Luiss Business School

Febbraio 2020

Il Sole 24 ORE Radiocor

DigitEconomy.24

L'INTERVISTA AL DIRETTORE GENERALE DEL DIS, GENNARO VECCHIONE

Tlc: Vecchione (Dis), concetto di sicurezza nazionale va circoscritto agli asset strategici

Il concetto di sicurezza nazionale, anche in ambito telco, non va dilatato all'estremo: vale per gli asset strategici, per il resto ci sono le regole del libero mercato.

È la posizione di Gennaro Vecchione, direttore generale del Dis, il Dipartimento delle informazioni per la sicurezza nell'intervista a DigitEconomy.24, una delle prime da lui rilasciate. «L'architettura della rete 5G è complessa e per ciò stesso presenta rischi per la sicurezza» e quindi «la principale preoccupazione è quella di coniugare la capacità di cogliere appieno tutte le opportunità che il 5G offre con l'abilità nel mitigare al massimo i fattori di rischio, agendo in ottica preventiva ». In generale in ambito telco, tra rete fissa e data center dove gli apparati cinesi sono presenti, Vecchione avverte che «non si può dilatare sino all'estremo il concetto di "sicurezza nazionale", a meno che non si ritenga di abbandonare il modello di economia aperta» e «quindi, il criterio in base al quale la protezione dei superiori interessi del Paese deve prevalere sulle regole del libero mercato è quello della rilevanza strategica dei settori e degli asset. Negli altri casi, non si interferisce nelle dinamiche della concorrenza».

Riguardo alla proprietà delle telco che in molti casi hanno azionisti di riferimento stranieri, Vecchione ricorda che c'è sempre la possibilità di applicare il Golden power, ma ribadisce: «deve trattarsi di asset strategici per la sicurezza nazionale. Altrimenti, non possono essere messe in discussione né la necessità di attrarre investimenti esteri né la contendibilità delle aziende».

>> continua a pag. 4

↑ **Gennaro Vecchione,** direttore generale del Dis

Coronavirus e ruolo delle telco da un lato; sicurezza delle reti e 5G dall'altro. Sono gli argomenti del IV report DigitEconomy.24, prodotto da Radiocor e Luiss Business School e pubblicato sul sito www.ilsole24ore.com. Con interventi di Gennaro Vecchione (Dis), Hu Kun (Zte Italia), Mirella Liuzzi (Mise), Nunzia Ciardi (Polizia postale).

Il ceo Italia, Hu Kun

«Per Zte nessun effetto coronavirus»

↑ **Hu Kun,** ceo di Zte Italia

L'impatto del coronavirus sul business della cinese Zte, uno dei più importanti fornitori di tecnologia per le telco che in Italia lavora con Wind Tre, Linkem, Fastweb, GoInternet e Tim, finora non c'è stato. Lo afferma in un'intervista a DigitEconomy.24 il presidente di Zte Western Europe e ceo di Zte Italia, Hu Kun.

>> continua a pag. 3

EMERGENZA CORONAVIRUS: PARLA LA SOTTOSEGRETARIA MIRELLA LIUZZI

Appello del Governo alle telco: accelerare sulle reti

Di fronte all'emergenza coronavirus il Governo chiede alle telco di accelerare gli investimenti nelle reti. L'appello arriva da Mirella Liuzzi, sottosegretaria al ministero dello Sviluppo economico, in una dichiarazione a DigitEconomy.24. La sperimentazione forzata del telelavoro, spiega Liuzzi, «ci porta a riflettere sull'effettiva necessità di assicurare, in tutto il territorio nazionale, condizioni infrastrutturali e servizi digitali di avanguardia, al fine di rendere il telelavoro una pratica stabile e consolidata e non solo una pronta risposta a necessità contingenti. Per fare questo occorre superare, una volta per tutte, l'annoso gap digitale che ancora oggi vede diversi distretti industriali del Paese tagliati fuori dalla banda ultra larga». Intanto le telco, dal canto loro, stanno monitorando l'evoluzione dell'epidemia e i suoi effetti, pensando a mettere in sicurezza i propri lavoratori, in primis proprio grazie a smart working e telelavoro.

