Memoria Scritta

Andrea Chiappetta, PhD – Docente di *Data, algorithms and identities* – Facoltà di Scienze della Comunicazione – Università Niccolò Cusano ed esperto di Cybersicurezza.

In merito alla
Conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale – C.3161.

Di seguito, riporto alcune mie considerazioni sul tema:

Da molto tempo si parla di "Mercato unico digitale", ma un importante passo avanti viene fatto nel 2015 e trova fondamento nell'articolo 114 del trattato sul funzionamento dell'Unione Europea (TFUE) in merito all'adozione di misure relative al ravvicinamento delle diverse disposizioni legislative, regolamentari ed amministrative degli Stati Membri che hanno per oggetto l'instaurazione o il funzionamento del mercato interno dell'UE.

Si passa quindi alla necessità di potenziare le regole e le opportunità del mercato unico Europeo che non si limiti al fisico ma anche al digitale. Si è partiti dalla necessità che la direttiva sui servizi di media audiovisivi sarebbe dovuta essere adattata ai cambiamenti tecnologici, con il passare degli anni sono stati fatti qualificati passi avanti. Tra questi: la volontà di adottare il principio del "digitale per default" da adottare per tutta la nuova produzione normativa dell'UE per dare maggiore rilevanza alla cybersicurezza (Cybersecurity Package, the Joint Communication on building a strong cybersecurity for the EU), alla protezione dei dati personali (GDPR), alla protezione delle infrastrutture critiche (NIS 1 e 2), alle tecnologie emergenti (AI, Blockchain e 5G). E' stato quindi posto al centro dello sviluppo delle politiche comunitarie l'utilizzo del Digitale quale pilastro per ogni settore dalle infrastrutture alla sanità, passando per l'ammodernamento della pubblica amministrazione e ricerca industriale, dove il tema della sicurezza informatica risulta dirimente ai fini dello sviluppo, della competitività e ad avviso delle scrivente anche a supporto degli investimenti esteri diretti. Un paese in grado di offrire livelli di sicurezza informatica, oltre che le infrastrutture, produce un valore sia in termini di vantaggio competitivo che di progresso.

Le conclusioni del Consiglio Europeo del 9 giugno 2020 hanno identificato le priorità per "plasmare il futuro digitale dell'Europa, indicando 6 priorità da perseguire, ovvero:

1) Connettività 2) Catene del valore digitali 3) Sanità elettronica 4) Economia dei dati 5) Intelligenza artificiale 6) Piattaforme digitali.

La Organisation for Economic Co-operation and Development (OECD) nel rapporto Multilingual Summaries, Measuring the Digital Economy ha fornito una analisi su come i Governi risultino essere sempre più consapevoli delle opportunità e delle sfide connesse alla trasformazione digitale che, con la sua capacità di stimolare le economie, è considerata come una delle principali priorità dell'Agenda globale.

Un importante passo è stato fatto con la dichiarazione ministeriale sull'e- Government a Tallin nell'ottobre 2017 che ha impegnato gli Stati Membri alla identificazione dei principi e relativi obiettivi dell'e-Government Action Plan 2016- 2020, i cui contenuti sono parte integrante della strategia del Digital Single Market europeo.

L'impianto alla base di questo approccio legislativo analizza aspetti relativi al blocco geografico ingiustificato, alla consegna transfrontaliera dei pacchi, la portabilità transfrontaliera dei servizi di contenuti online, ad una revisione del regolamento sulla cooperazione per la tutela dei consumatori, e i servizi di media audiovisivi, ai contratti di vendita online e di altri tipi di vendita a distanza di beni e i contratti di fornitura di contenuto digitale, ponendo quindi un accento sul ruolo attuale e futuro dei servizi digitali la cui adozione è stata accentuata dall'attuale pandemia. Unitamente alle regole di mercato, molto si è fatto verso la costituzione di un polo comunitario per costruire, in stretto raccordo pubblico-privato, le capacità tecnologiche per innalzare i livelli di sicurezza e resilienza alle sempre crescenti minacce informatiche, con la costituzione del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza", che collaborerà con una rete di centri di coordinamento nazionali designati dagli Stati membri, è stato inteso che la costituenda agenzia è stata individuata quale interfaccia Italiana del Centro Europeo.

Segue poi la raccomandazione della Commissione relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare e porre fine alla crisi COVID-19.

