuisce un ruolo più importante, nell'analisi della sicurezza, alle scelte fatte da ogni operatore di rete mobile nella fase di predisposizione della rete.

Le differenze nelle modalità di funzionamento del 5G implicano che le misure di sicurezza applicate sulle reti 4G possano non essere del tutto efficaci per mitigare i rischi di sicurezza identificati. Inoltre, la natura e le caratteristiche di alcuni di questi rischi rendono necessario determinare se possono essere affrontati solo con misure tecniche.

Come emerge dalla Relazione sui progressi degli Stati membri nell'attuazione del pacchetto di strumenti UE sulla sicurezza informatica 5G del luglio 2020, la maggior parte degli Stati membri ha già previsto obblighi di sicurezza che derivano dal vigente quadro normativo dell'UE in materia di telecomunicazioni, mentre alcuni hanno imposto requisiti dettagliati, per lo più di natura tecnica. Al riguardo, come già rilevato, il *Toolbox* del gennaio 2020 raccomanda l'introduzione di misure di sicurezza specifiche per le reti 5G, prendendo in considerazione i rischi identificati e tenendo conto di fattori sia tecnici sia strategico/regolamentare, che sono puntualmente identificati insieme alle corrispondenti azioni di supporto

Le misure strategiche comprendono interventi volti ad aumentare i poteri di intervento delle autorità per la realizzazione e la manutenzione della rete, strumenti specifici per affrontare i rischi legati alle vulnerabilità non tecniche, nonché possibili iniziative per promuovere un'offerta 5G diversificata ed evitare rischi di dipendenza a lungo termine. Le misure tecniche comprendono invece quelle per rafforzare la sicurezza delle reti e delle apparecchiature 5G affrontando i rischi derivanti da tecnologie, processi, fattori umani e fisici. Per ciascuna delle aree a rischio che sono state identificate, il *Toolbox* prevede specifici piani di mitigazione.

4.4. La metodologia di valutazione del rischio

L'ISO/IEC 27005 ("*Information security risk management*"), di cui a luglio 2018 è stata pubblicata una nuova edizione (la terza), è lo standard internazionale di riferimento per la valutazione del rischio relativo alla sicurezza delle informazioni.

Propone un approccio basato sulla valutazione di un insieme di parametri: i principali tipi di minaccia per le reti 5G, i principali attori, gli asset più rilevanti e il loro grado di sensibilità, le vulnerabilità, i e i relativi scenari.

Nel complesso, le minacce considerate più rilevanti per le reti 5G sono quelle tradizionali legate alla compromissione della riservatezza, della disponibilità e dell'integrità, quali l'interruzione locale o globale della rete 5G (disponibilità); lo spionaggio del traffico/dati nell'infrastruttura di rete 5G (riservatezza); la modifica o il reinstradamento del traffico/dati nell'infrastruttura di rete 5G (integrità e/o riservatezza); la distruzione o alterazione di altre infrastrutture digitali o sistemi informativi attraverso le reti 5G (integrità e/o disponibilità).

La gravità di specifici scenari di minaccia per le reti 5G varia a seconda di una serie di fattori, in particolare: il numero e il tipo di utenti interessati; la durata dell'evento prima del rilevamento o della riparazione; il tipo di servizi interessati (sicurezza pubblica, servizi di emergenza, salute, attività governative, elettricità, acqua, ecc.). Le minacce poste dagli Stati o dagli attori statali sono percepite come quelle di maggiore rilevanza; gli Stati rappresentano gli attori malevoli più temibili in quanto possono disporre della determinazione, degli obiettivi e soprattutto della capacità di condurre attacchi persistenti e sofisticati alla sicurezza delle reti 5G.

4.5. Vulnerabilità tecniche e regolamentari

Come rilevato, l'accresciuto ruolo del *software* e dei servizi forniti da fornitori terzi nelle reti 5G porta ad una maggiore esposizione ad una serie di vulnerabilità che possono derivare dal profilo di rischio dei singoli fornitori. Questo può essere valutato sulla base di diversi fattori, fra cui la probabilità che il fornitore sia soggetto a interferenze da parte di un paese non UE.

