Ilaria Garaffoni

Tra Covid e conflitto: sicurezza fisica e logica mai così intrecciate

Nel talk show di apertura di secsolutionforum2022 si è entrati a gamba tesa sulle questioni aperte in tema di sicurezza fisica e logica, amplificate dalle radicali trasformazioni indotte da due anni di pandemia prima, e dal conflitto in Ucraina poi.

secsolutionforum
The digital event for the security industry

ILARIA GARAFFONI
Giornalista, responsabile di redazione di Secsolution Magazine

ALVISE BIFFI
CEO Secure Network e vicepresidente Assolombarda

GIULIO IUCCI
Presidente ANIE Sicurezza

PIERLUIGI PERRI
Avvocato, Professore di Sicurezza informatica, privacy e protezione dei dati sensibili, Università Statale di Milano

ALESSANDRO BOVE
Ricercatore di tecnica e pianificazione urbanistica, Università di Padova

ALESSANDRO MANFREDINI
Direttore Group Security & Cyber Defence del Gruppo A2A e vicepresidente AIPSA

Alvise Biffi

Con la guerra ci siamo magicamente accorti che i principali sistemi ICT italiani sono protetti dal Signor Kaspersky, di passaporto russo. Il DL 21/22 ha quindi imposto alle P.A. di adottare soluzioni non riconducibili ad aziende/tecnologie di origine russa. Ci stiamo insomma orientando verso un processo di conseguimento della sovranità tecnologica in ambito cybersecurity. Ma secondo il Copasir per raggiungere l'obiettivo servono tre priorità: 5G, cloud nazionale e rete unica. Cosa significa in concreto? Cosa si dovrà fare e come? Con quali tempi? E comunque servirà energia: nelle more avremo dei buchi di sicurezza?

5G, cloud nazionale e rete unica richiedono ovviamente energia, e tanta, quindi dobbiamo ragionare a monte su una logica di sovranità energetica, non solo nazionale ma europea. Il progetto GAIA X, che collega i diversi ecosistemi cloud esistenti per far interagire dati e banche dati tra loro e renderli disponibili ai cittadini UE, con la creazione di nuove piattaforme multicloud, purtroppo sta già mostrando le prime difficoltà. Ma cloud cosa vuol dire? Banalmente: siamo passati dal tenere i dati sul nostro PC ad avere più computer dentro lo stesso PC con la virtualizzazione e da lì, grazie alla rapidità dei collegamenti, ci siamo spostati su server aziendali e infine sui data center terzi dei cloud provider. A quel punto abbiamo trovato più conveniente affittare direttamente lo storage e poi la capacità di calcolo e infine le piattaforme, i servizi, i software, e così via. Abbiamo certamente acquisito vantaggi in termini

di costo, capacità di calcolo e flessibilità, ma ci siamo portati in casa nuovi rischi. In particolare, guardando all'attualità, il rischio geopolitico: se i fornitori di cloud non sono nazionali, o se l'infrastruttura nazionale passa da nodi tecnologici di proprietà terza (ed è ormai così in un mondo globale), in assenza di un'alleanza forte tecnologica, potremmo subire un taglio netto di risorse da paesi ostili. Si tratta di una semplificazione perché ovviamente esistono clausole di salvaguardia, contrattuali e non solo, ma il rischio sussiste e va tenuto presente.

Giulio Iucci

In questo conflitto Anonymous ha dimostrato come sia facile "bucare" delle webcam, scoprendo un nervo piuttosto sensibile della videosorveglianza: la sicurezza cyber. Può cambiare qualcosa per il nostro settore con il DL 21/22? I nostri sistemi di protezione fisica su che reti viaggiano? Con quali soluzioni cyber sono protetti?

I relatori fanno parte del Comitato Scientifico di secsolutionforum e, in collaborazione con gli organizzatori, hanno definito gli indirizzi del palinsesto dell'edizione 2022

