



Le pubbliche amministrazioni nell'era delle tecnologie cloud ed *edge computing* tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali

Elena Montagnani

Le smart city e l'Industria 5.0 costituiscono elementi fondamentali nella strategia europea per la transizione verso un modello economico circolare. L'insieme di nuove tecnologie indispensabili al loro funzionamento, come *Internet of Things*, Intelligenza artificiale, *edge computing*, costringe ad un'attenta riflessione sullo stato dell'arte delle infrastrutture digitali dispiegate sul territorio nazionale in relazione alle missioni del PNRR, alla base della strategia digitale del paese. In tale contesto è proprio la pubblica amministrazione a rivestire un ruolo di raccordo tra i vari stakeholder (imprese, cittadini, terzo settore). Scopo del lavoro è dunque quello di verificare le criticità legate all'introduzione di tali nuove tecnologie e le possibili similitudini in termini di governance con i temi dell'implementazione e regolamentazione afferenti al cloud computing, al fine di avviare una serie di riflessioni sull'incidenza che la transizione verso una società integrata e digitale ha sulla sovranità digitale e sul trattamento del dato.

Sovranità digitale – *Internet of Things* – Cloud ed *edge computing* – Smart city – Economia circolare

SOMMARIO: 1. Introduzione – 2. Affacciati sul futuro: smart city, Industria 5.0, economia circolare – 3. Tecnologie abilitanti: tra innovazione e sperimentazione – 4. Il concetto di sicurezza alla prova della nuova società digitale – 5. Stato dell'arte e prospettive future dell'*edge computing* nel processo di trasformazione digitale dell'Italia – 6. Conclusioni

È inutile stabilire se Zenobia sia da classificare tra le città felici o tra quelle infelici. Non è in queste due specie che ha senso dividere le città, ma in altre due: quelle che continuano attraverso gli anni e le mutazioni a dare la loro forma ai desideri e quelle in cui i desideri o riescono a cancellare la città o ne sono cancellati.

Italo Calvino

1. Introduzione

L'emergenza pandemica ha messo in evidenza come le infrastrutture digitali siano fondamentali e strategiche per il nostro Paese, accelerando quel processo di trasformazione digitale della società iniziato da

anni ed ormai irreversibile. Al pari delle infrastrutture tradizionali, quelle digitali costituiscono mezzi essenziali per permettere nuove modalità di erogazione e fruizione dei servizi pubblici, di studio, di lavoro, nonché occasione di sviluppo per l'economia digitale (e non solo) del paese¹.

E. Montagnani è dottoranda di ricerca in Scienze giuridiche presso l'Università di Pisa.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.



In tale contesto socio-economico caratterizzato da un irreversibile processo di trasformazione digitale, ormai avviato da diversi anni, tale da non potersi considerare una novità dell'ultima ora imposta dalla pandemia, è divenuta dunque, improcrastinabile un'analoga trasformazione digitale delle pubbliche amministrazioni.

Obiettivo prioritario è quello di offrire ai cittadini e alle imprese servizi pubblici di maggiore qualità, responsabilità, efficacia ed efficienza al quale si affianca l'esigenza di rendere le aree urbane sempre più "smart" e sostenibili da un punto di vista ambientale attraverso l'*Internet of things* (c.d. IoT), l'utilizzo di sistemi di Intelligenza artificiale (c.d. A.I.) e *machine learning* (c.d. M.L.) e le loro tecnologie abilitanti quali 5G, cloud computing ed *edge computing*, al fine di permettere l'innovazione in quei settori oggi affidati a metodologie tradizionali (si pensi al settore della mobilità con le auto a guida autonoma; a quello ambientale con il monitoraggio tramite droni del territorio e delle emissioni di Co2, ma anche alla raccolta dei rifiuti robotizzata e al benessere dei cittadini, alla valorizzazione dei beni culturali e del settore turismo)².

È proprio intorno al tema delle smart city, come vedremo, che oggi si concentrano maggiormente i contributi innovativi e gli investimenti privati³ e pubblici, come mostrano anche le sperimentazioni messe in atto dal programma "Smarter Italy"⁴ promosso da MISE, MIUR e MITD, in ambiti come mobilità, ambiente, benessere della persona e beni culturali.

Tuttavia, i servizi legati alle smart city e all'IoT impongono delle scelte tecnologiche che sembrano oggi, se non in contrasto, quantomeno dimenticate dalla direzione generale delineata dal Piano Nazionale di Ripresa e Resilienza (PNRR), dal Piano Triennale per l'informatica nella pubblica amministrazione 2021-2023 e dalla Strategia Italia digitale 2026, i quali riservano un ruolo da protagonista nella trasformazione digitale della P.A. al cloud computing sulla base del paradigma *cloud first*, prevedendo una progressiva dismissione del patrimonio tecnologico delle pubbliche amministrazioni centrali e periferiche dislocato capillarmente sul territorio, in favore di una migrazione proprio verso il cloud.

Infatti, la natura "real-time" di alcuni dei servizi legati alle smart city implica la necessità di eseguire la computazione del dato proveniente dai dispositivi elettronici (*things*) attraverso sistemi allocati in prossimità di questi e quindi *data center* dislocati sul territorio in modo capillare. Questa tipologia di infrastrutture, denominata *edge computing*, non rappresenta ancora una realtà consolidata nel nostro territorio sebbene alcuni *cloud pro-*

vider (Google, Microsoft, Amazon) e alcune TELCO (TIM, Fastweb) abbiano avviato nelle principali città italiane ed europee delle sperimentazioni.

È possibile, quindi, pensare di valorizzare il patrimonio tecnologico ed infrastrutturale in dismissione delle pubbliche amministrazioni trasformandolo in una infrastruttura nazionale di *edge computing* che, affiancata alla nuova connettività 5G, vada a costituire un asset strategico fondamentale per la realizzazione proprio di quei servizi smart delle pubbliche amministrazioni sui quali verranno ridisegnate le città e le società del prossimo futuro? Quali sono i rischi per la sovranità digitale legati all'assenza di una infrastruttura *edge* nazionale a favore di infrastrutture gestite dai grandi attori del Web? Quali sono le nuove sfide che tali infrastrutture portano con sé in termini di trattamento del dato?

2. Affacciati sul futuro: smart city, Industria 5.0, economia circolare

L'avvento della digitalizzazione e di una società sempre più liquida e globale, caratterizzata da una capillare diffusione di smartphone e tablet e da una progressiva stabilità e disponibilità della connessione ad Internet, ha imposto nuove modalità di fruizione dei servizi informatici e contestualmente ha prodotto un aumento esponenziale della produzione dei dati da parte degli utenti e della loro circolazione.

È proprio intorno alla disponibilità di un'enorme mole di dati e delle tecnologie in grado di valorizzarli che si stanno progressivamente forgiando nuovi modelli sociali ed economici: si pensi in particolare alle città intelligenti (c.d. smart city), all'Industria 4.0 e 5.0, ai nuovi paradigmi di sviluppo in grado di armonizzare gli obiettivi dell'economia di mercato e quelli ambientali (c.d. *circular economy*).

La città diventa quindi una piattaforma integrata di sistemi ICT, una rete intelligente di oggetti e macchine connessi, che trasmettono dati usando la tecnologia wireless ed il cloud⁵.

Si tratta in realtà di qualcosa di molto più ampio, un nuovo modo di concepire il modo di vivere negli agglomerati urbani, dove il capitale infrastrutturale legato anche alle nuove tecnologie (che potremmo definire capitale fisico-digitale), il capitale umano, intellettuale, ambientale e sociale vengono massimizzati⁶. L'eterogeneità degli ambiti abbracciati dalle smart city pare anche essere confermata dall'approccio seguito dall'Unione europea⁷, la quale ne declina le specificità secondo sei dimensioni (*smart people, smart governance, smart economy, smart living, smart mobility, smart environment*) confermando co-



me quello tecnologico sia solo uno dei tanti aspetti che governeranno le future città intelligenti.

Se fino ad oggi il cittadino è stato considerato mero fruitore di servizi, digitali e non, il nuovo paradigma, incentrato sul concetto di *smart people*, impone un modello di *smart citizenship* in cui esso diviene soggetto attivo anche nell'erogazione e non solo nella fruizione del servizio, fornendo dati, decisioni e feedback, nello sviluppo della città e nelle decisioni dell'amministrazione locale secondo una logica *bottom-up*.

Per poter parlare di *smart citizenship* è però necessario fornire al cittadino gli strumenti indispensabili, quali infrastrutture di rete (banda ultra-larga, 5G, Wi-fi), sistemi di identità digitale, piattaforme di accesso ai dati. Le informazioni ed i dati prodotti dai sensori dovranno, infatti, essere resi disponibili agli utenti-cittadini attraverso servizi che consentano loro di vivere la città in *real time* ed assumere decisioni consapevoli, fornendo a loro volta nuovi dati necessari alla smart city per alimentare i sistemi di intelligenza artificiale (A.I.) in un ciclo continuo.