L'importanza delle telecomunicazioni per affrontare rischi sistemici come quello da coronavirus è sottolineata dalla stessa Etno, l'associazione europea di settore, che a DigitEconomy24 dice: « le telco rimangono un'infrastruttura importante in tutti i momenti della vita di un Paese:

>> continua a pag. 2

Il DIBATTITO AL CONVEGNO LBS: LE DENUNCE DI CYBERCRIME +579% IN DUE ANNI

Sicurezza reti è priorità per le forze dell'ordine

La sicurezza delle infrastrutture e delle reti di tlc, siano esse fisse o mobili, è una priorità per le forze dell'ordine e per le istituzioni che si occupano di proteggere persone e aziende online. Nunzia Ciardi, direttrice della Polizia postale, non ha dubbi: il crimine cyber è «un'emergenza assoluta. In due anni le denunce arrivate in questo ambito sono aumentate del 579 per cento». Intervenendo alla Luiss Business School, Ciardi ha sottolineato che l'Italia non è tuttavia arrivata impreparata alla sfida del cybercrime: «Nel 2005, creando il Centro nazionale di protezione delle infrastrutture critiche (Cnaipic) abbiamo individuato l'esigenza di dotarci di un apparato di contrasto e l'abbiamo coltivata nell'ottica di un partenariato diffuso». La rete, ha aggiunto Ciardi, «è una rivoluzione antropologica», per gestire la quale «occorrono preparazioni trasversali e non solo tecniche». La sicurezza totale

↑ **Paolo Ciocca,** commissario Consob e il generale **Francesco Presicce**

«non è pensabile, è un orizzonte che si allontana continuamente», ha chiosato la direttrice rivelando come tra gli obiettivi degli attacchi ci siano, oltre ai cittadini, le pmi italiane. Queste ultime, ha spiegato, «hanno meno fondi da investire nella sicurezza informatica e spesso costituiscono il cavallo di Troia per gli attacchi alle grandi imprese». Un settore che sta facendo registrare un grande aumento degli attacchi è poi quello dei dati sanitari: i furti, ha detto Ciardi, sono cresciuti del 99 per cento. Ma, oltre alla sanità, uno dei comparti maggiormente esposti agli attacchi cyber è e sarà sempre di più quello finanziario: la presidente della Bce, Christine Lagarde, ha recentemente citato i risultati di un rapporto dell'European systemic risk board che stima il costo degli attacchi informatici tra 45 e 654 miliardi di dollari. Sempre parlando alla Business School, il commissario Consob Paolo Ciocca, ex vicedirettore Dis, ha spiegato che le infrastrutture critiche finanziarie sono sempre più simili alle tradizionali: «Più dati equivalgono a più vulnerabilità». Proprio per questo, Banca d'Italia e Consob hanno concordato una strategia per rafforzare la sicurezza informatica del settore attraverso misure rivolte alle infrastrutture finanziarie, come sistemi di pagamento, controparti centrali, depositari centrali e sedi di negoziazione dei titoli. Sulla stessa lunghezza d'onda il generale Francesco Presicce, capo Ufficio generale del capo di Stato maggiore della Difesa, che ha sottolineato come la minaccia cyber sia «ad alto spettro con effetti peggiori di un conflitto tradizionale». Il generale ha infine evidenziato come sia fondamentale la diffusione della cultura come educazione e formazione per arrivare a un "ecosistema cyber". ■

>>>DALLA PRIMA PAGINA - EMERGENZA CORONAVIRUS E 5G

Etno: «telco importanti per superare la crisi»

sia come volano di crescita sia come strumento per superare momenti di crisi. La situazione coronavirus non fa eccezione: l'Italia può contare sui suoi operatori e sui loro servizi».

