



Questa rubrica
è promossa da:



L'Italia e le società di telecomunicazioni cinesi tra congiuntura politica globale e incertezze interne

Francesco Silvestri

School of International Relations, Beijing Foreign Studies University

Contatto: francesco.silvestri@tochina.it

Virginia Mariano

Dipartimento di Culture, Politica e Società, Università degli Studi di Torino

Contatto: virginia.mariano@tochina.it

L'interdizione delle società di telecomunicazioni cinesi nel contesto globale

Il 2020 non sarà ricordato solo per la pandemia da COVID-19 e per gli enormi costi umani, sociali ed economici da essa causati, ma rimarrà anche nella memoria storica come l'anno in cui le relazioni tra Cina e Stati Uniti hanno toccato il punto più basso dalla fine della Guerra fredda. Dopo aver inizialmente investito l'ambito commerciale, il deteriorarsi dei rapporti tra l'egemone che ha fondato l'attuale ordine internazionale e la principale potenza emergente ha evidenziato come sia un altro il dominio in cui si registra la tensione più acuta e strutturale: quello tecnologico. In questo quadro, l'opera di interdizione avviata dagli Stati Uniti nei confronti delle aziende di telecomunicazioni cinesi è la manifestazione più evidente di quello che Lim e Ferguson hanno definito il "dilemma della sicurezza tecnologica".¹ L'accentuarsi di una spirale di reciproca insicurezza sta rafforzando – da entrambi i lati – le posizioni di chi invoca un *decoupling* tecnologico, con effetti imprevedibili nel lungo periodo. Per via della profonda integrazione dei processi commerciali, industriali, culturali e scientifici, le implicazioni che il deteriorarsi di questa relazione porta con sé sono di rilevanza globale. In questo contributo, il campo d'analisi verrà ristretto alle sole tecnologie delle telecomunicazioni (ICT), ambito in cui è possibile osservare una delle evoluzioni più critiche nella relazione bilaterale.

Intensificando le misure restrittive applicate finora ai produttori cinesi, gli Stati Uniti stanno mettendo in atto una revisione dell'industria delle telecomunicazioni con l'obiettivo di minimizzare le vulnerabilità e l'esposizione alle interferenze esterne. L'interdizione delle aziende di telecomunicazioni cinesi dalle infrastrutture federali statunitensi è pressoché assoluta e gode di un consenso *bipartisan*; sembra dunque improbabile un cambio di direzione indipenden-

¹ Lim Darren e Victor Ferguson, "Conscious Decoupling: the Technology Security Dilemma", in *China Dreams* (China Story Yearbook 2019), a cura di Jane Golley, Ben Hillman, Linda Jaivin e Sharon Strange (Acton: ANU Press, 2019).

temente dagli esiti del ciclo elettorale che si è appena concluso. Obiettivo di queste misure è salvaguardare i dati di privati e imprese dalle interferenze di attori che il governo statunitense identifica come ostili. Tra questi vi è Huawei, considerata dal Dipartimento di Stato USA un'estensione dell'apparato di sorveglianza della Rpc. L'articolo 7 della *Legge nazionale della Rpc sull'intelligence* (che impone a organizzazioni e cittadini di sostenere, assistere e cooperare con il lavoro di *intelligence* statale)² viene frequentemente citato a supporto di questa categorizzazione. La direzione è quindi tracciata nonostante la stretta sulla tecnologia cinese ponga alcune aziende statunitensi di rilievo (come Apple, Microsoft e Qualcomm per citarne solo alcune) in una condizione di alta esposizione alle possibili ritorsioni da parte di Pechino a causa del loro forte posizionamento nel mercato cinese. Il Dipartimento di Stato ha uniformato le misure restrittive verso la tecnologia cinese nella cornice di un programma denominato "Clean Network", formulando un approccio che i paesi alleati sono invitati ad adottare; a questo scopo l'amministrazione Trump ha avviato un'azione persuasiva utilizzando come leva la cooperazione tra servizi di *intelligence*.³

La risposta delle aziende cinesi a queste accuse è stata netta. Secondo Ren Zhengfei, suo fondatore, Huawei è un'azienda privata e risponde solamente ai suoi dipendenti-azionisti. Gli azionisti (circa 97.000 nel 2018), che devono essere necessariamente dipendenti dell'azienda, eleggono un Comitato dei rappresentanti, che a sua volta elegge il Consiglio di amministrazione e il Consiglio di supervisione.⁴ Vari dibattiti sono emersi in merito alla struttura societaria di Huawei, in particolare dopo l'articolo pubblicato da Balding e Clarke nel 2019⁵ e alla conseguente eco propagatasi nei media occidentali su questo tema. I due autori osservano che la Huawei Investment & Holding Co., l'entità controllante, è a sua volta controllata per il 98,9% da un Comitato sindacale composto dai dipendenti-azionisti; secondo gli autori, questa tipologia di sindacato è direttamente subordinata alla Federazione nazionale dei sindacati cinesi (FNCS, *Zhōnghuá quánquó zōnggōnghuì*, 中华全国总工会), un organismo a sua volta controllato dal Partito comunista cinese (Pcc). Altri hanno rilevato come la quota di proprietà dei dipendenti, gestita tramite un *Employee stock ownership plan*,⁶ corrisponda ad azioni cosiddette "sintetiche": questa tipologia di azioni non è trasferibile al di fuori dell'azienda e non garantisce alcun potere di partecipazione all'amministrazione o agli assetti patrimoniali societari ma dà esclusivamente il diritto a riscuotere una quota dei profitti. La *governance* di ZTE è invece più esplicitamente legata alle imprese in mano pubblica, essendo nata come controllata dalla municipalità di Shenzhen, diventando successivamente una società per azioni a responsabilità limitata quotata nelle borse di Shenzhen e Hong Kong. Zhongxingxin è la holding controllante con il 30,34% della proprietà ed è controllata a sua volta da quattro azionisti, due dei quali (Xi'an Microelectronics e Aerospace Guangyu) sono controllati da

² Assemblea nazionale del popolo della Rpc, "National Intelligence Law of the PRC", 2017, disponibile all'Url https://cs.brown.edu/courses/cscit800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

³ Dipartimento di Stato degli Stati Uniti d'America, *The Clean Network*, 2020, disponibile all'Url <https://www.state.gov/the-clean-network>.

⁴ Huawei, "Who owns Huawei?", disponibile all'Url <https://www.huawei.com/en/facts/question-answer/who-owns-huawei>.

⁵ Christopher Balding e Donald Clarke, "Who Owns Huawei?", *SSRN 3372669* (2019), disponibile all'Url https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

⁶ David De Cremer e Tao Tian, "Huawei: A case study of when profit sharing works", *Harvard Business Review* 24 (2015), disponibile all'Url <https://hbr.org/2015/09/huawei-a-case-study-of-when-profit-sharing-works>.

● Figura 1

Principali sedi e iniziative di Huawei e ZTE in Italia.



Le attività e gli investimenti di Huawei e ZTE in Italia sono cresciuti in volume e varietà comprendendo, oltre alla commercializzazione dei prodotti consumer, le sperimentazioni nelle infrastrutture di rete, i servizi alle aziende e le attività di ricerca e sviluppo. La presente mappa non intende essere esaustiva di tutte le attività delle due aziende in Italia.

Fonte: Siti ufficiali e comunicati stampa di Huawei Italia, ZTE Italia, Governo italiano e agenzie di stampa.

due imprese di Stato, *China aerospace science and industry corporation* (Casic) e *China aerospace science and technology corporation* (Casc).⁷

In entrambi i casi, l'analisi della struttura societaria non è di per sé sufficiente a confermare o confutare una volta per tutte il controllo delle autorità cinesi sulle due aziende. Come hanno notato Li e Cheong in uno studio sulla struttura societaria di ZTE,⁸ il graduale processo di riforma delle imprese in Cina ha prodotto un progressivo ridimensionamento della proprietà statale nel settore privato senza tuttavia che questa riduzione corrispondesse a un proporzionale alleggerimento della guida statale nell'economia. Tale guida non si esprime necessariamente in un ruolo diretto del Pcc o dello Stato nella gestione dell'impresa o nella definizione degli obiettivi aziendali; si tratta invece di un meccanismo di definizione degli elementi contestuali

⁷ ZTE Corporation, "Annual report 2018", 2018, p. 93, disponibile all'Url <https://res-www.zte.com.cn/mediare/zte/Investor/20190410/EI.pdf>.