Si tratta di un aspetto chiave nella valutazione delle vulnerabilità non tecniche relative alle reti 5G. Se da un lato l'accesso diretto o l'influenza di un soggetto malevolo alla catena di fornitura delle telecomunicazioni può consentire azioni dannose e rendere l'impatto di tali azioni più grave, occorre rilevare che i soggetti con un'elevata capacità operativa, come un attore statale, hanno la possibilità di sfruttare le vulnerabilità in qualsiasi fase del ciclo di vita del prodotto.

Tale interferenza può essere facilitata da un forte legame tra il fornitore e un governo del paese terzo in questione; la legislazione in vigore, soprattutto quando non esistono controlli ed un quadro democratico, o in assenza di accordi in materia di sicurezza o di protezione dei dati tra l'UE e il paese in questione.

Al riguardo l'assetto normativo della Cina è alquanto problematico. Oltre alla legge sull'intelligence del 2016 che richiede che i cittadini e le società cinesi collaborino in modo segreto con i servizi di sicurezza statale per raccogliere informazioni, comprende quelle in materia di controspionaggio (2014), sicurezza dello Stato (2015), anti-terrorismo (2015), nonché la legge sulla gestione delle organizzazioni non governative straniere (2016) e quella sulla sicurezza informatica (2016).

Di qui il riferimento espresso, nella decisione del 7 agosto 2020, all'obbligo di non comunicare ad autorità governative estere o comunque a terzi dati e informazioni comunque acquisiti in relazione all'operazione notificata (articolo 1, lett. h).

Importanti vulnerabilità derivano altresì dalla mancanza di varietà di nelle apparecchiature e nelle soluzioni utilizzate. All'interno della singola rete, un elevato grado di dipendenza da un unico fornitore crea una dipendenza da soluzioni specifiche e rende più difficile l'approvvigionamento da altri fornitori, soprattutto quando le soluzioni non sono completamente interoperabili.

Di conseguenza, gli operatori UE che diventano eccessivamente dipendenti da un unico fornitore di attrezzature sono esposti al rischio derivante dal fatto che tale fornitore può subire un fallimento commerciale, essere oggetto di fusione, acquisizione o essere sottoposto a sanzione.

Il fatto di affidarsi ad un unico fornitore aumenta la vulnerabilità complessiva dell'infrastruttura 5G, in particolare se un gran numero di operatori acquisisce beni sensibili da un fornitore che presenta un elevato grado di rischio.

Sulla base ai risultati relativi ai vari parametri indicati nel *Toolbox,* sono state individuate alcune categorie di rischi di importanza strategica dal punto di vista dell'UE. Come per le attuali reti 3G e 4G, gran parte di essi deriva da sistemi mal progettati o mal configurati in cui sono presenti difetti nelle misure di sicurezza e nei processi messi in atto dagli operatori. Con il passaggio alle reti 5G è probabile che tali rischi si acuiscano notevolmente, a causa delle nuove caratteristiche tecnologiche di queste reti e della loro maggiore complessità.

Alcuni scenari di rischio sono direttamente associati alle capacità dei principali attori malevoli. In particolare, i paesi terzi ostili potrebbero esercitare pressioni sui fornitori di 5G per facilitare attacchi cibernetici al servizio dei loro interessi nazionali. In tal caso il grado di esposizione al rischio è influenzato dalla misura in cui il fornitore ha accesso alla rete e dal profilo di rischio del singolo fornitore. Aumenta inoltre in modo significativo laddove i controlli di sicurezza e di accesso siano carenti. L'interferenza può avvenire in vari modi, per esempio sfruttando le vulnerabilità incorporate non intenzionali o attraverso vulnerabilità deliberatamente iniettate.

A livello UE, i requisiti di sicurezza relativi all'ecosistema delle reti 5G e ai relativi sistemi critici sono stabiliti in particolare nella legislazione UE sulle telecomunicazioni e nella direttiva NIS. Ai sensi del quadro normativo dell'UE in materia di telecomunicazioni, possono essere imposti obblighi agli operatori di telecomunicazioni dallo Stato membro o dagli Stati membri in cui il servizio è fornito. L'articolo 13 bis della direttiva 2002/21/CE, modificata dalla direttiva 2009/140/CE, sostituita dal Codice delle comunicazioni elettroniche (direttiva 2018/1972), impone agli Stati membri sono tenuti a garantire che gli operatori delle telecomunicazioni: adottino misure adeguate e necessarie per gestire i rischi per la sicurezza e per garantire l'integrità delle loro reti, assicurando così la continuità della fornitura dei servizi forniti su di esse.