D'altro canto ci sono segnali che potrebbero far pensare a un rallentamento della corsa al 5G: il 3GPP, l'organismo che fissa gli standard tecnologici del 5G, ha stoppato le riunioni a causa dei timori del contagio e bisogna ricordare che importanti fornitori di tecnologia sono cinesi. A questo riguardo Etno sottolinea invece l'importanza di adottare la strategia multi-vendor scelta dalle telco europee. Strategia che «consiste nel differenziare i vari fornitori: siano essi europei, asiatici o americani. È importante che, nel rispetto dei più alti standard di sicurezza europei e italiani, gli operatori possano approvvigionarsi presso i vendor migliori e più competitivi. Questo vale anche alla luce di possibili interruzioni momentanee delle supply chain, che possono essere dovute a molti fattori, tra i quali anche eventuali problemi commerciali legati a situazioni di epidemia, o a crisi internazionali». In termini di catena di fornitura, non rilevano problemi, ad esempio, nel quartier generale di Ericsson dove fanno notare che il gruppo «può vantare una supply chain globale con la presenza di stabilimenti produttivi in Usa, Brasile, Polonia, Estonia, Messico, India e Cina».

Al momento, quindi, il coronavirus non sembra bloccare le telco e i vendor che lavorano in Italia. Anzi, il 5G in particolare potrebbe giocare un ruolo da protagonista nell'affrontare crisi di questo tipo. La pensa così, tra l'altro, lo stesso Governo cinese che ha sollecitato gli operatori ad accelerare la costruzione della rete 5G. Le opportunità del 5G, in situazioni di emergenza, sono riconosciute anche dall'ex monopolista italiano Tim: «il 5G e tutte le applicazioni abilitate dal 5G aiuteranno e favoriranno sempre più la gestione di queste situazioni sia in termini di servizi, come ad esempio la telemedicina, sia logistici, come ad esempio le teleconferenze».

Uno dei primi atti del Governo italiano per contenere l'epidemia è stato proprio il provvedimento che consente ai dipendenti che risiedono nelle aree in quarantena di lavorare da casa. « Il telelavoro – aggiunge la sottosegretaria Liuzzi - equivale a garantire risparmi in termini economici, ambientali e non ultimo un miglioramento della qualità della vita dei dipendenti, per adottare in maniera diffusa queste buone pratiche basta semplicemente una connessione veloce e il mio auspicio è che si possa fare uno sforzo corale in questa direzione». Peraltro, sottolinea Etno, «i servizi tlc in Italia e in Europa sono resilienti e la connettività è tra le migliori al mondo. Secondo i dati della Commissione europea, la copertura del broadband fisso e mobile, in Italia, è prossima al 100% del territorio, in linea con i partner europei. In particolare, l'Italia ha un'ottima copertura del 4G, sempre prossima al 100 per cento».

Le principali conseguenze del coronavirus, per il mondo delle comunicazioni mobili, «sembrano invece ad oggi più rilevanti – aggiunge Etno - per il settore degli smartphone, dove una value-chain "just-in-time" è messa sotto pressione dalla chiusura di alcuni stabilimenti asiatici». Intanto sono gli stessi vendor e le telco a dare l'esempio e a puntare su misure preventive. Solo per citare qualche esempio Ericsson «in Italia sta privilegiando il ricorso allo smart working» e Huawei «ha introdotto misure di smart working per i dipendenti di Milano, Torino e Bologna». ■

di Simona Rossitto

«Zte: Il Copasir ci convochi, noi siamo disponibili»

Zte, dice il top manager, «ha reagito prontamente, sia dal punto di vista della protezione, della salvaguardia della salute e della sicurezza dei suoi dipendenti, sia dal punto di vista della produzione». Quanto in generale al clima che si respira nel nostro Paese per le aziende extra-europee, Zte non riscontra problemi, anzi apprezza «l'ambiente favorevole agli investimenti creato dal governo italiano». Tuttavia, dopo che il Copasir ha rilevato preoccupazioni circa l'ingresso delle aziende cinesi nelle reti 5G in Italia, Hu Kun annuncia di aver scritto una lettera al presidente Volpi per chiedere un incontro. «Il rischio informatico del 5G – spiega - è una questione importante per l'industria, e una chiara regolazione per tutte le parti del network, è molto importante per gestire al meglio il rischio, a prescindere dalla parte. Il primo nostro Cyber lab, a Roma, è pronto a fornire qualsiasi contributo indispensabile in base alle esigenze del governo».

