di **Fabio Massimo Parenti e Igor Kranjec**

da http://www.beppegrillo.it

Con l'avanzare dell'era digitale molti paesi sono impegnati a riadattare i propri sistemi socioeconomici in funzione della "quarta rivoluzione tecnologica", incardinata in una crescente connettività tra persone, cose e luoghi, nonché in una straordinaria capacità di elaborazione dei dati, in termini quantitativi e qualitativi.

Un simile riadattamento sta generando inevitabilmente un enorme dibattito politico, che, a nostro avviso, dovrebbe ruotare intorno alle seguenti domande: Quali sono i "confini digitali" di un paese? Quali le vulnerabilità? In che modo è possibile ovviare ai problemi relativi alla insicurezza cibernetica?

La necessità di costruire una rete unica, a controllo statale

Il dibattito sui confini digitali nazionali è connesso a quello sulla necessità di costruire una rete unica sotto controllo pubblico, senza escludere collaborazioni con compagnie straniere. Cos'è la rete unica? È un insieme di infrastrutture di comunicazione statali che collegano gli utenti ai fornitori di servizi. Insomma, è quella che avevamo con Telecom e che abbiamo smantellato a partire dall'avvio del processo di privatizzazione. Oggi la rete nazionale è infatti composta da molteplici soggetti, per i ripetitori, i tralicci, le dorsali in fibra e l'ultimo miglio. Col 5G vi è l'occasione, potenziale, per ridefinire una rete unica statale.

Per fare chiarezza su ciò, ci siamo avvalsi dell'aiuto di Igor Kranjec, già Chief Security Officer del gruppo Engineering Ingegneria Informatica e con una lunga esperienza nel campo dell'IT,

soprattutto in relazione alle questioni della sicurezza informatica. Innanzitutto dobbiamo sgombrare il campo da un luogo comune: internet non è uno spazio libero da condizionamenti politici, economici e sociali, non è sinonimo di libertà in senso assoluto e, soprattutto, riflette la geografia dei rapporti di forza. La “rete” è un’entità fisica, dotata di una propria geografia che non sfugge alle dinamiche geopolitiche. Lo abbiamo visto e continuiamo a sperimentarlo nell’ambito della competizione tra Cina, Usa e Russia ed in molteplici altre dispute geopolitiche.

Internet ha dunque una sua geografia fisica che è composta dalle infrastrutture di rete, cavi ed antenne. Quest’ultime collegano abitazioni, uffici ed attività varie coi Centri di Elaborazione Dati (CED), dove vengono gestiti e immagazzinati tutti i dati che vi transitano. Cavi ed antenne rappresentano pertanto una sorta di sistema nervoso digitale governato da molteplici “cuori-cervelli”, che sono i CED. Dove si trovano questi centri? A parte poche eccezioni, i più importanti sono dislocati in paesi extraeuropei.

Date le numerose minacce digitali, i governi nazionali hanno il dovere di impiegare tutte le risorse necessarie atte a garantire la sicurezza dei propri cittadini. Ciò è tanto più evidente al giorno d’oggi quando la pandemia mondiale sta spingendo l’economia e le attività quotidiane verso una “trasformazione digitale” forzata. In questo contesto, i “virus” digitali sono in grado potenzialmente di bloccare una fabbrica, interrompere l’energia ad un ospedale, o ancor peggio essere veicoli di attacchi più sofisticati per manipolare l’opinione pubblica di un paese. Avere una rete unica permetterebbe di monitorare le infrastrutture e supervisionare le uniche vie digitali di accesso per operare all’interno di un paese; un aspetto tanto più importante se si considera che la maggior parte dei servizi informatici (posta elettronica, piattaforme social, messaggistica, antivirus ecc.) sono forniti quasi sempre da soggetti stranieri. E questo è vero non solo per l’Italia, ma per la maggior parte dei paesi del mondo, fatta eccezione per la Cina e in misura minore per la Russia.

La rete unica per la sicurezza dei dati

Negli anni i governi hanno predisposto accordi internazionali di cooperazione e regolamenti specifici. Tuttavia, queste normative non sono di facile applicazione. Le nostre istituzioni, le uniche titolate a difendere la privacy dei propri cittadini, obbligano un qualsiasi ente pubblico o privato a conformarsi alla normativa sulla privacy, ma non possono garantirne il rispetto, non essendo in grado di intervenire tempestivamente ed efficacemente su quei gestori di rete e soprattutto su quei fornitori di servizi che controllano, privatamente, la geografia fisica delle reti ed il relativo flusso di dati.

