COMMISSIONE IX
TRASPORTI, POSTE E TELECOMUNICAZIONI

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

19.

SEDUTA DI MERCOLEDÌ 17 LUGLIO 2019

PRESIDENZA DEL PRESIDENTE **ALESSANDRO MORELLI**

INDICE

PAG.

Sulla pubblicità dei lavori:

Morelli Alessandro, *Presidente* 3

INDAGINE CONOSCITIVA SULLE NUOVE TECNOLOGIE DELLE TELECOMUNICAZIONI, CON PARTICOLARE RIGUARDO ALLA TRANSIZIONE VERSO IL 5G ED ALLA GESTIONE DEI *BIG DATA*

Audizione di rappresentanti di Huawei Italia:

Morelli Alessandro, *Presidente* 3, 10, 11, 19, 20

PAG.

Capitanio Massimiliano (Lega) 11

De Vecchis Luigi, *presidente di Huawei Italia* . 3, 7, 8, 12, 14, 16, 19, 20

Mollicone Federico (FdI) 11, 19

Pignari Giuseppe, *responsabile tecnologia e sicurezza di Huawei Italia* ... 4, 7, 12, 13, 15, 16

Romano Paolo Nicolò (M5S) 10

Zanella Federica (FI) 10, 13

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Partito Democratico: PD; Forza Italia - Berlusconi Presidente: FI; Fratelli d'Italia: FdI; Liberi e Uguali: LeU; Misto: Misto; Misto-Civica Popolare-AP-PSI-Area Civica: Misto-CP-A-PS-A; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Noi con l'Italia-USEI: Misto-NcI-USEI; Misto-+Europa-Centro Democratico: Misto-+E-CD; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE; Misto-Sogno Italia - 10 Volte Meglio: Misto-SI-10VM.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE ALESSANDRO MORELLI

La seduta comincia alle 15.15.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione di rappresentanti di Huawei Italia.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G e alla gestione dei *big data*, l'audizione di rappresentanti di Huawei Italia.

Ringrazio il dottor De Vecchis, presidente di Huawei Italia, per aver accettato l'invito della Commissione e gli do la parola per lo svolgimento della propria relazione.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Buon pomeriggio a tutti. Grazie, presidente. Noi faremo una breve presentazione, che sarà divisa in due parti. Una prima parte è per condividere con voi le dimensioni dell'azienda nella quale operiamo e quali sono i nostri obiettivi. La seconda parte sarà più di natura tecnica e affronteremo i concetti di rete 5G e dell'evoluzione verso la trasformazione digitale, che di fatto si presenta più ampia del contesto 5G, come spiegheremo durante la presentazione. In ultimo, abbiamo predisposto uno schema riassuntivo delle principali tematiche che vi sottoponiamo nel nostro intervento, in maniera tale che possa essere eventualmente oggetto di discussione successiva.

Partirei con la presentazione parlando innanzitutto delle caratteristiche generali dell'azienda. L'azienda è un gruppo multinazionale che conta oggi quasi 190.000 persone nel mondo. La caratteristica importante del gruppo è che 80.000 di queste persone sono nella componente ricerca e sviluppo, divise su quattordici centri di ricerca e sviluppo nel mondo, di cui otto sono in Europa e in particolare uno in Italia. L'azienda è presente in 170 Paesi nel mondo e in questi Paesi i primi 50 grandi operatori sono clienti del gruppo.

In questi anni, se noi guardiamo la conoscenza del *brand*, Huawei ha raggiunto la sessantottesima posizione, scalando decine di posti ogni anno, e nell'ambito del Fortune 500 è la settantaduesimo nella classifica. Il fatturato dell'anno appena trascorso è di oltre 105 miliardi di euro. Stiamo dando semplicemente delle informazioni *flash*, presidente, non vogliamo fare una descrizione del gruppo troppo dettagliata.

La crescita degli investimenti in ricerca e sviluppo rappresentano effettivamente il fattore che ha portato l'azienda a diventare *leader* a livello mondiale: l'azienda, che nasce circa 30 anni fa, ha sviluppato a oggi a livello mondiale circa 90.000 patenti, di cui 43.000 autorizzate in Cina e oltre 44.000 autorizzate a livello mondiale e fuori della Cina.

Questo è un fatto particolarmente importante, poiché i brevetti sono condivisi tra tutta la filiera delle telecomunicazioni. Noi usiamo quelli dei nostri *competitor*-colleghi, così come i nostri brevetti sono

utilizzati da altri, quindi le macchine che noi vediamo in campo sono macchine di fatto « ibride », poiché sono l'insieme di più tecnologie.

In Italia la situazione è questa. Noi oggi abbiamo una struttura di circa 800 persone, l'85 per cento delle quali sono italiane. Lo stesso discorso vale a livello europeo, dove siamo circa 12.000 e il numero è un po' più basso, però siamo sempre nell'ordine dell'80 per cento. In Italia l'azienda ha un centro di ricerca e sviluppo a Milano, dove si studiano principalmente ponti radio e onde millimetriche. Le onde millimetriche sono quelle caratteristiche onde che consentono di arrivare a coprire tutto il territorio, ovvero, per chi è familiare con il concetto di ultimo miglio, per collegare case, abitazioni, imprese e persone nelle aree remote.

Ci sono quattro centri per l'innovazione. Tra questi uno dei più importanti è quello situato nella regione Sardegna. La regione Sardegna, sulla base di un accordo stipulato con l'azienda, sviluppa i sistemi di *smart and safe city*. Abbiamo diversi *business innovation center* che sono stati realizzati con gli operatori e che guardano le varie tecnologie di telecomunicazione in campo.

In Italia normalmente l'azienda investe, spende o compra prodotti e rapporti con terze parti, incluse le attività che vengono svolte con le università italiane, per circa 450 milioni. Collaboriamo con circa 20-25 università italiane. Proprio l'altra mattina a Milano il nostro amministratore delegato ha annunciato un piano di investimenti di circa 3 miliardi di dollari, che corrispondono a 2,7 miliardi di euro nei prossimi tre anni.

Passo alla seconda parte ed in particolare ad illustrare alcuni aspetti fondamentali che riguardano l'importanza della trasformazione digitale. Ogni 20 per cento di investimento nell'economia digitale si trasforma in una crescita dell'1 per cento del PIL. Gli investimenti hanno un ritorno di circa sei volte e mezzo maggiore di quello dell'economia tradizionale e la crescita dell'economia digitale è di circa due volte e mezzo superiore all'economia tradizionale.

Questo è un fatto importante e nell'ambito delle agende digitali dei vari Paesi nel mondo, l'Italia ha avuto un impulso superiore a tutti gli altri Paesi europei, soprattutto con la partenza dei famosi *trial* che sono stati realizzati in tre aree importanti del Paese: Bari e Matera, Prato e L'Aquila e Milano. In queste aree quello che è importante è che c'è stata una prima vera combinazione tra pubblico e privato, che ha creato un mini ecosistema per far capire cosa significa trasformazione digitale, di cui il 5G, come vedremo, è uno dei fattori abilitanti, ma non il solo.

Ci troviamo di fronte a una situazione *disruptive* – scusate l'inglese – rispetto al passato. Questa nuova rivoluzione industriale, che viene paragonata alle precedenti, partendo dal vapore, dall'elettricità e dall'introduzione dell'*information technology*, in realtà avrà un impatto importantissimo sulla sostenibilità di varie aree pubbliche e private. Mi riferisco, per esempio, alla sanità, dove oggi sappiamo benissimo che i costi non sono più sostenibili considerando il numero delle persone che cresce e le disabilità che aumentano. Ci sono nuovi impulsi ovviamente nella crescita, come abbiamo visto prima. L'esempio più importante riguarda in particolare le città intelligenti, dove tutto il caos odierno, che riguarda ovviamente il traffico, la manutenzione, i parcheggi e la viabilità, potrà essere indirizzato e risolto con queste nuove tecnologie.

Ho finito questa parte introduttiva. Mi riprometto intervenire di nuovo successivamente e passo ora la parola all'ingegner Pignari, che parlerà delle tematiche più strettamente tecnologiche.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Grazie a tutti, buongiorno. Mi chiamo Giuseppe Pignari e sono responsabile tecnologia e sicurezza in Huawei Italia. Come ha detto già l'ingegnere De Vecchis, il 5G è un fattore abilitante di significativi benefici economici e sociali. Il 5G, a differenza delle tecnologie che abbiamo visto nel mondo delle telecomunicazioni mobili fino a oggi (il 2G prima, il 3G e il 4G), nasce e viene concepito negli ambiti di standardizzazione

internazionale proprio per indirizzare una nuova catena del valore e per permettere uno sviluppo dell'economia.