Anonymous è un collettivo di complessa identificazione che opera su diversi fronti, come diverse sono le operazioni di disturbo cyber che può mettere in campo: intercettazione di dati, modifica, blocco. Il tema dell'attacco ai sistemi TVCC non è una novità; è invece relativamente recente il tema dell'hacking ottenuto per il tramite di Intelligenza Artificiale. La risposta potrebbe essere un uso della stessa AI a scopo difensivo, tuttavia occorre tenere presente che deve esserci rispondenza tra i dati di addestramento e quelli presenti nella realtà e che l'AI richiede training test di lunghissima durata, ottenuti peraltro con un'enorme quantità di dati. Il vero obiettivo difensivo, non potendo raggiungere un utopico rischio zero, è quindi fare in modo che l'attacco non risulti conveniente, per scarsa monetizzazione dei risultati ottenuti o per eccessivi tempi di aggressione richiesti. Si tenga presente che in molti casi il vero danno di un attacco è generato dal non essersi accorti in tempo utile della violazione. Il DL 21/22 porterà un miglioramento ma la parte industriale ha bisogno di strategie più lunghe e strutturate. Gli stessi sistemi di videosorveglianza sono peraltro molto variegati, presentano approcci diversi non solo in termini di prodotto, ma di gare e di reti, che invero rappresentano il maggior punto di vulnerabilità. In questo senso il 5G dovrebbe garantire maggior protezione cyber, anche se, soprattutto nella PA, si riscontra spesso una stratificazione di apparati che dovrà essere ristrutturata: lo Stato deve svecchiare la tecnologia e portarla su un livello di attualità, almeno in termini di infrastrutture e punti nodali.

Pierluigi Perri

Impossibile a questo punto non parlare di sicurezza del dato. Curioso che nell'azione di Anonymous sopra citata fossero inizialmente state hackerate anche diverse webcam domestiche, poi eliminate dal progetto per rispetto della privacy dei civili russi. Che pensiero delicato. L'Unione Europea, parlando di AI, si è espressa di recente regolamentando tutta la filiera coinvolta nella fornitura, importazione, distribuzione e uso di sistemi AI. Di cosa si tratta?

Nella videosorveglianza anche ai livelli più basici, penso ai sistemi domestici da lei citati, si generano dati che finiscono nel cloud: sono dati esposti. Esistono veri motori di ricerca che registrano i dispositivi IoT: ne catalogano modello, firmware, versione. Attaccare una webcam domestica non richiede quindi nemmeno una particolare perizia: basta che l'utente abbia installato il device senza le dovute attenzione, mantenendo ad esempio la password di default. Salendo di livello, la videosorveglianza è anche uno strumento importante di pubblica sicurezza e qui entra in gioco l'AI. Il caso Clearview AI (che pare stia peraltro offrendo i suoi servizi anche alle due parti attualmente in conflitto) ha usato la metodologia del web scraping per raccogliere i dati condivisi su social, content provider e user generated content per dar vita ad un immenso database di riconoscimento facciale. Clearview AI ha sostenuto di rivolgersi alle FFOO a scopi di law enforcement ma (a pensare male si fa peccato ma spesso ci si prende...) in genere le aziende operano per profitto, quindi i rischi sono notevoli. Se poi questo tipo di aziende fallisce, viene rivenduto con tutto il pacchetto dati: esistono in tal senso sono casi già attenzionati dalla giustizia. Il Garante è quindi intervenuto contro Clearview AI bloccando la raccolta di dati sul territorio italiano (ma non è detto che non si riesca a carpire dati di italiani su altri server esteri...). Il principio è: il fatto che una fonte sia accessibile non significa che di tali dati si possa fare un uso indiscriminato, soprattutto a fini commerciali.

Alessandro Bove

Parlando di AI entriamo ora nel tema della smart city. Una città che garantisce sicurezza contro i rischi ambientali, sanitari, criminali, anche nelle sue accezioni cyber, terroristici o - possibilità oggi da considerare - di altri paesi. Per ottenere questo, lato tecnologia serve una rete sensoristica avanzata, fatta magari di torri intelligenti che possano trasmettere dati di monitoring e alert su qualsiasi rischio in tempo reale. Ma serve anche una progettazione urbanistica pensata per garantire un approccio di sicurezza con una visione complessiva sulla città. Visione che in uno scenario di guerra può prevedere forse anche la definizione di bunker, nuove vie di esodo, altri tipi di alert? Come il Covid ci ha imposto di ripensare la gestione e la progettazione delle città anche in senso sanitario, la guerra ci imporrà un nuovo pensiero urbanistico?