⁸ Li Ran e Cheong Kee Cheok, "How Much «State» is in China's State Enterprises? A Case Study of ZTE Corporation in an Era of Reform", *International Journal of China Studies* 7 (2016), 3: 245.

e degli incentivi entro cui questi attori si muovono. L'influenza statale si esprime dunque nella conformità delle strategie aziendali rispetto agli obiettivi di medio-lungo periodo stabiliti a livello nazionale. Questa conformità permette alle imprese cinesi di crescere e consolidarsi grazie a sussidi, all'accesso privilegiato ai mercati – interno e in paesi terzi – a barriere non tariffarie che restringono i margini d'azione delle imprese straniere, ai partenariati pubblico-privati, alle gare di fornitura per progetti su larga scala e a un facilitato accesso al credito. Vi è in sostanza una complessa sinergia tra settore privato e politiche pubbliche che, a dispetto della formale separazione dei due ambiti, rende l'operato delle imprese cinesi coerente con la programmazione strategica del Partito-Stato.

È alla luce di questo scenario di incentivi e interessi – che risultano perlopiù opachi ai decisori nel mondo occidentale – che l'amministrazione Trump ha potuto legittimare un approccio di radicale chiusura alle società di telecomunicazioni e digitali cinesi. Le azioni intraprese per raggiungere questo obiettivo sono principalmente: limitazione degli investimenti cinesi (anche in *venture capital*); controllo delle esportazioni per le tecnologie chiave e *dual use*; divieto di appalto a imprese che utilizzano forniture cinesi. Più recentemente il governo statunitense ha introdotto un'altra modalità: la messa al bando delle applicazioni *social* cinesi più utilizzate al mondo, Tik Tok e WeChat. Questa soluzione è tuttavia incorsa in ostacoli giuridici non ancora risolti. L'amministrazione Trump ha intanto intrapreso un'azione di persuasione verso i paesi alleati per l'adozione del medesimo approccio. I paesi della cosiddetta "Alleanza *Five Eyes*" (Usa, Regno Unito, Canada, Australia e Nuova Zelanda) hanno infatti adottato misure analoghe, a eccezione del Canada (che si trova ancora in una fase consultiva). Londra, dopo l'iniziale apertura ai fornitori cinesi segnalata a inizio gennaio 2020, ha assecondato le richieste statunitensi (e di parte del Partito conservatore britannico) annunciando un *phase-out* di Huawei da completarsi entro il 2027.

L'emergere di un approccio europeo

Nello scenario appena delineato l'Europa si trova politicamente ed economicamente condizionata dalle strategie statunitensi e cinesi, mentre il potenziale dell'Unione Europea quale terza polarità si esprime tuttora in modo incerto. Nell'ambito della competizione per il primato tecnologico, la complessità e la frammentazione dei processi decisionali nell'Unione, unite all'assenza di imprese digitali di dimensioni equiparabili a quelle cinesi o statunitensi, hanno finora complicato il formarsi di una posizione chiara e univoca e la definizione di un modello di *governance* tecnologica in grado di porsi come riferimento globale. Pur se collocati nell'alleanza atlantica, i paesi europei hanno consentito nell'ultimo decennio una penetrazione significativa degli investimenti cinesi in settori strategici, con acquisizioni di imprese d'eccellenza e interventi importanti nelle infrastrutture e in snodi logistici. Accentuatesi in maniera diversificata e discontinua a partire dal lancio della Belt and Road Initiative (BRI), le preoccupazioni legate all'influenza cinese in Europa stanno oggi assumendo dei contorni più spiccati e uniformi.

Nel rapporto *EU-China - A strategic outlook* del 2019,⁹ l'UE definisce la Cina un partner negli ambiti di interesse comune e allo stesso tempo un "rivale sistemico", concetto indirettamente ribadito

⁹ Commissione Europea e Alto Rappresentante dell'Unione Europea per gli Affari Esteri e la Politica di Sicurezza, *EU-China – A strategic outlook*, 12 marzo 2019, disponibile all'Url <https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf>.

dalla Presidente della Commissione Europea von der Leyen¹⁰ in seguito agli incontri del Summit sino-europeo di giugno e settembre 2020. Il negoziato UE-Cina sugli investimenti vive una fase di stallo a causa delle spiccate asimmetrie nelle condizioni di accesso al mercato, circostanza ribadita dai governi europei in diverse sedi e sottolineata regolarmente nei *Position paper* annuali della Camera di commercio europea in Cina.¹¹ A ciò si aggiungono l'approccio maggiormente assertivo della Cina all'estero (associato a uno stile diplomatico sempre più pungente) e le denunce sempre più frequenti e circostanziate in merito alla gestione delle periferie del paese – da Hong Kong allo Xinjiang – da parte del governo cinese. Se a partire dall'inizio del 2019 le pressioni statunitensi avevano prodotto in Europa risultati disomogenei, oggi la comunità europea si sta gradualmente ricompattando.¹² Questo è anche dovuto al fatto che i generici ammonimenti diplomatici di Washington sugli alleati europei si sono trasformati, nel corso del 2020, in richieste più esplicite e puntuali, che richiamano gli alleati a un riallineamento rispetto a tematiche di sicurezza e a valori condivisi.

Nonostante questi fattori, l'Unione Europea non ha espresso un veto esplicito verso Huawei e ZTE, né verso altri operatori extra-UE. Vengono invece stabiliti requisiti di sicurezza rigorosi che confluiscono nelle raccomandazioni del Toolbox 5G.¹³ Questo documento, pubblicato dal Gruppo di cooperazione NIS (Network and Information Security) a inizio 2020, identifica misure strategiche e misure tecniche che i paesi membri sono chiamati ad adottare per mitigare i rischi di sicurezza nelle reti di quinta generazione. Il *Toolbox* incoraggia l'adeguamento del sistema normativo e il rafforzamento di alcune funzioni di tutela, come il coordinamento della risposta in caso di attacchi cibernetici e i processi di *testing* e *auditing* delle reti. Particolare enfasi viene posta sulla diversificazione dei fornitori, sui criteri adottati nella loro selezione, e sulla necessità di un'analisi approfondita degli stessi, in modo da mitigare l'esposizione a eventuali interferenze di paesi extra-UE; viene infatti raccomandata l'esclusione dei "fornitori ad alto rischio" dalle cosiddette funzioni core della rete. Per quanto riguarda la diversificazione della catena di fornitura, il *Rapporto sui progressi nell'attuazione del Toolbox 5G*¹⁴ individua l'applicazione del Golden power in Italia come un caso illustrativo; secondo il Rapporto, il governo italiano richiede agli operatori di rete mobile di diversificare sia in senso verticale (impiego di diversi fornitori per gli strati *hardware*, virtualizzazione e applicativo di ciascuna componente dell'infrastruttura di rete) sia in senso orizzontale (diversi fornitori per le diverse tipologie di componenti dell'infrastruttura di rete).

¹⁰ European Commission Press Corner, "Von der Leyen following EU-China Summit: We must make progress, one that implies reciprocity and trust", 22 giugno 2020, disponibile all'Url https://ec.europa.eu/commission/presscorner/detail/en/ac_20_1170.

¹¹ Camera di Commercio dell'Unione Europea in Cina, *European Business in China – Position Paper 2020/2021*, disponibile all'Url <http://www.europeanchamber.com.cn/en/publications-position-paper>.