5. IL NUOVO ECOSISTEMA DI SICUREZZA UE E LA PROTEZIONE DEL MERCATO UNICO CONTRO LE SOVVENZIONI ESTERE

5.1. La nuova strategia UE per l'Unione della sicurezza

Il 24 luglio 2020 la Commissione europea ha presentato la nuova strategia UE per l'Unione della sicurezza[50] con una Comunicazione con cui pone le basi per un "ecosistema" fatto di strumenti e misure da sviluppare nei prossimi 5 anni. Questo per garantire sicurezza all'ambiente fisico e digitale, dalla lotta al terrorismo alla criminalità organizzata, passando attraverso la prevenzione e l'individuazione delle minacce ibride e l'aumento della resilienza

[50] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell'UE per l'Unione della sicurezza COM(2020) 605 final del 24 luglio 2020.

delle infrastrutture critiche, fino al rafforzamento della cybersicurezza e alla promozione di ricerca e innovazione.

Le questioni relative alla sicurezza debbono essere considerate in una prospettiva più ampia rispetto al passato, superando la distinzione tra spazio fisico e spazio digitale, poiché le minacce non si fermano ai confini geografici, sicurezza interna ed esterna sono strettamente interconnesse e occorre concentrarsi sui settori critici per la sicurezza dell'UE.

Poiché sicurezza e diritti fondamentali sono obiettivi coerenti e complementari fra loro, l'Unione europea si trova in una posizione privilegiata per elaborare una risposta efficace alle nuove sfide e minacce globali che sia ancorata ai tradizionali valori europei: uguaglianza, Stato di diritto, trasparenza, responsabilità, controllo democratico. Ecco perché ogni politica di sicurezza deve fondarsi sui valori e diritti fondamentali, nel rispetto dei principi di necessità, proporzionalità e legalità, con salvaguardie appropriate che garantiscano assunzione di responsabilità e tutela giurisdizionale, a protezione delle persone più vulnerabili. Al riguardo gli strumenti giuridici in vigore devono essere rafforzati.

La strategia riguarda il periodo 2020-2025 e definisce un approccio volto a rispondere in modo efficace e coordinato a minacce in rapida evoluzione. Stabilisce le priorità strategiche e gli interventi corrispondenti per affrontare i rischi fisici e digitali in modo integrato, concentrandosi sui settori in cui l'UE può apportare un contributo effettivo. L'approccio dell'UE alla sicurezza esterna nel quadro della politica estera e di sicurezza comune (PESC) e della politica di sicurezza e di difesa comune (PSDC) rimane un elemento essenziale dell'attività dell'UE volta a rafforzare la sicurezza all'interno dell'UE.

L'analisi delle minacce evidenzia le quattro priorità strategiche interdipendenti su cui operare: i) un ambiente della sicurezza adeguato alle esigenze future, ii) affrontare le minacce in evoluzione, iii) proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata, iv) un ecosistema europeo forte in materia di sicurezza.

In concreto, la Comunicazione sottolinea che una strategia orientata ai risultati deve basarsi su un'attenta valutazione delle minacce e dei rischi, deve definire e applicare norme e strumenti adeguati e richiede una *intelligence* strategica. Laddove occorra un intervento normativo dell'UE, è necessario effettuare un follow-up degli atti legislativi per accertarsi che siano pienamente attuati, ad evitare frammentazioni e lacune.

Questo comporta una cooperazione più intensa tra Stati membri, il coinvolgimento delle autorità di contrasto e giudiziarie e di tutti i soggetti pubbliche competenti, con la partecipazione delle istituzioni e delle agenzie dell'UE, per la comprensione e il dialogo necessari per soluzioni comuni. Anche la cooperazione con il settore privato è fondamentale, laddove dispone di una parte importante degli strumenti e dell'infrastruttura digitale indispensabili per lottare efficacemente contro criminalità e terrorismo.

5.2. Le infrastrutture critiche

Quanto maggiore è la vulnerabilità, tanto maggiore è il rischio che possa essere sfruttata. Al centro dell'attenzione sono soprattutto le infrastrutture critiche e le tecnologie, che si basano sulla comunicazione e l'interazione.