"La città dei bits" di J. William Mitchell è un libro uscito negli anni 90 che paventava la nascita di ambienti digitali ed edifici virtuali disseminati in insediamenti senza apparenti frontiere, al contempo villaggi e megalopoli, che avrebbero "sgretolato" il concetto di città. In realtà neanche il Covid ha abbattuto le relazioni umane. È vero che la digitalizzazione impone di passare da impianti a base materica "a calcestruzzo" (che non necessita di manutenzione), a sistemi ICT che obbligano ad un costante aggiornamento. In un mondo che non conosce più città "locali" (ormai viviamo tutti in città *globali*), comunicazione, connessione e spostamenti diventano temi centrali. Il covid ce l'ha insegnato. Cosa chiede una città smart alla tecnologia? Chiede di integrare la tecnologia nella città, cioè di usare i dati raccolti anche a scopi di progettazione urbanistica, pianificazione e costruzione di servizi e welfare sociale. La vera sfida è quindi creare delle smart city technology-driven, ma sempre human centriche. Perchè le città smart non siano solo un aggregato di tecnologia, serve anche costruire una nuova fiducia partendo dal basso con un vasta operazione culturale che illustri opportunità e anche pericoli dell'ICT. In quel senso si potrà "sgretolare la dimensione di pietra (calcestruzzo) e acquisire la dimensione del dato (IT)".

Guarda il video del talk show

Alessandro Manfredini

La smart city deve creare welfare, ha detto Bove, portandoci dritti ad un altro tema, attualissimo: quello della razionalizzazione dei costi, degli interventi, delle procedure. Un tema che riguarda da vicino le competenze del Security Manager, che hanno vissuto un'evoluzione in parallelo all'evoluzione che ha subito il panorama di rischi. Il primo step è stato la pandemia, che ha dato una forte spinta al concetto di resilienza. Ma oggi il concetto di resilienza e le soluzioni conseguenti si sono estese ai temi della sostenibilità (Bio Security, Crisis Management ambientale, Data Ethics & Responsibility), portando i Security Manager a rivedere le proprie competenze, anche in ottica ESG. Cosa ne pensa? La sicurezza deve essere sostenibile? In che modo le organizzazioni devono rivedere i propri modelli tradizionali di governance e analisi dei rischi e quale può essere il ruolo-guida del security manager in questi processi?

Sicuramente stiamo vivendo un'evoluzione radicale: la security sta infatti entrando a gamba tesa, anche attraverso la cyber security, all'interno dei bilanci di sostenibilità delle organizzazioni. Molte società inseriscono oggi, tra gli indicatori di sostenibilità, anche le tematiche di security. Il vero tema e la sfida, a questo punto, è non essere autoreferenziati: anche per la security, per individuare gli indicatori in materia di sistemi ESG, si deve di necessità partire da una matrice. E' il mercato che chiede oggi alla aziende di prendere in considerazione tute le tematiche che riguardano la sicurezza: security, cyber security, protezione dei dati, tutto ciò che i cittadini/clienti conferiscono alle aziende per ottenere beni/servizi va protetto. Il security manager non può prescindere da queste tematiche ed è fondamentale abbinare questi indicatori ai tradizionali sistemi di gestione della sicurezza. Le stesse certificazioni aziendali ISO andrebbero riviste in una chiave di supporto al bilancio di sostenibilità con meccanismi di misurazione dell'impatto ambientale ed energetico. Il mercato ha già messo a disposizione delle piattaforme per misurare la predisposizione di un'organizzazione rispetto al tema ESG: come saranno applicati questi modelli parametrati dipenderà però molto dalle amministrazioni pubbliche, che giocano un ruolo primario.