Se già da anni nei grandi agglomerati urbani si è rilevata, ad opera di soggetti pubblici e privati, la tendenza ad introdurre intelligenza nella gestione dei servizi fondamentali al cittadino⁸, più di recente abbiamo assistito, in risposta all'emergenza sanitaria, all'introduzione di pratiche quali smart working, didattica a distanza e fruizione digitale di servizi delle pubbliche amministrazioni⁹.

Non solo, è interessante anche notare come in un territorio come quello italiano, caratterizzato dalla presenza di pochi grandi agglomerati urbani e di numerosi piccoli comuni e borghi, siano state avviate sia ad iniziativa pubblica che privata, una serie di sperimentazioni volte a replicare il modello della smart city all'interno di comunità di piccole dimensioni e diffuse capillarmente sul territorio, le quali presentano esigenze molto diverse da quelle di una grande città¹⁰.

Proprio osservando gli obiettivi delle sperimentazioni più recenti risulta evidente un netto cambio di paradigma nel percorso di trasformazione delle comunità in chiave digitale. Se in un primo momento, infatti, risultava preponderante l'aspetto tecnologico finalizzato ad un miglioramento dei parametri economici per gli operatori del settore, oggi viene privilegiato un approccio antropocentrico, adottato anche dall'Ue, attento ai bisogni e al miglioramento della qualità della vita del cittadino.

La progettazione di smart city del futuro avrà bisogno, quindi, di un continuo adattamento, dove le nuove tecnologie costituiranno leve strategiche nell'adozione di pratiche sostenibili dal punto di vista

economico, energetico, ambientale e sociale, il che implicherà una gestione cooperativa e inclusiva della società e del territorio per migliorare la qualità, le prestazioni e l'interattività dei servizi; ridurre i costi e il consumo di risorse; ottimizzare la relazione tra i cittadini e gli operatori della città.

La governance delle smart city deve essere, quindi, finalizzata a valorizzare l'interoperabilità tra i sistemi, creando una singola infrastruttura di base e un'unica piattaforma di delivery dei servizi in grado di elaborare le informazioni trasmesse dai sensori per erogare servizi a valore aggiunto per i cittadini.

Tale modello di sviluppo delle comunità in chiave digitale ed integrata acquisisce ancora più importanza se pensiamo al problema del rapporto tra ambiente e sviluppo, che sta alla base della questione ambientale e della grave crisi ecologica ed alla necessità sempre più impellente di superare il modello capitalistico e di mercato caratterizzato da un eccessivo sfruttamento delle risorse naturali e dal forte impatto delle attività antropiche sull'intero ecosistema, secondo la logica lineare "estrai, produci, usa, getta" (c.d. "paradigma meccanicistico" del mondo come macchina).

Se in un primo momento nel contesto delle Nazioni Unite si è trovata una risposta nei concetti di sviluppo sostenibile e di green economy, più di recente si è approdati a livello internazionale al concetto di *circular economy*¹¹, il quale garantirebbe un vero cambio di paradigma dell'economia tradizionale in chiave circolare, coesistente alla nuova concezione del mondo come "rete" (c.d. "paradigma economico-sistemico")¹².

Sia il "Nuovo piano d'azione per l'economia circolare" dell'Ue del marzo 2020¹³ sia la "Strategia nazionale per l'economia circolare" del settembre 2021¹⁴, hanno tuttavia messo in evidenza come la transizione all'economia circolare sia fortemente dipendente dall'introduzione di nuove tecnologie e servizi digitali, quali sensori di monitoraggio, servizi IoT ed A.I., necessari a governare la maggior complessità ed interdipendenza delle filiere di approvvigionamento e dei processi produttivi legati a tale modello economico.

Al di là dell'evidente affinità tecnologica tra le tematiche legate alle smart city ed all'economia circolare è da rilevare come queste siano lo strumento fondamentale attraverso il quale il cittadino diviene parte attiva nei processi produttivi circolari e mediante il quale tali processi generano conoscenza (sensori ed IoT) ed impatto sulla comunità (A.I.)¹⁵.

Il modello di smart city dovrà, quindi, andare di pari passo con gli obiettivi di efficienza energetica e di sostenibilità ambientale. Obiettivi che sono chiara-



mente espressi nell'Agenda 2030 delle Nazioni Unite e nel *Green Deal* europeo¹⁶.

Proprio in relazione ai processi produttivi la Commissione europea ha recentemente gettato le basi di un'Industria 5.0¹⁷ che, espandendo il concetto di Industria 4.0¹⁸, incorpora i principi e le tecnologie presenti all'interno delle smart city, introducendo al contempo i concetti di sostenibilità ed equità sociale. Il paradigma dell'Industria 5.0 mira a migliorare l'efficienza delle fabbriche intelligenti (c.d. *smart factory*) ed al contempo a minimizzare l'impatto sull'ambiente e le ricadute sulla società¹⁹.

Per implementare la visione di un'economia circolare basata sulla trasformazione digitale, sulla smart city e sull'Industria 5.0 risulta necessario fornire soluzioni in grado di integrare il mondo fisico e quello virtuale in modo efficiente e sostenibile.

3. Tecnologie abilitanti: tra innovazione e sperimentazione

Sebbene il panorama tecnologico, in continua evoluzione, offra un numero sempre crescente di soluzioni, strumenti, servizi ed infrastrutture, sono riconducibili a quattro gli abilitatori tecnologici fondamentali per una transizione digitale che privilegi la sostenibilità ed equità sociale: IoT, 5G, Intelligenza artificiale, *cloud* ed *edge computing*.

I dispositivi IoT²⁰ sono ad oggi impiegati in molteplici settori come ad esempio il monitoraggio remoto, l'automazione casalinga ed industriale (c.d. IIoT), l'agricoltura di precisione.

Cifra distintiva dell'IoT è evidentemente la capacità di interconnessione necessaria per trasmettere in tempo reale i dati raccolti da un lato e le decisioni da attuare dall'altro. Particolare importanza riveste quindi l'infrastruttura di rete che garantisce tale connettività. Fino ad oggi le reti geografiche a basso consumo energetico necessarie all'interconnessione dei dispositivi hanno mostrato numerose lacune e criticità, superate con l'introduzione delle nuove reti 5G attualmente in dispiegamento in Italia, che risultano un fattore determinante per garantire il percorso di digitalizzazione delle comunità e dell'industria, necessario ad avviare un processo di trasformazione dell'economia in chiave circolare. Non è un caso che vi siano numerose sperimentazioni a livello europeo e nazionale in ambito IoT che vanno progredendo di pari passo con lo stato di avanzamento dei lavori sull'infrastruttura di rete di nuova generazione²¹.

Come le reti di nuova generazione ed i dispositivi IoT possono essere paragonati al sistema nervoso centrale ed all'apparato sensoriale mediante cui un organismo biologico conosce e riconosce l'ambiente

che lo circonda, l'apparato neurale tramite il quale le informazioni acquisite vengono tradotte in soluzioni ed azioni da tale organismo può essere rappresentato dai sistemi di *machine learning* ed A.I.

Tale intelligenza, definita oggi dal Programma strategico Intelligenza Artificiale 2022-2024 come "l'insieme dei modelli digitali, algoritmi e tecnologie che riproducono la percezione, il ragionamento, l'interazione e l'apprendimento"²², consente di creare sistemi di raccomandazione, soluzioni di riconoscimento del linguaggio naturale, veicoli a guida autonoma che sono in grado di prendere decisioni in tempo reale senza bisogno dell'intervento umano.

Nel caso dei sistemi IoT, i sistemi di *machine learning* ricevono costantemente dati dai sensori della rete grazie ai quali riescono ad allenare e perfezionare le A.I. in un ciclo di apprendimento continuo²³. I sistemi di intelligenza artificiale possono, quindi, processare tali dati ed elaborare un risultato che viene comunicato ad un utente o agli attuatori della rete IoT sotto forma di decisione.

Se pensiamo ai servizi digitali che alimenteranno le città e le industrie del prossimo futuro, come le auto a guida autonoma, il monitoraggio ambientale tramite droni, la gestione della mobilità, i sistemi di logistica etc., risulta evidente come sia di fondamentale importanza che il tempo intercorso tra il rilevamento di un parametro ambientale (per esempio la presenza di un pedone sulla carreggiata), l'elaborazione di una decisione da parte di un sistema di A.I., e l'applicazione di tale decisione (l'attivazione dei sistemi di arresto dell'auto) sia il minore possibile.

Tuttavia, molti dei sistemi IoT che operano in tempo reale non riuscirebbero a garantire tale requisito attraverso architetture centralizzate basate su cloud, dal momento che i valori elevati di latenza (il tempo che intercorre tra una richiesta inoltrata ad un servizio e la relativa risposta) impediscono al sistema di fornire la reattività necessaria.