Dai dati elaborati dalle società di analisi e nell'ambito della comunità che studia questo fenomeno sappiamo che da qui ai prossimi dieci-quindici anni l'impatto riguarderà numeri molto importanti. In particolare sappiamo che sono tre i principi cardine, le tre aree su cui il 5G si sta sviluppando. Partiamo da quella che tutti conosciamo molto bene, che è quella che abbiamo utilizzato fino adesso, ovvero il *mobile broadband*, le connessioni sui nostri telefoni, sui nostri *smartphone*, su quello che facciamo tutti i giorni. In questo settore avremo un salto di un fattore dieci in termini di velocità, che andrà ad abilitare un'altra serie di applicazioni di realtà aumentata, di *virtual reality*, di video in tre dimensioni, grazie al fatto che potremo disporre mediamente di bande intorno a 700-800, fino a un gigabit al secondo, sui nostri dispositivi. Tenete conto che oggi nel 4G, quando va bene, parliamo di 70-80-100 megabit, quindi c'è veramente un fattore dieci che andrà ad abilitare applicazioni fino a oggi non immaginabili.

Vi sono in particolare due nuove aree che sono le cosiddette « comunicazioni ad altissima affidabilità e bassa latenza », che andranno ad abilitare una serie di applicazioni nell'ambito dei *connetted vehicles*, della gestione dei droni, dello *smart manufacturing* e quant'altro. La seconda area, invece, riguarda quello che tutti conosciamo come l'*internet of things* e le *massive machine-type communication*: sensoristiche sparse sul territorio per le *smart city*, con una densità di sensori che crescerà di un fattore mille probabilmente rispetto alla data odierna.

Il 5G è stato concepito proprio per soddisfare un numero di requisiti molto più ampio rispetto a quelli del 4G. Tuttavia, tengo a dire che il 5G è un fattore abilitante, ma non è solo tramite il 5G che potremo ottenere tutto questo. Infatti, quello che è stato fatto nei *trial* di Milano e di Matera qui in Italia è stato un esperimento a mio giudizio molto interessante, perché ha mostrato come per costruire questa applicazione siano necessari decine di *partner*. Non è più come in passato una questione tra operatore e *vendor* di tecnologia, come può essere Huawei o un nostro *competitor*, ma bisogna mettere insieme un bacino di competenze molto ampio. Si pensi al trasporto intelligente, dove ovviamente il 5G diventa la tecnologia abilitante, ma bisognerà poi costruire le applicazioni insieme a chi si occupa del settore specifico del trasporto. La stessa cosa vale per tutti gli altri ambiti applicativi.

Questo è un messaggio che ci tengo a condividere: il 5G è una tecnologia abilitante, ma, se vogliamo veramente scatenare il suo effetto benefico sull'economia del Paese, dobbiamo capire che questo deve essere fatto attraverso un ecosistema di *partner* che va oltre il semplice operatore e *vendor*, bisogna tirare in ballo un'altra serie di *player* che prima non erano in gioco.

Adesso entro più nell'ambito del 5G, per dare un messaggio molto forte: il 5G, come tutte le tecnologie mobili, nasce da uno sforzo di standardizzazione a livello mondiale.

C'è un gruppo che probabilmente avrete sentito nominare, che si chiama 3GPP (*Third generation partnership project*), che nasce all'inizio degli anni 2000, quando si standardizza la tecnologia 3G. A questo gruppo partecipano tutti i maggiori operatori mondiali, tutti i maggiori fornitori, gli enti di ricerca e gli enti governativi. Quando uno *standard* viene approvato nell'ambito di questo gruppo, si può dire che è stato analizzato in profondità da tutta la comunità tecnico-scientifica internazionale. Questa è anche la ragione per cui questo mondo così complesso, tutte le apparecchiature, dai telefoni ai dispositivi che noi mettiamo nelle reti e alle applicazioni, possono lavorare in collegamento in maniera semplice.

Come vedete, il 5G non è uno *standard* concluso, ma è uno *standard* in evoluzione. Le prime versioni si sono avute a fine 2017, poi nel 2018 e il processo sta comunque continuando, proprio per affinare e abilitare quella serie di applicazioni innovative di cui accennavo prima.

C'è un secondo concetto che terrei a sottolineare: la transizione verso il 5G. Il 5G vivrà due fasi sostanzialmente. La prima è la cosiddetta « *non-stand-alone* » ed è quella che attualmente gli operatori e anche lo *standard* hanno maggiormente definito e che, come vedete, andrà a utilizzare appieno tutto l'installato esistente della parte 4G e 4,5G, sia come rete di accesso, sia per la cosiddetta « rete *core* », la rete che governa tutta la parte di servizi.

Gli operatori che hanno investito finora nel 4G e nel 4,5G potranno ottimizzare i loro investimenti in una prima fase semplicemente aggiungendo un nuovo tipo di accesso radio, che darà immediatamente la possibilità di sfruttare le frequenze che loro hanno acquisito l'anno scorso durante l'asta e di cominciare a monetizzare i primi servizi, che saranno ancora di tipo tradizionale. Mi riferisco alla banda più ampia e all'accesso alle aree rurali tramite applicazioni che si chiamano « *fixed wireless access* ». Si tratta di fornire in quelle aree dove la fibra non arriva, un accesso che questa volta è veramente a larga banda, perché stiamo comunque parlando di disponibilità di un gigabit al secondo, valori confrontabili con la fibra. Questo permetterà intanto di stimolare lo sviluppo della rete.

Si arriverà poi – ma questo dipenderà molto dal mercato, dagli operatori, dalla disponibilità di investimento – a quella che chiamiamo « fase *stand-alone* », dove ci sarà una nuova *core* 5G, che sarà quella che andrà ad abilitare quei famosi servizi di cui parlavo prima, ovvero i servizi verticali, *massive* IOT (*internet of things*) e così via.

Credo che questo sia un concetto estremamente importante da tenere presente, perché tutto questo è stato concepito in ambito normativo proprio per facilitare lo sviluppo della rete 5G e non costringere gli operatori a investimenti massivi per rifare la rete nella sua totalità.

La sicurezza è un tema che non scopriamo oggi. La sicurezza è un tema che nasce da quando è nato il primo computer e da allora ha continuato a evolvere, sia nelle reti sia nei sistemi IT. Il 3GPP ha cominciato il suo percorso, come dicevo, molti anni fa con il 3G per il quale si è già cominciato a introdurre criteri di sicurezza ed è andato avanti col 4G dove questi criteri sono stati decisamente migliorati. Il 5G a sua volta continuerà su questo percorso già iniziato, facendo tesoro di tutte le esperienze passate, perché ovviamente c'è un grande bagaglio di esperienza che noi come *vendor*, gli operatori e tutti hanno accumulato negli anni con le tecnologie precedenti.

Tutto questo verrà riversato o è già stato riversato nella *release* 15, che è la *release* corrente, e verrà riversato via via nelle *release* successive, per rendere sempre più sicuri e sempre più robusti i meccanismi di sicurezza.

Questi meccanismi, come ho detto prima, sono *standard*, non sono inventati né da Huawei, né da Nokia, né da Ericsson né da nessun altro. Derivano da un comitato internazionale ampio, come dicevo prima, sono analizzati e una volta che escono approvati si ha la garanzia che siano veramente robusti e a prova di attacco.

Questo è il modo in cui noi schematizziamo la rete e qui vorremmo vedere quali sono le aree che possono essere più critiche per la *cyber security*. A grandi linee noi distinguiamo tre domini nella rete. Il primo è il dominio della rete di accesso, che riguarda la connessione dei nostri dispositivi mobili oggi e di tutti i nuovi dispositivi che vedremo in futuro, dai sensori ai visori per la *virtual reality*, ai robot industriali e quant'altro, che si connettono alla rete radio. In questa parte di rete noi vediamo un rischio rispetto alla vulnerabilità abbastanza ridotto, perché uno può attaccare uno o due dispositivi, ma non può creare grossi danni alla rete, in quanto verrebbe immediatamente bloccato dai sistemi dell'operatore.

Nella parte di rete di trasporto, che è la rete che raccoglie tutti i flussi di informazione delle stazioni radio e degli utenti e le trasporta verso la rete *core*, il traffico viaggia in maniera aggregata, non c'è nessuna cognizione dell'identità dell'utente e in ogni caso la maggior parte degli operatori usano anche in questo segmento di rete tecniche

di crittografia per rendere molto improbabile la possibilità di un attacco.

Infine, abbiamo il dominio critico della rete, quello che chiamiamo « il dominio della rete *core* » e di tutti gli strumenti OM che gli operatori usano per configurare i servizi sulla rete *core*. È chiaro che questo è il cuore della rete, come dice la parola stessa, e va molto ben protetto. Come vedete, ho evidenziato i dispositivi che chiamiamo « *firewall* », perché tutti gli operatori, ben consci ormai della necessità di proteggere la loro rete *core,* introducono sistemi di prevenzione, identificazione e mitigazione degli attacchi che possono provenire dalla rete internet. C'è una grande esperienza ormai nel proteggere questa parte di rete.

La protezione, quindi, si articola su due livelli, come vedremo: la protezione che mettiamo all'interno delle componenti di *software* che regolano la rete *core*, come ci prescrive lo *standard*, e in più dei bastioni, delle porte tagliafuoco, che impediscono l'accesso a questi elementi molto importanti.