Le infrastrutture critiche sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini e il loro

danneggiamento o distruzione avrebbe un impatto devastante, come evidenziato sin dalla direttiva 2008/114/CE[51].

La comunicazione della Commissione segnala che politiche industriali aggressive di alcuni paesi terzi, insieme agli incessanti furti di proprietà intellettuale favoriti dal digitale, stanno modificando il paradigma strategico della protezione e della promozione degli interessi europei. La crisi dovuta al COVID-19 ha altresì posto in evidenza che divisioni e incertezza sociale creano vulnerabilità sul piano della sicurezza. Ciò aumenta la possibilità di attacchi più sofisticati e ibridi da parte di soggetti statali e non statali, che sfruttano i punti deboli ricorrendo a una combinazione di attacchi informatici, danni alle infrastrutture critiche, campagne di disinformazione e radicalizzazione del discorso politico.

L'attuale quadro dell'UE in materia di protezione e resilienza delle infrastrutture critiche non è al passo con l'evoluzione dei rischi. L'accresciuta interdipendenza di settori e sistemi implica che le perturbazioni in un ambito possono avere un impatto immediato anche su altri: un attacco contro la produzione di energia elettrica potrebbe interrompere il funzionamento delle telecomunicazioni, degli ospedali, delle banche o degli aeroporti, mentre un attacco alle infrastrutture digitali potrebbe causare perturbazioni nelle reti energetiche o della finanza.

Il quadro legislativo deve far fronte all'aumento dell'interconnessione e dell'interdipendenza, con misure rigorose in materia di protezione e resilienza delle infrastrutture critiche, sia informatiche sia fisiche. I servizi essenziali, compresi quelli basati sulle infrastrutture spaziali, devono essere non solo adeguatamente protetti contro le minacce attuali e previste, ma anche essere resilienti.

Ciò comporta una serie di ulteriori interventi legislativi: oltre alla revisione delle norme vigenti per garantire un elevato livello di sicurezza delle reti e dei sistemi informatici nell'UE occorre aumentare gli investimenti in ricerca e innovazione, rafforzare le infrastrutture e le risorse internet, in particolare il sistema dei nomi di dominio.

Un elemento fondamentale per proteggere le principali risorse digitali dell'UE e nazionali consiste nel dotare le infrastrutture critiche di un canale sicuro per le comunicazioni. Al riguardo la Commissione sta collaborando con gli Stati membri per istituire un'infrastruttura quantistica "punto a punto sicura", terrestre e spaziale, associata al sistema di comunicazioni satellitari governative sicure previsto dal regolamento sul programma spaziale.

Il numero di attacchi informatici continua ad aumentare, sono sempre più sofisticati, provengono dall'interno e dall'esterno dell'UE e si incentrano sulle aree di massima vulnerabilità. Spesso vi sono coinvolti soggetti statali o attori sostenuti dallo Stato e gli attacchi sono diretti a infrastrutture digitali chiave come i principali fornitori di servizi *cloud.* I rischi informatici si stanno dimostrando una grave minaccia anche per il sistema finanziario. Il Fondo monetario internazionale ha stimato la perdita annua dovuta agli attacchi informatici al 9 % del reddito netto delle banche a livello mondiale, pari a circa 100 miliardi di USD.

5.3. Cybersicurezza e 5G

[51] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, in GUUE L 345, 23 dicembre 2008.

Il passaggio a dispositivi connessi senza dubbio comporta grandi vantaggi per gli utenti, tuttavia, con una quantità inferiore di dati conservati e trattati nei centri di dati e una quantità superiore trattata più vicino all'utente ai margini della rete (*edge*)[52] la cybersicurezza non sarà più in grado di concentrarsi sulla protezione dei punti centrali[53].

Dato il dispiegamento in corso dell'infrastruttura 5G nell'UE e la potenziale dipendenza di molti servizi critici dalle reti 5G, le conseguenze di una perturbazione sistemica e generalizzata sarebbero particolarmente gravi. Il processo avviato dalla raccomandazione della Commissione del 2019 sulla cybersicurezza delle reti 5G, di cui è prevista la revisione nell'ultimo trimestre del 2020 ha indotto gli Stati membri ad adottare interventi specifici per quanto riguarda le misure chiave stabilite nel *toolbox* per il 5G.