In tali casi l'uso di infrastrutture di computazione dispiegate in prossimità dei sensori (c.d. *edge computing*) può fornire un'adeguata soluzione al problema evitando potenziali "colli di bottiglia" e ritardi nella comunicazione tra dispositivi e sistemi di A.I.

Le soluzioni centralizzate basate sul cloud pongono, però, determinate limitazioni che non si esauriscono nei già citati requisiti di latenza. È prima di tutto necessario notare come il cloud stesso sia da considerarsi un singolo punto di vulnerabilità per la disponibilità del servizio (quello che in gergo tecnico viene definito *single point of failure*)²⁴ dal momento che attacchi informatici, vulnerabilità o anche semplici operazioni di manutenzione programmata possono interrompere l'erogazione del servizio. Inoltre,



si prevede che il numero di dispositivi IoT connessi alla rete aumenterà sensibilmente nei prossimi anni²⁵ e, di conseguenza, il numero di comunicazioni simultanee con i sistemi centralizzati potrebbe, in assenza di una progettazione adeguata, sovraccaricare il cloud²⁶.

L'*edge computing* si presenta anche in questo caso come uno strumento complementare al cloud computing in grado di alleggerire i sistemi centralizzati eseguendo le computazioni su una infrastruttura locale, dedicata ad un numero limitato di dispositivi IoT presenti su un territorio circoscritto e fornendo al contempo una sorta di camera a tenuta stagna (c.d. *bulkhead*) capace di limitare la propagazione all'intero sistema degli effetti di eventi disastrosi (si pensi ad esempio ad un attacco informatico che blocchi un sistema regionale il quale, su una infrastruttura centralizzata, verrebbe ad estendersi anche ai sistemi delle altre regioni).

Se è chiaro che il cloud computing continuerà a crescere fino a diventare lo standard definitivo delle architetture ICT, l'*edge computing* sarà la nuova area in cui i *cloud provider*, le Telco e i fornitori di servizi concentreranno i loro investimenti per l'innovazione nel prossimo futuro²⁷.

La vera sfida sarà piuttosto quella di integrare le nuove infrastrutture e le tecnologie abilitanti con le strutture esistenti sul territorio sfruttando l'interoperabilità tra sistemi.

4. Il concetto di sicurezza alla prova della nuova società digitale

Carlo Ratti, architetto ed ingegnere, fondatore e direttore di SENSEable City Lab del MIT di Boston, che studia lo sviluppo dei sensori dell'elettronica in relazione all'ambiente urbano, ha affermato che «l'impiego crescente di sistemi e sensori elettronici sta permettendo un nuovo approccio allo studio dell'ambiente costruito. Il nostro modo di descrivere e comprendere le città viene radicalmente trasformato, insieme agli strumenti che usiamo per crearle e all'impatto sulla struttura fisica. La dimensione digitale delle città esiste da tempo. L'importante è capire come usare i dati, come analizzarli ed elaborarli per rendere i contesti urbani più vivibili, più sicuri e più efficienti»²⁸.

Ecco che la vita della smart city, come agglomerati urbani più vivibili, sicuri ed efficienti, è strettamente dipendente dall'utilizzo di soluzioni e tecnologie IoT, che permettono il rilevamento, l'analisi e il trasferimento di grandi flussi di dati.

Tutto ciò ha evidenziato la necessità di dare rilevanza alla sicurezza nelle sue varie declinazioni (*secu-*

urity, safety, certainty, privacy) a seconda dell'ottica in cui viene osservata²⁹, alle quali oggi si aggiunge un quinto tipo di sicurezza, quella cyber, che si propone come macro settore sotto al quale porre tutti gli altri³⁰.

Un primo aspetto chiave che va preso seriamente in considerazione è, quindi, quello della cybersicurezza urbana ovvero del rapporto con le tecnologie dell'informazione e della comunicazione, radicato nell'essenza stessa della città, al fine di rendere resiliente l'insieme delle infrastrutture sulle quali tutta la smart city è fondata. Il rischio è quello di essere esposti ad attacchi o minacce cyber da parte di criminali informatici in settori sensibili quali quello sanitario, dei trasporti, della distribuzione e più in generale di tutti quei servizi essenziali per il funzionamento di una città.

La cyber security diventa un aspetto essenziale per qualsiasi iniziativa digitale applicata alle città intelligenti, un bisogno la cui soddisfazione diviene primaria per l'uomo, andando ad assumere un ruolo importante anche per la protezione della privacy dei cittadini da un lato, e per la protezione delle aree sensibili della città dall'altro. E questo è tanto più vero oggi a fronte dell'incremento esponenziale sia della digitalizzazione dei servizi offerti dalle P.A., sia degli attacchi informatici, decuplicati nell'arco di un anno³¹. Siamo di fronte a problematiche che per natura, gravità e dimensione hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica³², in grado di mettere in crisi la stabilità del sistema andando a colpire i dati delle strutture organizzative più sensibili³³.

Affinché il cittadino mantenga un alto grado di "fiducia computazionale" nelle istituzioni che governano questo modello di città, e conseguentemente nel modello stesso di smart city, queste saranno chiamate a garantire anche un livello adeguato di sicurezza della sua privacy sia da parte di soggetti pubblici che privati³⁴. È proprio questo aspetto di *multi-stakeholderism* che vede coinvolti soggetti di natura eterogenea che richiederà una particolare attenzione nell'elaborazione di protocolli di sicurezza e policy relative al trattamento dei dati.

Anche il PNRR ha dedicato attenzione alla cybersicurezza, destinando 620 milioni di euro a tale settore, a fronte, come vedremo, dello sviluppo di un ampio piano di digitalizzazione delle P.A.³⁵

Il cloud computing, in quanto infrastruttura centralizzata gestita nella maggior parte dei casi da soggetti privati, potrebbe presentare più di una criticità rispetto al tema della sicurezza in tutte le sue accezioni. Ecco che le infrastrutture di *edge computing*



potrebbero costituire una valida risposta non solo a criticità di tipo tecnico, come sopra messo in evidenza, ma anche garantire un elevato grado di resilienza del sistema smart city alle violazioni dei protocolli di sicurezza o delle policy relative alla gestione del dato, attraverso la creazione di infrastrutture locali autonome e segregate.

Non bisogna dimenticare, inoltre, che l'ambito IoT, fondamentale per la trasformazione digitale delle città, presenta numerose peculiarità sia da un punto di vista tecnico che del trattamento del dato, le quali lo distinguono fortemente dall'ambito dei servizi digitali che hanno come fruitore il cittadino ed il consumatore (si pensi ai portali informativi delle P.A., alle piattaforme di prenotazione dei vaccini etc.).

Nei servizi digitali che prevedono una interazione diretta con il cittadino o il consumatore la tutela della privacy viene garantita da un lato attraverso l'applicazione del principio di minimizzazione dei dati espresso dall'art. 5 c.1 lett. c) nel combinato disposto con l'art. 6 del regolamento europeo 679/2016, e dall'altro dalla possibilità di avere un contatto diretto con l'utente al quale viene data la facoltà di esprimere il proprio consenso al trattamento dei dati secondo le consuete formule di *opt-in* e *opt-out*.

Di contro i sistemi di IoT trattano dati che sono spesso semanticamente molto distanti da quelli trattati dai servizi appena descritti (ad esempio, rilevazioni di dati ambientali, immagini, video, posizioni) dove la raccolta del dato personale nella maggior parte dei casi avviene in modo incidentale (ad esempio, un drone di rilevamento del traffico che registra immagini nelle quali compaiono i volti degli individui intenti a fare shopping)³⁶.

Inoltre, se escludiamo i dispositivi personali o indossabili (ad esempio, smart watch o smart phone) i dispositivi IoT spesso operano nell'impossibilità di interfacciarsi direttamente con un utente i cui dati vengano incidentalmente rilevati, al fine di richiedere il consenso al loro trattamento o conservazione, aprendo sicuramente la strada ad un articolato dibattito intorno alla gestione ed al trattamento del dato personale in tale contesto³⁷.

Nell'attesa che vengano delineate delle policy in grado di superare tali problematiche le infrastrutture *edge* possono fornire un supporto essenziale nella loro mitigazione.

In primo luogo, vi sono numerosi casi d'uso in ambito IoT in cui i sistemi sono interessati unicamente al processamento dei dati e non alla loro conservazione. In tali casi il processamento dei dati su infrastrutture *edge*, vicine ai dispositivi IoT, consente di evitare la conservazione del dato funzionale ad un

successivo processamento. In sostanza, una volta che un dato viene catturato da un sensore ed una applicazione di A.I. lo ha utilizzato per prendere una decisione, tale dato diviene immediatamente superfluo e potrà essere cancellato³⁸.