¹² Janka Oertel, "The new China consensus: How Europe is growing wary of Beijing", *European Council on Foreign Relations*, 7 settembre 2020, disponibile all'Url https://www.ecfr.eu/publications/summary/the_new_china_consensus_how_europe_is_growing_wary_of_beijing.

¹³ Commissione Europea, NIS Cooperation Group, *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, 29 gennaio 2020, disponibile all'Url <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

¹⁴ Commissione Europea, NIS Cooperation Group, *Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity*, 24 luglio 2020, p. 22, disponibile all'Url <https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>.

Osservando le prassi dei singoli paesi membri si può rilevare come nei maggiori paesi europei (Francia, Italia, Spagna e Germania) l'approccio verso i fornitori cinesi sia stato graduale e privo di interdizioni formali dal forte valore simbolico e politico. Vi sono invece altri paesi membri il cui approccio, dopo una lunga fase di incertezza, è stato decisamente più netto. La Repubblica Ceca ha interdetto Huawei in seguito al parere vincolante dell'agenzia nazionale per la sicurezza cibernetica NÚkib, che identifica la società cinese come una minaccia per la sicurezza cibernetica.¹⁵ Estonia, Lettonia e Bulgaria hanno aderito al programma Clean Network tramite dichiarazioni congiunte con il governo statunitense.¹⁶ L'ultimo paese membro ad attuare un'interdizione di Huawei e ZTE è stata, ad oggi, la Svezia: l'Autorità svedese per le poste e le telecomunicazioni, dopo una valutazione delle Forze armate e dei Servizi di sicurezza, ha deciso di vietare l'utilizzo di componentistica delle due società cinesi per i bandi di gara nelle frequenze 3,5 e 2,3 GHz e di avviare un phase-out da completare entro il 1° gennaio 2025.¹⁷

Huawei e ZTE in Italia: investimenti, partenariati e progetti in corso

Mentre i paesi europei attraversano una fase interlocutoria e valutano i costi di un phase-out dei progetti ICT cinesi già in corso, è utile fare il punto su cosa avviene nella nostra penisola. L'intensificarsi del *decoupling* tecnologico ha chiaramente riflessi evidenti sulla presenza delle due società di Shenzhen in Italia. A partire dalla seconda metà degli anni Duemila, gli investimenti in Italia e in Europa si sono intensificati, non solo per quanto riguarda la commercializzazione di prodotti *consumer*, ma anche nelle infrastrutture di rete. Da questo punto di vista, l'Italia ha avuto un ruolo di primo piano come centro di sviluppo per le attività dei due fornitori di tecnologia in Europa occidentale.

Huawei in Italia

Huawei è ben radicata nella penisola, dove opera nel segmento *consumer* (telefoni cellulari, *tablet*, *smartwatch*, domotica, e altri dispositivi), nel segmento *enterprise* (soluzioni per le aziende) e nel segmento *carrier* (sviluppo delle reti), quest'ultimo coinvolto nella partecipazione ai bandi di gara 5G. Secondo i dati divulgati dall'azienda, Huawei impiega in Italia circa 800 persone¹⁸ generando un volume d'affari di 1,5 miliardi di euro, di cui metà provengono dai segmenti *enterprise* e *carrier*.¹⁹ La presenza di Huawei in Italia risale al 2004, anno di apertura del primo ufficio a Milano, che continuerà a essere il principale centro delle attività societarie nel paese. Nei primi anni di attività, Huawei contribuì alla messa in opera di reti per la telefonia mobile,

¹⁵ National Cyber and Information Security Agency (Nukib), "Warning - File Number 110-536/2018", 17 dicembre 2018, disponibile all'Url <https://nukib.cz/en/cyber-security/>.

¹⁶ Si vedano: Presidenza degli Stati Uniti d'America, "United States-Estonia Joint Declaration on 5G Security", 1 novembre 2019, disponibile all'Url <https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security>; Dipartimento di Stato degli Stati Uniti d'America, "Joint Statement on United States-Latvia Joint Declaration on 5G Security", 27 febbraio 2020, disponibile all'Url <https://www.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security>; Dipartimento di Stato degli Stati Uniti d'America, "United States - Republic of Bulgaria Joint Declaration on 5G Security", 23 ottobre 2020, disponibile all'Url <https://www.state.gov/united-states-republic-of-bulgaria-joint-declaration-on-5g-security>.

¹⁷ The Swedish Post and Telecom Authority, "Four companies approved for participation in the 3,5 GHz and 2,3 GHz auctions", 20 ottobre 2020, disponibile all'Url <https://pts.se/en/news/press-releases/2020/four-companies-approved-for-participation-in-the-3.5-ghz-and-2.3-ghz-auctions/>.

¹⁸ Huawei, "Huawei inaugura i nuovi uffici a Milano", 12 marzo 2019, disponibile all'Url https://solar.huawei.com/it/news/it_20190312.

¹⁹ Huawei, "Huawei Enterprise", 2020, disponibile all'Url <https://e.huawei.com/it/about/huawei-enterprise>.

lavorando in particolare sui protocolli della famiglia *high speed packet access* (HSPA).²⁰ Uno dei primi progetti su ampia scala viene realizzato in collaborazione con Telecom Italia, che nel 2007 seleziona Huawei come partner tecnologico per l'espansione della propria rete nel Sud Italia.²¹ La cooperazione con gli operatori Telecom presenti in Italia è proseguita fino a oggi: sono attive sperimentazioni in partenariato su vari protocolli di rete fissa e rete mobile single-RAN.²²

La presenza italiana di Huawei non è limitata allo sviluppo delle reti, ma si esprime anche nel campo della ricerca e sviluppo (R&S). A Segrate è stato inaugurato nel 2011 il Centro globale di competenza *microwave*²³ che è per Huawei il riferimento mondiale per lo sviluppo della tecnologia *wireless* a microonde; il centro ha attivato collaborazioni di ricerca con diversi atenei italiani tra cui i politecnici di Milano e Torino. Secondo una dichiarazione alla stampa dell'amministratore delegato di Huawei, Thomas Miao, il piano aziendale in Italia prevede investimenti per circa 2,75 miliardi di euro di cui 50 milioni in R&S.²⁴ Nell'ottobre 2019 Huawei ha inaugurato a Roma l'*Innovation experience and competence center* dedicato alla dimostrazione di soluzioni e casi d'uso negli ambiti *smart city* e 5G.²⁵ Il 30 settembre 2020 è stata annunciata l'apertura nella capitale di un *Cybersecurity and transparency center*,²⁶ con funzioni analoghe al *Cybersecurity lab* inaugurato da ZTE nel 2019.

Cooperazione con la Regione Sardegna

Tra i progetti legati alle *smart city*, degno di nota è il *Joint Innovation Center* (JIC) presso il Parco Tecnologico di Pula (Cagliari) dove Huawei è il partner tecnologico di un partenariato pubblico-privato costituito dalla Regione Sardegna, dal CRS4 (centro di ricerca fondato dal premio Nobel Carlo Rubbia), da Fastweb e altri attori pubblici e privati, come atenei e piccole-medie imprese del territorio.²⁷ L'accordo di collaborazione, firmato ad Hannover durante la fiera CeBIT del 2016, prevede lo sviluppo di servizi ICT nei settori della sicurezza, dei trasporti, della salute, dei servizi ambientali e della manifattura. Huawei è incaricata di realizzare la parte tecnica del progetto pilota che prevede la distribuzione di sensori diffusi nell'area urbana di Cagliari (semafori, telecamere, sensori di parcheggio, ecc.), la raccolta e l'elaborazione dei dati generati e il conseguente

²⁰ "Mobile IP surges across Europe", *Huawei Technologies* 38 (2008), 16, disponibile all'Url https://www.huawei.com/mediafiles/CORPORATE/PDF/Magazine/communicate/38/HW_081661.pdf.