↑ **ZTE Italia:** la sede di Roma

Il 2020 sarà l'anno del 5G, quali sono i progetti e gli obiettivi di Zte per l'Italia?

Siamo uno dei principali protagonisti del 5G, anche in Italia, e vorremmo contribuire all'industria del 5G del Paese sotti diversi aspetti, tra cui l'innovazione, la ricerca e la sicurezza. Zte è stata in grado di stabilire una partnership per il 5G con la maggior parte degli operatori telco italiani, al riguardo mi piace ricordare anche il lavoro fatto nell'ambito della sperimentazione 5G con il Mise (ministero dello Sviluppo economico). I nostri investimenti sono già partiti da tempo. Negli ultimi anni, Zte ha investito quasi 500 milioni di euro e nel 2020 continueremo ad attuare il piano stabilito.

Di recente avete annunciato il vostro interesse per la tecnologia fwa e in fibra. A che punto sono i vostri progetti?

Crediamo che l'fwa sia uno dei principali casi d'uso 5G in Italia. Lavoriamo da anni nel Paese per fornire le migliori soluzioni. Inoltre stiamo anche lavorando con gli operatori per offrire la tecnologia in fibra. Sia l'fwa che le tecnologie in fibra sono in linea con la situazione attuale, ma l'obiettivo è sicuramente fare molto di più rispetto a oggi in questi due settori.

Assieme agli investimenti avete in programma nuove assunzioni?

Il reclutamento è legato all'andamento del mercato, che dipende dagli sforzi di Zte, oltre che dalle politiche di investimento in Italia. Devo dire che riconosco al Governo italiano gli enormi sforzi per arrivare al risultato di un environment amichevole sia verso gli investitori stranieri che verso quello del nostro settore. Questo approccio è indispensabile e necessario per continuare. Abbiamo recentemente assunto ingegneri di sicurezza cibernetica al nostro Cyber security lab di Roma.

La commissione Ue ha chiesto di recente agli Stati membri di applicare regole rigide e restrizioni ai fornitori ritenuti rischiosi. Come commentate questo indirizzo che gli Stati dovranno applicare entro il 30 aprile?

Noi rispettiamo le decisioni prese dalla Commissione europea e dal Governo italiano. Zte è collaborativa e trasparente con qualsiasi richiesta governativa e continuerà a seguire questo approccio. Consideriamo come un buon inizio l'approccio scientifico e una valutazione onesta.

A dicembre il Copasir ha ritenuto fondate le preoccupazioni circa l'ingresso delle aziende cinesi nelle reti 5G in Italia. Che cosa vi sentite di rispondere e come valutate il clima in Italia nei confronti delle aziende extraeuropee?

Come appena sottolineato, l'ambiente favorevole agli investimenti, creato con successo dal governo Italiano, è molto apprezzato. Credo che sia fondamentale continuare questo approccio, soprattutto nelle complesse condizioni macro attuali. Per quanto riguarda il Copasir, noi non siamo stati convocati. Ho scritto una lettera al presidente Volpi per chiedere un incontro, esprimendo la nostra totale disponibilità e sono in attesa di una risposta. Il rischio informatico del 5G è una questione importante per l'industria, ed una chiara regolazione per tutte le parti del network è molto importante per gestire al meglio il rischio, a prescindere dalla parte. Il primo nostro primo Cyber lab, proprio a Roma, è pronto a fornire qualsiasi contributo indispensabile in base alle esigenze del governo.

Vedete problemi per il vostro business italiano a causa della diffusione del nuovo coronavirus?