In secondo luogo, anche nei casi in cui i sistemi centrali cloud avessero necessità di ricevere le rilevazioni contenenti dati personali al fine di conservarli, tali dati potrebbero essere anonimizzati o pseudonimizzati direttamente sui sistemi periferici *edge*, senza quindi essere mai scritti su alcun supporto informatico. Di conseguenza ogni successivo accesso a tali rilevazioni, sia che avvenga sui sistemi *edge* che sui sistemi cloud, sia che avvenga ad opera di un automa che di un essere umano, non comporterà l'esposizione di dati personali, ottenendo così una tutela della *privacy by design* e consentendo al contempo di minimizzare gli effetti di eventuali *data breach*³⁹.

Questo è ancora più importante se messo in relazione al fatto che l'ambito IoT, come abbiamo visto, rende particolarmente complessa se non quasi impossibile la richiesta del consenso ai soggetti i cui dati verranno trattati, il che rende di fatto l'*edge* una infrastruttura strategica nella pianificazione della transizione verso le nuove comunità digitali, l'Industria 5.0 e il modello economico circolare.

L'importanza di questo tipo di infrastruttura e della sua distribuzione capillare sul territorio è ben evidenziata anche dalla "Roadmap della tecnologia industriale europea per l'offerta *cloud-edge* di nuova generazione", in cui si evidenzia non solo la necessità di una sinergia tra cloud ed *edge* ma anche di un intervento delle istituzioni europee e nazionali nella loro realizzazione al fine di garantire un adeguato livello di sovranità sul dato e sulle infrastrutture⁴⁰.

5. Stato dell'arte e prospettive future dell'*edge computing* nel processo di trasformazione digitale dell'Italia

È proprio nel solco della strada tracciata dall'Europa per avviare una transizione verso una società smart e green sorretta da un'economia di tipo circolare, dove la trasformazione digitale delle comunità e dell'industria è orientata ad una maggiore sostenibilità, che sembra muoversi il PNRR⁴¹ sviluppato dall'Italia. Sebbene il tema della transizione al digitale sia trasversale a tutte le missioni nelle quali il piano si articola, è nella prima missione "Digitalizzazione, innovazione, competitività, cultura e turismo" che si concentrano gli investimenti per l'ammodernamento non solo delle P.A. ma anche del sistema produttivo e del turismo, vero motore economico del paese⁴².



Con riferimento alle infrastrutture di connettività, il PNRR include ingenti investimenti volti a garantire la copertura di tutto il territorio con reti a banda ultra-larga (fibra FTTH, FWA e 5G)⁴³ per consentire alle P.A., alle imprese e ai cittadini di catturare i benefici della transizione digitale, ponendosi in linea con la strategia europea per la creazione di un mercato unico europeo del dato.

Per quanto riguarda le infrastrutture computazionali il PNRR adotta un approccio *cloud first*, con lo scopo non solo di migrare i dati e gli applicativi informatici esistenti delle singole amministrazioni verso un ambiente cloud, ma anche di stabilire un nuovo paradigma per la governance dei dati e lo sviluppo dei futuri servizi delle P.A.

Questo processo si pone quale obiettivo la razionalizzazione e il consolidamento di molti dei *data center* delle P.A. oggi distribuiti sul territorio, attraverso una dismissione progressiva del patrimonio ICT secondo una classificazione stilata da AgID che tiene conto dell'obsolescenza e del livello di sicurezza delle tecnologie impiegate, a favore delle infrastrutture cloud.

Si prevede altresì che la migrazione venga attuata secondo due modelli complementari, l'uno che prevede la creazione di un Polo Strategico Nazionale (PSN) costituito da una nuova infrastruttura cloud dedicata (completamente privata o ibrida) localizzata sul territorio nazionale in linea con gli standard di prestazione e sicurezza tipici dei cloud pubblici; l'altro che prevede l'uso di un cloud pubblico di uno tra gli operatori di mercato certificati da AgID.

La scelta di quali servizi migrare verso soluzioni cloud qualificate da AgID o verso il PSN avverrà sulla base della classificazione dei dati definita all'interno della Strategia Cloud Italia⁴⁴.

In particolare, i dati e servizi categorizzati come strategici ovvero la cui compromissione può avere un impatto sulla sicurezza nazionale dovranno necessariamente migrare⁴⁵ sull'infrastruttura cloud fornita dal PSN, con l'obiettivo di garantire la massima resilienza ed autonomia tecnologica e controllo sui dati per quei servizi ritenuti essenziali al funzionamento del paese.

Sia il PNRR sia le strategie ed i piani nazionali ad esso collegati pongono particolare enfasi sul principio *cloud first*, favorendo la creazione di poli centralizzati per il processamento e la conservazione dei dati, nulla predisponendo tuttavia con riferimento all'adozione di sistemi di *edge computing* e all'implementazione di piattaforme IoT.

La Strategia Cloud Italia, basandosi sulla situazione del patrimonio ICT delle P.A. fotografata da AgID⁴⁶, è orientata nel medio-lungo termine alla

completa dismissione della maggior parte dei *data center* locali ad eccezione di poche infrastrutture che si sono dimostrate adeguate in termini di performance e sicurezza e che andranno in parte a costituire l'infrastruttura del PSN⁴⁷.

È quindi evidente come la maggior parte delle infrastrutture computazionali oggi presenti capillarmente sul territorio sia destinata a scomparire, per lasciare il posto ad un PSN dispiegato su due regioni, che costituirà una infrastruttura cloud non adatta ai casi d'uso relativi alle infrastrutture di *edge computing*.

È da notare come ad oggi non esista un piano di finanziamenti volto ad adeguare tali strutture in dismissione ai requisiti richiesti dai sistemi IoT e conseguentemente dalle infrastrutture *edge*, ma è previsto solo il finanziamento delle attività volte a garantire la continuità del servizio durante il periodo di migrazione o le attività di consolidamento di alcuni *data center* centrali.

Tuttavia l'assenza di una strategia per le infrastrutture *edge* ed IoT rischia di porre il Paese in una situazione di forte ritardo rispetto alla transizione verso il nuovo modello di società che va ad integrare proprio i nuovi paradigmi di economia circolare; e questo è tanto più vero se pensiamo a quanto affermato dall'Ue nella "Strategia europea per i dati", secondo la quale entro il 2025 l'80% dei dati raccolti dai sistemi informatici verrà processata su infrastrutture periferiche di tipo *edge* e solo il 20% su infrastrutture centralizzate⁴⁸.

Possibili strategie per affrontare le sfide poste dagli ambiziosi obiettivi delineati dall'Ue in tema di transizione digitale e green, potrebbero essere rinvenute nel modello operativo impiegato per l'adozione del cloud nelle P.A.

In primo luogo, potrebbe essere approntato un PSN dedicato all'*edge computing*, distribuito capillarmente sul territorio nazionale ed in grado di ospitare i servizi strategici per l'implementazione delle smart city e dell'Industria 5.0 di cui anche le P.A. sono parte integrante. Questa infrastruttura potrebbe essere implementata a partire proprio dai 35 *data center* delle P.A. che AgID ha individuato come possibili candidati per un PSN cloud (solo quattro, infatti, costituiranno il PSN cloud, gli altri saranno destinati alla progressiva dismissione) previa verifica della loro distribuzione omogenea sul territorio, in mancanza della quale saranno ovviamente richiesti ulteriori investimenti per la creazione dei *data center* mancanti.

In secondo luogo, attraverso un processo di certificazione e la stesura di linee guida per l'adozione di infrastrutture e servizi *edge* da parte di AgID, in modo



analogo a quanto avvenuto per l'adozione del cloud pubblico, potrebbero essere utilizzate infrastrutture e servizi messi a disposizione dal mercato per tutti quei casi catalogati come non strategici o che non trattino dati personali o sensibili.

È da notare, tuttavia, come quest'ultima strada risulti ad oggi di difficile percorribilità non esistendo sul mercato, a differenza del cloud computing, un'offerta di infrastruttura e servizi *edge* sufficientemente matura, distribuita sul territorio e completa di servizi⁴⁹.

L'affidamento della gestione di tali infrastrutture ai grandi attori del Web, tipicamente aziende extra-Ue (si pensi a Google ed AWS), obbliga, inoltre, ad una riflessione particolarmente attenta sul trattamento dei dati. Tale problema già presentatosi in ambito cloud, ha dato vita a nuovi modelli di governance del dato, come il c.d. *Data Trust*⁵⁰, che potrebbero riproporsi con riferimento all'*edge*.

Ancora più importante diviene, in tale circostanza, la perdita di sovranità sull'infrastruttura con il rischio che aziende extra-Ue possano decidere di interrompere l'erogazione del servizio bloccando di fatto il funzionamento di intere comunità e processi industriali, fortemente dipendenti dai servizi IoT.