Sulla rete *core* ho già detto le motivazioni che ci spingono a dire che questa è veramente la rete sulla quale bisogna concentrare tutti gli sforzi e il 3GPP in questo senso sta standardizzando una serie di criteri, processi, procedure e protocolli che permettono di irrobustire, anche rispetto al passato, questa parte della rete.

Vorrei spendere, invece, qualche parola in più per far capire come la sicurezza in realtà non sia un qualcosa che è limitato al 5G, ma va vista in un'ottica, come diciamo noi, « *end to end* ». Il mondo oggi è composto da tre grossi *player*. Ci sono gli operatori di telecomunicazioni, che sono responsabili di sviluppare la rete di telecomunicazione: progettazione, servizi, sicurezza. Ovviamente controllano i dati dei loro utenti e hanno tutte le chiavi di criptazione di cui parlavamo in precedenza. Loro sono i depositari delle chiavi di criptazione, che cambiano nel tempo proprio per rendere sempre più sicura la rete e ridurre la possibilità di un attacco. Dalla parte opposta abbiamo gli *over-the-top*, quelli che siamo abituati a usare tutti i giorni: Google, Amazon, Facebook, Netflix, che si connettono alle reti degli operatori per dare modo ai loro clienti di accedervi. Infine, ci sono i *vendor*, coloro che forniscono la tecnologia degli apparati di rete.

Noi forniamo le scatole e forniamo la competenza. Ogni operatore, come voi sapete, non si rifornisce da un unico *vendor*, ma tipicamente utilizza diversi *vendor* e, quindi, la progettazione della rete è un compito prettamente suo, perché deve fare in modo che tutto l'insieme degli apparati che lui ha selezionato per costruire la sua rete lavorino. Noi non possediamo i dati, non possediamo le chiavi di criptazione, non operiamo la rete, in quanto la rete è fatta da una molteplicità di *vendor* diversi.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Faccio una velocissima chiosa. Innanzitutto all'interno di una rete nessun operatore ha i dati dell'utente, ma i dati dell'utente per tutte le attività a latere (la fatturazione, il riconoscimento e altre cose) sono su sistemi totalmente separati, quindi sulla rete non c'è nulla, anche se fosse acceduta in un'ipotesi remota, da andare a leggere. Sono semplicemente delle parole, delle aree crittografate, con dei valori numerici che sono assolutamente irriconoscibili.

Da quest'altra parte gli OTT (*over-the-top*) hanno ovviamente accesso alla rete per consentire i collegamenti, ma tutta la parte dati e la profilazione degli utenti viene fatta in casa propria. Per esempio, Amazon ha i propri *cloud* e *data center* che sono sparsi per il mondo. Quelli non hanno nulla a che vedere con la rete di telecomunicazione.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Vorrei sviluppare ancora questo concetto, per far capire bene come la sicurezza vada veramente affrontata su tutta la filiera.

In basso ci sono i fornitori di apparati, che devono garantire ovviamente la sicurezza dell'apparato singolo: confidenzialità, integrità, disponibilità e tracciabilità. Sopra c'è l'operatore che, acquisendo appa-

rati di diversi *vendor*, costruisce la propria rete; 5G, 4G o quant'altro nulla cambia. Sopra, invece, cambierà qualcosa, perché avremo una molteplicità di fornitori di applicazioni, oltre agli *over-the-top* che conosciamo oggi, che svilupperanno applicazioni per i segmenti verticali, per l'*automotive*, per l'*energy* e per l'*entertainment*.

Tutto questo mondo effettivamente deve essere regolamentato e deve seguire delle precise regole, perché una qualunque lacuna in uno di questi punti può mettere in crisi la sicurezza dell'intero sistema. Io fornisco la cassaforte più blindata che posso, dopodiché però, se tu mi lasci il codice segreto sulla credenza di casa, tutto casca. Qui è lo stesso: o tutti seguiamo le stesse regole, o tutti adottiamo le *best practice* di sicurezza, oppure, se qualcuno non le adotta, alla fine tutta la catena cade.

Questo credo che sia un concetto estremamente importante, che va capito, perché mi pare che fino a oggi ci sia stata una focalizzazione forse eccessiva sul 5G come tecnologie di comunicazione mobile, perdendo un po' di vista il fatto che la sicurezza deve essere veramente affrontata *end to end*. Non è il singolo apparato del venditore *x* o del venditore *z* che può mettere in crisi una rete, ma se tutta la filiera non segue questi criteri di sicurezza.

La sicurezza è un concetto globale, non è limitata al 5G. Credo che le reti mobili, per la storia che abbiamo visto negli ultimi 30 anni, siano quelle che hanno il maggior grado di standardizzazione in tutti i settori della tecnologia. In effetti, sulle reti in quanto tali non si sono mai riscontrati grossissimi problemi.

Noi serviamo, come ha detto prima il dottor De Vecchis, 50 tra i *top operator* nel mondo. Questi operatori ogni volta che noi rilasciamo una *release* eseguono migliaia di test sui nostri apparati e in 20-30 anni di cooperazione non è mai venuto fuori nulla, perché noi stiamo seguendo degli *standard* estremamente rigorosi.

Vorrei chiudere illustrando come noi garantiamo la sicurezza degli apparati di rete. Noi abbiamo già deciso molti anni fa, nel 2010, di sviluppare un processo integrato di sviluppo dei nostri prodotti, in cui la sicurezza viene inserita e tenuta in considerazione in ciascuno di questi *step*, dal concepimento del prodotto alla sua messa in pianificazione, dallo sviluppo al processo di certificazione di qualità, dal lancio commerciale alla gestione del ciclo di vita. Abbiamo messo in piedi una serie di *best practice*, di strumenti e di *team* indipendenti che vanno a verificare che i nostri ingegneri softweristi che scrivono il codice dei nostri apparati lo facciano seguendo le più strette regole e le *best practice* mondiali.

Eseguiamo *penetration test*. Ciò vuol dire che ci sono dei *team* all'interno della nostra organizzazione, completamente segregati rispetto ai *team* che sviluppano, che prendono i nostri prodotti come fossero una scatola nera e agiscono – lasciatemi usare questa parola – un po' come *hacker*, andando a verificare che non siano rimaste delle vulnerabilità dentro il codice.

Se troviamo dei problemi in fase di progetto oppure durante il ciclo di vita interveniamo. Ovviamente può succedere, le vulnerabilità non possono essere eliminate, così come non possono essere eliminati i bachi dentro il *software*, lo sappiamo molto bene. Se un nostro operatore o un nostro cliente ci segnala un problema, questo problema viene indirizzato, viene risolto e viene reinserito nella libreria dei problemi da indirizzare nella prossima *release*.

Spero di essere stato chiaro e di non essere andato troppo veloce. Lascio ancora la parola al presidente De Vecchis.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Riprendendo il tema, che è già stato affrontato dal mio collega, vorrei soffermarmi ancora sull'architettura della rete di un operatore. Da una parte abbiamo il sistema che l'operatore utilizza per il controllo e il monitoraggio della rete. Possiamo distinguere da una parte l'accesso, quindi gli utenti terminali, ma anche la componente IOT e altre tipologie di applicazioni.

Sottolineo questo per dire che innanzitutto da questo punto di vista io ho due accessi al sistema di telecomunicazione: uno è *wireless*, ovviamente se mi trovo in

una condizione di non presenza di reti *wi-fi* o fibra, l'altro è proprio *wi-fi* o fibra, che è un percorso totalmente diverso da questo. Il sistema che chiamiamo « O&M » (*operation and management system*) non è altro che il sistema che gli operatori usano per controllare dal punto di vista tecnico la funzionalità ed eventuali criticità nei percorsi, quindi la rottura e la manutenzione dei dati, ma anche i flussi di dati.

Quello che è importante è che l'operatore riconosce perfettamente a ogni domanda che viene fatta alla rete il flusso che viene generato. Non appena un flusso parte in maniera spontanea, questo sistema lo riconosce e di conseguenza riconosce che non è una richiesta di questo tipo, per cui abbatte totalmente quel tipo di funzione. Io credo che l'abbiano già spiegato bene i colleghi operatori.

L'ultima osservazione che vorrei fare è che noi, che siamo purtroppo del settore delle telecomunicazioni, disegniamo questo aspetto della rete di telecomunicazioni come se fosse effettivamente il sistema globale. In realtà, se lo stesso schema fosse stato fatto da uno dei nostri colleghi di internet, come Google, Amazon o uno degli OTT, avrebbe messo al posto di questa parte di disegno la nuvola, quindi avrebbero descritto bene il loro funzionamento.

Qui dentro c'è tutto quel mondo in cui in realtà, essendo interconnesso e non derivando da sistemi di standardizzazione come i comitati di cui il collega ha parlato, ciascuno sviluppa, probabilmente anche in modo migliore del comitato ma non in modo armonico, sistemi di protezione del proprio sistema.