Una delle principali esigenze a lungo termine è lo sviluppo di una cultura della cybersicurezza fin dalla progettazione, per il quale l'elemento della sicurezza è direttamente integrato nei prodotti e nei servizi. Un importante contributo in tal senso sarà fornito dal nuovo quadro di certificazione di cui al regolamento 2019/881[54] relativo all'ENISA (Agenzia dell'Unione europea per la cybersicurezza) e alla certificazione della cybersicurezza delle tecnologie dell'informazione e della comunicazione. Il quadro peraltro è già in fase di elaborazione: due sistemi di certificazione sono in preparazione e le priorità per gli ulteriori regimi saranno definite nel corso dell'anno. Al riguardo la cooperazione tra l'Agenzia dell'Unione europea per la cybersicurezza (ENISA), le autorità preposte alla protezione dei dati e il comitato europeo per la protezione dei dati[55] è di fondamentale importanza.

5.4. Il Libro bianco sulle sovvenzioni estere nel mercato unico

A dimostrazione della stretta correlazione fra sicurezza e mercato, regolarità degli scambi e tutela dei diritti, qualche settimana prima di presentare la nuova strategia per l'Unione della sicurezza la Commissione europea ha adottato, il 17 giugno 2020, un Libro bianco[56] sugli effetti distorsivi causati dalle sovvenzioni estere nel mercato unico.

Nelle sue conclusioni del 21 e 22 marzo 2019, il Consiglio europeo aveva incaricato la Commissione di individuare nuovi strumenti per far fronte agli effetti pregiudizievoli, per il mercato e le imprese europee, delle sovvenzioni estere nel mercato unico e nella sua comunicazione del 10 marzo 2020 dal titolo "Una nuova strategia industriale per l'Europa", la Commissione aveva confermato l'intenzione di assumere tale iniziativa entro la metà del 2020.

Alla base, la considerazione che le regole di concorrenza, gli strumenti di difesa commerciale e le norme sugli appalti pubblici dell'UE svolgano un ruolo importante nel garantire

[52] L'*edge computing* è un'architettura informatica distribuita e aperta dotata di un potere di trattamento decentrato, su cui si fondano l'informatica mobile e le tecnologie dell'Internet delle cose. Nell'*edge computing* i dati sono trattati dal dispositivo stesso o da un computer o un server locale, anziché essere trasmessi a un centro dati.

[53] Così la Comunicazione su una strategia europea per i dati, COM(2020) 66 final

[54] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)

[55] Comunicazione sulla protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, COM(2020) 264 final

[56] Libro bianco relativo all'introduzione di pari condizioni di concorrenza in materia di sovvenzioni estere, 17 giugno 2020 COM(2020) 253 final

condizioni eque per le imprese nel mercato unico. Il problema risiede nel fatto che mentre le sovvenzioni degli Stati membri sono soggette alle norme UE sugli aiuti di Stato al fine di evitare distorsioni, quelle concesse da governi di paesi terzi a imprese nell'UE hanno un impatto negativo, in quanto alterano le normali condizioni di mercato e falsano la concorrenza, ma sfuggono al controllo previsto dalle regole in tema di aiuti di Stato UE. Sono sempre più numerosi i casi in cui si ritiene che le sovvenzioni estere abbiano facilitato l'acquisizione di imprese dell'UE o falsato decisioni di investimento, operazioni di mercato o politiche tariffarie dei beneficiari oppure la partecipazione a gare d'appalto pubbliche, a scapito delle imprese non sovvenzionate.

Inoltre le norme di difesa commerciale vigenti si applicano solo alle esportazioni di beni da Paesi terzi, e quindi non coprono tutte le distorsioni causate dalle sovvenzioni estere concesse dagli stessi.

Il Libro bianco propone pertanto nuovi strumenti di intervento prospettando diversi approcci. Le prime tre opzioni (i cosiddetti "moduli") mirano a contrastare gli effetti distorsivi causati dalle sovvenzioni estere nel mercato unico in generale (modulo 1), nelle acquisizioni di imprese dell'UE (modulo 2) e durante le procedure di appalto pubblico dell'UE (modulo 3). In merito alle varie opzioni previste è stata avviata una consultazione pubblica che si è conclusa il 23 settembre 2020; sulla base dei pareri e contributi pervenuti la Commissione presenterà a breve adeguate proposte legislative.

