DIMENSIONE GIURIDICA | LEGAL DIMENSION
Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

5

Smart cities

Diritti, libertà e governance

a cura di

Matteo Giannelli e Valentina Pagnanelli

G. Giappichelli Editore

DIMENSIONE GIURIDICA | LEGAL DIMENSION

Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

5

Dimensione giuridica/Legal dimension *si pone in continuità ideale con i "Quaderni del dottorato fiorentino in scienze giuridiche" pubblicati tra il 2013 e il 2017 e vuole porre in evidenza come quanto avviato negli anni passati sia diventato ora un dato strutturale. È questo il caso anzitutto del processo di internazionalizzazione, che ha condotto a un'elaborazione scientifica che è bene sia accolta in una tipologia di pubblicazione capace di evidenziare, anche già nel nome, la rilevanza non puramente municipale del suo contenuto.*

Il percorso costruito attraverso gli anni ha permesso di gettare le basi anche dell'elemento di innovazione introdotto in questa nuova fase, ossia la valorizzazione del lavoro dei dottorandi e di chi si è recentemente formato nel dottorato fiorentino e sta costruendo il proprio percorso scientifico. Dimensione giuridica/Legal dimension *non vuole infatti proporsi come luogo dove i "giovani" sono semplicemente invitati a fornire contributi all'interno di iniziative ideate e dirette da altri, più avanti negli anni e nella carriera, ma intende accogliere principalmente ricerche proposte e coordinate in prima persona proprio da* early career scholars, *pur senza escludere a priori l'inclusione di scritti di studiosi affermati.*

Smart cities
Diritti, libertà e governance

a cura di

Matteo Giannelli e Valentina Pagnanelli

G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 978-88-921-2361-8
ISBN/EAN 978-88-921-7267-8 (ebook - pdf)

Volume pubblicato con il contributo del Miur per i progetti di eccellenza 2018-2022.

Stampa: Stampatre s.r.l. - Torino

INDICE

pag.

pag.

pag.

GLI AUTORI

NICOLÒ ACQUARELLI, Dottorando in Scienze giuridiche (diritto pubblico) presso l'Università di Firenze.

STEFANO ATERNO, Avvocato; Professore a contratto di Diritto delle nuove tecnologie presso l'Università di Foggia.

PAOLA BECCHERLE, Dottoranda in Development Economics and Local Systems (DELoS) presso l'Università di Firenze.

SILVIA A. CARRETTA, Dottoranda in diritto privato e intelligenza artificiale presso l'Università di Uppsala; affiliata alla Wallenberg Artificial Intelligence, Autonomous Systems and Software Program – Humanities and Society Graduate School (WASP-HS).

CARLO COLAPIETRO, Professore ordinario di Diritto costituzionale presso l'Università di Roma Tre.

FABRIZIO DALL'ACQUA, Segretario generale del Comune di Milano.

MATTEO GIANNELLI, Ricercatore a tempo determinato di Diritto costituzionale presso l'Università di Firenze.

MARCO MACCHIA, Professore associato di Diritto amministrativo presso l'Università di Roma Tor Vergata.

VALENTINA PAGNANELLI, Dottoressa di ricerca in Scienze giuridiche (diritto pubblico) presso l'Università di Firenze.

FEDERICA PAOLUCCI, Dottoranda in Diritto pubblico presso l'Università commerciale "L. Bocconi" di Milano.

ORESTE POLLICINO, Professore ordinario di Diritto costituzionale presso l'Università commerciale "L. Bocconi" di Milano.

GIORGIO RESTA, professore ordinario di Diritto privato comparato presso l'Università di Roma Tre.

ANDREA SIMONCINI, Professore ordinario di Diritto costituzionale presso l'Università di Firenze.

PASQUALE STANZIONE, Professore emerito di Diritto privato presso l'Università di Salerno; Presidente del Garante per la protezione dei dati personali.

GIULIA TAVELLA, Dottoranda in Scienze giuridiche (discipline penalistiche) presso l'Università di Firenze; Magistrato ordinario in tirocinio presso il Tribunale ordinario di Firenze.

NOTA INTRODUTTIVA

I volumi di questa collana non comprendono, di norma, presentazioni da parte del suo coordinatore, una funzione questa che non è d'altronde stabile, ma è svolta da chi è *pro tempore* coordinatore del dottorato in scienze giuridiche attivo presso l'Università di Firenze. Nel primo volume, pubblicato nel 2020, era presente però una "nota introduttiva", volta non tanto a sottolineare il valore delle ricerche presentate, quanto a illustrare le caratteristiche del progetto editoriale che in quel momento prendeva il via. Dopo tre anni e altri quattro volumi completati, può essere utile spendere di nuovo qualche parola per fare un breve bilancio consuntivo rispetto a quanto promesso in quella sede.

Come i volumi precedenti, anche questo si ricollega a un convegno organizzato presso il Dipartimento di scienze giuridiche dell'Università di Firenze, senza tuttavia essere semplicemente la riproduzione di quanto detto. In questo come in tutti gli altri volumi sinora pubblicati si è cercato d'altronde sempre di presentare elaborazioni scientifiche mature, lasciando agli autori il tempo necessario ed eventualmente accogliendo scritti di ricercatori che non erano presenti, ma che si è ritenuto potessero con le loro competenze elevare il valore complessivo dell'opera.

L'iniziativa che ha rappresentato il punto di partenza in questo caso rappresentava l'evento conclusivo delle attività del dottorato collegate al progetto "Dipartimento di eccellenza", finanziato dal MIUR per il quinquennio 2018-2022, che ha fornito le risorse necessarie alla pubblicazione di tutti i volumi sinora usciti. Come noto, il dipartimento ha visto rinnovata la propria posizione quale "Dipartimento di eccellenza" anche per il quinquennio successivo (2023-2027), e in fondo già questo sarebbe bastato a dichiarare "*mission accomplished*", passando alla fase successiva senza troppo ricamare su quanto fatto.

Cedere alla pigrizia avrebbe però comportato perdere un'occasione preziosa per rivisitare il percorso che ha portato sin qui. Cose che sono forse note a chi fa parte del dipartimento fiorentino, ma che possono rivestire interesse per i lettori con altre radici accademiche, che crediamo saranno moltissimi, come è avvenuto per altri titoli della collana.

Una prima considerazione di carattere generale è che l'indice del volume è già di per sé una sorta di "cartografia culturale" di cosa è stato fatto a Firenze negli ultimi anni. Salta subito all'occhio anzitutto la centralità che il dipartimento ha assunto in Italia nella ricerca circa le implicazioni giuridiche della radicale trasformazione della società indotta dall'esplosione dell'intelligenza artificiale, ricerca declinata – secondo il classico "stile fiorentino" – a partire dai valori costituzionali. A questa tela di fondo si è aggiunta una solida interdisciplinarietà, come reso evidente dai contributi che abbracciano dimensioni penalistiche e amministrativistiche e dall'integrazione di prospettive extragiuridiche, queste ultime come ricaduta diretta della recente istituzione presso l'ateneo fiorentino di una Scuola di dottorato in scienze sociali, di cui il dottorato in scienze giuridiche è stato tra i promotori. Nulla è casuale in questo volume, e anche la presenza tra gli autori di una dottoranda dell'Università di Uppsala, seppur italiana di formazione, si spiega con il filo che ci lega all'ateneo svedese da ormai più di trent'anni. Importantissimo è poi il rapporto con le istituzioni statali e gli enti locali, che dimostra la capacità dei nostri dottorandi e ricercatori di far valere le proprie competenze anche confrontandosi con le difficoltà del quotidiano operare delle pubbliche amministrazioni.

Riprendendo il "manifesto" della prima "nota introduttiva" crediamo, tuttavia, che il principale motivo di orgoglio debba essere un altro. In quelle pagine si ambiva, infatti, ad avviare una collana dove dottorandi e neodottori – così scrivevamo – "non sono semplicemente invitati a produrre un elaborato all'interno di un'iniziativa ideata e diretta da altri più avanti negli anni e nella carriera", ma dove si accolgono "ricerche proposte e coordinate in prima persona proprio da *early career scholars*, senza ovviamente escludere a priori l'inclusione di scritti di studiosi affermati". Ancora una volta, saranno i lettori a giudicare il valore del volume, a prescindere dalle qualifiche degli autori. Crediamo però che la scommessa circa la possibilità di una collana di alto livello basata sulle intuizioni e il lavoro di chi il dottorato lo sta vivendo, e dove si rinuncia nella sostanza – ma anche nella forma – alla curatela di un "maestro" o "maestra", sia stata abbondantemente vinta.