I dati di questi signori sono all'interno della nuvola. Nuvola significa ovunque nel mondo. Per esempio, prendo il dato di un *WhatsApp* quando mando un'immagine da un utente ad un altro utente di questa rete. Io ho la foto che è crittografata, questa foto entra in questa rete, come se entrasse un passeggero su un vagone. Il treno partirebbe, consegnerebbe all'indirizzo finale che sta all'interno di questa rete quel dato crittografato che questo sistema non è in grado di riconoscere e ovviamente ciò che accade al termine di questo viaggio non è competenza di questa parte della rete.

In conclusione, possiamo dire che il concetto fondamentale di cui abbiamo parlato è che il 5G è il fattore abilitante per la trasformazione digitale, ma ha bisogno di un ecosistema, come diceva prima il collega, ovvero di altri attori che sviluppano le applicazioni.

Per esempio, abbiamo parlato di guida autonoma. Lì ci sono delle realtà che non sono ovviamente le aziende e le società di telecomunicazioni né tantomeno noi, perché non abbiamo quella competenza, le quali si collegano a questi sensori che abbiamo visto e, attraverso questa rete o attraverso la rete fissa, generano tutte le applicazioni e le caratteristiche per consentire la guida sicura. Qui ancora una volta la componente telecomunicazioni avviene soltanto per trasportare un dato da un luogo ad un altro.

L'altro fatto che è emerso è che il 5G si appoggia sulle reti 4G e 4,5G esistenti, quindi la prima *release* poggia su queste reti già esistenti. Noi abbiamo una presenza sul mercato che è abbastanza ampia. Insieme ai nostri colleghi di ZTE abbiamo circa il 40 per cento del mercato a livello europeo. Senza la rete 4G, gli operatori sarebbero costretti a sostituire tutti questi apparati, quindi il costo della realizzazione della rete 5G dovrebbe includere anche la sostituzione di queste tecnologie. La GSM *Association* ha stimato che a livello europeo il costo per gli operatori, se dovesse accadere una discriminazione sulla presenza di *vendor* come la società che rappresentiamo, sarebbe di 55 miliardi di euro.

Abbiamo visto anche che in tutto questo mondo interconnesso, che va dalla parte di accesso fino a internet, attraversando tutta la rete, la *cyber security* è una questione globale che per quanto ci riguarda è definita in maniera ordinata soltanto su questa componente. Non conosciamo quello che accade da quest'altra parte. Tutti gli *standard* delle reti TLC mobili nascono da questo comitato di standardizzazione: il 3GPP, la GSMA, l'ITU e l'IETF. Recentemente per quanto riguarda il 5G c'è stata la nascita del 5GPP, che si occupa di estendere e di

incrementare tutto quanto già fatto nelle precedenti reti verso le nuove. Abbiamo detto che non conosciamo quello che accade nell'altra componente.

La sicurezza è un fatto incrementale. Io porto con me ogni tecnologia nuova che arriva, tutto ciò che ho già fatto, quindi non perdo assolutamente niente. Di conseguenza, se una rete 4G è sicura, non vedo perché una rete 5G che poggia sulla 4G debba avere dei problemi.

Un'ulteriore questione che è emersa riguarda il fatto che un'emarginazione del *vendor* cinese nel mercato EU, come abbiamo detto prima, avrebbe un costo per gli operatori di circa 55 miliardi. Non esageriamo se diciamo che in Italia costerebbe 15 miliardi, quindi il 20 per cento di questa componente o forse di più.

L'altra cosa importante che abbiamo visto durante la presentazione è che la trasformazione digitale comporta un incremento nel PIL del Paese in un *range* di valori che va dall'1 al 2,5 per cento. In Italia voi sapete che un punto percentuale di PIL vale circa 20 miliardi, quindi ogni anno di ritardo bisogna vedere esattamente a posteriori quant'è il costo effettivo.

L'ultima osservazione, e forse quella più importante per noi, è che attualmente, da quello che abbiamo compreso, il quadro normativo sul *golden power* che va delineandosi rischia effettivamente di mettere Huawei in una posizione di difficoltà tale da discriminarla dalla competizione.

Abbiamo concluso. Siamo a vostra disposizione per le eventuali domande.

PRESIDENTE. Grazie. Do la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

FEDERICA ZANELLA. Mi scuso. Io purtroppo avevo un impegno precedente, quindi non ho seguito tutta la presentazione, però da quello che ho evinto voi avete puntato molto sul tema della sicurezza, anche perché necessariamente siete oggetto di grande attenzione sotto questo profilo, anche per le note vicende americane.

Nel vostro intervento giustamente avete fatto riferimento al fatto che voi siete stati oggetto di particolari verifiche e che non sono state trovate falle nel corso degli anni. Tuttavia, è di un paio di mesi fa uno *scoop* di Bloomberg, se non erro, sulla vicenda che riguarda Vodafone, che è la più grande compagnia di telecomunicazioni europea, che ha spiegato di aver identificato una vulnerabilità presente nei vostri *router* domestici a partire dal 2011.

Il capo della sicurezza informatica di Vodafone ha sottolineato come ci fosse stata preoccupazione per il vostro comportamento, perché, dopo aver detto che avreste rimosso il codice, avete rifiutato di rimuoverlo per questioni legate alla qualità del prodotto. Hanno scoperto che in realtà queste *backdoor* che erano state trovate non erano state rimosse prontamente, col rischio che un soggetto terzo potesse aver avuto informazioni e quant'altro. Sotto questo profilo, voi cosa potete fare per assicurare che, in concreto, non ci possano essere più eventi di questo tipo, non ci possano essere *backdoor* da cui potrebbero accedere terzi ? Sempre il responsabile della sicurezza di Vodafone ha detto che non ci sono state prove di accessi non autorizzati, ma è ovvio ed evidente che la cosa crea tensione, anche perché credo sia fondamentale per noi, soprattutto in prospettiva del 5G, capire di cosa stiamo parlando e con chi abbiamo a che fare. Voi avete fatto, giustamente, riferimento alla normativa sul *golden power*, che vi penalizzerebbe, però è ovvio che il *background* genera più attenzione sul vostro *brand*.

In secondo luogo, non so se abbiate fatto distinzioni o ne abbiate parlato, però ho sentito che avete parlato di *core*, quindi di rete. Voi fate una distinzione tra *core* e *edge*. Secondo molti che si occupano di sicurezza, un singolo punto di debolezza pregiudica la sicurezza dell'intera rete, sia che si parli di *core* sia che si parli di *edge*. Vorrei capire quali sono i vostri progetti e che cosa potete dirci in merito.

PAOLO NICOLÒ ROMANO. Ringrazio i rappresentanti di Huawei.

Io ho una serie di domande da fare. Cerco di metterle in ordine. All'inizio avete parlato delle frequenze che attualmente si stanno usando, le 3,5 gigahertz, per imple-

mentare la copertura di rete mobile, assolutamente simile a quella del 4G, mentre i 26 gigahertz andrebbero per l'FWA (*Fixed Wireless Access*). Siamo in attesa anche della liberazione dei 700 megahertz.

Considerati questi tre pacchetti di frequenze, vorrei sapere qual è la vostra posizione sui limiti emissivi che ci sono in Italia, che – come sappiamo – sono estremamente bassi. È in corso un grosso dibattito anche sulla sicurezza della salute, non sulla sicurezza informatica. Vorrei sapere se avete fatto degli studi e se i limiti potrebbero essere differenziati anche in base alle frequenze di utilizzo, visto che c'è molta diversità. Andiamo dai 700 megahertz fino ai 26 gigahertz.

Per quanto riguarda la sicurezza informatica, invece, vorrei sapere se il vostro codice sul software è *open*, anche se non credo, visto che ci sono sicuramente dei brevetti, e se mettete almeno a disposizione dei vostri *partner* la possibilità di accedere al codice, proprio per dare loro modo di studiare e vedere se ci sono lacune, *backdoor* o altro.

Per quanto riguarda, invece, l'ultimo punto, quello sul *golden power*, mi piacerebbe capire nello specifico quali sono gli elementi che risulterebbero discriminatori per le aziende cinesi.

MASSIMILIANO CAPITANIO. Ringrazio i rappresentanti di Huawei per la presentazione. Abbiamo apprezzato anche alcuni dei contributi che sono stati portati alla nostra attenzione. Il nostro è un Paese che crede fortemente nello sviluppo della tecnologia dell'innovazione, quindi sosterrà fortemente lo sviluppo del 5G.

Sappiamo che lo scenario è internazionale. Sappiamo quali sono i contenuti di alcuni progetti di legge presentati negli Stati Uniti, come il *Defending America's 5G Future Act*. Per cui, non è un'esigenza solo italiana quella di tutelarsi e di stabilire un sistema di regole che ci consenta di garantire la sicurezza. Devo dire, solo a livello di cronaca, che ho trovato un po' indelicato l'annuncio degli investimenti miliardari in Italia. Sembrava quasi che si volesse sostenere la necessità di accompagnarci in un percorso comune. Ricordiamo che dei 2,6 miliardi annunciati, se non sbaglio e non ho letto male, 1,2 miliardi saranno destinati all'attività di *marketing* e solo 52 milioni in ricerca e sviluppo. Condividiamo, ovviamente, la necessità di porre delle regole che impongano la sicurezza a tutta la filiera. Non vogliamo, naturalmente, confrontarci solo su un pezzo del sistema, ma crediamo nel dover scrivere, seppur in ritardo... Noi arriviamo in ritardo nel rafforzare le misure di *golden power*.