6. Conclusioni

La creazione di una infrastruttura tecnologica per la connettività (5G, banda ultra-larga) e la computazione (cloud, *edge*, IoT) sia a livello nazionale che europeo, necessaria a favorire la nascita di un "Mercato unico digitale", acquisisce quindi un'importanza strategica, essendo chiamata a sostenere la transizione digitale dell'intera società, dell'industria e dell'economia, così come evidenziato anche dalla Commissione europea⁵¹.

Visto lo stato di forte ritardo nel quale versa l'infrastruttura *edge* in Italia, quella che ci si pone di fronte non è soltanto una sfida tecnologica ma, proprio a causa della pervasività dei sistemi IoT nei processi produttivi e di governance della comunità, anche normativa, dove il legislatore sarà chiamato di concerto con le istituzioni europolitane ad affrontare tematiche relative ai problemi di sovranità sulle infrastrutture e ai nuovi scenari che si prospettano in tema di privacy e trattamento del dato.

Note

¹M. BREQUE, L. DE NUL, A. PETRIDIS, *European Commission, Industry 5.0, Towards a sustainable, human-centric and resilient European industry*, EU publication, 2021.

²T. MUHAMMED, R. MEHMOOD, A. ALBESHRI, *Enabling Reliable and Resilient IoT Based Smart City Applications*, in

R. Mehmood, B. Bhaduri, I. Katib, I. Chlamtac (eds.), "Smart Societies, Infrastructure, Technologies and Applications", Proceedings of the First International Conference SCITA 2017, LNCS, vol. 224, 2018, Springer, p. 169-184. M. MAZHAR RATHORE, P. ANAND, A. AWAI, J. GWANGIL, *IoT-Based Big data: from Smart city towards next generation super city planning*, in "International Journal on Semantic web and information system", vol. 13, 2017, n. 1, p. 28-47. D. LUCKEY, H. FRITZ, D. LEGATIUK, K. DRAGOS, K. SMARSLY, *Artificial intelligence techniques for smart city applications*, in E. Toledo Santos, S. Scheer (eds.), "Proceedings of the 18th International Conference on Computing in Civil and Building Engineering" – ICCBE 2020 (São Paulo, Brazil on August 18-20), p. 3-15.

³Le principali società di telecomunicazioni presenti in Italia hanno avviato progetti volti ad introdurre infrastrutture *edge* sul territorio nazionale complementare al dispiegamento dell'infrastruttura di rete 5G. In particolare, si veda il progetto **AI@EDGE**, cui partecipa anche il gruppo **TIM**.

⁴V. l'approfondimento sul **Progetto Smarter Italy**.

⁵L'enciclopedia Treccani definisce la **Smart city** come l'insieme delle «strategie di pianificazione urbanistica correlate all'innovazione e in particolare alle opportunità offerte dalle nuove tecnologie della comunicazione per migliorare la qualità della vita dei cittadini. Il concetto di "città intelligente" parte dall'assunto dell'intelligenza distribuita, inscritta nello spazio pubblico, in una sorta di ridefinizione dell'antico *genius loci*. Con s.c. si tende sempre più a mettere in relazione le infrastrutture materiali delle città con il capitale umano, intellettuale e sociale di chi le abita. Un capitale potenziato e messo a sistema dalle infrastrutture immateriali del Web. Nella s.c. la connettività telematica è quindi considerata una fonte di crescita e di sviluppo urbano per promuovere l'idea di città inclusiva, attraverso la promozione di nuove forme di coesione sociale. Una città sostenibile per le misure ecologiche sia di controllo sia di risparmio energetico e tesa a ottimizzare le soluzioni per la mobilità e la sicurezza grazie a pratiche d'innovazione territoriale. Una s.c. è tale in via direttamente proporzionale alla qualità della partecipazione attiva dei suoi cittadini, in un contesto in cui lo spazio pubblico della città viene interpretato con particolari forme di creatività sociale, come quelle di *urban experience* nell'interazione tra Web e territorio (ambito di progettazione culturale e di azione multimediale attraverso le reti)». A livello globale sono 153 le città che hanno pubblicato una strategia ufficiale di smart city. Secondo lo studio *The Smart City Breakaway 2019* condotto dalla società di consulenza Roland Berger, sono da annoverare tra di esse Vienna, Londra e la canadese Saint Albert. In particolare, Vienna al fine di gestire i big data ha adottato la piattaforma *VeroCity* ed è stata una delle prime città a pubblicare dati governativi aperti. Attraverso la sua piattaforma è in grado di aggregare ed analizzare tali dati basandosi su *Context Broker* della Commissione europea, sistema in grado di ordinare i dati di tutti i tipi e provenienti da fonti di tutta la città, consentendo di offrire informazione in tempo reale su mobilità urbana, monitoraggio ambientale, infrastrutture urbane, efficienza energetica, facilitando così le attività quotidiane. Interessante anche il caso di Saint Albert la quale annovera tra i suoi progetti smart l'implementazione di un nuovo sistema di gestione delle prenotazioni e registrazione per migliorare i servizi per la salute mentale dei cittadini, la creazione di una foresta comunitaria per le locali banche del cibo, supportata da una mappatura on-line, lo sviluppo della tecnologia necessaria a supporto degli anziani nelle loro case (reti a banda larga, telematica, medicina); la realizzazione di un sistema di trasporto intelligente con segnali adattivi come sistemi di monitoraggio centrale, situazioni di conteggio permanente, stazioni RWIS. Per il *City mobility index 2020* di Deloitte, invece, è Stoccolma la città più smart nella mobilità.



⁶R. GIFFINGER, C. FERTNER, H. KARMAH et al., *Smart cities. Ranking of European medium sized cities*, final report, October 2007; D. HARVEY, *L'esperienza urbana*, il Saggiatore, 1998; R.G. HOLLANDS, *Will the Real Smart City Stand Up? Intelligent, Progressive, or Entrepreneurial?*, in "City. Analysis of Urban Change, Theory, Action", vol. 12, 2008, n. 3, p. 303.

⁷EUROPEAN COMMISSION, *Smart cities*.

⁸Volendo fare alcuni esempi, si pensi al moltiplicarsi di iniziative pionieristiche volte a sperimentare l'introduzione di servizi digitali integrati nel tessuto urbano come sistemi di *smart grid* per la gestione intelligente delle reti elettriche ed idriche; progetti di mobilità urbana; sistemi di rilevamento di parametri ambientali; l'utilizzo dei droni per il monitoraggio del territorio o di robot per la raccolta dei rifiuti.

⁹Si pensi al potenziamento del sistema di identità digitale SpID, all'introduzione dell'app IO.it, alla creazione di piattaforme digitali per la gestione della campagna vaccinale.

¹⁰Un esempio significativo è rintracciabile nel programma *Smarter Italy*, che nasce con il decreto del Ministero dello sviluppo economico del 31 gennaio 2019 e diviene operativo con la convenzione tra MISE ed AgID. Con il Protocollo d'intesa, firmato ad aprile 2020, il Ministero dell'università e ricerca e il Dipartimento per la trasformazione digitale entrano a far parte del progetto, inserendo al suo interno il segmento "Borghi del futuro", una delle 20 azioni di "Italia 2025" del MITD, che sperimenta le soluzioni innovative del programma anche su comuni di minore dimensione. Il laboratorio *Smarter Italy* è così costituito da 11 centri urbani (le c.d. smart city: Bari, Cagliari, Catania, Genova, L'Aquila, Matera, Milano, Modena, Prato, Roma, Torino) che rappresentano il luogo di sperimentazione delle soluzioni proposte, ai quali si aggiungono 12 piccoli centri che costituiscono i "Borghi del futuro" (veri e propri laboratori di innovazione tecnologica che vedono quali protagonisti: Alghero, Bardonecchia, Campobasso, Carbonia, Cetraro, Concorezzo, Ginosa, Grottole, Otranto, Pantelleria, Pietrelcina e Sestri Levante). Le prime aree di intervento del programma sono: *Smart mobility*, per il miglioramento sostanziale dei servizi per la mobilità di persone e merci nelle aree urbane; valorizzazione dei beni culturali (*Cultural Heritage*), per la valorizzazione economica e turistica delle aree di rilevanza storica e artistica; benessere sociale e delle persone (*Wellbeing*) per il miglioramento dello stato psico-fisico dei cittadini; protezione dell'ambiente per il miglioramento della situazione ambientale in tutti i suoi aspetti. Sono previste ulteriori aree di intervento con l'avanzamento del Programma, tenendo conto degli obiettivi posti dai soggetti che vi aderiranno.

¹¹N.M. GUSMEROTTI, M. FREY, F. IRALDO, *Management dell'economia circolare*, Franco Angeli, 2020.

¹²A. MOLITERNI, *La sfida ambientale e il ruolo dei pubblici poteri in campo economico*, in "Rivista quadrimestrale di diritto dell'ambiente", 2020, n. 2, pp. 32-71.