Alessandro Simoni

INTRODUZIONE

INTELLIGENZA ARTIFICIALE E *SMART CITIES* A MO' DI INTRODUZIONE

di *Carlo Colapietro*

1. *Dalla* polis *alla* smart city

La città è da sempre la prima forma di comunità "politica" [1]. Non a caso, quest'ultimo lemma deriva proprio dal greco *polis*, quasi ad indicare che il governo della collettività umana sia, in realtà, riconducibile al governo di una grande città. Per un costituzionalista, dunque, riflettere sulla città significa approfondire i fenomeni di convivenza sociale nella loro dimensione "micro", andando ad individuare le dinamiche dei rapporti tra governanti e governati, il rispetto delle libertà fondamentali dei "cittadini" e la garanzia della loro reale inclusione nel contesto comunitario [2], anche mediante il go-

[1] Sul ruolo delle città (in particolare della *polis* greca e del comune medievale) nell'evoluzione della civiltà occidentale cfr. M. WEBER, *La città*, Milano, 1950; L. MUMFORD, *La città nella storia (1961)*, Milano, 1977; in particolare, per un'approfondita riflessione sul periodo medievale, vedi J. LE GOFF, *La città medievale*, Firenze, 2011. Per quanto attiene, invece, l'importanza delle città nella storia d'Italia cfr. S. CATTANEO, voce *Città*, in *Enciclopedia del diritto*, vol. VII, 1960; vedi anche C. CATTANEO, *La città considerato come principio ideale delle istorie italiane (1858)*, Milano, 2001. Un interessante orizzonte di senso viene offerto da E. CARLONI, M. VAQUERO PIÑEIRO, *Le città intelligenti e l'Europa. Tendenze di fondo e nuove strategie di sviluppo urbano*, in *Istituzioni del Federalismo*, n. 4, 2015.

[2] Al riguardo, l'art. 1 della Carta europea dei diritti umani nella città – adottata a Saint Denis il 18 maggio 2000 dalla Seconda Conferenza Europea delle città per i diritti umani – ha formalizzato il diritto alla città quale «*spazio collettivo che appartiene a tutti gli abitanti, i quali hanno il diritto di trovarvi le condizioni necessarie per appagare le proprie aspirazioni dal punto di vista politico, sociale ed ambientale, assumendo nel contempo i loro doveri di solidarietà*». Per ap-

dimento di quei diritti sociali, che devono essere assicurati dall'azione delle istituzioni comunali.

È bene, del resto, tener presente che l'art. 118 della Costituzione attribuisce in primo luogo ai Comuni le funzioni amministrative, «*salvo che, per assicurarne l'esercizio unitario*» non sia necessario conferirle ad enti superiori, in base ai «*principi di sussidiarietà, differenziazione ed adeguatezza*»[3]. In particolare, è il *principio di sussidiarietà* a venire in rilievo, in quanto ormai interiorizzato non solo dall'ordinamento nazionale, ma anche da quello eurounitario[4]. Alla stregua di questo principio, così come formulato nell'enciclica *Quadragesimo Anno* del 1931 di Papa Pio XI, «*una società di ordine superiore non deve interferire nella vita interna di una società di ordine inferiore, privandola delle sue competenze, ma deve piuttosto sostenerla in caso di necessità ed aiutarla a coordinare la sua azione con quella delle altre componenti sociali, in vista del bene comune*», dal momento che, «*come è illecito togliere agli individui ciò che essi possono compiere con le proprie forze e con l'iniziativa propria, per affidarlo alla comunità, così è ingiusto rimettere ad una maggiore e più alta società quello che dalle minori e inferiori comunità può esser fatto*».

Ciò premesso, appare del tutto evidente che se la strategia dell'Unione Europea[5] è quella di procedere ad una valorizzazione del governo dei dati e attraverso i dati, nonché ad un'implementazione dell'impiego di strumenti di Intelligenza artificiale al fine di utilizzare al meglio quegli stessi dati al fine di effettuare predizioni e prendere decisioni più rapide ed efficienti, allora tale

---

profondimenti si veda F. SAITTA, *Il «diritto alla città»: l'attualità di una tesi antica*, in *Ordines*, n. 2, 2020; C. ACOCELLA, G. LANEVE, *Città intelligenti e diritti: nuove prospettive di consumo nel prisma della socialità*, in *P.A. Persona e Amministrazione*, vol. IX, n. 2, 2021, pp. 105-152.

[3] Vedi sul punto, tra i tanti, F. CORTESE, *Le competenze amministrative nel nuovo ordinamento della Repubblica. Sussidiarietà, differenziazione ed adeguatezza come criteri allocativi*, in *Istituzioni del Federalismo*, n. 5, 2003; A. ALBANESE, *Il principio di sussidiarietà orizzontale: autonomia sociale e compiti pubblici*, in *Dir. pubbl.*, n. 1, 2002, p. 51 ss.; G. BERTI, G. C. DE MARTIN (a cura di), *Il sistema amministrativo dopo la riforma del Titolo V della Costituzione*, Luiss Edizioni, Roma, 2002; R. BIN, *La funzione amministrativa nel nuovo Titolo V della Costituzione*, in *Le Regioni*, n. 2-3, 2002, p. 365 ss.

[4] Cfr. S. ANTONIAZZI, Smart city*: diritto, competenze e obiettivi (realizzabili?) di innovazione*, in *Federalismi.it*, n. 10, 2019; F. PIZZETTI, *Le città metropolitane per lo sviluppo strategico del territorio: tra livello locale e livello sovranazionale*, in *Federalismi.it*, n. 12, 2015; A. STERPA, *Il principio di sussidiarietà nel diritto comunitario e nella Costituzione*, in *Federalismi.it*, n. 15, 2010.

[5] Si veda il *Parere del Comitato europeo delle regioni – Le città intelligenti: nuove sfide per una transizione giusta verso la neutralità climatica: come realizzare gli OSS nella pratica?*, 5 febbraio 2020 (consultabile in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019IR2974&from=EN*). Cfr. anche S. AUCI, L. MUNDULA, *La misura delle* smart cities *e gli obiettivi della strategia EU 2020: una riflessione critica*, in *AGEI – Geotema*, n. 59, 2019.

strategia non possa certo ignorare come, in ambito pubblico, questi aspetti debbano realizzarsi primariamente nel rapporto tra i cittadini e le istituzioni e i servizi a loro più prossimi; vale a dire, quelli comunali. Tale processo di sviluppo di forme di governo del territorio ed erogazione di servizi sempre più *data-driven*, trova uno snodo fondamentale nelle cc.dd. *smart cities*.

Per giunta, la mutazione del servizio pubblico verso nuovi modelli [6] sempre più personalizzati – oggetto, peraltro, dell'intervento del dott. Acquarelli – provocherà necessariamente una mutazione anche del tipo di rapporto tra il cittadino e il servizio, dal momento che allo *user* e al *consumer* va affiancandosi – o forse sostituendosi – il *prosumer*, che è allo stesso tempo produttore (*producer*) e consumatore. D'altronde, questa mutazione comporterà la predisposizione di servizi sempre più attenti al cittadino e, più in generale, alla persona, di cui parla anche l'intervento della dott.ssa Beccherle relativa al caso specifico dei musei.

Del resto, quel che più importa rimarcare in questa sede è che qualsiasi tipo di progresso, anche quello della città e della sua declinazione in versione "intelligente", deve avere al centro l'uomo, i suoi diritti e le sue aspirazioni, nell'ambito di una città che non è più individuata nei soli confini geografici, ma è oggetto di "deterritorializzazione" e caratterizzata da "iper-industrializzazione informatica", risultando dunque l'aspetto tipizzante non più solo la cittadinanza ma, invece, la possibilità o meno di connessione [7].

2. *Definizione e caratteri della* smart city *in Europa*

Non esiste una definizione univoca di *smart city* [8] – come messo in luce anche dalla dott.ssa Caretta, la quale, anzi, evidenzia come tale concetto appartenga "*in parte all'immaginazione*" – ma, al contrario, il termine si riferisce in

---

[6] Per approfondimenti relativi allo sviluppo dei servizi pubblici si veda F. BASSANINI, M.R. MAZZOLA, A. VIGNERI, *Una nuova politica industriale dei servizi pubblici locali: aggregare e semplificare*, in *Astrid Rassegna*, n. 19, 2014.

[7] Cfr. A. VENANZONI, Smart cities *e capitalismo di sorveglianza: una prospettiva costituzionale*, in *Forum di Quaderni costituzionali – Rassegna*, n. 10, 2019, *passim*, spec. p. 24.