Dopo queste considerazioni introduttive, passo alle domande. Non mi è chiaro se l'azienda sia critica nei confronti delle misure che sta intraprendendo l'Italia sul *golden power* perché ritenga critica la misura o perché semplicemente voglia estenderla ad altri operatori o ad altri soggetti. In questo forse starebbe la discriminazione. Noi, invece, stiamo valutando seriamente la questione dei limiti elettromagnetici. Non siamo pregiudizialmente contrari a un innalzamento di tali limiti. Sappiamo che in Italia i limiti sono dieci volte inferiori a quelli praticati in quasi tutta Europa. Vorremmo capire se avete fatto delle stime su un limite sufficiente per un eventuale innalzamento.

FEDERICO MOLLICONE. Io sono un deputato ospite, diciamo così, però ho seguito il tema di Huawei anche in altre Commissioni e sotto altri risvolti come Intergruppo Innovazione della Camera. Intanto, vi ringrazio per essere venuti in audizione. Ovviamente, sarà mia cura approfondire la lettura della documentazione che avete depositato. Anzi, mi scuso di essere arrivato in ritardo.

La mia più che altro – non so se avete già trattato il punto – è una domanda di carattere generale, di *diplomacy* dell'azienda Huawei Italia rispetto alla casa madre cinese. Vorrei sapere se esistono e sussistono obblighi nella gestione dei dati, se esiste un rapporto nella gestione dei dati tra la casa madre, lo Stato cinese e Huawei Italia.

PRESIDENTE. Desidero anche io porre una domanda ai nostri ospiti. Come lei stesso ha ricordato, dottor De Vecchis, e il

collega Capitanio ha stigmatizzato, il fatto che ci siano circa 3,1 miliardi di dollari di investimento nei prossimi tre anni e che, di questi, solo 52 milioni circa siano investiti sulla ricerca e sviluppo è un dato piuttosto emblematico. Sicuramente siamo ben contenti che vengano investiti soldi in Italia. Siamo fortemente colpiti dal fatto che l'Italia, purtroppo, avrà un investimento assai contenuto da parte di un'azienda tanto importante che ha, come dicevamo, numerosi centri di ricerca e sviluppo in giro per il mondo.

In un momento nel quale l'Italia si è sicuramente esposta, seguendo le scelte del Governo, sulle tematiche internazionali (inutile girarci troppo intorno, Via della Seta *in primis*), è piuttosto emblematico il fatto che una delle principali aziende cinesi decida di fare un investimento di così scarso respiro per quanto riguarda la promozione non solo di un mercato, che sicuramente – questo lo riconoscono tutte le aziende di telecomunicazioni – è una vera gallina dalle uova d'oro, altrimenti le altre aziende di telecomunicazioni non avrebbero investito 6,5 miliardi sulle frequenze 5G.

Anche su questo aspetto, è inutile girarci troppo intorno. Altre aziende internazionali riconoscono nell'Italia indubbiamente il ruolo di grande mercato per quanto riguarda il tema della vendita di servizi. Oggettivamente ci saremmo aspettati un maggiore impegno per quanto riguarda non solo la vendita di servizi e il puro *marketing*, ma anche la stabilizzazione di una logica che guardi anche al futuro, con investimenti veri, quindi non solo di una quindicina di milioni all'anno, per quanto riguarda ricerca e sviluppo basati in Italia.

Ricordo, peraltro, che la sfida che questo Parlamento, tutto, sta cercando di compiere – qui non ci sono verdi, rossi, gialli, bandiere di sinistra o di destra – è quella di ottenere il Tribunale dei brevetti proprio in Italia, magari a Milno. Per questa ragione, ci potrebbe essere una valorizzazione ulteriore, una motivazione ulteriore per ampliare la possibilità di investimenti in un Paese strategico dal punto di vista geopolitico, per le ragioni che ho espresso, e strategico per quanto riguarda il ruolo europeo anche sul tema dei brevetti.

Siamo rimasti piuttosto colpiti positivamente dall'annuncio di 3 miliardi e – come avrà capito – siamo rimasti colpiti in generale dal fatto che, purtroppo, ci sia stata (dal nostro punto di vista, siamo italiani e, chiaramente, cerchiamo di portare acqua al nostro mulino) scarsa visione per quanto riguarda gli investimenti sul nostro territorio di lunga durata.

Per quanto riguarda il tema della sicurezza, la posizione del Governo sul tema del *golden power* è assolutamente chiara. La domanda che vi pongo riguarda i rapporti anche con gli altri interlocutori. Forse siamo abituati ad altre realtà, realtà nelle quali un unico operatore produce un determinato strumento. Oggi gli strumenti che abbiamo a disposizione, dai *device* che abbiamo nel taschino o nella borsetta alla tv, hanno una serie di *chip*, dispositivi, *software* che vengono prodotti da numerose aziende. La domanda che vi pongo è se, all'interno dell'ipotesi *golden power*, che rimane un'ipotesi di applicazione, oltre direttamente a Huawei o alle aziende extraeuropee, secondo voi potrebbero essere colpite anche altre aziende che, logicamente, hanno collaborato con voi nella produzione di *device*, *smartphone*, altri strumenti tecnologici, comprese, chiaramente, le reti.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Vi ringrazio per le domande. Sono state poste una serie di domande, alcune tecniche e altre un po' meno tecniche. Andrei in ordine rispetto ai discorsi affrontati. Siccome il collega, tra l'altro, per pura coincidenza, lavorava proprio in Vodafone in quel periodo, probabilmente può spiegare in modo più chiaro la vicenda a cui si è fatto cenno, inclusa la questione delle differenze tra *core* e accesso, perché abbiamo detto che il *core* è più vulnerabile rispetto al dominio di accesso.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Confermo che ero in Vodafone quando abbiamo iniziato lo sviluppo della *Vodafone Station* con Huawei, un prodotto vera-

mente innovativo sul mercato che ha fatto, poi, il successo di Vodafone nel mondo della rete fissa. Essendo innovativo e dovendo noi correre, è stato uno sviluppo fatto a tappe forzate.

Credo sia stato ampiamente dimostrato nei giorni successivi che il giornalista di Bloomberg, che ha tirato fuori la storia della *backdoor*, ha detto, purtroppo, una grossa imprecisione, per non dire di peggio. Qui stiamo parlando di un protocollo, che si chiama *Telnet*, che esiste dai tempi in cui è nato l'IP. Tutti i modem di questa terra usano il *Telnet*. Il *Telnet* era aperto su quel dispositivo perché è l'unico modo di intervenire. Quando il cliente ti dice di avere un problema a casa e di non riuscire a usare il *wi-fi*, per esempio, un modo per accedere e capire che cosa sta succedendo è il Telnet.

Nella fase di sviluppo di un nuovo prodotto, come quello, chiaramente avevamo bisogno anche noi, come operatore, di poter accedere con strumenti *standard*. Andate a vedere cos'è il *Telnet*. Il *Telnet* è un protocollo standardizzato in IETF (*Internet Engineering Task Force*). Quindi, chi dice che è una *backdoor* dice una grande fesseria. Questo, scusate, tengo a sottolinearlo.

FEDERICA ZANELLA. Mi scusi se la interrompo. Il collega di Bloomberg che ha scritto quel pezzo lo conosco personalmente. Due mesi fa, quando mi ha mandato il secondo articolo, mi ha scritto che l'IT *incident report* confidenziale che ha ottenuto segnala non un semplice servizio *Telnet* su porta *standard*, ma un *Telnet* aggiuntivo con altre credenziali su porta non *standard* fatto rimuovere da Vodafone e poi rimesso da Huawei. Il documento parla di Telnet *backdoor*.

Non è un'inquisizione, però quello che ci interessa è capire che grado di sicurezza hanno, effettivamente, i vostri dispositivi.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Le posso spiegare. Non si tratta del grado di sicurezza. Gli apparati sono configurabili. Io il *Telnet* lo posso abilitare, disabilitare, riabilitare, a seconda delle richieste dell'operatore, se c'è una necessità. Il *Telnet* opera su una porta *standard*.