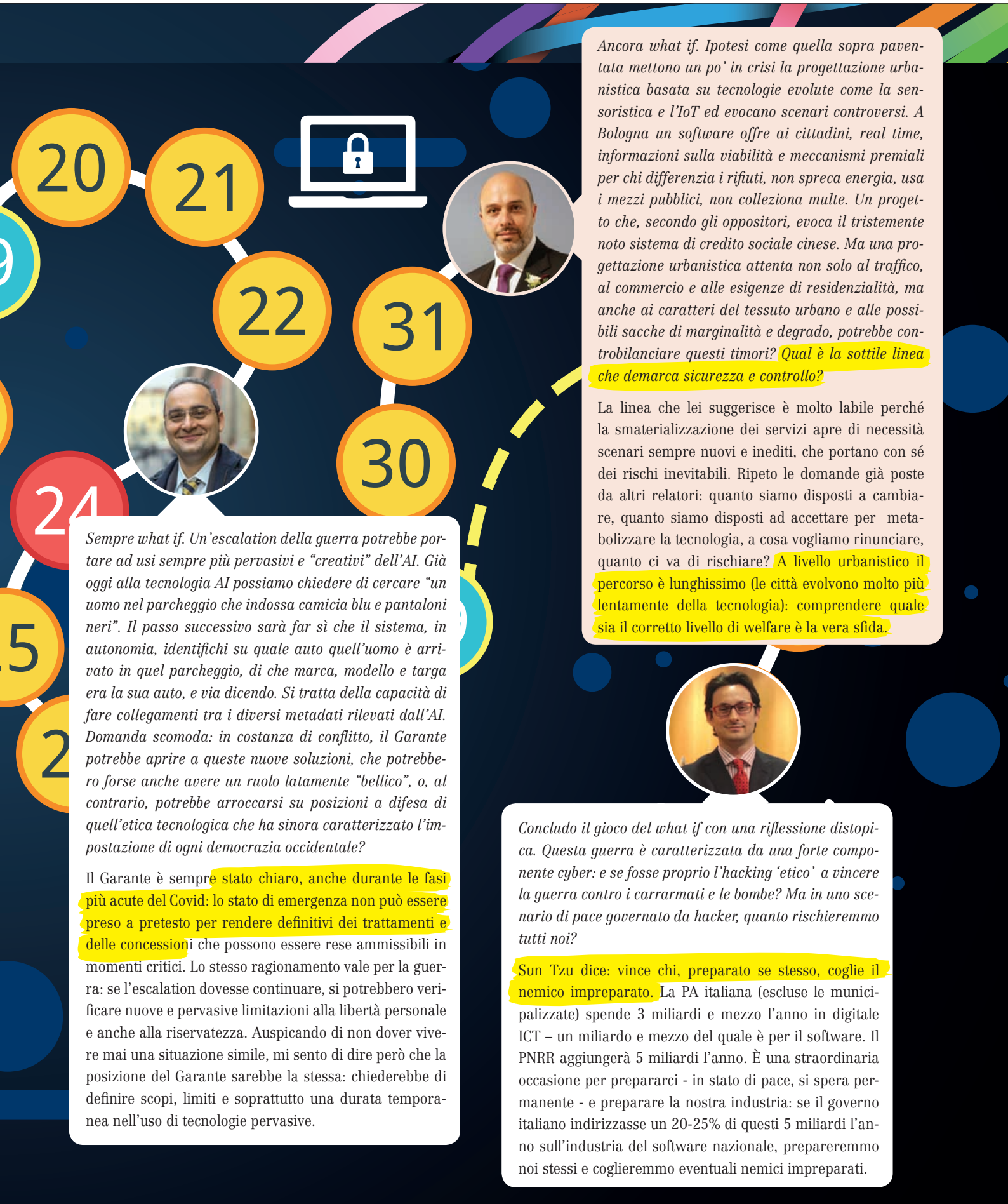
Giochiamo a what if. Viviamo ormai in un contesto di sanzioni e controsanzioni, dove le attività industriali possono dover cessare da un momento all'altro le proprie relazioni commerciali con alcuni paesi o magari essere costrette ad importare componenti o materiali da nuovi partner, con altre condizioni. Il nostro però è un comparto che produce un "bene" sensibile, che non ammette buchi o disservizi. Come si arginano questi rischi?

La globalizzazione è un fenomeno irreversibile: tutte le filiere hanno processi produttivi "globali", che la business continuity impone peraltro di tenere interamente sotto controllo. Il PNRR ci offre però importanti opportunità da cavalcare per sviluppare un software nazionale (che è cosa ben diversa da un apparato, un prodotto o da un componente nazionale). In tal senso vantiamo vere eccellenze italiane, sia in ambito industriale che accademico: se il Governo sosterrà le PMI italiane nel processo di R&D (evitandone l'immediata acquisizione da multinazionali una volta "startuppate...), potremo tenerci "in casa" - se non il mattone - almeno il cuore dei sistemi.

Ancora what if. In uno scenario come quello attuale, sarebbe pensabile che il mercato della sicurezza venisse selezionato dalla stessa utenza, oltre che sulla base dell'etica, della sicurezza cyber, del rispetto del GDPR, della vicinanza territoriale e politica, anche sulla base della sostenibilità industriale (che peraltro è diventato esso stesso un tema strettamente politico, vista la situazione energetica)? E' lecito pensare che l'attuale scacchiera italiana del mercato della sicurezza possa riorganizzarsi su altri cardini, ad esempio l'affidabilità cyber, la sovranità tecnologica, l'affinità geopolitica rispetto agli utilizzatori?