Nel giugno 2020 la Commissione ha pubblicato la comunicazione dal titolo «Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione» secondo cui il mercato unico digitale giocherà un ruolo da attore principale nella ripresa dell'UE dalla crisi scaturita dal COVID-19. I settori identificati per il rilancio post Covid saranno incentrati sui seguenti aspetti:
1) Investimenti in una migliore connettività; 2) Una maggior presenza industriale e tecnologica in comparti strategici della catena di approvvigionamento (ad es. IA, cybersicurezza, 5G infrastrutture cloud); 3) Un'economia basata su dati reali e spazi comuni europei di dati; 4) Un ambiente imprenditoriale agevolato e più equo.

Tecnologia e innovazione sono quindi i capisaldi per disegnare l'Europa di domani, che dovrà essere competitiva e agile per recuperare il terreno perso e per colmare i gap strutturali, già noti, ma che ora la pandemia ha imposto di tamponare se non superare.

Le nuove tecnologie abilitanti, non solo in termini di soluzioni, devono considerare anche l'ambiente su cui essere gestite, adottando anche formule miste di tipo PPP.
Da qui la sfida ulteriore è il CLOUD EUROPEO una infrastruttura che avrà il compito di aumentare l'autonomia tecnologica, i livelli di sicurezza, integrità e allo stesso tempo allineerà i Paesi membri con la strategia dei dati europea. Questa infrastruttura rappresenta, una, se non, la sfida più importante per la digitalizzazione Europea. Per far fronte a questa esigenza ci sono progetti in corso in sede nazionale e comunitaria,

che devono essere sviluppati sinergicamente ed in parallelo con il progetto europeo GAIA-X' le cui finalità sono quelle di definire uno standard e quindi le regole di funzionamento dei servizi cloud perseguendo la strategia del decentramento dei dati grazie alle ultime tecnologie disponibili (multi-edge, multi-cloud o edge-to cloud).

Un elemento di valutazione a supporto è relativo all'indice DESI "The Digital Economy and Society Index", che nel seguito riporta la classifica Europea, che indica il livello di crescita in base alla Connettività (misurando le reti fisse e mobili a banda larga e relativi prezzi), il Capitale Umano (uso di internet e competenze digitali di base), uso dei servizi internet (contenuti, canali di comunicazione e transazioni online da parte dei cittadini), integrazione delle tecnologie digitali (digitalizzazione delle imprese e e- commerce, servizi pubblici digitali (egov e e-health).

Cybersicurezza, uno sfida che non si può perdere.

Arbiter indiscusso della partita è la *cybersecurity*: in un mondo sempre più interconnesso e *smart*, i punti e i vettori di minaccia si moltiplica, e le superfici di attacco esposte delle infrastrutture critiche sono particolarmente vulnerabili[1].

Si pensi a cosa potrebbe accadere a causa di una compro- missione cibernetica del sistema di automazione delle linee ferroviarie, o dei sistemi di controllo radar degli aeroporti; o ancora, alle conseguenze dell'intrusione e controllo dei sistemi di sicurezza delle centrali elettriche o, a seguito di un black-out maggiore, della manomissione della sequenza di ripartenza della filiera energetica. Restare "al passo" dello stato dell'arte in tema di *cybersecurity* non è quindi un'opzione, ma una necessità: anche qui, i dati attuali per il Belpaese non sono propriamente incorag- gianti, mostrando una capacità complessiva di portata mediocre: secondo un recente studio di Comparitech, su 60 Paesi l'Italia si collocherebbe alla 36ª posizione, tra l'Argentina (migliore di noi) e la Malesia.

La sicurezza informatica è uno degli argomenti che governi e imprese stanno sempre più considerando una priorità per il benessere di una Nazione e la tutela dei cittadini, della libertà e delle imprese. Un tema cruciale è legato alla necessità di avere figure professionali che possano rispondere al tema dello *skill shortage* e alla importanza di avere, anche in seno ai consigli di amministrazione di società che operano in settori rilevanti, membri che abbiano la capacità di comprendere meglio la posi- zione dell'organizzazione sullo stato della sicurezza informatica, in quanto essa è uno dei temi su cui si concentra l'attenzione dei top manager.

Le aziende di qualsiasi settore sono maggiormente esposte al rischio di minacce e attacchi informatici, in special modo quelle la cui attività rientra nella categoria di operatori di servizi essenziali o infrastrutture critiche.