Se un cittadino utilizza un servizio di posta elettronica come Gmail, Apple, Outlook, QQ, Sina, Sohu, la sua vita privata e professionale viene affidata ai gestori di questi servizi. Chi avrà la responsabilità di garantirne la sicurezza? Se un utente italiano utilizza un servizio erogato da una società cinese, russa o statunitense dovrà rispettare le leggi italiane, ed è lo stato italiano a doverne garantire la sicurezza. Tutto ciò richiede il controllo nazionale delle reti.

Il dibattito in Italia

Dai recenti dibattiti sull’impiego di tecnologie straniere si evince che il problema della sicurezza

informatica non è sempre compreso appieno nel nostro paese. Sebbene il governo italiano si sia speso negli ultimi anni per definire nuovi organi statali (CSIRT, COR e CVCN), nel contempo si è concentrato sulla possibilità di imporre veti tecnologici, ponendo questo come uno dei principali problemi di sicurezza nazionale. Di fatto si tratta per lo più di una questione geopolitica e di proteggere un oligopolio commerciale, autorizzando implicitamente le compagnie statunitensi a governare i dati di mezzo mondo, indipendentemente dalla loro paternità nazionale.

Molta attenzione è stata posta sull'impiego di tecnologia cinese per l'allestimento delle nuove reti 5G, dimenticando tuttavia che la maggior parte degli apparati utilizzati per il 4G e per le reti in fibra ottica sono già da tempo di società straniere. Per di più le accuse non si fondano su evidenze tecniche (si veda il rapporto GSMA), ma rappresentano un processo alle intenzioni che, in qualunque caso, andrebbero valutate sul piano della fattibilità tecnica, anziché della speculazione puramente politica.

È opportuno ricordare che trafugare dati da antenne 5G è piuttosto improbabile: la quantità di dati che un'antenna gestisce è tale da inibire la possibilità di fare un "doppio lavoro" (raccogliere dati e garantire il normale funzionamento), senza impattare sulle prestazioni e senza destare sospetto. Diversamente, se lo stesso ragionamento lo applicassimo ai servizi di posta elettronica o ai Sistemi Operativi (Windows, Android, Ios), la possibilità di interrompere un servizio o manipolare e trafugare dati sarebbe tecnicamente più agevole. Si potrebbero ad esempio prendere informazioni utilizzando "falle" su questi sistemi e quindi raccogliere capillarmente informazioni da qualunque dispositivo, in qualunque momento e luogo, impattando minimamente sulle prestazioni dei servizi erogati al pubblico. Non dovrebbe sorprendere, dunque, come questa tipologia di minacce non rappresenti un'ipotesi, bensì una realtà, come dimostrato in modo incontrovertibile dall'esistenza degli antivirus e di innumerevoli altri prodotti nati con l'obiettivo di "ridurre" questi rischi. Altre evidenze vengono direttamente dalle prove sulla vulnerabilità dei servizi informatici eseguite dagli addetti ai lavori. In sintesi: sono i servizi informatici e le loro società di gestione dei dati a rappresentare maggiormente l'ecosistema ombra della cyber (in)security.

Alla luce di queste considerazioni, suggeriamo di guardare ai problemi della sicurezza informatica nel loro insieme. Chi incrimina dei paesi come possibili "spioni" fa leva sull'impreparazione diffusa, spesso anche al livello politico, su questi temi. Quali sono pertanto le priorità dell'Italia in materia di sicurezza cibernetica? Il punto non è in alcun modo estromettere questo o quell'operatore straniero, ma costruire una visione a lungo termine che garantisca all'Italia, ai suoi cittadini, la realizzazione di una rete unica di nuova generazione sotto stretto controllo statale.

GLI AUTORI

Fabio Massimo Parenti è attualmente Foreign Associate Professor di Politica Economica Internazionale alla CFAU. In Italia insegna all'Istituto Internazionale Lorenzo de' Medici a Firenze, è membro del think tank CCERRI, Zhengzhou, e membro di EURISPES, Laboratorio BRICS, Roma. Il suo ultimo libro è Geofinance and Geopolitics, Egea.
Su twitter @fabiomassimos

Igor Kranjec, esperto e ricercatore nell’ambito tecnologico. Ex Corporate CSO – Chief (Information) Security Officer presso Engineering Ingegneria Informatica Spa