[8] La mancanza di una definizione chiara di *smart city* ha comportato l'adozione di qualificazioni differenti, più o meno generiche: contrario ad un concetto troppo estensivo di *smart city* si veda R. FERRARA, *The Smart City and the Green Economy in Europe: a Critical Approach*, in *Energies*, n. 8, 2015, p. 4724 ss.; favorevole ad una qualificazione a maglie più larghe, invece, cfr. E. MASIERO, *Essere smart*, in A. BONOMI, R. MASIERO (a cura di), *Dalla* smart city *alla* smart land, Venezia, 2014, p. 111 ss.

generale ad un insieme integrato di iniziative volte a utilizzare le tecnologie digitali, compresa l'Intelligenza artificiale, per migliorare il benessere e la qualità della vita [9], superando, ad esempio, le criticità dovute al sovraffollamento delle città, rendendole vivibili e sostenibili [10]. Non tutte le "città intelligenti", però, sono necessariamente basate sull'Intelligenza artificiale, sebbene le ipotesi più avanzate facciano sempre più riferimento a questo tipo di tecnologia. Tuttavia, il concetto di città intelligente è più ampio rispetto a quello di città digitalizzata, in quanto implica la presenza di meccanismi atti a "disciplinare" gli sviluppi tecnologici, come la partecipazione dei cittadini [11].

Nel definire cosa s'intende per *smart city* occorre, dunque, scegliere se valorizzare l'elemento tecnologico [12] – vale a dire l'impiego delle *Information and Communication Technology* (ICT), al fine di rendere più intelligenti, interconnessi ed efficienti l'amministrazione e servizi pubblici [13] – ovvero tenere in considerazione anche aspetti economici e sociali [14]. Una definizione molto accreditata di *smart city* è quella fondata su sei dimensioni tipiche, quali *smart economy*, *smart mobility*, *smart environment*, *smart people*, *smart living* e *smart governance* [15], riportate anche da un interessante studio commissionato dalla

[9] Vedi, al riguardo, F. FRACCHIA, P. PANTALONE, *Condividere per innovare (e con il rischio di escludere?)*, in *Federalismi.it*, n. 22, 2015; G. SICILIANO, A. BIGHINZOLI, Smart City *tra definizioni e metodologie di misurazione*, in L. SENN (a cura di), Smart City*, la città si reinventa: Strumenti, politiche e soluzioni per un futuro sostenibile*, Milano, 2015; E. FERRERO, *Le* smart cities *nell'ordinamento giuridico*, in *Foro amm*., n. 4, 2015, p. 1267 ss.; A. CASINELLI, *Le città e le comunità intelligenti*, in *Giorn. dir. amm.*, n. 3, 2013, p. 240 ss.

[10] Cfr. M. CAPORALE, *Dalle* smart cities *alla cittadinanza digitale*, in *Federalismi.it*, n. 2, 2020.

[11] Così J. PELLEGRIN, L. COLNOT, L. DELPONTE, *Artificial Intelligence and Urban Development*, ricerca effettuata su richiesta della Commissione REGI del Parlamento europeo, pubblicata nel luglio 2021.

[12] Vedi T. NAM, T.A. PARDO, *Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*, in *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times,* New York, 2011 (disponibile al link *https://doi.org/10.1145/2037556.2037602*).

[13] Cfr. D. WASHBURN, U. SINDHU, *Helping CIOs Understand "Smart City" Initiatives,* Forrester research, 2010 (disponibile al link *https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Themes/Hubs/Brainstorm/forrester_help_cios_smart_city.pdf*).

[14] Si veda sul punto H. SCHAFFERS N. KOMNINOS, M. PALLOT, B. TROUSSE, M. NILSSON, A. OLIVEIRA, *Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation, Future Internet Assembly*, Heidelberg, 2011 (disponibile al link *https://link.springer.com/content/pdf/10.1007/978-3-642-20898-0.pdf*) e J. GORSKI, E. YANTOVSKY, *Zero Emissions Future City*, 2010 (disponibile in *https://www.researchgate.net/publication/221909547_Zero_Emissions_Future_City*).

[15] In proposito cfr. il report finale del Progetto di ricerca curato da R. GIFFINGER, C. FERTNER, H. KRAMAR, R. KALASEK, N. PICHLER-MILANOVIC, E. MEIJERS, *Smart cities. Ranking of Eu-*

Commissione Itre (Industria, Ricerca ed Energia) del Parlamento Europeo e pubblicato nel gennaio 2014 [16].

Alla luce di quanto riportato nel sito internet della Commissione Europea, «*una città intelligente è un luogo in cui le reti e i servizi tradizionali sono resi più efficienti con l'uso di soluzioni digitali a beneficio dei suoi abitanti e del business. Una città intelligente va oltre l'uso di tecnologie digitali per un migliore uso delle risorse e meno emissioni. Significa reti di trasporto urbano più intelligenti, rifornimento idrico aggiornato e strutture per lo smaltimento dei rifiuti e modi più efficienti per illuminare e riscaldare gli edifici. Significa anche un'amministrazione cittadina più interattiva e reattiva, spazi pubblici più sicuri e soddisfare le esigenze di una popolazione che invecchia*» [17].

Peraltro, è bene specificare che il modello europeo di *smart city* differisce da quello statunitense. Quest'ultimo, infatti, secondo la tradizionale tendenza americana a privilegiare l'iniziativa privata, non richiede un ruolo particolarmente attivo da parte degli apparati amministrativi. La versione europea della *smart city*, invece, per trovare attuazione, presuppone investimenti pubblici considerevoli ed una certa attività di indirizzo e pianificazione da parte degli organi di governo. Si evidenzia così la differente concezione dell'idea di innovazione: secondo l'approccio statunitense, l'innovazione rappresenta un processo dal basso verso l'alto (c.d. *bottom-up*) [18], nel cui ambito si verifica un effetto di sostanziale ritrazione delle autorità pubbliche [19], mentre invece in Europa v'è un'azione di direzione e di coordinamento che guida questo genere di processo [20].

---

ropean medium-sized cities, Vienna, University of Technology, 2007 (disponibile al link *http://www.smart– cities.eu/download/smart_cities_final_report.pdf*) e richiamato anche da M. CAPORALE, *Dalle smart cities alla cittadinanza digitale*, cit., p. 34.

[16] Cfr. lo studio del Parlamento europeo, *Mapping Smart cities in the EU,* Bruxelles, 2014 (consultabile al link *https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf*), in cui si afferma che è sufficiente la presenza di almeno uno degli elementi citati per rendere una città una *smart city*; diversamente da tale studio, nel parere del Comitato economico e sociale europeo *Le città intelligenti quale volano di sviluppo di una nuova politica industriale europea*, 1 luglio 2015 (consultabile in *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52015IE0586&from=IT*), viene sostenuto che i sei elementi individuati quali pilastri dal richiamato studio del Parlamento europeo, debbano invece coesistere affinché si possa parlare di *smart city*.

[17] Questa definizione è riportata nell'apposita sezione dedicata alle "*Smart cities*" del sito della Commissione Europea, raggiungibile al seguente collegamento web Smart cities | European Commission (*europa.eu*).

[18] Con riferimento alla differenza tra i due diversi approcci, si veda l'approfondimento di F. GASPARI, *Il* social housing *nel nuovo diritto delle città*, in *Federalismi.it*, n. 21, 2018.

[19] Vedi E. FERRERO, *Le* smart cities *nell'ordinamento giuridico*, in *Foro amm.*, n. 4, 2015.

[20] Pur esistendo visioni diverse relative alle *smart cities*, queste costituiscono al contempo un «fenomeno universale»: al riguardo si veda J.-B. AUBY, V. DE GREGORIO, *Le* smart cities *in Francia*,

Da ultimo, occorre considerare come il processo di trasformazione urbana connesso allo sviluppo delle *smart cities* non debba essere inteso come mera consequenzialità dello sviluppo tecnologico, ma, invece, come un processo "tecnomorfo", che è sì espressione dello sviluppo tecnologico ma, soprattutto, frutto delle scelte dovute ad esigenze sociali, culturali ed economiche [21], nei confronti delle quali la tecnologia deve essere servente.

3. *Le* smart cities *in Italia*

Al riguardo, va osservato che l'Italia non si pone certo come eccezione rispetto al modello europeo. Tuttavia, se questo approccio di carattere "pubblicistico", per un verso, ha rappresentato una modalità di realizzazione del bene comune mediante la predisposizione di infrastrutture tecnologiche e immateriali, per l'altro, ha mostrato talune debolezze di un approccio "burocratico" al problema.

Ebbene, l'art. 20 del d.l. n. 179/2012 (convertito nella legge n. 221/2012) definiva un modello di *governance* [22] diretto a facilitare ed accelerare il processo di realizzazione di *smart cities* e *communities*, sotto la responsabilità e la guida dell'Agenzia per l'Italia digitale (AgID) [23], incaricata di definire le strategie e gli obiettivi, nonché di predisporre gli strumenti per lo sviluppo delle "comunità intelligenti". L'intento sotteso al modello citato spaziava dall'idea di principio di mettere in comunicazione persone e oggetti, integrando informazioni e generando intelligenze che migliorassero la gestione inclusiva dei cittadini, fino a concretizzarsi nella definizione dei modelli di architettura e di piattaforme in cui inserire i metadati, i riferimenti geospaziali ed i servizi.