Negli Stati Uniti, un gruppo bipartisan di senatori ha posto le basi per un disegno di legge volto a mappare figure tecniche come quella del *chief information security officer* e alla necessità di avere in seno ai consigli di amministrazione esperti con compro- vata e qualificata conoscenza del fenomeno della cybersicurezza, per meglio affrontare un rischio aziendale cruciale di non facile comprensione. Anche in Italia è stato fatto molto con il Dl *cyber (105/2019)*, che definisce il perimetro di sicurezza nazionale cibernetica, per il quale, in sede di conversione in legge, sono stati

[1] Tratto dal capitolo Cybersicurezza – del volume ITALIA.NEXT – edito da Rubettino nel giugno 2020 redatto dallo scrivente.

presentati emendamenti volti a prevedere, nell'ambito della governance dei soggetti inclusi nel perimetro, la presenza di tali figure professionali, che però non stati approvati.

Questo basso livello di preparazione sul piano della cybersi- curezza diffuso nel sistema Paese si riflette in una bassa consa- pevolezza nei cittadini-utenti; tutti noi utilizziamo quotidiana- mente dispositivi *smart* che ci consentono di avere tutto a portata di mano ma trascuriamo che allo stesso modo anche noi siamo alla portata di tutti, anche di malintenzionati. A un'esposizio- ne al mondo estremamente amplificata, tramite multicanalità e interconnessione di reti globali, corrisponde specularmente l'accessibilità a una mole sconfinata di contenuti, che prima non potevamo nemmeno immaginare; ma «da un grande potere de- rivano grandi responsabilità», e in particolare quella di fruire delle informazioni e dei contenuti in maniera appropriata, di- fendendoci da disinformazione e *fake news* che manipolano la nostra conoscenza.

A tal riguardo desta sempre più preoccupazione il fenomeno dei *deep-fake*, reso possibile dall'avanzato livello tecnologico raggiunto in termini di processamento e manipolazione delle immagini e dal concomitante dilagare dei *social* e della condi- visione in tempo reale di contenuti multimediali.

Tale tecnica sfrutta la potenza di elaborazione dei moderni computer e l'intelligenza artificiale per sovrapporre il volto di una persona a quello di un'altra ripresa in un video – in questo modo, il manipolatore "impersonifica" la vittima inconsapevole, diffondendo in rete messaggi per conto suo, risultando uno strumento che può essere usato per scopi criminali gravissimi, anche nel mondo politico e finanziario, in un contesto globale dove è più facile raccogliere informazioni, spesso purtroppo sensibili. La disintermediazione oggi è fluida, ovvero è sicuramente più facile entrare in contatto con livelli apicali, bypassare rivenditori se si tratta di beni, e ovviamente anche di dati, intesi come pa- rametri di configurazione, basti pensare a portali come shodan. io (un motore di ricerca per l'Internet delle cose ma non solo).

Orwell ci insegna nei suoi scritti come in politica, in guerra e negli affari «le bugie sembrino sincere e l'omicidio rispettabile». Ma nostro compito è quello di guardare sempre in maniera critica alle informazioni che ci arrivano, e a tutto ciò che ci circonda.

Siamo quotidianamente oggetto di attacchi alla nostra privacy, alle nostre informazioni finanziarie, sanitarie, ai dati sulle nostre preferenze politiche e sessuali; qualsiasi tipo di dato che fluisce dai nostri dispositivi è sistematicamente messo a rischio da una serie di minacce che variano molto per complessità e portata. Non tutti sanno che esiste un vero e proprio mercato nero in cui hacker-imprenditori vendono e comprano *malware* di diversa natura che poi vengono iniettati e distribuiti attraverso apposite reti (bot); esempio ben noto ne è Zeus (Zbots), un *trojan* che ruba informazioni bancarie e non solo attraverso *keylogger* e *form*. L'utente medio è spesso inconsapevole della presenza di *malware* che si annidano all'interno delle app del proprio *smartphone* e che lo espongono a rischi di ogni tipo a partire dal furto di informazioni (numeri di carte di credito) fino al controllo stesso del dispositivo da parte di un agente malevolo. Quest'ultimo può acquisire la possibilità, ad esempio, di inserire nella memoria del *device* file e informazioni rubate e/o illegali, quali foto di natura pedopornografica, senza che il legittimo proprietario ne sia minimamente consapevole.

Tale analisi non deve però scoraggiarci dal reagire, in maniera energica e decisa: anche qui, il progresso ci mette a disposizione tutti gli anticorpi necessari; un nuovo approccio positivo-propositivo è necessario per avviare una nuova *governance*, un

“Piano Marshall” della Sicurezza supportato da un Programma di educazione e sensibilizzazione sociale che catalizzi l’attenzione e la partecipazione da parte degli utenti-cittadini, aspetti fondamentali e contenuti nel Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021.
La sicurezza, in special modo la cybersecurity, è uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo".