Conclusione

1. In base agli elementi conoscitivi di cui si dispone (la decisione TIM-Huawei non è stata pubblicata) e alle considerazioni che precedono, risulta come nel caso di specie siano configurabili, a tutela della sicurezza della rete 5G di TIM, tre successive fasi di verifica e controllo, secondo il percorso procedimentale delineato dal decreto ai sensi delle norme sul *Golden Power.*

La prima, demandata all'amministrazione (nella specie il Ministero dello sviluppo economico che ha svolto l'istruttoria e la Presidenza del Consiglio dei Ministri, che ha assunto la decisione su conforme deliberazione del Consiglio dei Ministri) sulla base della documentazione che le è stata sottoposta; la seconda a TIM ed in particolare alla sua funzione *Security,* in sede di applicazione del decreto e degli adempimenti da esso previsti; la terza ancora all'amministrazione, che dovrà esaminare le relazioni periodiche di TIM e potrà decidere, se del caso, di far venir meno l'autorizzazione ove ritenga che non si sia ottemperato alle prescrizioni o in caso di sopraggiunti rischi alla sicurezza.

2. Le prescrizioni contenute in decreto sono riconducibili allo strumentario previsto dal *Toolbox* del 29 gennaio 2020 e appaiono di per sé corrette dal punto di vista giuridico, fermo restando che solo all'esito delle verifiche, degli interventi e della vigilanza sulle attività di *operation and maintenance*, ad opera della funzione *Security,* sarà possibile valutare l'adeguatezza e la congruità delle specifiche misure tecniche di mitigazione adottate in rapporto alla valutazione dei rischi.

3. Una delle prescrizioni (articolo 1, lett. h) attiene alla valutazione del rischio del fornitore, vale a dire la possibilità che lo stesso sia soggetto a interferenze di un paese extra UE. Huawei Technologies Italia s.r.l. è una società di diritto cinese controllata dal gruppo Huawei Technologies Co. che, ancorché stabilita giuridicamente in Italia, è tenuta al rispetto della legislazione cinese, fra cui la citata legge sulla sicurezza del 2016 che impone di

collaborare con i servizi di sicurezza statale per raccogliere informazioni senza rivelare tale collaborazione.

Tale aspetto è qualificato dal *Toolbox* europeo come criterio di tipo strategico-regolamentare e costituisce uno dei suoi elementi qualificanti e rilevanti, alla luce delle delicate implicazioni di sicurezza della rete 5G. Si tratta in sostanza della possibilità di poter valutare una fornitura non solo in base alla sua adeguatezza tecnica ma anche alle caratteristiche del contraente, desunte dal regime giuridico al quale è sottoposto.

Con riferimento a tale delicato profilo, il decreto prevede l'obbligo di integrare il contratto con clausole che stabiliscano, a pena di risoluzione espressa ai sensi dell'articolo 1456 del codice civile, l'obbligo per i fornitori e le società a non comunicare ad autorità governative estere o comunque a terzi dati e informazioni comunque acquisiti in relazione all'operazione notificata.

La stessa prescrizione impone a TIM (tenuta ad assicurare l'integrità della propria rete ai sensi delle norme in tema di comunicazioni elettroniche) di vigilare sul comportamento dell'operatore cinese al fine di rilevare eventuali violazioni, all'esito delle quali potrà scattare la risoluzione del contratto, con la possibilità per l'amministrazione di vietare l'operazione, in base alla rilevata inaffidabilità del contraente.

4. Quanto evidenziato induce a segnalare l'opportunità che il *Toolbox* sia integrato con la previsione di un sistema centralizzato a livello UE di segnalazione e raccolta delle violazioni degli obblighi strategico-regolamentari da parte dei fornitori extra UE, su comunicazione da parte delle varie autorità nazionali. Tale sistema potrebbe prevedere l'istituzione una *Black List* in cui inserire i fornitori a carico dei quali sono state rilevate le violazioni. In tal modo le autorità nazionali saranno in grado di conoscere e valutare *ex ante* i profili di rischio e affidabilità di un determinato soggetto su base pan-europea e adottare i conseguenti provvedimenti di esclusione o veto, a beneficio della certezza del diritto e della tenuta giuridica della decisione finale.

Roma, 15 novembre 2020