¹³Risoluzione del Parlamento europeo, *Nuovo piano d'azione per l'economia circolare*, 10 febbraio 2021.

¹⁴MINISTERO DELLA TRANSIZIONE ECOLOGICA, *Strategia nazionale per l'economia circolare*, 30 settembre 2021.

¹⁵Volendo fare un esempio si pensi allo *Smart Bin* del progetto INNOWEE, promosso dall'ENEA, che dal 2018 si propone di creare un modello innovativo per la gestione della raccolta dei rifiuti da apparecchiature elettriche ed elettroniche (c.d. RAEE). Si tratta di un sistema di riconoscimento che consente il conferimento del rifiuto solo se l'utente si fa riconoscere tramite tessera sanitaria ed è dotato di sensori di riempimento che, collegati a piattaforma Web, forniscono in tempo reale ed in autonomia, informazioni su quantità e tipo di RAEE raccolti. R. MORABITO, *La transizione verso l'economia circolare in aree e comunità urbane: approccio ENEA*, Firenze University Press, 2020.

¹⁶Per un approfondimento sull'*Agenda 2030 NU* e sul *Green Deal europeo*, L. KAPPLER, *Il recepimento dell'Agenda 2030 per lo sviluppo sostenibile: spunti metodologici dalle esperienze statunitensi dei distretti d'innovazione dell'area di Boston*.

¹⁷EUROPEAN COMMISSION, *Industry 5.0: Towards more sustainable, resilient and human-centric industry*, 7 January 2021.

¹⁸MINISTERO DELLO SVILUPPO ECONOMICO, *Piano nazionale Industria 4.0*.

¹⁹L'Industria 4.0, basata sulla digitalizzazione, sull'automatizzazione e sull'interconnessione dei processi produttivi, si è affermata ormai da un decennio. Si tratta di quell'industria che ha visto nascere, evolversi ed affermarsi tecnologie avanzate come cloud computing e *Information Technology*, *Internet of Things (IoT)* e Intelligenza Artificiale, realtà aumentata, Big data, l'HMI ovvero l'interfaccia uomo-macchina innovativa, volte ad incrementare flessibilità e efficienza della produzione. Se scopo dell'Industria 4.0 è quello di massimizzare efficienza, produttività e migliorare la qualità della vita del lavoratore, da più parti sono stati sollevati dubbi sulla effettiva capacità di questo tipo di organizzazione di migliorare la qualità del lavoro e delle condizioni del lavoratore, ritenendo disattese le aspettative iniziali e ravvisando nell'introduzione di robot nell'organizzazione dei cicli produttivi delle aziende un rischio proprio per i posti di lavoro. L'Industria 5.0 propone, invece, una visione dell'industria che va al di là dell'efficienza e della produttività come unici obiettivi, proponendo un ruolo attivo e da protagonista del mondo produttivo nel fornire soluzioni alle sfide che la società si troverà ad affrontare, compresa la conservazione delle risorse, il cambiamento climatico, l'equità, la sostenibilità e la stabilità sociale. Parole chiave dell'industria 5.0 sono dunque resilienza, sostenibilità e visione umanocentrica. Si tratta, infatti, di un approccio che mette in risalto l'importanza della ricerca e dell'innovazione a supporto non solo dell'industria ma soprattutto dell'umanità. La Commissione europea ha riconosciuto all'Industria 5.0 il potere di raggiungere gli obiettivi sociali al di là della crescita e del lavoro, per diventare fornitrice resiliente di prosperità attraverso produzioni che rispettino l'ambiente ed il nostro pianeta ponendo il benessere del lavoro aziendale al centro dei processi produttivi. L'approccio Industria 5.0 contribuisce, infatti, a tre delle priorità della Commissione: "Un'economia al servizio delle persone", "Green Deal europeo" e "L'Europa pronta per l'era digitale". Gli elementi pertinenti a Industria 5.0 fanno già parte delle principali iniziative politiche della Commissione: adottare un approccio incentrato sull'uomo per le tecnologie digitali, compresa l'intelligenza artificiale; riqualificazione dei lavoratori europei, in particolare delle competenze digitali; industrie moderne, efficienti sotto il profilo delle risorse e sostenibili e transizione verso un'economia circolare; un'industria globalmente competitiva e leader mondiale, accelerando gli investimenti in ricerca e innovazione. EUROPEAN COMMISSION, *Industry 5.0*. La differenza principale tra Industria 4.0 e 5.0 risiede, quindi, nella capacità di quest'ultima di creare le condizioni affinché il rapporto uomo-tecnologie intelligenti al servizio del settore del lavoro sia sempre più equilibrato e dia vita ad una collaborazione tra uomo e robot. Antonio Frisoli, docente di robotica presso la Scuola Superiore Sant'Anna, ha affermato che i robot collaborativi (c.d. Cobot) sono una leva per un'industria che si avvia verso la fase 5.0 della propria evoluzione, con notevoli cambiamenti sulla società e nuovi scenari di applicazione di tali innovazioni. Con "robotica collaborativa" ci si riferisce a quei sistemi robotici di nuova generazione che sono in grado di interagire fisicamente in sicurezza con l'uomo e di dividerne lo spazio, non rimanendo pertanto più confinati in una "gabbia" che separa lo spazio dell'uomo da quello del robot. A. DI MININ, *L'empatia dei robot - dialogo con Antonio*



Frisoli, in “Il sole 24ore”, 7 ottobre 2021. Non è un caso che i concetti di Industria 5.0 e Società 5.0 siano strettamente legati tra di loro in quanto si propongono di delineare un cambio di paradigma sia da un punto di vista sociale che economico attraverso un approccio antropocentrico. Scopo della Società 5.0 è quello di bilanciare lo sviluppo economico con la risoluzione di problematiche sociali ed ambientali. Tale cambio di paradigma non è limitato solo al settore della produzione ma anche alla maggior parte dei problemi sociali ed ambientali provocati dal rapporto tra mondo reale e virtuale. La Commissione europea nel suo paper *Industry 5.0: towards a sustainable, human-centric and resilient European industry* ha affermato che la Società 5.0 è una società nella quale le tecnologie informatiche avanzate, IoT, robots, A.I. e realtà aumentata sono utilizzate nella vita di tutti i giorni, nell'industria, nell'assistenza sanitaria, ed in altre sfere di attività, a vantaggio non solo e principalmente dell'industria ma anche e soprattutto per il bene e la convenienza dei cittadini. M. BREQUE, L. DE NUL, A. PETRIDIS, *op. cit.*; A. AJODANI, A. ZANCHETTIN, S. IVALDI et al., *Progress and Prospects of the Human-Robot Collaboration. Autonomous Robots*, Springer Verlag, 2017, p. 1-17.

²⁰Il termine IoT si riferisce ad una rete di dispositivi fisici (*things*) che possono essere connessi tra loro e con altri servizi dispiegati su reti locali o globali. Tali dispositivi sono tipicamente composti da sensori, attuatori, apparati di telecomunicazioni e unità di processamento di modesta capacità computazionale (c.d. microcontrollori).

²¹MINISTERO DELLO SVILUPPO ECONOMICO, *Programma di supporto alle tecnologie emergenti 5G*.

²²GOVERNO ITALIANO, *Programma strategico Intelligenza Artificiale 2022-2024*, 24 novembre 2021. Di recente il Consiglio di Stato con sentenza n. 7891/2021 ha avuto modo di precisare la differenza tra algoritmo ed AI sottolineando come in quest'ultima “l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo “tradizionale”) ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico”. Anche la Commissione europea nella sua Proposta di regolazione dell'AI, del 21 aprile 2021, all'art. 3 ha definito i sistemi di Intelligenza artificiale come “software sviluppato con una o più tecniche e approcci elencati nell'allegato I e che può, per una data serie di obiettivi definiti dall'uomo, generare risultati quali contenuto, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono”. *Proposta di Regolazione del Parlamento europeo e del Consiglio europeo che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM/2021/206 final)*.

²³L. HARDESTY, *Explained: Neural networks. Ballyhooed artificial-intelligence technique known as “deep learning” revives 70-year-old idea*, MIT News Office, April 14, 2017.

²⁴K. RANJITHPRABHU, D. SASIREGA, *Eliminating Single Point of Failure and Data Loss in Cloud Computing*, in “International Journal of Science and Research”, vol. 3, 2014, n. 4, p. 335-337.

²⁵P. MIDDLETON, J. TULLY, P. KJELDSSEN, *Forecast: The Internet of Things, Worldwide*, 2013.

²⁶P. FRAGA-LAMAS, S.I. LOPES, T.M. FERNÁNDEZ-CARAMÉS, *Green IoT and Edge AI as Key Technological Enablers for a Sustainable Digital Transition towards a Smart Circular Economy: An Industry 5.0 Use Case*, in “Sensors”, vol. 21, 2021, n. 17, 5745.