In questo orizzonte tematico risulta opportuno inserire e rafforzare le materie tecnico-scientifiche con particolare riguardo all’informatica, sin dalle scuole primarie; introdurre la disciplina dell’etica tecnologica nell’ottica di una più ampia sensibilizzazione civica risulta necessario se si considera che la frontiera informatica è entrata a pieno titolo nell’*unicum* sociale.

Molti Paesi che hanno fatto progressi nella tecnologia dell’informazione e della comunicazione hanno escogitato strategie e politiche per il cyberspazio, la creazione di corpi militari specializzati, l’istituzione di unità e dipartimenti specifici finanche alla creazione di ministeri dedicati (Uk, Australia, Giappone ecc.).

La preparazione alla guerra cibernetica, il controllo degli armamenti nel cyberspazio e la corsa alla supremazia sono ormai realtà per molti Stati a che si legano alle crescenti minacce che verranno giocate su questo terreno “digitale”.

La geopolitica, in special modo in questo contesto, è un fattore cruciale per comprendere, spiegare e prevedere la condotta internazionale dei Paesi. Dal punto di vista del cyberspazio, occorre comprendere le influenze geopolitiche per fronteggiare e in taluni casi prevedere le gravi minacce che corrono in rete. Un’analisi delle operazioni informatiche negli ultimi dieci anni mostra una chiara connessione tra motivazioni geopolitiche e campagne informati- che sponsorizzate da Stati il cui obiettivo era duplice, sabotare e acquisire conoscenza. La geopolitica moderna deve essere combinata con la tradizionale raccolta di informazioni sulle minacce per aiutare aziende e Stati a determinare come, dove e quando rischiano di ottenere attacchi da parti esterne, coniugando quindi gli aspetti digitali e aprendo alla geopolitica ibrida.

Su di noi grava la grande responsabilità di decodificare la realtà di oggi, coglierne le opportunità e lavorare seriamente per impostare una strategia di crescita sostenibile, economica, sociale ed etica; le scelte che prendiamo e che dovranno essere prese nell’immediato futuro, detteranno le condizioni di vita di quella che sarà l’Italia di domani, quella che non vediamo e che necessariamente dobbiamo tutelare.

In questo senso la scelta del Governo volta a creare l’Agenzia di Cybersicurezza Nazionale sembra poter far ben sperare.

Leonardo da Vinci scriveva: «la prospettiva è guida e porta, e senza questa nulla si fa bene». Si dovrà lavorare inesorabilmente sulla prospettiva, immaginando come vorremmo fosse il nostro Paese tra 20 e 30 anni; si dovrà lavorare sul concetto di demo- crazia pragmatica e diretta, per la stabilità del sistema paese, di cittadini, imprese, mercati, e investitori, ricordando sempre che le persone sono la vera ricchezza dell’uomo.

Decodificare il presente significa esserne attenti osservatori, non abbandonandosi al pensiero *mainstream*, ma ponendo sempre al centro la Persona e le sue esigenze, anche a salvaguardia dei principi sociali.

Guardare oltre, Cybersicurezza ed Open Innovation[2]