²¹ Xu Yan, "LTE, Are you ready?", *Huawei Technologies* 38 (2008), 54-55, disponibile all'Url https://www.huawei.com/mediafiles/CORPORATE/PDF/Magazine/communicate/38/HW_081688.pdf.

²² "Editoriale", *Notiziario tecnico Telecom Italia* 3, 2010, disponibile all'Url <https://www.gruppotim.it/content/dam/telecomitalia/it/archivio/documenti/Innovazione/MnisitoNotiziario/archivio/numeri%20vecchi/3-2010.pdf>.

²³ "Huawei apre a Segrate il centro di ricerca sul microwave", *Corriere Comunicazioni*, 17 novembre 2011, disponibile all'Url <https://www.corrierecomunicazioni.it/telco/huawei-apre-a-segrate-il-centro-di-ricerca-sul-microwave>.

²⁴ "Miao (Huawei): «Investiremo in Italia 3,1 miliardi di dollari nei prossimi tre anni»", *La Repubblica*, 15 luglio 2019, disponibile all'Url https://www.repubblica.it/economia/2019/07/15/news/miao_huawei_investiremo_in_italia_3_1_miliardi_di_euro_nei_prossimi_tra_anni_-231227220/.

²⁵ Huawei, "Huawei inaugura i nuovi uffici a Roma", 24 ottobre 2019, disponibile all'Url https://e.huawei.com/it/news/it/2019/20191024_Huawei_nuovi_uffici_Roma.

²⁶ Huawei, "Huawei annuncia il suo «Italy Cyber Security and Transparency Center» di Roma", 30 settembre 2020, disponibile all'Url https://e.huawei.com/it/news/it/2020/20200930_Huawei_Italy_Cyber_Security_Transparency_Center.

²⁷ Regione Autonoma della Sardegna, "Continua il processo di innovazione in Sardegna: annunciati nuovi progetti del Joint Innovation Center di Huawei e CRS4 per le Smart & Safe City", 7 novembre 2018, disponibile all'Url <https://www.regione.sardegna.it/j/v/2568?s=378283&v=2&c=392&t=1>.

raccordo con i servizi urbani per la gestione del traffico, la riduzione dell'inquinamento, la previsione meteorologica e l'invio di notifiche a cittadini e autorità. I dati generati grazie ai sensori confluiscono nell'*Intelligent operation center*,²⁸ una centrale di controllo che è abilitata a comunicare con le autorità e i servizi pubblici locali. Il progetto ha molte caratteristiche analoghe al sistema *ET City Brain* che Alibaba Cloud ha sviluppato nella città di Hangzhou e sta esportando in alcune città del Sud-Est asiatico.²⁹

L'utilizzo delle tecnologie di ultima generazione per la risoluzione di problemi di *governance* urbana è uno degli ambiti su cui la Cina sta sperimentando a pieno regime. Huawei ha promosso questo pacchetto di soluzioni per le amministrazioni locali definendolo "*Smart & Safe City*", volendo indicare sia l'ottimizzazione delle funzioni di gestione urbana sia l'ambito della sicurezza. Secondo quanto divulgato dell'azienda, Huawei ha contribuito a oltre 160 progetti *smart city* nel mondo in oltre 100 paesi.³⁰ La collaborazione con la Regione Sardegna prevede, inoltre, la ricerca sulla tecnologia *cloud* e sulla nuova generazione di reti e-LTE, sviluppate da Huawei per lo sviluppo di un *wireless* a banda larga.

Partecipazione ai bandi di gara 5G

In linea con il "5G Action Plan" della Commissione Europea,³¹ il Ministero dello sviluppo economico ha avviato nel 2018 la sperimentazione pre-commerciale del 5G in cinque centri urbani, mettendo a gara 1275 MHz di spettro di frequenza.³² La gara è stata aperta a operatori e fornitori di tecnologia per sperimentare la rete nelle città di Milano, Prato, L'Aquila, Bari e Matera; nel settembre 2018 sono state presentate le offerte economiche iniziali.³³ Huawei ha vinto come partner tecnologico di Vodafone il bando per l'area di Milano. È presente come partner tecnologico anche a Bari e Matera per le frequenze di spettro 3,6-3,8 GHz insieme a Telecom Italia e Fastweb, per un investimento totale di 60 milioni di euro.³⁴ Il progetto prevede una cooperazione con oltre cinquanta enti internazionali, nazionali e locali, e include soggetti privati, pubbliche amministrazioni, atenei e centri di ricerca. Mentre Matera è stata selezionata in quanto capitale della cultura per il 2019, puntando dunque sulla digitalizzazione dell'esperienza museale e archeologica, la scelta di Bari mira allo sviluppo tecnologico del

²⁸ Joint Innovation Center, Regione Autonoma della Sardegna, "The journey in the digital transformation of Italy stages in Sardinia", disponibile all'Url <http://www.jicsardegna.it/en/news-en/huawei-and-the-digital-transformation-in-sardinia-the-smart-region-of-the-future-is-already-here>.

²⁹ Jenny W. Hsu, "Alibaba Cloud launched «ET City Brain 2.0» in Hangzhou", *Alizil*, 20 settembre 2018, disponibile all'Url <https://www.alizila.com/alibaba-cloud-launched-city-brain-2-0-hangzhou/>.

³⁰ Yao Jiankui, "AI + Cloud-Pipe-Device Promotes Smart Society", *ICT Insights Issue 23*, Huawei Enterprise, agosto 2018, disponibile all'Url https://e.huawei.com/en/publications/global/ict_insights/201806041630/focus/201808170838.

³¹ Commissione Europea, *5G for Europe: An Action Plan*, 14 settembre 2016, disponibile all'Url <https://ec.europa.eu/digital-single-market/en/news/communication-5g-europe-action-plan-and-accompanying-staff-working-document>.

³² Autorità per le garanzie nelle comunicazioni, *Delibera n.231/18/CONS*, 8 maggio 2018, disponibile all'Url https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=10721193&_101_INSTANCE_FnOw5lVOIXoE_type=document.

³³ Ministero dello sviluppo economico, *Gara 5G: presentate le offerte iniziali da parte degli operatori*, 10 settembre 2018, disponibile all'Url <https://www.mise.gov.it/index.php/it/per-i-media/notizie/it/198-notizie/2038588-5g>.

³⁴ Gruppo Tim, "Telecom Italia, TIM, Fastweb e Huawei: insieme per il progetto «Bari Matera 5G»", 8 novembre 2017, disponibile all'Url <https://www.gruppotim.it/it/archivio-stampa/corporate/2017/CS-Progetto-Bari-Matera-5G-8-11-2017-ITA.html>.

porto della città che aspira a diventare un “porto 4.0” dotato di servizi connessi, automatizzati e collegati al *cloud*. I progetti 5G a Bari e Matera prevedono inoltre lo sviluppo della sensoristica, della videosorveglianza e della telemedicina.³⁵

ZTE in Italia

Entrata in Italia nel 2005, un anno dopo Huawei, l'altra grande società di telecomunicazioni di Shenzhen è ZTE. L'azienda dirige le attività in Italia dalle sedi di Roma e Milano, quest'ultima considerata dall'azienda il suo *hub* europeo;³⁶ il CEO per l'Europa occidentale, Hu Kun, ha affermato che l'Italia è per ZTE il più importante mercato in Europa (soprattutto per lo sviluppo del 5G e del *Fixed wireless access*), oltre a essere un centro strategico a livello mondiale.³⁷ Vi sono inoltre sedi minori in altre dodici città della penisola, operate tramite la sussidiaria ZTE Italia, attive nella vendita e manutenzione di equipaggiamento *software* e *hardware* per le telecomunicazioni, nella formazione e nella consulenza. ZTE Italia ha costituito due sussidiarie, ZTE Italia Servizi (con sede a Milano, attiva nella gestione delle infrastrutture e nell'internet delle cose) e ZTE Italia *research & innovation center* (con sede a L'Aquila e impegnata in R&S e commercializzazione del 5G).³⁸