Il fatto che nella prima *release* noi non siamo riusciti a rimuoverlo completamente è sicuramente stato un errore del softwarista, può succedere. Vodafone ha ricevuto la nostra *release*, l'ha testata, l'ha fatta verificare dai suoi ingegneri e ha visto che in una particolare situazione quel *Telnet* era accessibile. Adesso, però, statemi a sentire molto bene: il *Telnet* era accessibile dall'utente che l'aveva a casa propria. Quindi, l'unica cosa che quell'utente poteva fare era aprire il proprio *home gateway* e andare a vedere un pezzo di codice dentro la sua *Vodafone Station*. Finito. Quel *Telnet* non era accessibile da *internet*. Questo l'ha chiarito molto bene Vodafone e l'abbiamo chiarito molto bene noi. La cosa più grave che poteva fare era guardare i dati della propria *Station*.

A un certo punto, Vodafone ha detto: « Non voglio che succeda neanche questo ». Abbiamo, quindi, chiuso completamente quella porta. Abbiamo dovuto fare due rilasci. Può succedere. Siamo tutti esseri umani. Al secondo rilascio, la porta è stata completamente chiusa.

Dire che *Telnet* è una *backdoor* – lo ripeto – è veramente una fesseria. Se io veramente volessi fare una *backdoor*, scusatemi, non userei il *Telnet*, ma userei un pezzo di codice nascosto. Tutti quelli che conoscono questo mondo credo sappiano benissimo che le *backdoor* si fanno in maniera molto diversa. Io l'ho vissuta sia da Vodafone, quando l'abbiamo creata, sia da Huawei (perché poi sono passato a Huawei, per combinazione), quindi posso testimoniare assolutamente che non c'è mai stata alcuna intenzione di mettere *backdoor*.

Era un normale sviluppo. Avevamo bisogno di uno strumento di diagnostica. Il *Telnet* – potete informarvi – viene largamente usato tutt'oggi per la diagnostica, anche su apparati di rete. Quindi, lo ripeto, non sono assolutamente d'accordo con l'interpretazione del collega di Bloomberg. Lo abbiamo detto in maniera molto chiara e credo l'abbia detto in maniera altrettanto chiara Vodafone nelle sue spiegazioni. Non c'è stato *breach* di dati proprio perché il *Telnet* era accessibile solo dal *computer*

collegato alla *Vodafone Station*. Questo per quanto riguarda il *Telnet*.

Per quanto riguarda il discorso di *core and access*, si tratta di distinguere i gradi di pericolosità. Lei ha ragione nel momento in cui dice che, ovviamente, qualunque punto di vulnerabilità può essere un pericolo, però gli operatori hanno una grandissima esperienza nella gestione di reti e nella gestione di attacchi. Pensi che ogni operatore riceve migliaia di attacchi durante il giorno che vengono fermati da quei *firewall* che vi ho mostrato. Forse lei non era ancora presente quando ne ho accennato.

Se un *hacker* tenta con il proprio telefonino di attaccare la rete, è evidente che l'operatore lo potrà bloccare in maniera molto semplice andando a disattivare il suo accesso tramite la BTS (*base transceiver station*). Viceversa, se un *hacker* riesce ad entrare e a prendere possesso di un elemento della rete *core*, da lì può veramente dilagare per tutta la rete e causare un *crash* totale – come diciamo noi – della rete. Noi facciamo un distinguo sul grado di pericolosità dell'evento. Quando parliamo di sicurezza nazionale, chiaramente un attacco che proviene da uno o due terminali mi può mettere in crisi una BTS per un'ora. Dopodiché, l'operatore interviene, disattiva quei due terminali e l'attacco finisce. Se, però, dovesse mai capitare che un *hacker* entra nella rete *core*, ne prende possesso e la tira giù, lì il danno potrebbe essere molto più ampio e l'impatto, quindi, sui servizi, soprattutto un domani, quando parleremo di servizi anche molto critici, come l'*autonomous driving*, di cui parlava prima... È chiaro che lì la disponibilità della rete deve essere vicinissima al cento per cento. È per quello che stiamo dicendo che la rete *core* deve essere quella sulla quale dobbiamo spingere per la maggiore focalizzazione.

Non vogliamo minimizzare il fatto che un attacco può provenire da qualunque punto. Noi ne stiamo facendo una questione di rischiosità, mi lasci usare questo termine.

Non so se sono stato chiaro.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Se posso, aggiungerei ancora un paio di osservazioni. A questo livello, dall'utente che si connette alla rete per ottenere un servizio, nel momento in cui io dal telefonino spingo il tastino *send* accadono una serie di comunicazioni tra questo oggetto e gli oggetti di riconoscimento e autenticazione. Avvengono con una velocità di cui noi non ci accorgiamo. È il tempo che passa tra il momento in cui pigio il tasto e il momento in cui sento la centrale che risponde con il suono. In quel periodo se quell'utente non è riconosciuto e non è autenticato io non riesco a collegarmi. Questo è un fatto importante. A questo livello, invece, dove vengono raccolte tutte le chiamate di tutti i milioni di telefonini collegati, quando si parlava di aggregazione significa che tutti questi dati vengono raggruppati insieme e diventa difficilissimo distinguerli l'uno dall'altro.

Questo aspetto della rete – non lo diciamo noi, lo dice anche l'operatore che progetta la rete, perché noi mettiamo dentro gli elementi e insieme si progetta e ogni volta che una nostra persona entra a questo livello riceve una *password* temporanea e tutto ciò che fa viene tracciato dall'operatore, questo è importantissimo, quindi non c'è nessuno che fa un'operazione che non sia presa in considerazione e presa sotto controllo – è protetto abbastanza, anche perché questo colloquio è crittografato con chiavi a 128 bit. Con l'ingresso della 5G queste chiavi diventano a 256.

Abbiamo fatto un piccolo calcolo: un potentissimo calcolatore quantico per decifrare dei dati crittografati a 256 bit impiegherebbe alcuni anni. Di conseguenza, li leggerebbe quando sono obsoleti. Confermiamo che è un aspetto critico, perché qui c'è la maggior parte del *software* della rete. È critico perché c'è un *software* e non perché non è protetto dall'operatore. Questa è la distinzione.

Passiamo all'altra domanda, se non ci sono altre osservazioni su questo. Magari ora andiamo più velocemente.

Si parla di frequenze, di tre pacchetti di frequenze e di sicurezza per la salute. Lascio la risposta sempre tecnica, però se devo effettivamente fare una transizione verso una economia digitale ho bisogno di

banda, di dati, ho bisogno di far passare i dati.

Quando parlo di *cloud*, quando parlo di *big data*, quando parlo di applicazioni che devono consentire ad un'auto senza guida di poter tranquillamente e velocemente arrivare a destinazione senza incidenti non come è oggi i cui sensori sono unicamente sull'auto per cui possono accadere gli incidenti che voi sapete, ma dialogare con i sensori che sono in campo, serve banda.

Oggi abbiamo avuto una disponibilità di piccole *slide* di banda, ma non sono queste quelle che poi serviranno quando il 5G sarà quello della fase di cui abbiamo parlato prima.

Vengo ora all'aspetto della salute. A differenza delle antenne, delle reti precedenti e quindi fino al 4G, il 5G è fatto in maniera diversa, ovvero funziona come se fosse uno *spot* di luce. Immaginate all'interno di questa stanza questa luce e quindi l'illuminazione delle antenne precedenti. Al di là del fatto che 6 volt/metro comunque cadono con il quadrato della distanza e sappiamo... Purtroppo non abbiamo noi i dati epidemiologici, però ci sono studi che confermano la non pericolosità di tutto questo.

Il 5G lavora come se fosse uno *spot*, quindi anziché avere le luci diffuse, ho una lampada che illumina soltanto me nel momento in cui parlo o illumina il presidente nel momento in cui parla. Di conseguenza, lei che sta lì non è sotto l'effetto di questo campo elettromagnetico, ma lo è semplicemente se diventa utente.

Questo, a parità di emissione, già è un fatto importante, distintivo rispetto alle reti precedenti. In termini di pericolosità delle reti 5G, passare alle antenne 5G rispetto al 4G ci porta ad andare verso una situazione di maggiore sicurezza.

Il fatto che in Europa ci siano 5-6 volt o ci siano 30-40 volt/metro significa che il numero delle antenne che metto è inferiore rispetto a quelle che ho. Non sono un medico, non abbiamo fatto studi, per questo non sono in grado di rispondere su questo tema.

Chiedo ora al collega Pignari di aggiungere qualcosa dal punto di vista tecnico.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Vorrei dare un piccolo chiarimento. Dal punto di vista elettromagnetico 4G, 5G e quant'altro non fa nessuna differenza. Un'onda elettromagnetica è un'onda elettromagnetica. La modulazione con cui portiamo i dati non è importante. Quindi, le frequenze da 700 megahertz sono prossime a quelle da 800 che già stiamo usando. La 3,4, la 3,6 sono state già usate ampiamente in Italia e nel mondo. La 3,6-3,8 dista pochissimo.

Quello che conta quando si parla di pericolosità per la salute di un'onda elettromagnetica è chiaramente la potenza irradiata. Ci sono due aspetti. Il primo aspetto è, come è già stato ricordato, che c'è una normativa internazionale, una normativa europea e una normativa poi italiana che regolamenta le potenze in gioco.