Il Covid-19 ha suscitato un'ampia varietà di risposte rapide e collaborative, da parte di imprese pubbliche e private, singoli cittadini e associazioni, che hanno condiviso soluzioni, per far fronte alla pandemia, con azioni che rientrano a pieno nel concetto di "Open Innovation".
Abbiamo un'occasione unica per poter contribuire ad un ammodernamento del Paese, agendo su tutte le leve che coinvolgono le imprese, le nuove generazioni e i territori.
I fondi destinati alla digitalizzazione, all'innovazione, alla competitività e alla cultura sono somme ingenti, trattandosi di quasi 50 miliardi di euro dobbiamo usarli tutti e bene ma con progetti puntuali.
L'Open Innovation è il luogo, il metodo, la modalità, con cui le aziende, ma non solo, lavorano con soggetti esterni, che, proprio perché privi di "struttura" o aderenza a modalità consolidate, possono sviluppare nuovi prodotti e soluzioni che deve essere portata anche dentro la cosa pubblica.
L'innovazione, implica un approccio guidato dalla domanda, in cui le aziende –e in questo momento storico in sinergia con il governo – definiscono i punti deboli o le nuove opportunità che pagheranno per affrontare, attraverso un invito aperto per attingere a fonti esterne, come startup e piccole e medie imprese (PMI) per sviluppare insieme soluzioni innovative.
Il nostro Paese ha visto raggiungere risultati eccezionali con i distretti industriali che raccolgono le diverse competenze, per rendere altamente qualificato il prodotto, legato al Made in Italy. Oggi, accanto alla produzione fisica, dobbiamo fare i conti con quello che porta con se l'innovazione, la trasformazione digitale e l'open innovation, ovvero, unire, sempre più, competenze fisiche e digitali, per andare verso l'era Phygital.
Ma questo risultato *si avrà solo* lavorando con partner pubblici e privati, per far crescere ed in alcuni casi creare, l'ecosistema dell'innovazione e delle startup e sarebbe opportuno che questo piano venga declinato nella sezione Rete Nazionale IT.
In questa direzione si renderebbe necessario rivedere i modelli e gli strumenti su cui costruire la partnership pubblico-privato (PPP), ad oggi basata principalmente su rapporti di carattere commerciale, e più raramente di collaborazione per il raggiungimento di obiettivi comuni tra P.A. ed aziende, tuttavia troppo spesso con visioni sul breve periodo.
In contesti sempre più guidati dalla capacità di innovazione e ricerca, e dal controllo di domini informativi virtuali, ma plasmanti la realtà, è l'investimento sulla qualità delle risorse umane il vero fattore *game changer*: ecco quindi che emerge la necessità di immaginare una PPP basata sul riconoscimento del valore della varietà delle esperienze.
Si prenda a veloce esempio il contesto di altre nazioni vicine, dove soprattutto nei settori ad elevata specializzazione (tecnologie per la difesa, lo spazio, le comunicazioni,…) il transito di professionisti da enti governativi a privato – e ritorno – rappresenta un elemento fondamentale per creare quel tessuto di competenze complesse ed aggiornate necessarie per rispondere alle moderne esigenze.
Costruire i riferimenti normativi, il contesto culturale e gli strumenti operativi per una partnership pubblico-privato che incentivi la transizione di esperienze dei professionisti è quindi un fattore

[2] Tratto dall'articolo Cyber Recovery (modello Israele). Dal Cloud al 5G, tutte le priorità
redatto dallo scrivente insieme a Massimo Ravenna (CISO ACEA) e pubblicato sulla rivista formiche in data 26.02.2021
- https://formiche.net/2021/02/cyber-recovery-modello-israele-dal-cloud-al-5g-tutte-le-priorita/

chiave per rilanciare la competitività del sistema Paese. Non si sottovaluti inoltre come, accanto ad evidenti ricadute positive di natura economica, questa nuova visione della PPP possa contribuire a superare quelle barriere ideologiche tra P.A. e privato, aiutando a consolidare una visione più solidale ed integrata di comunità.

In sede di pianificazione del Recovery Plan italiano, uno spazio di tutto rispetto deve e dovrà essere lasciato alla costituzione di un gateway di raccordo nazionale per aggregare tutte le sfide dell'innovazione, che veda promozione culturale e imprenditoriale, in grado di generare una forte relazione con le nostre startup, le nostre università, ma soprattutto gli enti pubblici che hanno difficoltà nel comprendere tali azioni per trasformarle in migliori servizi efficaci ed efficienti.
Pensiamo alle sfide che abbiamo da affrontare già oggi: il 5G, la *cybersecurity*, la mobilità, l'energia, la sanità, la sostenibilità e le infrastrutture fisiche e digitali che devono essere pensate "in chiave futura".
Tale aspetto è contenuto sia nella versione finale del PNRR e chiarito in diverse sedi dal Ministro Colao, dal Sottosegretario Gabrielli per quanto di competenza dell'autorità delegata e dal Prof. Baldoni in qualità di vice direttore del DIS. Tutti gli attori hanno evidenziato la necessità di dotare il Paese di un'Agenzia che possa unire esigenze di carattere pubblico e privato e che funga da elemento di collegamento e condivisione con le realtà comunitarie e non solo, in quanto la diffusione delle minacce impone una costante linea aperta.