Secondo i vertici aziendali, vi sono nel nostro paese circa 700 dipendenti (nel 2017),³⁹ con un indotto di oltre duemila lavoratori e un fatturato di oltre 170 milioni di euro nel 2017. ZTE Italia ha stabilito collaborazioni e partenariati con oltre un centinaio di aziende nazionali. Nel 2016, in partenariato con Telecom Italia, ZTE ha vinto la gara per l'aggiornamento della rete fissa per la diffusione del segnale broadcast video a Siena⁴⁰ e l'anno dopo ha ottenuto l'appalto per due sperimentazioni 5G con Wind Tre e Open Fiber, come sarà dettagliato in seguito. Per il quinquennio 2019-2023, l'azienda ha dichiarato un obiettivo di 250 milioni di euro in ricavi annui e un volume di investimenti pari a 500 milioni di euro,⁴¹ rimarcando come gli investimenti in Italia facciano parte di una logica di lungo periodo. L'azienda ha dichiarato un investimento del 14,6% del fatturato in attività di R&S nei primi nove mesi del 2020 con particolare attenzione all'ambito 5G.⁴²

³⁵ Camera dei Deputati – IX Commissione Trasporti, poste e telecomunicazioni, “Audizione Fastweb nell'ambito dell'Indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei big data”, 18 dicembre 2018, disponibile all'Url https://www.camera.it/leg18/824?tipo=I&anno=2018& mese=12 &giorno=18&view=filtered_scheda&commissione=09. Secondo l'audizione di Fastweb presso la Camera dei Deputati, nel porto di Bari saranno testate soluzioni “di *logistica avanzata, videosorveglianza, people counting e controllo degli accessi grazie a telecamere ad altissima definizione e sensoristica*”.

³⁶ “China's ZTE Corp to set up 5G tech hub in Italy”, *Xinhua*, 30 giugno 2017, disponibile all'Url http://www.xinhuanet.com/english/2017-06/30/c_136405001.htm.

³⁷ Andrea Biondi, “L'Italia è l'hub europeo di ZTE. Collaboriamo su 5G e smart city”, *Il Sole 24 Ore*, 25 ottobre 2019, disponibile all'Url <https://www.ilssole24ore.com/art/l-italia-e-l-hub-europeo-zte-collaboriamo-5g-e-smart-city-ACmxW8t>.

³⁸ ZTE, “ZTE in Italy”, 2018, disponibile all'Url <http://www.zteitalia.it/wp-content/uploads/2018/09/ZTE-Italia-Eng.pdf>.

³⁹ ZTE, “Dichiarazioni aziendali”, 2019, disponibile presso il sito web della Camera dei Deputati della Repubblica italiana all'Url https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/002/358/ZTE_Documento_completo.pdf.

⁴⁰ *Ibidem*.

⁴¹ “ZTE punta sul 5G italiano, fatturato verso 250 milioni di euro”, *La Repubblica*, 23 ottobre 2019, disponibile all'Url https://www.repubblica.it/economia/rapporti/impresa-italia/tecnologia/2019/10/23/news/zte_punta_sul_5g_italiano_fatturato_verso_250_milioni_di_euro-239260923.

⁴² ZTE, “ZTE: nei primi 9 mesi dell'anno il fatturato sale a 74,13 miliardi di RMB” 28 ottobre 2020, disponibile all'Url <http://www.zteitalia.it/2020/10/28/zte-nei-primi-9-mesi-dell'anno-il-fatturato-sale-a-7413-miliardi-di-rmb>.

Come illustrato nella Figura 2, ZTE è attualmente al terzo posto nella classifica globale delle famiglie di brevetti per le reti di quinta generazione.

Accordo con Roma Capitale e Regione Abruzzo

Nel 2018, ZTE Italia ha firmato un'intesa con Roma Capitale per entrare come partner tecnologico nel progetto “#Roma5G”, di cui fanno parte anche Fastweb e Ericsson, e sperimentare soluzioni per la videosorveglianza, le *smart city* e il turismo.⁴³ L'azienda ha inoltre attivato una collaborazione tra ZTE University e Università di Roma Tor Vergata, che si aggiunge alle numerose convenzioni firmate con le università italiane per consolidare i rapporti con il mondo scientifico e formativo e favorire l'inserimento di personale qualificato nell'azienda.⁴⁴ Nel maggio 2019

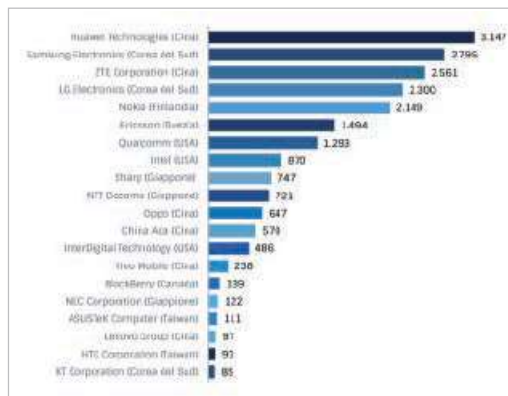
è stato inaugurato il *ZTE Cybersecurity lab*, il primo centro privato in Europa dedicato alla formazione e alla ricerca congiunta sul tema della sicurezza cibernetica. Il laboratorio servirà anche da spazio dimostrativo per la sicurezza dei prodotti ZTE, fornendo a clienti, decisori e regolatori un punto di confronto per la valutazione dei prodotti (ad esempio, per facilitare la revisione dei codici sorgente, l'*audit* in fase di progettazione e i test delle scatole nere).⁴⁵ ZTE ha inoltre stabilito una solida cooperazione con la Regione Abruzzo sul tema *smart city* e banda ultralarga, proponendosi come uno dei partner privati impegnati nei piani di ripresa post-sisma. Nell'aprile 2018, ZTE e Università de L'Aquila hanno inaugurato presso il Tecnopolo d'Abruzzo il Centro di innovazione e ricerca (ZIRC), dedicato alla sperimentazione pre-commerciale di casi d'uso del 5G.⁴⁶

Partecipazione ai bandi di gara 5G

I due principali partenariati di ZTE Italia per la realizzazione delle reti di quinta generazione sono stati avviati con Wind Tre e Open Fiber (controllata di CDP Reti ed Enel). Nel 2016, ZTE e Wind Tre hanno firmato un accordo per il “golden network”, la rete unica di Wind Tre.⁴⁷ L'anno successivo, ZTE ha avviato insieme a Open Fiber una collaborazione per la banda ultralarga a Forlì e Vercelli e nel 2019 le due aziende hanno inaugurato a Milano la prima connessione con

● Figura 2

Famiglie di brevetti 5G dichiarate.



Huawei e ZTE si collocano rispettivamente alla prima e terza posizione a livello globale per numero di famiglie di brevetti dichiarate; le aziende coreane Samsung e LG si collocano al secondo e quarto posto.

Fonte: Tim Pohlmann, “Fact finding study on patents declared to the 5G standard”, Berlin Institute of Technology, commissionato dal Ministero tedesco per l'economia e la tecnologia, gennaio 2020.

⁴³ Comune di Roma, “#Roma5G: arte e innovazione per il futuro del patrimonio”, 4 febbraio 2020, disponibile all'Url <https://www.comune.roma.it/web/it/notizia.page?contentId=NWS522717>.

⁴⁴ Università degli Studi di Roma “Tor Vergata”, “Accordo ZTE - Ateneo di “Tor Vergata” per formare i manager del futuro”, 6 ottobre 2017, disponibile all'Url https://web.uniroma2.it/module/name/Content/action/showpage/content_id/49325.

⁴⁵ “Dichiarazioni aziendali”, ZTE, 2019.

⁴⁶ Ibidem.

⁴⁷ Ibidem.