Sul punto è bene svolgere, però, qualche considerazione.

In primo luogo, occorre evidenziare come il testo del d.l. n. 179/2012 ha,

---

in *Istituzioni del Federalismo*, n. 4, 2015, i quali sottolineano che le *smart cities* si basano, nelle diverse esperienze, sui medesimi principi, quali «*l'utilizzo massiccio delle nuove tecnologie dell'informazione e della comunicazione (Ntic), obiettivo di risparmio energetico (la smart city è figlia della città sostenibile), mobilità, ecc. Gli standard tecnici utilizzati (qualora esistano) sono pressoché gli stessi: per esempio, quando si riflette sullo sviluppo e sulla diffusione di nuove reti per gli IoT (Internet of Things), i protocolli Sigfox et LoRa appartengono alla stessa categoria e presentano similitudini*».

[21] Così S. ANDREANI, F. BIANCONI, M. FILIPPUCCI, *Smart cities e contratti di paesaggio: l'intelligenza del territorio oltre i sistemi urbani*, in *Istituzioni del Federalismo*, n. 4, 2015, p. 896.

[22] Sul punto v. R.P. DAMERI, B. D'AURIA, *Modelli di governo e di* governance *delle* smart city*, il caso italiano*, in *ImpresaProgetto*, *Electronic Journal of Management*, n. 4, 2014.

[23] Cfr. E. CARLONI*, Il decreto «Crescita»*, in *Gior. dir. amm*., n. 11, 2012, p. 1041 ss.

in realtà, considerato soltanto alcuni elementi ascrivibili all'ambito di realizzazione delle *smart cities*. Il Legislatore non utilizza, peraltro, la locuzione "città intelligenti", bensì "comunità intelligenti" [24]. Ciò si può, forse, ricondurre al fatto che la *ratio* che ha sorretto la redazione di tale disposizione fosse, in realtà, quella di accentuare non tanto una "dimensione cittadina", ma "a misura di cittadino", evitando di circoscrivere il concetto alla città, ma mettendo, piuttosto, in evidenza l'elemento umano. Peraltro, si può aggiungere che, così facendo, si favorisce una migliore modalità di realizzazione dell'obiettivo, lasciando, cioè, spazio alle amministrazioni locali nella scelta di un modello di *governance* più adatto ai singoli aspetti geografici e sociologici, in onore al già richiamato principio di sussidiarietà.

A ciò si ricollega, inoltre, un secondo aspetto rilevante. Il tema delle *smart cities*, infatti, riporta il fulcro delle riflessioni teorico-applicative, non solo intorno alle questioni afferenti al bene comune e all'interesse pubblico, ma anche a concetti dotati di un elevato grado di politicità, quale l'appartenenza, l'identità sociale, la rappresentanza. In altri termini, il ragionamento sulla dimensione *smart* investe le declinazioni ed il senso del concetto stesso di cittadinanza (che diventa *smart citizenship*) [25], nonché di democrazia [26]. Rispetto a tale profilo, è bene tener presente che il diritto del cittadino singolo, utente nei rapporti con la PA mediante strumenti digitali, si fa "*smart*" non solo sul piano locale, ma anche con una potenzialità di respiro nazionale. Di qui il tema della *smart citizenship* trova il suo spazio nella definizione (seppur qualitativamente diversa) di "cittadinanza digitale", così come inserita nel nostro ordinamento dal Codice dell'Amministrazione Digitale [27].

Infine, non ci si può esimere dal prendere atto che, nonostante il nutrito e dettagliato novero di obiettivi, potenzialità e finalità si deve tuttora rilevare una certa genericità nelle formulazioni adottate sul tema, talvolta facendo temere di essere distratti dal miraggio della "norma manifesto" [28], con pochi episodi di applicazione effettiva.

---

[24] Come rileva anche M. CAPORALE, *Dalle smart cities alla cittadinanza digitale*, cit., p. 36.

[25] Vedi P. FERRONATO, S. RUECKER, *Smart citizenship: designing the interaction between cities and smart cities*, in *Design Research Society*, 2018, University of Limerick; L. SARTORI, *Alla ricerca della smart citizenship*, in *Istituzioni del federalismo*, n. 4, 2015.

[26] Cfr. E. MASIERO, *Essere smart*, in A. BONOMI, R. MASIERO (a cura di), *Dalla smart city alla smart land*, Venezia, 2014, p. 111 s.

[27] Vedi gli artt. 3 ss. del d.lgs. n. 82/2005. Sul punto, cfr. S. D'ANCONA, P. PROVENZANO, *Gli strumenti della cittadinanza digitale*, in R. CAVALLO PERIN, D.U. GALETTA, *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 223 ss.

[28] COSÌ F. FRACCHIA, P. PANTALONE, *Smart city: condividere per innovare (e con il rischio di escludere?)*, cit., p. 8.

Uno dei pochi esempi applicativi in campo nazionale è rappresentato dal progetto "*Smart Ivrea*", lanciato a febbraio 2021. Il progetto, di cui AGID è soggetto capofila, mira a realizzare il primo prototipo di piattaforma nazionale per la gestione delle comunità intelligenti (per cui è stata scelta in sperimentazione la città di Ivrea) e conta sulle competenze del centro di eccellenza sulla ricerca in ambito di Intelligenza Artificiale e *Internet of Things* del Politecnico di Torino e sul raggruppamento TIM - Olivetti - Trust Technologies, oltre che sulle soluzioni tecnologicamente innovative delle due Startup Fleetmatica srl e ToBe srl[29].

Tuttavia, nel contesto odierno, un punto di svolta sembra profilarsi in un orizzonte molto vicino. Il tema delle *smart cities* interseca, infatti, trasversalmente gran parte del PNRR e delle sue Mission, proprio a riprova della grande varietà ontologica e tecnica dei suoi ambiti applicativi, permettendo così intersezioni anche con altre importanti istanze, come, ad esempio, quelle relative alla sostenibilità ed all'ambiente.

Tre sono, infatti, le Mission del PNRR[30] in cui si riscontrano obiettivi riguardanti lo sviluppo delle *smart cities*.

Nella Mission 1, tra i *Servizi digitali e la cittadinanza digitale*, trova spazio una nota dedicata al "*Mobility as a Service*" (MaaS), nuova modalità di trasporto integrato da sperimentare nelle Città Metropolitane. Il proposito dell'innovativo servizio è quello di radicare un sistema di mobilità sostenibile che raccolga differenti modalità di trasporto in un unico canale digitale, facilitando così gli spostamenti nei centri urbani.

La Mission 2, relativa alla *Rivoluzione Verde e Transizione Ecologica*, ha un ampio respiro applicativo che supera i confini della dimensione urbana; tuttavia, in alcuni progetti di attuazione la città diventa il volano del cambiamento.

---

[29] Diversamente, molteplici sono gli esempi in essere negli altri Paesi, sia europei che *extra* UE, quali i progetti che vedono protagoniste le città di Vienna, Monaco di Baviera, Lione, Songdo e Toronto, approfonditamente descritti in O. GASSMANN, J. BOHM, M. PALMIÈ, *Smart Cities: Introducing Digital Innovation to Cities*, Bingley, 2019. L'eterogeneità di esperienze trova conferma nel caso francese, caratterizzato dalla mancanza di una normativa generale in materia, dovuta al rifiuto di un approccio "dirigista", a favore, invece di una normativa settoriale e del vasto intervento di soggetti privati ai quali, notoriamente, è affidata la gestione di molteplici servizi pubblici: si veda, al riguardo, J.B. AUBY, V. DE GREGORIO, *Le smart cities in Francia*, cit.

[30] Per avere una visione complessiva delle misure previste si veda il *report* "*Piano Nazionale di Ripresa e Resilienza*", predisposto dal Governo e consultabile al seguente collegamento web PNRR.pdf (*governo.it*), nonché il Dossier predisposto dal Servizio Studi della Camera dei Deputati e del Senato della Repubblica, "*Il Piano Nazionale di Ripresa e Resilienza*", Documentazione di finanza pubblica n. 28/1, aggiornato al 15 luglio 2021 e consultabile al seguente link BILA – Dossier – 10 (*camera.it*).

Sono diverse, infatti, le soluzioni articolate riconducibili, direttamente o indirettamente, al novero degli interventi abilitanti le *smart cities*[31].

In primis, vengono destinate ingenti risorse all'implementazione di un trasporto pubblico locale più sostenibile, attento alla mobilità ciclistica, al trasporto rapido di massa ed alle infrastrutture di ricarica elettrica.

Vengono enucleati, inoltre, progetti di *smart building* con fondi stanziati per l'efficientamento energetico e la riqualificazione degli edifici pubblici. In scuole, sedi giudiziarie ed unità abitative pubbliche vengono previste tecnologie intelligenti volte alla riduzione dei consumi e ad una concreta svolta *green*.