²⁷L'edge computing è una parte rilevante del mercato OT (*Operational Technology*) e crescerà rapidamente nei prossimi cinque anni. All'interno del mercato delle infrastrutture, il cloud computing si imporrà sia nel cluster Europe-5 che in

quello Big-5, laddove l'edge computing costituirà un'area in forte crescita nei prossimi 5 anni. La Germania sarà il più grande mercato europeo sia per il cloud computing che per l'edge computing con una crescita del 28% (2025 vs 2020). Osservando il cluster Big-5, è previsto che le cifre crescano sia per il mercato del cloud hosted pubblico/privato sia per quello dell'infrastruttura OT e dell'edge, con un impressionante aumento fino al 60% (2025 vs 2020) negli USA. Cfr. *From Cloud to Edge. Una panoramica sul mercato mondiale del Cloud Computing con un focus sulle nuove opportunità offerte dall'Edge Computing*.

²⁸C. RATTI, M. CLAUDEL, *La città di domani, come le reti stanno cambiando il futuro*, Einaudi, 2017.

²⁹La sicurezza ha da sempre assunto un ruolo centrale nella società: per Castel il mondo sociale «è stato organizzato in funzione della continua, affannosa ricerca di protezione e sicurezza»; Malinowsky asseriva che ogni cultura è costituita dall'insieme di risposte che la società fornisce ai bisogni dell'attore sociale, suddividendo i bisogni in fondamentali e in derivati. La sicurezza intesa sia come tutela dell'integrità fisica sia come dimensione sociale stabile e sicura, è da collocarsi proprio tra i bisogni primari, è il primo tra i bisogni primari, propedeutico a tutti gli altri bisogni, come ha affermato Maslow essa costituisce «una componente cruciale per la qualità della vita». Bauman distingue tre tipi di sicurezza che con la post-modernità sembrano essere entrati in crisi: «una sicurezza (*security*) che ha a che vedere con la propria condizione sociale e lavorativa e si poggia sulla stabilità e affidabilità del mondo; una sicurezza (*certainty*) di tipo cognitivo che ha a che fare con la prevedibilità e intelligibilità dell'ambiente che ci circonda e della nostra posizione in esso; una sicurezza (*safety*) di tipo fisico che riguarda le minacce alla incolumità propria e dei propri beni». R. CASTEL, *L'insicurezza sociale. Che significa essere protetti?*, Einaudi, 2011. B. MALINOWSKY, *Freedom and Civilization*, Greenwood Press, 1976. A. MASLOW, *Motivation and Personality*, Harper & Row Publishing, 1954. Z. BAUMAN, *Paura liquida*, Laterza, 2006.

³⁰M. SESSA, *Smart Safe City: criticità e prospettive sociali*, in “Rivista trimestrale di scienza dell'amministrazione”, 2020, n. 3.

³¹Il Ministero dell'Interno nel *Dossier* del Viminale 1° agosto 2020-31 luglio 2021, ha evidenziato come rispetto all'anno precedente gli attacchi informatici siano decuplicati (da 460 nel periodo 2019-2020 a 4.938 nel periodo 2020-2021) così come gli alert diramati hanno subito un aumento del 212%).

³²Si veda al riguardo *Rapporto Clusit sulla sicurezza ICT in Italia*, marzo 2022.

³³Si pensi a titolo esemplificativo al settore sanitario e a quello della mobilità; si ricordino gli attacchi ai sistemi informatici di LazioCrea e a tutti i siti di riferimento (Regione Lazio, Lazio salute, portale prenotazione vaccini) dell'agosto 2021.

³⁴S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in “Harvard Law Review”, vol. 4, 1890, n. 5, p. 193-220. Furono Samuel Warren e Louis Brandies a definire per la prima volta la privacy come «the right to be let alone» ovvero, il diritto a essere lasciati soli, a godere del proprio privato, una sorta di estensione soggettiva del diritto lockiano alla proprietà privata. «The Right to Privacy» rappresenta la pietra angolare su cui poggia il moderno istituto giuridico della privacy; diritto fondamentale su cui si fonda la libertà individuale di fronte a quello che Zuboff ha definito «Capitalismo della Sorveglianza». Sono proprio i cambiamenti sociali, politici, ed economici ad imporre una rilettura del concetto di privacy e della sua estensione.

³⁵Non è un caso che negli ultimi anni e soprattutto a seguito dell'accelerazione impressa dalla Pandemia al processo di digitalizzazione della società, privacy e cybersecurity siano



stati oggetto di intervento sia da parte dell'Unione europea che dei singoli Stati. In particolare, si ricordino l'introduzione della c.d. direttiva NIS - *Network and information security* (direttiva 2016/1148 che nel 2020 ha visto una proposta di revisione c.d. NIS2) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi, nonché il *Cybersecurity Act* (Regolamento (UE) 2019/881) attraverso il quale è stato potenziato il ruolo dell'Enisa (Agenzia europea per la sicurezza delle reti e dell'informazione); l'introduzione del GDPR Regolamento (UE) 2016/679. Anche l'Italia si è mossa in tal senso. La direttiva NIS è stata recepita nell'ordinamento italiano con il d.lgs. 18 maggio 2018, n. 65, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. Successivamente, è stato adottato il d.l. 21 settembre 2019, n. 105 al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal d.l. 30 dicembre 2019, n. 162, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione. In attuazione del d.l. 105/2019 sono stati definiti in particolare il d.P.C.M. 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il d.P.C.M. 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC. Infine, con il d.l. 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.

³⁶L'uso di droni dotati di dispositivi tecnologici può avere un forte impatto sulla privacy e sulla protezione dei dati personali degli interessati, in quanto gli operatori di droni che registrano e/o elaborano immagini, video, suoni e che si avvalgono di dati biometrici e di geolocalizzazione relativi a una persona, possono identificarla direttamente (mediante una foto o un video) o renderla identificabile attraverso una successiva elaborazione (come nel caso delle informazioni relative alla geolocalizzazione) o l'"arricchimento" con altri dati aggiuntivi come quelli acquisiti da Internet. In questi ultimi casi, anche se una persona potrà essere identificabile, il risultato finale riguarderebbe un'identificazione possibile grazie a informazioni incrociate provenienti da diverse fonti. Sia nel caso in cui i dati raccolti dai droni identificano inequivocabilmente una persona, sia nel caso in cui ciò possa avvenire successivamente, si applica comunque la normativa in materia di protezione dei dati personali Regolamento (UE) 2016/679 (GDPR). È da notare, inoltre, che quando ci troviamo di fronte ad un insieme di "dati misti" ovvero dati personali e non personali, il Regolamento sui dati non personali RDNP (Regolamento (UE) 2018/1807) sembra vacillare: all'art. 2 stabilisce infatti che il Regolamento generale sulla protezione dei dati personali e quello sulla libera circolazione dei dati non personali si applicano alla rispettiva categoria di dati; tuttavia quando tali insieme di dati sono indissolubilmente legati, il GDPR troverà applicazione all'intero *dataset* anche quando i dati personali rappresentano solo una piccola parte dell'insieme, in ossequio alla costante logica del primato della protezione rispetto alla circolazione. In tale direzione sembra essersi mosso anche il Garante della Privacy nell'affrontare tale questione. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Droni e privacy - Il Vademecum del Garante*.

³⁷È da notare anche come ad oggi la maggior parte dei costruttori di device mostri gravi carenze nella tutela della privacy degli utenti. Come mostrato nell'indagine condotta

nel maggio del 2017 dal *Global Privacy Enforcement Network* (GpEN) del quale fa parte anche il Garante italiano, per verificare il rispetto della privacy nella IoT, su oltre trecento dispositivi elettronici connessi a Internet, più del 60% non ha superato l'esame dei Garanti della privacy di 26 paesi. È emerso in particolare che: il 59% degli apparecchi non offre informazioni adeguate su come i dati personali degli interessati sono raccolti, utilizzati e comunicati a terzi; il 68% non fornisce appropriate informazioni sulle modalità di conservazione dei dati; il 72% non spiega agli utenti come cancellare i dati dal dispositivo; il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria privacy GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Privacy: "Internet delle cose", utenti poco tutelati. I risultati dell'analisi internazionale svolta dalle Autorità garanti della privacy di 26 Paesi per il "Privacy Sweep 2016"*, 22 settembre 2016.

³⁸Si pensi ad un sistema informatico per il rilevamento di sinistri stradali dotato: di un drone per l'acquisizione delle immagini, di una AI dispiegata su sistemi *edge* in grado di riconoscere un sinistro analizzando una serie di immagini, ed infine di un sistema centralizzato dispiegato su cloud che, ricevuta una segnalazione di sinistro dalla AI, invia i soccorsi. In tale casistica il drone potrebbe rilevare la presenza di individui nelle vicinanze delle auto fotografate. L'AI, valutando esclusivamente le immagini che rappresentano lo stato attuale del traffico, è in grado di valutare se sono presenti situazioni critiche, ma una volta presa tale decisione non avrà più la necessità di accedere alle medesime immagini, che verranno quindi cancellate. Il sistema centrale cloud non avrà mai bisogno delle singole immagini per erogare il proprio servizio, ma necessiterà solamente di ricevere una asettica segnalazione di avvenuto sinistro da parte dell'AI.