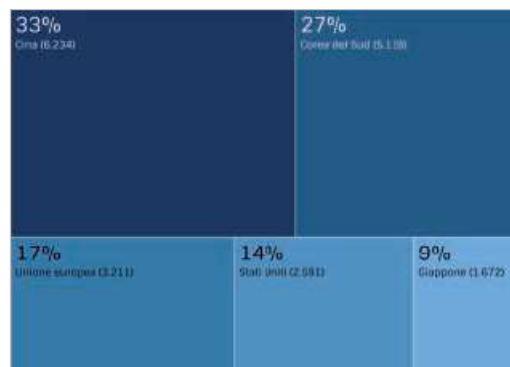
standard XGS-PON in Italia (che garantisce 10 Gbps di velocità).⁴⁸ Nel 2017, Wind Tre e Open Fiber hanno vinto il bando di gara per le sperimentazioni 5G a Prato e L'Aquila, con ZTE come partner tecnologico.⁴⁹ Nelle due città, la cordata sperimenterà la rete 5G nelle frequenze 3.6-3.8 GHz e saranno coadiuvate dalle amministrazioni locali, le piccole medie imprese del territorio, il Polo Universitario Città di Prato, l'Università di Firenze e l'Università de L'Aquila. ZTE Italia ha inoltre affiancato Wind Tre nel progetto "super rete 4.5G", ovvero la costruzione di 20.000 siti di trasmissione, distribuiti capillarmente nel territorio italiano con tecnologia idonea alla trasmissione 5G.⁵⁰

La posizione del governo italiano

La posizione del governo italiano è ancora sospesa in uno stato di relativa indeterminata, sebbene sia emerso un vivo e articolato dibattito – tra ministeri, amministrazioni dello Stato, partiti e stampa – e siano stati attuati interventi significativi con riferimento all'impianto normativo in materia di sicurezza cibernetica e di protezione delle infrastrutture critiche nazionali. Se, da una parte, dopo la breve esperienza di governo della coalizione Lega–Movimento Cinque Stelle, il paese torna a presentarsi come saldamente inserito nell'alleanza atlantica, dall'altra, gli interessi economici e sociali legati agli investimenti cinesi in Italia sono ragguardevoli e non possono essere oggetto di interventi senza una ponderata riflessione di lungo periodo. Nel dibattito pesa un evidente problema di *path-dependancy*: gli investimenti nelle reti e nelle infrastrutture, nei centri di ricerca, nelle catene di fornitura e nei contratti di lavoro sono elementi non facilmente reversibili e impongono alti costi di riconversione e un marcato impatto socio-economico. In effetti, la presenza di Huawei e ZTE sul territorio nazionale, come si è rilevato nei precedenti paragrafi, è significativa e rappresenta una parte importante nello sviluppo tecnologico del settore ICT nazionale. Se ci si sofferma sull'impatto occupazionale, sommando i dati di entrambe le aziende, è verosimile stimare che il numero dei soli dipendenti superi le 1.500 unità, senza valutare l'indotto.⁵¹

● Figura 3

Famiglie di brevetti 5G a livello globale (per provenienza).



Huawei e ZTE si collocano rispettivamente alla prima e terza posizione a livello globale per numero di famiglie di brevetti dichiarate; le aziende coreane Samsung e LG si collocano al secondo e quarto posto.

Fonte: Tim Pohlmann, "Fact finding study on patents declared to the 5G standard", Berlin Institute of Technology, commissionato dal Ministero tedesco per l'economia e la tecnologia, gennaio 2020.

⁴⁸ Ibidem.

⁴⁹ ZTE, "ZTE partners with Wind Tre and Open Fiber to build Europe's first 5G pre-commercial network", 2017, disponibile all'Url <https://www.zte.com.cn/global/about/news/1025ma3>.

⁵⁰ ZTE Italia, "ZTE e WindTre celebrano la fine del progetto della Super Rete", 16 dicembre 2019, disponibile all'Url <http://www.zteitalia.it/2019/12/16/zte-e-windtre-celebrano-la-fine-del-progetto-della-super-rete>.

⁵¹ ZTE, "Presentazione ZTE", 2019, documento disponibile presso il sito web della Camera dei Deputati della Repubblica italiana, disponibile all'Url https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/002/035/01_PresentazioneZTE_072019_ITA.pdf.

È inoltre opinione diffusa che l'esclusione delle due aziende dai bandi di gara provocherebbe differimenti nell'attuazione dei piani di sviluppo del 5G in Italia, causando un ritardo nella tecnologia che rappresenta il prossimo *standard* nelle telecomunicazioni e, come enfatizzato dalla Commissione Europea, uno dei più importanti elementi costitutivi dell'economia digitale nei decenni a venire.⁵² È dunque difficile perimetrare con precisione i costi economici, tecnologici e sociali dell'interdizione dei fornitori cinesi. Secondo le dichiarazioni rese da Huawei Italia durante un'audizione alla Camera dei Deputati,⁵³ escludere le due aziende comporterebbe anche uno smantellamento della componentistica 4G già in uso, che rappresenta oggi il 40% di tutta l'infrastruttura 4G a livello europeo; i costi stimati dalla GSMA Association⁵⁴ relativi a un'eventuale esclusione di Huawei e ZTE nella costruzione del 5G in Europa sono di 55 miliardi di euro. Questo stato d'incertezza emerge in un contesto già di per sé difficile per il settore delle telecomunicazioni, che attraversa da anni una fase di contrazione degli utili. Secondo un'audizione di Assotelecomunicazioni-Asstel presso la IX Commissione Trasporti, poste e telecomunicazioni della Camera dei Deputati, i ricavi netti aggregati degli operatori nel decennio compreso tra il 2007 e il 2017 hanno subito una contrazione del 25%, il margine lordo è diminuito del 30% e la capacità di auto-finanziamento del 52%.⁵⁵

Per le reti 5G, il quadro di riferimento entro cui si muove il Governo italiano è l'approccio europeo definito nel sopraccitato *Toolbox 5G* che raccomanda la diversificazione della catena di fornitura ed evidenzia il rischio di esposizione a interferenze di paesi extra-UE, sottolineando dunque l'importanza di un'analisi approfondita del profilo dei singoli fornitori e la messa a punto di un impianto normativo stringente. Le pressioni statunitensi per escludere le due società cinesi sono state sostanzialmente arginate per tutto l'arco del 2019. Nel febbraio 2019, il Ministero dello sviluppo economico aveva specificato l'impraticabilità di un blocco degli operatori cinesi alla luce dell'assenza di prove certe in merito a rischi per la sicurezza e in virtù del principio di libero accesso al mercato.⁵⁶ È inoltre opportuno rilevare che nel quadro del sistema legale italiano l'interdizione di imprese specifiche presenta notevoli complessità giuridiche che ne rendono incerto l'esito, a differenza invece del sistema statunitense dove gli *executive order* della Presidenza possono essere implementati con maggiore agilità. Il rischio di una messa al bando degli operatori cinesi da parte del Governo italiano è dunque quello di avviare un lungo iter giudiziario dall'esito non scontato; da qui l'esigenza di intervenire sull'impianto normativo che possa giustificare misure di sicurezza straordinarie.

⁵² Commissione Europea, *Towards 5G*, 2020, disponibile all'Url <https://ec.europa.eu/digital-single-market/en/towards-5g>.

⁵³ Camera dei Deputati della Repubblica italiana, *5G e big data: audizione Huawei Italia*, Roma, 17 luglio 2019, disponibile all'Url https://www.camera.it/leg18/1132?shadow_primapagina=9383.

⁵⁴ Gwénaëlle Barzic, "Europe's 5G to cost \$62 billion more if Chinese vendors banned: telcos", *Reuters*, 7 giugno 2019, disponibile all'Url <https://www.reuters.com/article/us-huawei-europe-gsma-idUSKCN1T8oY3>.

⁵⁵ Camera dei Deputati della Repubblica italiana, "Audizione di Assotelecomunicazioni-Asstel sulle nuove tecnologie delle telecomunicazioni, con particolare riferimento al 5G e big data, con attenzione al tema dell'elettromagnetismo", Roma, 9 aprile 2019, disponibile all'Url https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/001/516/Memoria_ASSTEL.pdf.