Sappiamo che le potenze che sono state normate dagli enti preposti, che ovviamente non siamo noi, sono almeno dieci volte inferiori a quelle che vengono ritenute potenzialmente dannose per la salute, dieci volte quindi un fattore dieci è senza dubbio elevato.

In Italia siamo stati giustamente anche più prudenti per determinati ambiti e siamo scesi di altre dieci volte. Questi limiti vanno rispettati, a prescindere che ci sia un'antenna 3G, 4G o 5G. Gli operatori quando andranno a progettare un sito dovranno presentare tutta la documentazione che certifica che sommando tutte le emissioni delle antenne 3G, 4G e 5G sempre i 6 volt/metro devono essere rispettati piuttosto che i 20 volt/metro. Questo non cambia.

Quello che diceva il dottor De Vecchis è un fattore importante. Il 5G sotto questo aspetto migliora la situazione perché mentre un'antenna 4G irradia costantemente un certo spazio, che ci sia o non ci sia traffico comunque deve irradiare. Nel 5G viene inserita una tecnologia, che si chiama « *massive MIMO* » che consente di ottimizzare l'uso della potenza, riducendo anche la potenza che viene irradiata nella cella. Questa tecnologia consente di spostare il fascio elettromagnetico sull'utente che in quel momento ha diritto di parlare. In questo millisecondo parla lei, nel prossimo

millisecondo parla lei. Questa tecnologia sposta il fascio.

Questo, ovviamente, permette ancor di più di ridurre i livelli di potenza irradiata oltre, ovviamente, a far risparmiare. È una tecnologia *green* perché non irradia inutilmente potenza se non ci sono utenti che parlano. Il 5G va nella direzione di ottimizzare sia l'uso dell'energia sia di andare a ottimizzare anche la radiazione elettromagnetica.

Ovviamente, noi non siamo medici, non siamo esperti del settore e ci affidiamo agli studi internazionali. Tuttavia, ripeto, da un punto di vista puramente elettromagnetico il 5G è esattamente identico al 4G e a qualunque altra tecnologia. Parliamo di onde elettromagnetiche. È chiaro che un'antenna di un *broadcaster* dal mio punto di vista è molto più pericolosa perché essendo piazzata magari in cima a una collina per poter andare a raggiungere tutta la città utilizza delle potenze decisamente più alte.

Una cosa che ci terrei anche a demistificare riguarda il numero delle antenne presenti. Sembra un po' assurdo, ma in realtà più antenne io riesco a mettere minore è la potenza che io devo irradiare e minori sono i problemi eventualmente di irraggiamento.

L'intensificazione delle antenne non è un grande problema, anzi è una circostanza che porta a ridurre il problema. Se ho due antenne distanti 50 metri devo irradiare una certa potenza. Se le mie due antenne sono distanti 300 metri ovviamente per garantire lo stesso livello di servizio devo innalzare la potenza che sparo. Più riesco a tenere le antenne dense e più il livello di potenza è costante e basso.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. C'è poi il problema dei permessi.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. La normativa relativa ai permessi è anche legata a questo aspetto.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Certo.

GIUSEPPE PIGNARI, *responsabile tecnologia e sicurezza di Huawei Italia*. Se la gente capisse il concetto che anziché mettere gli altoparlanti sul palco e sparare 100 chilowatt a chi sta ascoltando un concerto rock per far sentire a chi sta in fondo, bruciando le orecchie a chi sta davanti, se si distribuissero gli altoparlanti si sparerebbe magari a 100 watt e sentirebbero tutti bene. Il concetto è abbastanza banale.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Provo a mettere insieme alcune delle domande che sono state poste. Sul discorso della sicurezza abbiamo già risposto. L'onorevole Capitanio ha sollevato il problema delle criticità del 5G, anche se si tratta di una tecnologia che l'Italia intende sostenere fortemente, e ha chiesto chiarimenti sul perché noi riteniamo vi sia un effetto discriminatorio derivante dalle norme sul *golden power*; poi c'è il discorso fatto dal presidente Morelli sugli investimenti in Italia. Tra l'altro, lei era presente a Milano, quindi lo ha sentito in diretta prima di me.

Punti e motivi di discriminazione delle norme sul *golden power*, in realtà, sono effetti indiretti, che noi evidenziamo sulla base di ciò che è stato preannunciato da parte del Governo. In questa situazione devo dire, con molta trasparenza, che noi siamo stati coinvolti insieme a tutti gli attori della filiera in una serie di incontri per analizzare il problema dello sviluppo delle reti 5G e siamo stati coinvolti in una serie di confronti sulla semplificazione prevista nel primo decreto-legge sulla *Brexit*. Abbiamo lavorato alacremente tutti, ognuno per conto proprio, e abbiamo cercato di convogliare tutte queste attività presso l'ente che ci aveva comunque richiesto questa riflessione. Proprio durante questa attività di studio e di analisi delle semplificazioni possibili, è stato emanato questo nuovo decreto-legge, vanificando un po' tutto quello che era in corso. Se lei mi consente, ci ha lasciato un po' perplessi questo aspetto, che arriva proprio mentre ci stanno chiedendo un approfondimento. Questo lo segnalo semplicemente come fatto.

Per quanto riguarda la questione di un trattamento discriminatorio che noi pen-

siamo sia presente (nella normativa sul *golden power*), questo riguarda le previste modalità operative attraverso le quali deve essere fatta una notifica e soprattutto il fatto che la notifica deve avvenire più volte, anche se l'elemento che io prendo in considerazione è lo stesso; quindi se effettivamente l'operatore ha elaborato un piano di sviluppo di un certo tipo, questo piano viene rallentato dal fatto che l'operatore ha considerato la tecnologia Huawei e di conseguenza alla fine potrebbe accadere che per non aspettare 45 giorni più altri 45 e più altri 30 o in caso di difficoltà questo tempo viene fermato, in realtà l'operatore potrebbe decidere, a questo punto, di scegliere strade diverse. Da questo punto di vista potrebbe essere per noi, anzi noi la riteniamo una discriminazione vera e propria.

Dal punto di vista della notifica, gli eventuali elementi da considerare sono innumerevoli, sono centinaia gli elementi di rete che devono essere analizzati. Il fatto che si possa dire che un'antenna, un telefono, un solo nodo rispetto ad una fornitura globale possano rappresentare l'elemento di difficoltà, questo ci lascia molto perplessi, perché ciò che va valutato effettivamente è l'affidabilità del fornitore e non l'affidabilità del singolo apparato, anche perché, mi lasci dire una cosa molto semplice, onorevole Capitanio, se lei prende ad esempio oggi una centrale Huawei – me lo faccia dire in modo molto semplice – in questa centrale Huawei il 70 per cento del *chip*, il 70 per cento del *firmware*, il 70 per cento delle componenti è di provenienza internazionale. Questo vale anche per tutti gli altri.

Di conseguenza, anche se io sono sicuro del mio comportamento, quando io compro un *chip* dall'esterno – chiedo scusa, ma come ingegneri dobbiamo lavorare in questo modo – devo vedere cosa richiede e cosa mi dà come risultato. Quindi andare a vedere come è fatto il *firmware* internamente è praticamente impossibile. Lì dentro potrebbe esserci benissimo una situazione critica che io non sono in grado di rilevare, così come non è in grado di rilevare nessun altro. Ed è questo il motivo per cui noi, tra l'altro, andando al di là dell'aspetto della mera discriminazione, abbiamo parlato di *cyber security* a livello globale, perché comunque se io proteggo una parte e poi entro da un'altra parte, del sistema, il problema rimane inalterato. Ho solo messo in difficoltà un processo che vede soltanto uno degli aspetti dell'intera filiera e su quello costruisco un progetto di sicurezza per il Paese. Io vedo una debolezza anziché vederlo a livello complessivo.

Mi preme dire due cose prima che si diffonda qualche altra informazione su questo tema. In questo momento ci sono altre segnalazioni che mi piacerebbe condividere con voi. C'è una società americana, non conosciuta, non sappiamo nulla al riguardo, abbiamo solo ricevuto recentemente anche noi alcuni dati, che ha rilevato delle vulnerabilità. Attenzione, si parla di vulnerabilità sempre, mai di situazioni critiche. Noi abbiamo un sistema che è messo a disposizione delle terze parti e degli utenti proprio perché nel caso in cui fossero trovate queste vulnerabilità, questa unità informata reagisce e identifica immediatamente quello che è necessario fare per superare quella difficoltà e quindi rilasciare un sistema « patchato » alla fine.

Interpellati questi signori abbiamo appreso che si tratta di una società americana, che non ha assolutamente descritto né il tipo di problema, né su quale tecnologia esso è stato rilevato. Sappiamo che negli Stati Uniti non esiste nessuna tecnologia Huawei. Quindi, il fatto che venga intrapresa un'azione del genere negli Stati Uniti è quantomeno dubbio. Lo leggerà sui giornali, se non l'ha già letto, ma noi abbiamo completamente trascurato l'informazione.