I temi citati hanno inoltre come denominatore comune l'esigenza di un contesto che stimoli, valorizzi la formazione e la ricerca: ecco quindi l'occasione per trarre spunti da iniziative in cui lo Stato ha svolto un ruolo di forte indirizzo strategico nell'individuare le esigenze, nel coordinare la distribuzione delle risorse e nel valorizzare i percorsi individuali successivi.
Nel campo delle tecnologie per l'IT e la cybersecurity il progetto CyberSpark in Israele è il riferimento: un'organizzazione senza scopo di lucro, progettata per essere l'ente centrale di coordinamento per le attività congiunte con tutti gli *stakeholder*, per sviluppare una specifica area geografica e massimizzarne il potenziale come centro di competenze globale, per incoraggiare i partenariati del settore accademico, ed attirare società locali ed internazionali.
Questo è il momento per evolvere il concetto di "polo industriale" verso un "Polo 4.0": una struttura che sia centro di ricerca, con ruolo diretto dell'Università, che sia un hub di R&D per aziende, con specifici incentivi fiscali per chi vi trasferisce le proprie unità di ricerca, che sia un Innovation Hub ed incubatore, con programmi di supporto specializzati per le startup innovative e tecnologiche, il cui animo merita una chiara dignità, possibilmente all'interno della costituenda struttura organizzativa dell'agenzia che possa valorizzare l'ecosistema e partnership tra i diversi attori.
Realizzare un CyberSpark italiano è possibile, la modernità ed mercati ci pongono i quesiti, ora ci saranno anche le risorse, serve un impegno pubblico veloce ed operativo nell'individuare gli obiettivi e la rotta da seguire.

Inoltre, le sfide globali come la Space economy, l'intelligenza artificiale, la *cybersecurity*, la Data governance (attualmente in discussione in sede comunitaria la nuova governance dei dati) sono tecnologie abilitanti valide a 360°, si dovrà quindi costruire seguendo una logica di data "interoperability" reale e non decantata, impegni che il Ministero dell'Innovazione di concerto con il Ministero dello Sviluppo Economico e quello della Transizione Ecologica dovranno mettere a fattor comune energie e competenze per dare vita ad un piano nazionale che sia dirompente, dove la sinergia e interazione costante saranno fondamentali.
Senza tuttavia l'identificazione di chiari obiettivi strategici nazionali non è possibile costruire sinergia ed integrazione, per questo sarà importante che tutto il comparto Sicurezza, Difesa ed Intelligence

si faccia motore di progetti di ampio respiro – su tutti il Cloud Nazionale, con una Cloud Strategy nazionale ed una Data Governance Security Strategy – con cui definire nuovi standard, processi e strumenti con cui governare la complessità del presente, oltre che ad avviare una una puntuale ricognizione, quanto mai necessaria, per mappare le filiere italiane a rischio, esigenza dirimente.

Durante questi momenti complessi, l'innovazione può aiutare le organizzazioni, sia pubbliche che private, come abbiamo avuto modo di vedere, imponendoci di darle dignità e, quindi, un ruolo di primo piano, nel trovare nuovi modi per risolvere problemi urgenti e allo stesso tempo costruire nuovi servizi.
Soprattutto, può servire come base per un patto per l'Italia, poichè, come hanno dimostrato diversi e recenti studi, la fiducia si sviluppa quando i partner fanno autonomamente e volontariamente azioni a sostegno del cambiamento, dando un contributo senza chiedere, che possono fare la differenza, come è avvenuto durante la pandemia.
Una grande crisi, come quella che stiamo vivendo, ha alterato in un modo o nell'altro il comportamento di cittadini, dipendenti e partner.
Dovremmo ridisegnare le nostre città, le abitudini, le nostre esigenze e tutto questo è possibile solo con l'innovazione.

Non sprechiamo queste esperienze pianificando come tornare alla vecchia normalità. Pianifichiamo la nuova normalità.

Ciò che è fondamentale, dal punto di vista strategico, è quello di definire le priorità che dovranno essere perseguite.

Sintetizzando le riflessioni sin qui esposte, si ritiene che l'Agenzia per la Cybersicurezza Nazionale potrebbe, qualora ritenuto utile, effettuare i seguenti approfondimenti volti a:

1) La definizione di un piano strategico per la creazione/istituzione di un ecosistema nazionale che veda la partecipazione di diversi stakeholders per pianificare un piano sinergico tra start up, PMI e Grandi Imprese oltre che università e spin off (Ecosystem & Partnership)
2) L'istituzione di un programma di ricerca ad hoc per lo sviluppo di nuovi prototipi/servizi/prodotti/piattaforme da utilizzare nelle infrastrutture critiche (Joint Service and Product Development)
3) La mappatura costante delle figure, in special modo CISO all'interno delle infrastrutture critiche e operatori servizi essenziali