⁵⁶ Ministero dello Sviluppo Economico, *Huawei e ZTE, nessun blocco per il 5G*, 7 febbraio 2019, disponibile all'Url <https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039194-huawei-e-zte-nessun-blocco-per-il-5g>.

Dal punto di vista normativo, la politica di sicurezza italiana per lo spazio cibernetico si basa sui DPCM 24/1/2013⁵⁷ e 17/2/2017,⁵⁸ che definiscono l'architettura istituzionale per la protezione delle infrastrutture critiche nazionali, oltre che sui principi indicati a livello europeo dalla Direttiva (UE) 2016/1148,⁵⁹ la cosiddetta "Direttiva NIS". Sulla base dei due DPCM sono stati definiti il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (2013)⁶⁰ e il Piano nazionale per la protezione cibernetica e la sicurezza informatica (2017),⁶¹ che identificano nella Presidenza del Consiglio dei Ministri (PdC) l'organo apicale del sistema di sicurezza cibernetica, altresì deputato a impartire direttive al Dipartimento di Informazioni per la Sicurezza (DIS). All'interno del DIS, il Nucleo per la sicurezza cibernetica (NSC) è il centro dell'architettura nazionale a protezione delle infrastrutture critiche materiali e immateriali. La PdC presiede inoltre il *Computer security incident response team* (CISRT), istituito per adeguarsi alla Direttiva NIS.⁶² Questa architettura è stata integrata con il rafforzamento della disciplina sul Golden power (già stabilita con il DL 21/2012), che conferisce poteri speciali al governo al fine di salvaguardare gli assetti delle imprese operanti in ambiti ritenuti strategici e di interesse nazionale. Il DL sul Golden power è stato infatti modificato nel 2019 tramite l'introduzione dell'articolo 1-bis che estende gli ambiti strategici alle tecnologie 5G.⁶³ In seguito a una Comunicazione della Commissione Europea del marzo 2020,⁶⁴ il Golden power è stato ancora rafforzato nel mese di aprile 2020 (durante la fase più acuta della pandemia di coronavirus) tramite il DL 23/2020⁶⁵ che espande ulteriormente gli ambiti e i poteri di controllo del governo per proteggere gli assetti e le tecnologie critiche del paese. Il DL 105/2019⁶⁶ ha introdotto nella normativa italiana il "Perimetro di sicurezza nazionale cibernetica", de-

⁵⁷ Gazzetta Ufficiale, *Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, disponibile all'Url <https://www.gazzettaufficiale.it/eli/gu/2013/03/19/66/sg/pdf>.

⁵⁸ Gazzetta Ufficiale, *Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, disponibile all'Url <https://www.gazzettaufficiale.it/eli/gu/2017/04/13/87/sg/pdf>.

⁵⁹ Gazzetta Ufficiale dell'Unione Europea, *Direttiva UE 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*, 6 luglio 2016, disponibile all'Url <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=IT>.

⁶⁰ Presidenza del Consiglio dei Ministri, *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*, dicembre 2013, disponibile all'Url <https://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf>.

⁶¹ Presidenza del Consiglio dei Ministri, *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*, marzo 2017, disponibile all'Url <https://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf>.

⁶² Comitato parlamentare per la sicurezza della Repubblica, *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*, 11 dicembre 2019, disponibile all'Url https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf.

⁶³ Presidenza del Consiglio dei Ministri, *Golden Power*, disponibile all'Url <http://www.governo.it/it/dipartimenti/dip-il-coordinamento-amministrativo/dica-att-goldenpower/9296>.

⁶⁴ Gazzetta Ufficiale dell'Unione 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*, 26 marzo 2020, disponibile all'Url <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2020:099I:FULL&from=EN>.

⁶⁵ Gazzetta Ufficiale della Repubblica italiana, *Decreto Legge 8 aprile 2020*, n. 23, disponibile all'Url <https://www.gazzettaufficiale.it/eli/id/2020/04/08/20G00043/s>.

⁶⁶ Gazzetta Ufficiale della Repubblica italiana, *Decreto Legge 21 settembre 2019*, n. 105, disponibile all'Url <https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg>.

● Figura 4

Misure salienti a livello nazionale ed europeo a tutela delle infrastrutture critiche.



La normativa a tutela delle infrastrutture critiche in Italia si è evoluta in parallelo alle raccomandazioni della Commissione Europea nell'ambito dello sviluppo e della protezione delle reti 5G.

Fonte: Commissione Europea, Governo italiano.

finendo gli organi incaricati della tutela della sicurezza cibernetica e i loro compiti, e dando disposizioni per la definizione dei soggetti e delle aree della rete inclusi nel perimetro. Il DL stabilisce inoltre le sanzioni per l'inosservanza delle misure di sicurezza, chiarisce i compiti del Centro di Valutazione e Certificazione Nazionale (CVCN) e conferisce alla PdC il potere di disattivare gli apparati all'interno del perimetro su deliberazione del Comitato interministeriale per la sicurezza della Repubblica. Il DL 105/2019 è stato convertito con modificazioni in legge (133/2019) nel novembre 2019.⁶⁷

In occasione della visita di Stato in Italia del Presidente Xi Jinping, nel marzo 2019, è stato firmato il *Memorandum of Understanding per la collaborazione sulla Belt and Road Initiative*, il cui testo – nonostante le forti pressioni di cui fu oggetto il Governo Conte I – contiene esplicita menzione della collaborazione nello sviluppo della connettività nell'ambito delle telecomunicazioni.⁶⁸ Nel dicembre 2019, il Ministro dello sviluppo economico Patuanelli ha ribadito che, con le opportune garanzie, le società cinesi avrebbero potuto accedere ai bandi di gara per il 5G,⁶⁹ nonostante il parere negativo espresso dalla Relazione del Comitato parlamentare per la sicurezza della Repubblica (Copasir) lo stesso mese.⁷⁰ È utile rilevare che il Copasir, organo bicamerale composto da cinque senatori e cinque deputati rappresentanti in modo

⁶⁷ Presidenza del Consiglio dei Ministri, *Sicurezza cibernetica. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (decreto-legge)*, 19 settembre 2019, disponibile all'Url <http://www.governo.it/it/articolo/consiglio-dei-ministri-n-4/12844>.

⁶⁸ Governo italiano, *Memorandum of Understanding per la collaborazione sulla Belt and Road Initiative*, disponibile all'Url http://www.governo.it/sites/governo.it/files/documenti/documenti/Notizie-allegati/Italia-Cina_20190323/Memorandum_Italia-Cina_IT.pdf.

⁶⁹ "L'Italia, la Cina e il 5G. L'audizione di Patuanelli al Copasir", *Formiche.net*, 30 gennaio 2020, disponibile all'Url <https://formiche.net/2020/01/5g-cina-banche-copasir-patuanelli>.

⁷⁰ Comitato parlamentare per la sicurezza della Repubblica, 2019, si veda la precedente nota 62.

paritario maggioranza e opposizione (e presieduto da un esponente dell'opposizione), ha approvato la Relazione all'unanimità, esprimendo dunque preoccupazioni che attraversano trasversalmente lo spettro politico del paese. La Relazione ripercorre l'aggiornamento in più fasi della politica di cybersicurezza nazionale e identifica la presenza dei fornitori cinesi come un pericolo per la sicurezza nazionale a causa dei legami con il governo cinese; la *Legge sulla sicurezza nazionale* e la *Legge sulla Cybersicurezza* della Rpc sono il fondamento su cui si basa la valutazione espressa dal Copasir.