Finora il nostro business in Italia non ha subito alcun impatto. Zte ha reagito prontamente, sia dal punto di vista della protezione che della salvaguardia della salute e della sicurezza dei suoi dipendenti, sia dal punto di vista della produzione. Inoltre, Zte ha contribuito alla costruzione della rete nel Wuhan Lei Shen Shan Hospital e ha supportato la costruzione di vari sistemi di comunicazione emergenti per il sistema medico nell'area dell'epidemia. ■

Volpi (Copasir): «Non sentiremo né Zte né Huawei»

↑ **Raffaele Volpi**, presidente del Copasir

"Botta e riposta tra Zte e Copasir che per il momento non sentirà i fornitori cinesi riguardo al tema della sicurezza delle reti 5G. «Se il Copasir ha preso determinate posizioni – ha dichiarato il presidente Raffaele Volpi a Radiocor - vuol dire che ha delle evidenze che non possono esser rese pubbliche». Al momento, ha chiosato Volpi parlando alla Luiss Business School, «non c'è necessità di sentire né Huawei né Zte». Il Comitato parlamentare per la sicurezza della Repubblica nella relazione diffusa il 19 dicembre scorso ha ritenuto «in gran parte fondate le preoccupazioni circa l'ingresso delle aziende cinesi nelle attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G»"

di Simona Rossitto

«Su 5G cogliere opportunità e mitigare rischi»

Il 5G costituirà il futuro delle tlc, ma abiliterà anche servizi cruciali come le smart cities o la telemedicina: la sicurezza di queste reti è quindi fondamentale. Qual è l'approccio del DIS?

Buona parte della risposta sta già nella sua domanda. Il 5G è una tecnologia abilitante. È un acceleratore della trasformazione digitale, offre opportunità di innovazione imperdibili. Ma, allo stesso tempo, costituisce un cambio di paradigma: non sono più i servizi ad adattarsi alla rete, è la rete che si adatta ai servizi, quindi chi la controlla si ritrova ad avere in mano leve importanti dello sviluppo economico. Non solo. L'architettura della rete 5G è complessa e per ciò stesso presenta rischi per la sicurezza. Al contempo, nella filiera del 5G si intrecciano, al livello globale, numerosi attori, in forte competizione fra loro, intenti a guadagnare posizioni di supremazia tecnologica. Il nostro approccio prende le mosse da queste consapevolezze. La principale preoccupazione è quella di coniugare la capacità di cogliere appieno tutte le opportunità che il 5G offre con l'abilità nel mitigare al massimo i fattori di rischio, agendo in ottica preventiva.

Con il 5G e l'IoT, il perimetro dei potenziali cyber attacchi crescerà. Come tutelarsi?

Certo, è come se in una casa aumentassero le finestre e le porte ed allo stesso tempo diminuisse la superficie dei muri. È evidente che quella casa sarà molto vulnerabile, specie se, fuor di metafora, i produttori e i fornitori dei diversi dispositivi e servizi tendono a privilegiare l'abbattimento dei costi rispetto alle funzionalità di sicurezza. Ci si tutela mettendo il giusto accento sulle misure di sicurezza cibernetica e sul controllo degli approvvigionamenti. Con "giusto accento" intendo dire che guardiamo non alla totalità delle infrastrutture tecnologiche, ma solo a quelle dalla cui permeabilità può derivare un pregiudizio per la nostra sicurezza. La nostra preoccupazione riguarda le componenti più sensibili degli asset digitali critici, il cui malfunzionamento può danneggiare gravemente i nostri interessi nazionali. L'iniziativa legislativa del Perimetro di sicurezza nazionale cibernetica nasce proprio dall'esigenza di tutelare quegli asset.

Dati, intelligenza artificiale, profilazione da una parte, privacy e sicurezza dall'altra: quale equilibrio?

Rispondo relativamente alla sfera di responsabilità che mi compete. Nel nostro ordinamento vige un articolato sistema di garanzie che assicura il giusto bilanciamento tra le istanze di protezione dei dati personali e le esigenze operative degli organismi informativi. Noi possiamo raccogliere e trattare notizie e informazioni esclusivamente per il perseguimento degli scopi istituzionali dell'Intelligence, secondo criteri sottoposti al controllo parlamentare. A completare la cornice delle garanzie, oltre ad una disciplina ad hoc armonizzata con quella comunitaria, vi è anche una nostra collaborazione strutturata con il Garante della Privacy, estesa pure alla cooperazione nel campo della sicurezza informatica.