Le leve di cui gode il security manager per consigliare le aziende partono dalla stessa compliance aziendale. Ma il tema è a monte ed è culturale: quanto siamo disposti a spendere in più per avere un prodotto o servizio sicuro e sostenibile? Quanto siamo disposti a mettere in discussione le nostre abitudini quotidiane, a partire da un uso razionale del termostato di casa? La stessa cosa deve avvenire nell'industria e nella filiera della sicurezza, comprensiva dell'utenza. Serve maggiore consapevolezza nell'acquisto da soggetti sostenibili, etici, valoriali e questo passa per forza da un'autonomia della produzione: diversamente si soffrirebbe una competizione insostenibile. Qualche segnale già si coglie nel mondo cyber, io sono fiducioso.

Concludo con una frase di CEO di Apple, Tim Cook: *"non credo sia utile barattare dati personali contro servizi solo perché sono gratuiti, anche perché alla fine questi servizi sono tutto fuorché gratuiti..."*



Sempre what if. Un'escalation della guerra potrebbe portare ad usi sempre più pervasivi e "creativi" dell'AI. Già oggi alla tecnologia AI possiamo chiedere di cercare "un uomo nel parcheggio che indossa camicia blu e pantaloni neri". Il passo successivo sarà far sì che il sistema, in autonomia, identifichi su quale auto quell'uomo è arrivato in quel parcheggio, di che marca, modello e targa era la sua auto, e via dicendo. Si tratta della capacità di fare collegamenti tra i diversi metadati rilevati dall'AI. Domanda scomoda: in costanza di conflitto, il Garante potrebbe aprire a queste nuove soluzioni, che potrebbero forse anche avere un ruolo latamente "bellico", o, al contrario, potrebbe arroccarsi su posizioni a difesa di quell'etica tecnologica che ha sinora caratterizzato l'impostazione di ogni democrazia occidentale?

Il Garante è sempre stato chiaro, anche durante le fasi più acute del Covid: lo stato di emergenza non può essere preso a pretesto per rendere definitivi dei trattamenti e delle concessioni che possono essere rese ammissibili in momenti critici. Lo stesso ragionamento vale per la guerra: se l'escalation dovesse continuare, si potrebbero verificare nuove e pervasive limitazioni alla libertà personale e anche alla riservatezza. Auspicando di non dover vivere mai una situazione simile, mi sento di dire però che la posizione del Garante sarebbe la stessa: chiederebbe di definire scopi, limiti e soprattutto una durata temporanea nell'uso di tecnologie pervasive.

Ancora what if. Ipotesi come quella sopra paventata mettono un po' in crisi la progettazione urbanistica basata su tecnologie evolute come la sensoristica e l'IoT ed evocano scenari controversi. A Bologna un software offre ai cittadini, real time, informazioni sulla viabilità e meccanismi premiali per chi differenzia i rifiuti, non spreca energia, usa i mezzi pubblici, non colleziona multe. Un progetto che, secondo gli oppositori, evoca il tristemente noto sistema di credito sociale cinese. Ma una progettazione urbanistica attenta non solo al traffico, al commercio e alle esigenze di residenzialità, ma anche ai caratteri del tessuto urbano e alle possibili sacche di marginalità e degrado, potrebbe controbilanciare questi timori? Qual è la sottile linea che demarca sicurezza e controllo?

La linea che lei suggerisce è molto labile perché la smaterializzazione dei servizi apre di necessità scenari sempre nuovi e inediti, che portano con sé dei rischi inevitabili. Ripeto le domande già poste da altri relatori: quanto siamo disposti a cambiare, quanto siamo disposti ad accettare per metabolizzare la tecnologia, a cosa vogliamo rinunciare, quanto ci va di rischiare? A livello urbanistico il percorso è lunghissimo (le città evolvono molto più lentamente della tecnologia): comprendere quale sia il corretto livello di welfare è la vera sfida.

Concludo il gioco del what if con una riflessione distopica. Questa guerra è caratterizzata da una forte componente cyber: e se fosse proprio l'hacking 'etico' a vincere la guerra contro i carrarmati e le bombe? Ma in uno scenario di pace governato da hacker, quanto rischieremmo tutti noi?

Sun Tzu dice: vince chi, preparato se stesso, coglie il nemico impreparato. La PA italiana (escluse le municipalizzate) spende 3 miliardi e mezzo l'anno in digitale ICT – un miliardo e mezzo del quale è per il software. Il PNRR aggiungerà 5 miliardi l'anno. È una straordinaria occasione per prepararci - in stato di pace, si spera permanente - e preparare la nostra industria: se il governo italiano indirizzasse un 20-25% di questi 5 miliardi l'anno sull'industria del software nazionale, prepareremmo noi stessi e coglieremmo eventuali nemici impreparati.