³⁹M. AHMED, P. HASKELL-DOWLAND (eds.), *Secure Edge Computing. Applications, Techniques and Challenges*, CRC Press, 2021.

⁴⁰*European industrial technology roadmap for the next generation cloud-edge offering*, May 2021.

⁴¹Il Piano Nazionale di Ripresa e Resilienza (PNRR), grazie ai fondi del *Next Generation Europe EU* (NGEU), prevede un investimento di oltre 190 miliardi di euro in risposta alla crisi pandemica destinati in parte a finanziare proprio l'implementazione del Piano Triennale per l'informatica nella pubblica amministrazione 2021-2023 al fine di produrre nei prossimi anni una ulteriore forte accelerazione nei processi di innovazione in atto. Il Piano triennale per l'informatica nella pubblica amministrazione, dell'ottobre 2021, è il risultato della collaborazione tra AGID ed il Dipartimento per la trasformazione digitale ed elenca tra i principi guida del processo di digitalizzazione: *digital & mobile first*; *digital identity only*; *cloud first*; servizi inclusivi e accessibili; dati pubblici un bene comune; interoperabile *by design*; sicurezza e *privacy by design*; *user-centric*, *data driven* e agile; *once only*; le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite; *transfrontaliero by design*; codice aperto. Si veda anche, EUROPEAN COMMISSION, *Bussola per il digitale 2030: il modello europeo per il decennio digitale (c.d. Digital compass)*, 9 marzo 2021. Id., *2030 Digital Compass: your digital decade*.

⁴²La digitalizzazione delle pubbliche amministrazioni si inserisce in un disegno di più ampio respiro di matrice europea, delineato dal *Green Deal europeo* COM(2019) 640 dell'11 dicembre 2019 e dalla Nuova strategia industriale, parte integrante della strategia Ue per riorientare il processo macroeconomico ed attuare i 17 obiettivi di sviluppo sostenibile previsti dall'Agenda 2030 (UNITED NATIONS, *Transforming our world: the 2030 Agenda for Sustainable Development*) andando a costituire un primo indispensabile passo per far



si che si realizzi l'incontro tra i diversi stakeholder (imprese, terzo settore, cittadini, P.A.) che daranno vita alle future città e comunità digitali.

⁴³La diffusione della banda ultra-veloce e le reti 5G è affidata a cinque progetti: "Italia a 1 Giga", "Italia 5G", "Scuole connesse", "Sanità connessa" e "Collegamento isole minori". Il progetto di maggiore rilevanza è rappresentato da MINISTRO PER L'INNOVAZIONE TECNOLOGICA E LA TRANSIZIONE DIGITALE, *Piano "Italia 5G". Consultazione pubblica ai sensi del paragrafo 64 e 78, lettera b) degli Orientamenti dell'Unione europea per l'applicazione delle norme in materia di aiuti di Stato in relazione allo sviluppo rapido di reti a banda larga*, 15 novembre 2021.

⁴⁴DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE, AGENZIA PER LA CYBERSICUREZZA NAZIONALE, *Strategia Cloud Italia. Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA*; MINISTRO PER L'INNOVAZIONE TECNOLOGICA E LA TRANSIZIONE DIGITALE, *Italia digitale 2026. Obiettivi e iniziative per il digitale nel Piano nazionale di ripresa e resilienza*.

⁴⁵Al fine di rendere effettivi ed efficaci gli interventi appena descritti è intervenuta poi la novità in campo normativo del Decreto Semplificazioni "bis" (d.l. 31 maggio 2021, n. 77 come convertito con la l. 29 luglio 2021, n. 108) il quale ha introdotto l'art. 18-bis del CAD (Violazione degli obblighi di transizione digitale). La norma richiede una maggior attenzione all'adempimento di tutte le indicazioni riportate nel Piano Triennale, con il supporto da parte dell'AgID, nell'orientare l'approccio operativo secondo principi di indirizzo, collaborazione, supporto e deterrenza agli attori interessati dalle norme in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione. All'AgID è altresì attribuito il compito di stabilire con proprio regolamento le procedure di contestazione, accertamento, segnalazione e irrogazione delle sanzioni per le violazioni di cui alla presente disposizione. Tutto ciò sarà necessario al fine di raggiungere gli obiettivi preposti nei tempi previsti, evitando eventuali provvedimenti sanzionatori per mancata ottemperanza degli obblighi di transizione digitale.

⁴⁶Dal Censimento AgID del patrimonio ICT è risultato che dei 1.252 data center censiti: 35 sono risultati candidabili all'utilizzo da parte del polo strategico nazionale; 27 sono stati classificati nel gruppo A; i restanti 1.190 sono stati classificati nel gruppo B.

⁴⁷Il *Piano triennale per l'informatica nella pubblica amministrazione 2019-2021* al capitolo 3.2.3, predispone le linee di azione per la migrazione al cloud.

⁴⁸Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e

al Comitato delle regioni. *Una strategia europea per i dati*, 19 febbraio 2020 COM(2020) 66 final: «il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2051. Ogni nuova ondata di dati offre all'UE grandi opportunità per divenire un leader mondiale nel settore. Anche le modalità di conservazione ed elaborazione dei dati cambieranno significativamente nei prossimi cinque anni. Attualmente l'80% delle elaborazioni e delle analisi dei dati si svolge in centri di dati e strutture di calcolo centralizzate, e il 20% in oggetti connessi intelligenti, quali automobili, elettrodomestici o robot di fabbricazione, e in strutture di calcolo vicine all'utente ("edge computing"). Entro il 2025 tali percentuali probabilmente si invertiranno. Una simile evoluzione, oltre a presentare vantaggi economici e in termini di sostenibilità, crea ulteriori opportunità per lo sviluppo, da parte delle imprese, di strumenti che consentano ai produttori di dati di incrementare il controllo sui propri dati».

⁴⁹Ad oggi solo alcuni operatori di telecomunicazioni e cloud provider, pionieri del settore, hanno avviato sperimentazioni in ambito IoT ed *edge computing* sul territorio nazionale. Volendo fare alcuni esempi si vedano i progetti di Reply, Fastweb, Google ed Amazon. Sempre il gruppo TIM partecipa ad una iniziativa congiunta con Google volta a creare un nuovo soggetto Noovle.

⁵⁰L'approvazione del *Cloud Act* da parte del Congresso USA e la pretesa di poter accedere ai dati degli utenti custoditi dai fornitori cloud americani indipendentemente dal luogo in cui sono conservati, superando così il concetto e le garanzie assicurate dal modello c.d. *Data Location*, ha alimentato i timori di indesiderate interferenze da parte degli Stati Uniti sui dati dei cittadini di altri Paesi. Nel modello *Data trust*, il fornitore di servizi cloud si avvale di un soggetto esterno (c.d. *data trustee*) per la gestione di tutto ciò che esula dalla stretta manutenzione operativa dell'infrastruttura. Attraverso la figura negoziale del trust il fornitore si spoglia completamente della facoltà giuridica di accedere ai dati che transitano sull'infrastruttura per affidarli ad una terza parte. Tutte le richieste di accesso ai dati dovranno essere indirizzate al *Trustee* (l'unico in possesso delle chiavi di cifratura), il quale sarà tenuto a valutare tali richieste sulla base del solo diritto nazionale. Per un approfondimento si veda V. BONCINELLI, *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in questa Rivista, 2021, n. 1, pp. 27-45.

⁵¹EUROPEAN COMMISSION, *Sovranità digitale: la Commissione dà il via ad alleanze per i semiconduttori e le tecnologie cloud industriali*, Bruxelles, 19 luglio 2021; Id., *European Chips Act*, 8 February 2022.

* * *

The Public administration in the age of cloud and edge computing, between opportunities and risks: PNRR and digital communities

Abstract: *Smart cities* and *Industry 5.0* are essential pieces of the European strategy for the transition to a more sustainable and fair economy. The introduction of fundamental enabling technologies, such as Internet of Things, Artificial Intelligence and Edge Computing, requires an assessment of the current state of national digital infrastructures in relation to the missions of the PNRR, which is the foundation of the Italian digital strategy. In this context, the public administration plays a leading role in connecting all the stakeholders (companies, citizens, third sector). This article aims to verify possible criticalities introduced by those technologies and possible similitudes with the governance of the implementation and regulation of cloud computing, in order to evaluate the impact of the transition to a digital and integrated society on digital sovereignty and data protection.

Keywords: Digital Sovereignty – Internet of Things – Cloud and edge computing – Smart city – Circular economy