La sicurezza nazionale viene prima di ogni altra cosa: i produttori cinesi tuttavia investono e creano posti di lavoro in Italia. Il Copasir ha di recente invitato ad alzare la guardia: quale l'approccio corretto di lungo termine?

Dipende, bisogna distinguere fra tre aspetti, che comunque sono collegati fra loro, anche sul piano normativo. Per quel che riguarda il procurement, l'approccio corretto è quello che ha ispirato il Governo nel promuovere l'iniziativa del Perimetro, di cui parlavo prima. È una soluzione legislativa che non lascia margini all'arbitrarietà, non ci saranno né aperture a priori né chiusure pregiudiziali, verso nessuno. Verranno sottoposti a scrutinio tecnologico i dispositivi identificati come particolarmente sensibili da un'analisi del rischio effettuata dal competente Centro di valutazione. Per quanto concerne gli investimenti esteri, l'impianto legislativo nazionale è coerente con la normativa europea. Nel marzo del 2019 è stato introdotto un Regolamento che prevede un significativo ampliamento dei settori rispetto ai quali gli Stati membri possono scrutinare operazioni di investimento da parte di soggetti extraeuropei, tra cui l'alta tecnologia. Con le iniziative legislative nazionali abbiamo saputo anticipare l'implementazione di quelle norme europee.

Per quel che attiene, infine, al 5G, la principale novità apportata lo scorso anno alla normativa sull'esercizio dei poteri speciali, il cosiddetto Golden Power, ha inteso ricomprendere proprio il 5G tra le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Anche in questo caso, ci siamo trovati avanti in Europa, tanto da sedere nel gruppo di testa dell'assessment comunitario sulle reti 5G che ha originato il toolbox pubblicato a gennaio.

Naturalmente, le norme sull'estensione dei poteri speciali al 5G sono raccordate con quelle del Perimetro, così che possiamo fare affidamento su un quadro legislativo coerente ed organico.

Sicurezza delle reti non è solo 5G, ma anche rete fissa e data center, dove gli apparati cinesi sono presenti a tutti i livelli. La "vigilanza" su questi elementi è meno importante?

La legge attribuisce all'Intelligence il compito di difendere i nostri interessi politici, militari, economici, scientifici ed industriali. Come vede, è un novero molto ampio, nel cui ambito è fondamentale distinguere fra gli interessi vitali, che se venissero compromessi metterebbero a repentaglio il Paese, e tutti gli altri. Non si può dilatare sino all'estremo il concetto di "sicurezza nazionale", a meno che non si ritenga di abbandonare il modello di economia aperta, che invece deve continuare a caratterizzarci al pari delle altre democrazie occidentali, per abbracciare formule dirigistiche o protezionistiche che non ci appartengono. Quindi, il criterio in base al quale la protezione dei superiori interessi del Paese deve prevalere sulle regole del libero mercato è quello della rilevanza strategica dei settori e degli asset. Negli altri casi, non si interferisce nelle dinamiche della concorrenza.

Gli assetti proprietari delle telco nel nostro Paese vedono azionisti di riferimento cinesi, inglesi, francesi: può essere un problema nel lungo periodo?

Il punto importante è che, qualora lo divenisse, saremmo in grado di intervenire alla luce della normativa vigente. Quanto alle telco, la disciplina sul Golden Power può applicarsi o alle reti attraverso le quali transitano dati e informazioni sensibili; oppure agli operatori, a fronte di operazioni di acquisto di partecipazioni societarie, fusioni, scissioni, trasferimento di controllate.

In entrambi i casi, a seguito della notifica che la legge impone, il Governo valuta l'esercizio dei poteri speciali, attenendosi ai criteri stabiliti.

Ma, ripeto, deve trattarsi di asset strategici per la sicurezza nazionale. Altrimenti, non possono essere messe in discussione né la necessità di attrarre investimenti esteri né la contendibilità delle aziende. ■

di Ivan Dompé