L'altra questione cui volevo accennare dal punto di vista della sicurezza, prima che fosse evidenziata da parte dell'amministrazione degli Stati Uniti la pericolosità del sistema, riguarda il fatto che Google aveva rilasciato un'intervista che per noi è illuminante. Google è il maggior partner di Huawei perché, grazie a Huawei, ha messo a punto il sistema Android che oggi è presente, come sapete, in tutti gli apparati Huawei e in tutti gli apparati Samsung.

Google ha fatto una dichiarazione molto importante e ha detto che ha tenuto sotto osservazione l'apparato cellulare della Huawei e non ha mai riscontrato situazioni nelle quali un dato sia uscito al di fuori del sistema. Questo è importante dirlo, perché spesso sento qualcuno che, agitando il telefonino, dice « Non voglio che i miei dati vadano a finire da un'altra parte ».

Devo anche dire che se un telefonino è gestito da un sistema come Android, nel caso in cui accadesse una cosa del genere, non possiamo prendercela con il costruttore del telefonino, il quale lo mette solo a disposizione. Google ha fatto questa grande affermazione e, come voi sapete benissimo, ha preso molto male il concetto della *entry* list elaborata dal presidente Trump.

Vengo al tema degli investimenti. Non so se sono riuscito a rispondere a tutte le domande.

È verissimo, gli investimenti in ricerca e sviluppo, ancorché poi per completarli sarebbe anche opportuno avere la componente produttiva di quella ricerca, riteniamo che siano abbastanza importanti. Nel centro di ricerca e sviluppo che abbiamo a Milano i brevetti sono fatti in compartecipazione con il Politecnico di Milano, con il Politecnico di Torino e con il Politecnico di Padova. Chiedo scusa se non siamo arrivati più giù, più nel sud in Italia, però diciamo l'Italia è un Paese che sebbene sia conosciuto in realtà non è conosciuto così in fondo, quindi non sappiamo o comunque ancora dobbiamo spiegare quanto siano importanti alcuni centri di eccellenza del sud come il Politecnico di Bari, per esempio, o l'Università Federico II a Napoli.

Noi abbiamo inteso questi investimenti in un'area che è completamente innovativa, perché è quella dove l'Italia potrà recitare nuovamente un ruolo dominante in futuro ed è quella dell'intelligenza artificiale, è quella dello sviluppo delle applicazioni che si basano proprio su queste tecnologie nuove, quindi sulla realtà virtuale, sulla realtà aumentata, che sono, guarda caso, proprio i modelli che sono stati messi in piedi nei due *trial* dove noi siamo presenti, Milano e Bari. Abbiamo sviluppato questa collaborazione pubblico-privato con oltre 600 enti tra amministrazioni locali, quindi comuni, province, aziende locali e multinazionali italiane, le poche rimaste, e abbiamo sperimentato una cosa molto importante, che la realizzazione di applicazioni che facciano uso di intelligenza artificiale in realtà non è ancora matura in nessuna parte del mondo.

Un contributo nostro in quest'area, ancorché ovviamente l'interesse nel mondo della ricerca e sviluppo è maggiore, credo che possa dare un impulso maggiore al Paese.

Devo fare un'ultima considerazione e poi concludo. Ovviamente, questo è frutto di nostre elaborazioni, è frutto del pensiero che noi abbiamo per far sviluppare un Paese, per metterci al servizio del Paese. Però noi abbiamo tentato in questi giorni, approfittando del fatto che è arrivato il Presidente europeo, cioè la persona che può decidere molto di più rispetto alle organizzazioni locali, abbiamo tentato di avere dei colloqui con i *decision maker* della politica.

Purtroppo il momento è molto critico, il momento è un po' complicato e non ci siamo riusciti. Però, se avessimo acquisito alcune informazioni che possono anche indicare degli interessi o delle aree diverse, credo che Huawei sarebbe stata disponibile ad ascoltarli e magari a reindirizzare il suo operato. Non vuol dire che questo non possa essere ancora fatto, però mi preme ancora dire che l'Europa è importante per la Cina, l'Italia un po' più dell'Europa. Il nostro presidente aveva incontri programmati con l'Italia, con la Spagna, con la Francia, con la Germania, l'Inghilterra non sappiamo se rimane, però in Inghilterra noi abbiamo già una presenza molto grande. In Inghilterra abbiamo investito 4 miliardi di euro nei passati dieci anni. Ovviamente, non possiamo fare centri di ricerca e sviluppo di grandi dimensioni o fabbriche in tutta l'Europa. Noi dobbiamo scegliere un Paese e chiaramente ascoltare le esigenze da parte dei *decision makers* è un fatto importante.

Mi auguro che alla prossima occasione ci sia un'occasione utile per poter incon-

trare i *decision maker* ed avere apertamente ciò che ha detto in questo momento il Presidente Morelli e che io riporterò in alto alla catena, anche al di fuori del mio territorio, in realtà troverebbe molta più credibilità se effettivamente non fosse la Huawei a dover pensare a cosa investire e come investirle a livello centralizzato, ma se ci fosse uno scambio di opinioni che, ripeto, per ragioni che tutti sappiamo, in realtà non ha potuto svolgersi. Ci avevamo pensato con anticipo. Probabilmente avremmo potuto fare non un annuncio diverso, perché quello era già stato pensato, ma avremmo potuto elaborare un concetto diverso e magari prepararci per un secondo *step*.

Noi abbiamo concluso, presidente.

FEDERICO MOLLICONE. Mi scusi, presidente. Sempre da deputato ospite, avevo fatto una domanda molto semplice, a cui credo sia semplice rispondere: Quali rapporti ha Huawei Italia con Huawei Cina ? Vorrei sapere se la gestione dei dati degli utenti o altre interazioni con Huawei Cina e con lo Stato cinese erano codificate, se esistevano.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. In realtà abbiamo già risposto durante la presentazione per quanto riguarda i dati. Se vi ricordate la *slide* dove erano descritti i ruoli dei tre attori principali, Huawei era quello centrale.

Noi, ovviamente, forniamo le apparecchiature che poi servono per fare la rete. La rete, per quanto riguarda la copertura, per quanto riguarda la topologia, per quanto riguarda la distribuzione delle antenne non la facciamo noi, la fa ovviamente l'operatore. Non abbiamo chiavi di accesso. Ogni volta che nasce un problema, per esempio, di manutenzione di un apparato che è all'interno della rete noi non possiamo né entrare fisicamente, né entrare da un punto remoto. Veniamo chiamati, viene identificato il personaggio, questo signore entra dentro e viene tracciato, come ho detto prima. Non abbiamo nessuna possibilità di accedere. I dati non sono gestiti da noi. Di conseguenza, noi non siamo in grado. Se anche fosse, quello che dice lei, possibile che il Presidente Xi Jinping mi dicesse di andare a prendere i dati del Presidente Morelli perché vuole capire che fa nella vita se mi desse un miliardo dovrei uccidere perché non sarei in grado di farlo. Sono dati protetti. È difficile accedervi.

Per quanto riguarda la legge, la legge è vigente all'interno del Paese, non si estende al di fuori.

Il presidente e fondatore dell'azienda è Ren Zhengfei. L'ho anche scritto in una intervista, il Paese, il partito, il presidente non possono assolutamente permettersi... Non esiste nessuna legge che lo imponga. Abbiamo fatto uno studio, mi dispiace a questo punto che non lo abbiamo mandato, dato ad una società indipendente che ha studiato questa legge a livello cinese e ha descritto le implicazioni che ha questa legge a livello interno, quindi a livello del Paese Cina e non applicabile all'esterno.

Ad oggi non abbiamo mai ricevuto nessuna imposizione, nessuna richiesta. In questo momento si può dire tutto e il contrario di tutto, però se mi permette il Presidente Morelli io potrei fare avere direttamente questo studio indipendente. Possiamo metterlo a disposizione della Commissione successivamente.

PRESIDENTE. La ringrazio per questa disponibilità, e inoltreremo questo studio a tutti i colleghi della Commissione.

FEDERICO MOLLICONE. La legge dice il contrario.

Poi lo comunicheremo anche pubblicamente. C'è una legge dell'*intelligence* cinese che, invece, dice che anche all'estero le strutture cinesi devono contribuire a raccogliere informazioni. Però, se a loro risulta così, va benissimo.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. C'è una distinzione grossa da fare, me la lasci fare. Stiamo parlando di operatore e di *vendor*. Noi non siamo in grado di farlo perché non abbiamo i dati.

PRESIDENTE. Però, la questione rimane aperta. Se uno non lo può fare, lo

può fare quell'altro. Comunque, valuteremo.

LUIGI DE VECCHIS, *presidente di Huawei Italia*. Io non l'ho detto.

PRESIDENTE. L'ho detto io. Grazie per la vostra partecipazione e grazie a tutti.

Ringrazio i rappresentanti di Huawei Italia per il loro contributo e dichiaro conclusa l'audizione.

La seduta termina alle 16.45.

Licenziato per la stampa
il 20 novembre 2019

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

18STC0072890