Esaminando, poi, gli interventi di digitalizzazione delle infrastrutture previsti spicca, inoltre, la *smart grid*, che mira a rafforzare la rete di distribuzione elettrica in chiave digitale e flessibile. Tutte le città possono essere incluse nella rete, abilitando così la transizione dei consumi energetici verso l'elettrico.

Nella sfera applicativa della Mission 2 deve esser considerato, altresì, il tema del monitoraggio del territorio. In tale ambito i progetti urbani *smart* possono essere utilizzati per migliorare la capacità previsionale sul cambiamento climatico, anticipandone e risolvendone così gli effetti sulla vulnerabilità del territorio. Le misure tecnologiche e innovative, così pensate, mirano non solo alla gestione dei rischi, ma anche all'aumento della resilienza dei Comuni, per esempio nell'implementazione e l'efficientamento del sistema idrico.

Da ultimo, va evidenziato che nella Mission 5, tra i 9 miliardi di euro destinati alla *Rigenerazione Urbana*, circa 2,5 miliardi sono dedicati ai Piani Urbani Integrati comprendenti proprio progetti di pianificazione urbanistica partecipata, al fine di trasformare territori vulnerabili in città *smart* e sostenibili.

Gli interventi mirano a creare sinergie di pianificazione tra Città Metropolitane[32] e Comuni limitrofi meno estesi. La sfida è quella di creare un tessuto urbano ed *extra*-urbano maggiormente omogeneo in cui vengano superate le carenze infrastrutturali. Di qui, la condivisione di progetti di *smart land* o *smart city* agevolerebbe l'interoperabilità e il riuso di informazioni, permettendo così un significativo incremento in termini qualitativi della vita dei cittadini.

Se è indubbia la potenzialità di questi interventi, tuttavia studi di settore

---

[31] In merito all'importante ruolo che le *smart cities* possono avere nel raggiungere l'obiettivo della sostenibilità ambientale, si veda il *report* informativo predisposto dalla Commissione Europea, dal titolo *European Missions: 100 Climate-Neutral and Smart Cities by 2030*, pubblicato il 29 ottobre 2021. Sull'esigenza di rendere le città del futuro non solo *smart*, ma anche sostenibili, si veda anche E. FALCONIO, F. CAPRIOLI (a cura di), *Smart city. Sostenibilità, efficienza e governance partecipata. Parola d'ordine per le città del futuro*, Milano, 2015.

[32] Si veda S. ANTONIAZZI, Smart City*: diritto, competenze e obiettivi (realizzabili?) di innovazione*, cit., p. 11 ss., il quale sottolinea l'importanza delle città metropolitane nello sviluppo delle *smart cities*.

denotano come l'intento si debba scontrare, non solo con tempistiche ristrette, ma anche con uno stadio ancora basilare di consapevolezza nell'utilizzo e nell'implementazione di sistemi organizzativi di Intelligenza artificiale così applicati. Per superare questa *impasse* sono, quindi, necessarie scelte strategiche che tengano insieme una considerevole lungimiranza ed un utilizzo efficiente delle risorse a disposizione.

In questo percorso potrà essere rilevante il ruolo rivestito dalle cc.dd. *startup*, quali giovani organizzazioni innovative che possono trovare nelle *smart cities* terreno fertile per lo sviluppo e, allo stesso tempo, in quanto realtà flessibili e ancora in grado di mutare, rappresentare una pietra angolare per le città intelligenti [33].

Altrettanto rilevante, nell'ottica di promuovere i principi di una città *smart*, potrà essere il ruolo rivestito dalla macchina degli appalti pubblici, nello specifico quelli "innovativi", quali strumenti per promuovere, ad esempio, lo sviluppo *green* e tecnologico, condizionando e interferendo con l'oggetto della procedura, seppure in ottica di necessaria flessibilità e semplificazione, ponderandone le relative conseguenze [34].

4. *Profili critici delle* smart cities

Per quanto attiene agli aspetti più marcatamente giuridici della questione, è forse bene svolgere una breve analisi anche per quanto riguarda l'impatto delle *smart cities* sui diritti fondamentali.

Senza voler entrare nel merito di problemi più ampi, come ad esempio le potenziali sfide che l'istituzione di una polizia predittiva e la sua incorporazione nell'architettura urbana possono porre – argomento trattato dalla dott.ssa Tavella – ovvero dei problemi etici e di *accountability* – analizzati nel dettaglio

---

[33] Così D. CUNY, *Les start-up, pierres angulaires des smart cities?*, in *La Tribune*, 6 novembre 2014.

[34] Al riguardo cfr. C. BENETAZZO, *Appalti innovativi e* smart cities*: verso una nuova dimensione pubblico-privata?*, in *Federalismi.it*, n. 9, 2021. Da tenere in considerazione è anche il progetto strategico *Smarter Italy,* previsto dal d.m. 31 gennaio 2019 del Ministero dello Sviluppo Economico e divenuto operativo con la convenzione tra il Ministero stesso e l'Agenzia per l'Italia Digitale, al fine di attuare bandi di domanda pubblica innovativi. Peraltro, con un Protocollo d'intesa, dell'aprile 2020, anche il Ministero dell'Università e Ricerca e il Dipartimento per la Trasformazione Digitale sono entrati a far parte del progetto, inserendo al suo interno il segmento "Borghi del futuro". Questa rappresenta una delle azioni di "Italia 2025" del Ministero per l'Innovazione e la Trasformazione Digitale, volte alla sperimentazione di soluzioni innovative del programma anche su Comuni di minore dimensione (cfr. *https://innovazione.gov.it/progetti/smarter-italy/*).

dalla dott.ssa Carretta nel suo intervento relativo alle soluzioni applicative in Svezia – è forse bene procedere ad una rapida panoramica degli aspetti che presentano le principali criticità, partendo dal sottolineare l'imprescindibile necessità che un cittadino – che accetta di essere sottoposto all'attività di determinati dispositivi tecnologici – sia consapevole, se non addirittura accetti, che ciò determini una *deminutio capitis* per talune libertà.

In primis, bisogna tener presente che la *smart city* può rappresentare un nuovo paradigma di condivisione delle informazioni relative all'individuo, dal momento che vi è un impatto nella gestione e nell'utilizzo dei flussi di dati [35], anche nel livello più prossimo ai cittadini, come ben evidenziato dalla dott.ssa Pagnanelli. Ciò comporta una riflessione sia per quanto riguarda il necessario bilanciamento con la protezione dei dati personali che con le necessità di sicurezza informatica, questioni che si intersecano inevitabilmente con quella visione «*paternalistica delle città intelligenti di migliorare la qualità della vita dei loro residenti e di fornire servizi che consentano loro di vivere in modo sano e sostenibile* [36]».

Anche il Garante per la protezione dei dati personali, in una sua *newsletter* del 6 ottobre 2021 dal titolo *Sì alle smart cities, ma occorre proteggere i dati delle persone* – a commento dello studio *Artificial Intelligence and Urban Development* commissionato dal Parlamento UE – ha evidenziato le criticità emerse sul tema, chiarendo però come l'AI possa divenire forza trainante in questo processo, pur sempre ponendo però attenzione alla tutela dei dati personali, affinché l'Intelligenza artificiale non si tramuti in un eccessivo controllo tecnologico nelle vite quotidiane dei cittadini.

In particolare, per quanto attiene ai profili di maggiore interesse relativi all'impatto sulla *data protection*, si deve sottolineare che il principio di *privacy by design* deve rappresentare, ancor di più nella costruzione delle fondamenta teoriche [37] delle *smart cities*, il principio portante al quale improntare lo sviluppo, l'applicazione e la valorizzazione delle tecnologie utilizzate, costruendo delle reti "a prova di *privacy*" [38].

Il Garante si è già espresso, non a caso, rispetto ai rischi che può compor-

---

[35] Cfr. G. PEDRAZZI*, Big urban data nella smart city. Dai dati degli utenti ai servizi per il cittadino*, in G. FRANCO FERRARI (a cura di), *La prossima città*, Milano, 2018, p. 757 ss.

[36] S. RANCHORDÁS, *Nudging citizens through technology in smart cities*, in *International Review of Law, Computers & Technology*, n. 3, 2020, p. 255; A. CARAGLIU, C. DEL BO, P. NIJKAMP, *Smart Cities in Europe*, in *Journal of Urban Technology*, n. 18, 2011, p. 65 ss.

[37] Sull'importanza strutturale che i dati hanno nell'attuale società digitale, si veda F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019, p. 11.