In un'audizione di Huawei Italia presso la Camera dei Deputati nel luglio 2019,⁷¹ durante la quale è stato interpellato anche il responsabile di Huawei per la sicurezza, sono condivise le specifiche delle attività aziendali in Italia e vengono date garanzie sui punti seguenti: Huawei Italia dichiara di essere soggetto autonomo rispetto alla società controllante cinese ed è vincolata al rispetto della legislazione italiana; non esiste una legislazione cinese che induca proattivamente all'attività di spionaggio; non esistono precedenti in tal senso nei paesi in cui l'azienda è presente; Huawei non possiede le chiavi di accesso ai dati trasmessi sulle reti; le vulnerabilità per la sicurezza dei dati provengono da un'inadeguata protezione degli stessi e non da vulnerabilità intrinseche della rete. L'audizione non ha però soddisfatto appieno il Copasir, che nella Relazione sottolinea come ritenga necessario innalzare gli *standard* di sicurezza, valutando anche l'ipotesi di escludere le aziende cinesi dalle reti 5G.

Alla luce di quanto espresso nella Relazione del Copasir, non sorprende come nel corso del 2020 l'approccio delle autorità italiane abbia iniziato a mutare. Influenzato anche dai nuovi equilibri politici del Governo Conte II e, più in generale, dal riallineamento dei paesi europei rispetto alle richieste statunitensi, si intensifica la cautela nei confronti di Huawei e ZTE.⁷² Nel luglio 2020, Telecom Italia ha escluso Huawei dai bandi di gara per l'acquisto di apparecchiature 5G in Italia e Brasile citando un'esigenza di diversificazione dei fornitori;⁷³ questa decisione rappresenta dunque il primo caso di esclusione di fatto di un fornitore cinese nella rete 5G in Italia.⁷⁴

⁷¹ Camera dei Deputati della Repubblica italiana, *5G e big data: audizione Huawei Italia*, si veda la precedente nota 53.

⁷² Alcune fonti di stampa hanno riportato la formulazione di linee guida che la Presidenza del Consiglio avrebbe condiviso con i principali operatori mobili in merito alle forniture di rete da parte di aziende extra-UE. Secondo tali fonti, le verifiche imposte sarebbero a tal punto stringenti da rendere di fatto impossibile la partecipazione di Huawei e ZTE nello sviluppo del 5G in Italia; in particolare si fa riferimento a ispezioni settimanali della componentistica e alla condivisione del codice sorgente. Non vi sono tuttavia fonti ufficiali che riportano la formulazione o i contenuti di tali linee guida.

⁷³ "Huawei esclusa dalla gara Telecom Italia per il 5G", *Ansa*, 10 luglio 2020, disponibile all'Url https://www.ansa.it/sito/notizie/tecnologia/tlc/2020/07/10/huawei-esclusa-dalla-gara-italiana-per-il-5g_b35603aa-f910-468d-8ebe-29027ae212d7.html.

⁷⁴ *Formiche.net* ha inoltre riportato l'esistenza di un DPCM firmato il 7 agosto recante disposizioni che non interdicono l'utilizzo di apparecchiature Huawei da parte di Telecom Italia ma richiedono il coinvolgimento della funzione Sicurezza dell'azienda nelle attività di controllo e ispezione. Tra le azioni richieste all'operatore, vi sono l'attivazione di adeguate misure di controllo degli accessi alla rete, verifiche di sicurezza semestrali, diversificazione verticale e orizzontale dei fornitori, e comunicazioni periodiche alla PdC in merito alle misure di sicurezza adottate. Si veda: Andrea Monti, "Il Dpcm Tim-Huawei e il superamento del nodo Cina. L'opinione del prof. Monti", *Formiche.net*, 23 agosto 2020, disponibile all'Url <https://formiche.net/2020/08/dpcm-tim-huawei-superamento-del-nodo-cina-lopinione-del-prof-monti>. *Formiche.net* riporta, inoltre, che il 23 ottobre il Governo Italiano, esercitando il Golden power, ha temporaneamente vietato all'operatore Fastweb l'utilizzo di componentistica Huawei nella parte core della rete, fino al momento in cui l'operatore chiarirà la sua strategia di sviluppo del 5G. Si veda: Otto Lanzavecchia, "Italy creates another roadblock for Huawei's 5G", *Formiche.net*, 23 ottobre 2020, disponibile all'Url <https://formiche.net/2020/10/italy-temporary-ban-huawei-5g-fastweb>.

Considerazioni conclusive

L'approccio italiano, evitando una formale esclusione delle due società cinesi o una scelta di campo dal forte valore simbolico, sembra dunque optare per un progressivo, seppur complicato, affrancamento dalla tecnologia cinese. Ciò si realizza, da una parte, irrobustendo la normativa nazionale a protezione delle infrastrutture critiche (sforzo che trova pieno riconoscimento in ambito europeo), dall'altra lasciando emergere un certo grado di incertezza tra gli operatori privati rispetto all'utilizzo delle forniture cinesi. Questo approccio ricalca per certi aspetti la posizione già adottata da altri paesi europei, tra cui la Francia. A fine settembre 2020 si è svolto un confronto sul tema del 5G presso la Presidenza del Consiglio dei Ministri, qualche giorno prima della visita del Segretario di Stato statunitense Pompeo. Qualificate notizie di stampa riportano una sostanziale comunità d'intenti tra maggioranza e opposizione nel procedere con l'approccio sopra descritto: la progressiva messa a punto della normativa, in senso sempre più stringente, e l'esclusione di fatto – non formalizzata – delle due società cinesi dalla rete di telecomunicazione nazionale. È opportuno inoltre segnalare l'esistenza di un dibattito in merito a un potenziale "open 5G"⁷⁵ che si baserebbe sulla costruzione di un ecosistema aperto e interoperabile che non si appoggi esclusivamente su pochi fornitori ma possa incoraggiare la partecipazione di una pluralità di imprese, vincolate da standard e requisiti di sicurezza comuni, in grado di offrire soluzioni per le varie componenti della rete, favorendo così la competizione e l'innovazione (come proposto dalla *O-Ran alliance*, di cui fanno parte alcuni tra i maggiori operatori mobili globali tra cui Tim e Vodafone).⁷⁶

In Italia sembra dunque consolidarsi un approccio che a livello nazionale prevede un aggiornamento dell'impianto normativo in senso sempre più restrittivo e una dotazione di poteri speciali agli organi di governo per la protezione delle infrastrutture critiche. A livello europeo, l'Italia si muove all'interno delle raccomandazioni della Commissione Europea seguendo il principio della sovranità tecnologica dell'UE, enunciato nella strategia *Shaping Europe's digital future* (2020).⁷⁷ Come descritto nel documento, la sovranità tecnologica europea si sostanzia nell'integrità e nella resilienza dell'infrastruttura di dati, reti e comunicazioni, riducendo la dipendenza dai paesi extra-UE e potenziando le capacità tecnologiche comunitarie. In ambito globale, si rileva un riallineamento dei paesi europei, compresa l'Italia, verso le richieste di Washington. Le misure messe in atto dall'amministrazione Trump e l'appoggio unanime del Congresso hanno contribuito a ridefinire la struttura degli incentivi per gli alleati europei e globali degli Stati Uniti. L'intensificarsi del conflitto tecnologico tra USA e Rpc non appare più inquadrato in una logica estemporanea e meramente reattiva della Casa Bianca, ma come una postura di medio-lungo periodo destinata a consolidarsi. La cristallizzazione di questa postura ha dunque incrementato sensibilmente i costi di un avvicinamento verso Pechino, facilitando la ricomposizione delle divergenze interne al campo atlantico.

⁷⁵ John Watts, "A framework for an open, trusted, and resilient 5G global telecommunications network", *Atlantic Council*, 4 marzo 2020, disponibile all'Url <https://www.atlanticcouncil.org/in-depth-research-reports/report/a-framework-for-an-open-trusted-and-resilient-5g-global-telecommunications-network>.

⁷⁶ O-Ran Alliance, "Operator members", 2020, disponibile all'Url <https://www.o-ran.org/membership>.

⁷⁷ Commissione Europea, *Shaping Europe's Digital Future*, febbraio 2020, disponibile all'Url https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.