[38] Così M.V. OTTERLO, *Automated experimentation in Walden 3.0: The next step in profiling, predicting, control and surveillance*, in *Surveillance & Society*, n. 2, 2014, p. 255 ss.

tare l'utilizzo su larga scala, in aree accessibili al pubblico, di telecamere capaci di trattamenti biometrici e, dunque, di riconoscimento facciale. Basti citare, a questo proposito, il parere negativo espresso con riferimento al sistema *Sari Real Time* del Ministero dell'interno [39], nonché alla recente sanzione di 20 milioni di euro comminata a Clearview AI [40], società che offre un servizio attraverso cui è possibile incrociare i dati delle proprie immagini con quelle di un *database* costruito sulla base di banche dati pubblicamente accessibili, come i *social network*, con rischi imponenti per la *privacy*.

Preoccupazioni simili, dunque, emergono con riferimento all'implementazione di dispositivi nell'ambito dell'*Internet of Things* (IoT) nelle città.

Difatti, l'inserimento delle tecnologie utilizzate nel sistema delle *smart cities* nella più ampia rete dell'*Internet of Things* (IoT), così da garantire una interconnessione delle tecnologie ed un efficiente riuso dei dati, presenta potenziali rischi collegati soprattutto alla capacità di raccogliere, elaborare e trasformare grandi quantità di dati, sfruttando anche le sinergie con altre tecnologie, come *big data* e *cloud*, così come puntualizzato anche dal Garante. È stato evidenziato che la tecnica della pseudonimizzazione [41] si presenta come il miglior strumento atto a coniugare, da un lato, le esigenze di monitoraggio e miglioramento dell'erogazione di servizi per il cittadino con, dall'altro, il diritto alla tutela della protezione dei dati, quale strumento che da una parte consente il trattamento dei dati personali e, dall'altra, consente l'identificazione degli interessati solamente da chi sia in possesso delle "chiavi" per ricondurre il dato all'interessato cui si riferisce.

Non si può, peraltro ignorare, il ruolo essenziale che sarà rivestito dalle

---

[39] Provvedimento del Garante per la protezione dei dati personali*, Parere sul sistema Sari Real Time,* pubblicato il 25 marzo 2021, docweb n. 9575877 (reperibile al link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877*). Si veda in proposito V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *Osservatorio sulle fonti,* 2/2021, pp. 796-797.

[40] Si veda il provvedimento sanzionatorio del Garante per la protezione dei dati personali pubblicato il 10 febbraio 2022, *Ordinanza ingiunzione nei confronti di Clearview AI*, doc. web 9751362 (consultabile al seguente collegamento Ordinanza ingiunzione nei confronti di Clearview AI – 10 febbraio 2022 ... – Garante Privacy). Più ampiamente su *Clearview* cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regulative*, Napoli, 2021, pp. 178 ss.; I. NERONI REZENDE, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective,* in *New Journal of European Criminal Law*, 3/2020, p. 375 ss.; K. HILL, G.J.X. DANCE*, Clearview's Facial Recognition App is Identifying Child Victims of Abuse*, in *The New York Times*, 10 febbraio 2020 [*nyti.ms/39Nilef*].

[41] Sull'efficacia delle tecniche di pseudonimizzazione e anonimizzazione si veda S.Y. ESAYAS, *The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach*, in *European Journal of Law and Technology*, n. 6, 2015.

nuove normative di matrice eurounitaria in tema di società *data driven,* quale contesto all'interno del quale necessariamente si collocheranno le *smart cities*. Si pensi al *Data Governance Act* (DGA) – approvato nella sua ultima versione il 15 maggio 2022 dal Consiglio dell'Unione Europea – che si pone, tra gli obiettivi principali, quello di creare uno spazio di condivisione dei dati al quale anche le pubbliche amministrazioni potranno contribuire, fornendo i dati di cui sono titolari al fine di un loro riutilizzo, gratuito o oneroso, da parte di altri soggetti pubblici o privati. In quest'ottica, meritano una apposita menzione le "*Organizzazioni per l'altruismo*", per le quali il DGA prevede una apposita disciplina volta a regolare la possibilità di riutilizzo dei dati a beneficio di quelle organizzazioni che intendano trattarli per fini di interesse generale, quali la ricerca scientifica o il miglioramento dei servizi pubblici. È evidente, dunque, come la possibilità di riutilizzare i dati generati dalle amministrazioni rivestirà un ruolo fondamentale nella costruzione e nello sviluppo delle *smart cities*, le quali saranno da una parte il "luogo" ove quei dati verranno generati (dalle rispettive amministrazioni) e, dall'altro, il "luogo" ove quei dati potranno trovare nuovi impieghi e funzioni.

Con riferimento agli aspetti attinenti alla cybersicurezza [42] – intesa sia come difesa da attacchi esterni, sia come adeguato e protetto funzionamento delle tecnologie impiegate – viene in rilievo la necessità di rafforzare il perimetro di sicurezza, potenziando le misure di sicurezze messe in atto non solo dalle amministrazioni, ma anche dagli operatori di servizi essenziali e dai fornitori di servizi digitali che con esse collaborano. Soltanto così i servizi digitali potranno svolgersi in piena sicurezza e con la garanzia della necessaria continuità, la quale diventa un elemento essenziale, una volta che il sistema della *smart city* sia entrato a regime. Peraltro, il malfunzionamento dei sistemi adottati per le *smart cities* dovuto ad attacchi malevoli non è da confondere con quello che in gergo viene definito "*glitch urban*o", ossia un fenomeno di mancato funzionamento che genera, però, effetti positivi creando nuovi processi, spazi per la sperimentazione e l'innovazione [43].

Da un punto di vista più marcatamente costituzionalistico, non possono es-

---

[42] Per approfondimenti sui profili tecnici relativi alla cybersicurezza ed al trattamento dei dati nell'ambito delle *smart cities* cfr. E. AL NUAIMI, H. AL NEYADI, N. MOHAMED, J. AL-JAROODI, *Applications of big data to smart cities*, in *Journal of Internet Services and Applications*, 6, 2015; A. S. ELMAGHRABY, M.M. LOSAVIO, *Cyber security challenges in smart cities: Safety, security and privacy*, in *Journal of Advanced Research*, n. 4, 2014, p. 491 ss. e G. CHIESA, *Dati, big data e città intelligenti. Riflessioni e caso studio per monitoraggi ambientali*, in *TECHNE. Journal of Technology for Architecture and Environment*, 8, 2014.

[43] Sul punto v. S. ANDREANI, F. BIANCONI, M. FILIPPUCCI, *Smart cities e contratti di paesaggio: l'intelligenza del territorio oltre i sistemi urbani*, cit., p. 904 ss.

sere pretermessi i rischi concernenti le disparità dovute alle differenti opportunità di accesso alla tecnologia e al *digital divide*, fenomeno che deve, viceversa, vincolare il potere pubblico a dare maggiore vigore al principio di uguaglianza sostanziale, intervenendo per rimuovere gli ostacoli di accesso alla tecnologia [44], al fine di prevenire ed evitare le relative conseguenze connesse alla tutela dei dati da parte dell'interessato. Ad esempio, l'impossibilità di accedere alle tecnologie comporta il mancato riconoscimento dello stato di *smart citizen*, con la conseguente mortificazione dei nuovi diritti sociali digitali. Inoltre, preso atto del diritto all'utilizzo della tecnologia, reso concreto in Italia dall'art. 3 del Codice dell'Amministrazione Digitale, al fine di colmare il divario tecnologico tra i cittadini e proiettare nel futuro le amministrazioni, è anche vero che non tutti gli "*smart citizen*" sono, in realtà, in grado di utilizzare adeguatamente la tecnologia, traendone effettivo beneficio [45]. È evidente, quindi, come il *digital divide*, quale fenomeno ancora persistente, potrebbe rivelarsi in maniera ancora più accentuata all'interno delle città intelligenti, fungendo quale limite per il cittadino all'accesso ai servizi forniti dalle amministrazioni, con rischi e ripercussioni ancora maggiori quando oggetto fossero servizi essenziali.

Peraltro, v'è anche da sottolineare che l'eccessiva invasività del controllo tecnologico dei dati personali degli *smart citizens* può dar luogo al fenomeno delle cc.dd. "*black boxes*" legato all'opacità o addirittura alla totale impenetrabilità dei processi automatizzati ed alle implicazioni etiche connesse ai processi decisionali dell'AI [46]. La declinazione pubblicistica di tale pro-

---

[44] Cfr. F. FRACCHIA, P. PANTALONE, *Smart City: condividere per innovare (e con il rischio di escludere?)*, cit., p. 17.

[45] In proposito cfr. A. TROMBADORE, *Approccio integrato e multilevel per una visione condivisa di città*, in A. TROMBADORE (a cura di), *Mediterranean smart cities*, Firenze, 2015, p. 57, il quale ha sottolineato come «*non esistono città intelligenti senza cittadini intelligenti*».

[46] Sul punto si veda, tra i tanti, F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *Federalismi.it*, 16/2020; A. MORETTI, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Diritto dell'informazione e dell'informatica,* 2018. Si segnala anche, tra l'ampia letteratura internazionale sul punto, S. WACHTER, B. MITTELSTAND, C. RUSSELL, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, in *Harvard Journal of Law & Technology*, 2/2018; S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017; G. MALGIERI, G. COMANDÈ, *Why a right to legibility of automated decision-making exists in the General Data Protection Regulation* in *International Data Privacy Law*, 2017; A.D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 2017; ed, infine, L. EDWARDS, M. VEALE, *Slave to the algorithm? Why*

blema, che concerne la spiegabilità, la comprensibilità e conoscibilità, nell'ambito della c.d. trasparenza algoritmica, è peraltro già stato oggetto di alcune decisioni della Giustizia amministrativa, la quale si è appellata al rispetto dei principi della l. n. 241/1990 anche con riferimento a questi nuovi fenomeni [47].

Infine, per concludere questa rassegna – da considerare esemplificativa, più che esaustiva – delle criticità giuridiche connesse alle *smart cities*, va sottolineata la mancanza di regole generali ed omogenee, tali da consentire alle amministrazioni di sviluppare più agevolmente le città del futuro. Del resto, l'Unione Europea ha competenze ridotte in materia e non può, quindi, intervenire direttamente per armonizzare le esperienze in atto nei diversi Stati membri, se non, come avviene, mediante atti di *soft law* o contribuendo a fi-

---

a right to an explanation is probably not the remedy you are looking for, in *16 Duke Law & Technology Review*, 2017.

[47] Cfr. *ex multis* R. CAVALLO PERIN, D.-U. GALETTA, *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020; G. AVANZINI, *Decisioni amministrative e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 4, 2019, p. 1149 ss.; ID., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1/2019; D.U. GALETTA, J.C. CORVALÀN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3/2019; L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Federalismi.it*, 7/2018; M. CAVALLARO, G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16/2019. Per quanto concerne i rapporti tra IA e protezione dei dati personali, cfr. F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit. Inoltre, si tenga anche presente che vi è vasta letteratura concernente tale tema anche a livello internazionale: vedi, al riguardo, C. COGLIANESE, D. LEHR, *Regulating by robot: administrative decision making in the machine-learning era*, in *The Georgetown law journal,* 2017; M. VEALE, I. BRASS, *Administration by Algorithm? Public Management meets Public Sector Machine Learning*, in K. YEUNG, M. LODGE, *Algorithmic Regulation*, Oxford, 2019; J.B. AUBY, *Contrôle de la puissance publique et gouvernance par algorithme*, in D.U. GALETTA, J. ZILLER (hrsg. v.), *Das öffentliche Recht vor den Herausforderungen der Informations- und Kommunikationstechnologien jenseits des Datenschutzes | Information and Communication Technologies Challenging Public Law, Beyond Data Protection | Le droit public au défi des technologies de l'information et de la communication, au-delà de la protection des donnés,* Baden-Baden, 2018; W. FRÖHLICH, I. SPIECKER, *Können Algorithmen diskriminieren?*, in *https://verfassungsblog.de/koennen-algorithmen-diskriminieren/* 2018; H. PAULIAT, *La décision administrative et les algorithmes: une loyauté à consacrer*, in *Revue du droit public*, 2018.; P. TIFINE, *Les algorithmes publics: rapport conclusif*, in *Revue générale du droit* (*https://www.revuegeneraledudroit.eu/blog/2019/03/15/rapport-conclusif/*). Si vedano anche G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, cit., p. 266 e F. LAVIOLA, *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *BioLaw Journal*, 3/2020.

nanziare progetti di studio e sviluppo di *smart cities* con caratteristiche predeterminate e comuni [48]. Tale problematica si riflette e si amplifica ulteriormente all'interno dei singoli Stati membri, ove le competenze in materia sono suddivise, spesso in modo confuso, tra i diversi livelli di governo, statale, regionale e locale, sovente restii a comunicare tra di loro in una prospettiva di efficiente collaborazione.

5. *Considerazioni conclusive*

In conclusione, ci tengo a ricordare come Andrea Simoncini abbia evidenziato la comune radice del termine "*cibernetica*" e della parola "*gubernum*", entrambi derivanti dal greco *kybernetes*, cioè pilota della nave. L'obiettivo tanto delle nuove tecnologie quanto dell'amministrazione è, d'altronde, il medesimo, vale a dire l'orientamento e la gestione della collettività [49].

L'innesto di queste due scienze può condurre ad una nuova dimensione politica, in cui *al* cittadino vengono offerti servizi "su misura" e *dal* cittadino vengono assunte informazioni al fine di rendere sempre più efficaci e particolareggiati tali servizi. Come evidenziato in precedenza, ciò implica dei rischi per i diritti fondamentali dei cittadini, per i loro dati e soprattutto per la loro libertà di scelta.

Il rischio che le derive del "*capitalismo di sorveglianza*" [50] si manifestino anche nel contesto dell'amministrazione comunale può essere molto elevato se il progresso tecnologico e sociale non è accompagnato da un diritto capace di mettere un limite agli eccessi e, soprattutto, di regolare i nuovi poteri. Un diritto che, inoltre, si faccia portatore di politiche di inclusione sociale tecnologica [51].

---

[48] Questo aspetto viene messo in luce dal Comitato economico e sociale europeo nel parere concernente *Le città intelligenti quale volano di sviluppo di una nuova politica industriale europea*, cit. Sull'argomento si veda anche E. CARLONI, M.V. PINEIRO, *Le città intelligenti e l'Europa. Tendenze di fondo e nuove strategie di sviluppo urbano*, in *Istituzioni del Federalismo*, 4, 2015, p. 870 ss.

[49] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 66.

[50] Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* trad. it. P. Bassotti, Roma, 2019.

[51] Il tema è molto ben affrontato in P. FERRONATO, S. RUECKER, *Smart citizenship: designing the interaction between cities and smart cities*, in C. STORNI, K. LEAHY, M. MCMAHON, P. LLOYD, E. BOHEMIA (a cura di), *Design as a catalyst for change – DRS International Conference 2018*, 25-28 June, Limerick, 2018.

Di estrema rilevanza è, altresì, l'inscindibile connessione, in un rapporto di reciproca utilità e dipendenza, tra il tema dello sviluppo delle *smart cities* e quello dello sviluppo sostenibile, così come formalizzato nella Carta di Lipsia del 2007. È evidente, infatti, come la progettazione e costruzione delle nuove città debba dare reali ed efficaci risposte alle esigenze di tutela ambientale[52], ancor di più dopo l'espressa previsione costituzionale, attraverso l'adozione di progetti volti al risparmio energetico, l'economia circolare, il miglioramento dei trasporti[53], la creazione di aree industriali a basso impatto e la minor erosione possibile del suolo pubblico.

La sfida fondamentale nello sviluppo delle *smart cities* è, dunque, il raggiungimento di un equilibrio tra il pieno sfruttamento del potenziale delle innovazioni tecnologiche, tra cui in primo piano si pone l'AI, ed il perseguimento di obiettivi di sviluppo urbano sostenibile, di tutela dei nuovi diritti digitali degli *smart citizens* nel quadro delle garanzie per la libertà e la dignità umana.

Tra questi diritti non si possono, peraltro, ignorare quelli legati a profili solidaristici. Una *smart city* improntata ai principi costituzionali del nostro ordinamento, infatti, non può prescindere dalla garanzia non soltanto dell'efficienza della connessione, per permettere il corretto ed efficace funzionamento delle infrastrutture e dei servizi, ma anche e soprattutto delle necessarie competenze per i cittadini, i quali devono essere messi nelle condizioni di superare gli ostacoli posti dal *digital divide* culturale, al fine di usufruire pienamente dei servizi e delle possibilità offerte della tecnologia; nonché per i dipendenti pubblici, i quali devono essere in grado di lavorare a pieno regime nel contesto amministrativo della *smart city*.

Peraltro, non si può certo dimenticare anche il profilo legato all'inclusività e, di conseguenza, all'accessibilità ai servizi digitali anche da parte dei soggetti disabili. Al riguardo, è molto importante tenere in considerazione il fatto che deve essere garantita la piena fruibilità per questi soggetti, così come previsto già dalla legge 9 gennaio 2004, n. 4, c.d. "legge Stanca", la quale reca «*Dispo-*

---

[52] A tal fine rileva il ruolo che potrà avere il contratto di paesaggio, quale contratto che «deve essere inteso come un accordo fra la cittadinanza e le amministrazioni, per la costruzione di progettualità integrate per lo sviluppo dell'ambito, specificatamente indirizzato verso una *governance* del territorio e delle relazioni sociali capace di attuarsi in una mitigazione e un adattamento ai cambiamenti climatici»: così S. ANDREANI, F. BIANCONI, M. FILIPPUCCI, Smart cities *e contratti di paesaggio: l'intelligenza del territorio oltre i sistemi urbani*, in *Istituzioni del federalismo*, 4, 2015, p. 920 ss.

[53] Si veda, ad esempio, F. LEALI, L. CHIANTORE, *Un ambiente urbano per la sperimentazione di soluzioni innovative per la mobilità: il caso di Modena Automotive Smart Area*, in S. SCAGLIARINI (a cura di), *Smart roads e driverless cars: tra diritto, tecnologie, etica pubblica*, Torino, 2019, p. 3.

sizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici», la quale prevede all'art. 1 che: «*1. La Repubblica riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione e ai relativi servizi, ivi compresi quelli che si articolano attraverso gli strumenti informatici e telematici. 2. È tutelato e garantito, in particolare, il diritto di accesso ai servizi informatici e telematici della pubblica amministrazione, nonché alle strutture ed ai servizi aperti o forniti al pubblico attraverso i nuovi sistemi e le tecnologie di informazione e comunicazione in rete e ai servizi di pubblica utilità da parte delle persone con disabilità, in ottemperanza al principio di uguaglianza ai sensi dell'articolo 3 della Costituzione*».

In conclusione, lo sviluppo tecnologico non può e non deve essere scisso dal progresso sociale ed umano, anche perché esso non può mai rappresentare uno scopo fine a se stesso, ma sempre un mezzo per favorire il pieno sviluppo della persona umana come singolo e nelle formazioni sociali. La solidarietà politica, sociale ed economica non viene, dunque, meno nella *smart city*, ma viene soltanto declinata diversamente, in funzione dei diversi mezzi di cui l'uomo del XXI secolo dispone rispetto a quelli che la tecnica ha messo a disposizione fino all'avvento della rivoluzione digitale.

PARTE I
CORNICE COSTITUZIONALE

IA E *SMART CITIES*: UNA CORNICE COSTITUZIONALE

di *Andrea Simoncini*

SOMMARIO: 1. Diritto costituzionale e intelligenza artificiale: profili generali. – 2. Il progressivo cambio di paradigma nei rapporti tra potere pubblico e poteri privati. – 3. Verso un diritto costituzionale delle *smart cities*?

1. *Diritto costituzionale e intelligenza artificiale: profili generali*

L'utilizzo dell'Intelligenza Artificiale pone oggi un problema di costituzionalità?

Si potrebbe, ritenere che, essendo una forma di strumentazione tecnologica, essa possa porre semmai problemi di "legalità" ovvero di "liceità", nel senso che ci si potrebbe chiedere se tali ritrovati tecnici violino o meno le regole dell'ordinamento giuridico-legislativo. Ma ha senso porre il problema in termini addirittura "costituzionali"?

La realtà è che questo tipo di tecnologia che chiamiamo "intelligenza artificiale" viene utilizzata non tanto per "eseguire" decisioni precedentemente prese dagli esseri umani, ma viene utilizzata per *prendere* quelle decisioni.

Questa tecnologia può sostituire (interamente o parzialmente) la nostra stessa volontà e ciò configura una situazione radicalmente nuova per il diritto. Siamo dinanzi ad una delega (totale o parziale) di funzioni cognitive ritenute proprie degli esseri umani a sistemi tecnici e questo fatto pone domande affatto nuove ai sistemi giuridici.

Prendiamo ad esempio alcuni casi.

Un giudice penale deve decidere che pena applicare ad un imputato.

Un algoritmo di Intelligenza Artificiale, sulla base di dati personali e non, riguardanti l'imputato, propone un *rating* della sua pericolosità sociale (distinguendo in *Low - Medium - High Risk*); il giudice prende la sua decisione sulla base di tale *rating*.

Un direttore di banca deve decidere se concedere una linea di credito ad un cliente.

Un algoritmo di Intelligenza Artificiale fornisce al direttore un profilo del merito di credito del richiedente; i dati sui quali si basa questo profilo sono sia quelli già in possesso dalla banca – se chi chiede il credito è già cliente e ha autorizzato la banca al trattamento dei propri dati per finalità connesse all'esecuzione del contratto – sia le informazioni derivanti dall'utilizzo delle carte di credito, le segnalazioni della centrale rischi; il sistema automatico propone un profilo. Il direttore se intende discostarsi dal profilo automatizzato deve chiedere un'autorizzazione al livello di responsabilità superiore.

Un medico specialista in radiologia deve stilare il referto di una TAC.

Un algoritmo di Intelligenza Artificiale propone al medico una *pre-view* del possibile referto, basata sull'analisi di milioni di referti già effettuati.

Una azienda che fa *riding* (del tipo Uber, Deliveroo, Glovo) deve decidere quali lavoratori iscritti alla piattaforma avranno priorità nell'accesso alle richieste di servizi di trasporto; un algoritmo di Intelligenza Artificiale stila una classifica tra i possibili *riders* assegnando automaticamente i servizi.

Una azienda produce *web engines* (motori di ricerca di informazioni sul *web* del tipo di Google) il che vuol dire che essa deve fornire risposte alle richieste di informazioni, cercandole tra miliardi di fonti di informazioni presenti sulla rete *web* ed ordinarle in una lista; un algoritmo di Intelligenza Artificiale cerca automaticamente le risposte sulla rete e stila la lista di priorità.

Un ente pubblico deve erogare ai soggetti che ne hanno diritto servizi o benefici sociali (indennità di disoccupazione, reddito cittadinanza, riduzione nei costi del *ticket* farmaceutico, sussidi o sovvenzioni); un algoritmo provvede ad esaminare le richieste, a stimare il rischio di frode e ad erogare automaticamente i sussidi.

Un ministero svolge un concorso a cattedra per migliaia di posti e alla fine deve emanare i provvedimenti di assegnazione in servizio combinando i risultati e le graduatorie del concorso, le varie priorità che le leggi attribuiscono ai candidati o alle categorie speciali, il fabbisogno di cattedre esistente nelle diverse direzioni scolastiche regionali e provinciali e le preferenze di assegnazione indicate dai vincitori; per questo decide di affidarsi ad un algoritmo di decisione sviluppato da una società di programmazione per determinare le assegnazioni.

Un ente di area vasta incaricato della gestione delle infrastrutture della mobilità, dell'energia ovvero ambientali – rete idrogeologica, smaltimento rifiuti, qualità aria – deve decidere come organizzare il piano strutturale per la gestione e la regolazione di queste reti; un algoritmo organizza la gestione ot-

timale di queste reti di mobilità o di energia configurando automaticamente soglie e divieti sulla base dei dati di monitoraggio che vengono provvisti.

Come si sarà capito, quelli che abbiamo ipotizzato sono tutt'altro che casi teorici o di scuola. Tutti, in realtà, descrivono fattispecie realmente esistenti e potremmo andare avanti esemplificandone molte altre, tanto è pervasivo l'uso di queste tecnologie che oggi vengono applicate non soltanto nell'ambito della meccanica, della termodinamica o della progettazione industriale, ma sempre più per le decisioni di carattere sociale (giuridiche, amministrative, giudiziarie, regolative).

A ben vedere, questi casi, sebbene tra loro molto differenti, hanno in comune alcuni caratteri che può essere interessante mettere in evidenza.

a) La decisione è *complessa*

In primo luogo, tutte le circostanze in cui si usano questi algoritmi presentano elevati profili di complessità. Esse impongono di tenere in considerazione fattori tra loro diversi che spesso chiedono ciascuno competenze e capacità specialistiche difficilmente reperibili nello stesso soggetto. In secondo luogo, sono decisioni che coinvolgono quantità notevoli di dati da esaminare: precedenti, requisiti, valutazioni.

b) La decisione è *automatizzabile*

In questa travolgente espansione dell'utilizzo di sistemi di Intelligenza Artificiale, non va sottovalutato il ruolo che svolge la condizione di scarsa efficienza dei sistemi di decisione pubblica o privata (si pensi alle persistenti inefficienze del sistema giudiziario, della amministrazione pubblica ovvero del sistema sanitario). In tutti questi casi le soluzioni "automatizzate" sono estremamente attrattive perché abbattono i tempi di decisione e forniscono giustificazioni di natura – apparentemente – tecnico-neutrale per le decisioni, rendendole così più omogenee, prevedibili e tra loro non contraddittorie.

Non vanno poi sottovalutati i regimi di responsabilità civile, penale e amministrativa, cui sono soggetti coloro che debbono prendere queste decisioni (il medico, il direttore di banca, il gestore del sistema infrastrutturale, l'amministratore di società). Gli algoritmi di supporto della decisione possono ovviamente influire nella successiva definizione dei profili di responsabilità e delle conseguenze dannose derivanti dalle decisioni stesse.

c) La decisione incide sulle *libertà costituzionali*

Infine, in molti dei casi che abbiamo preso in considerazione la decisione assistita dall'algoritmo incide su libertà costituzionalmente garantite (si pensi alla decisione del giudice sulla libertà dell'imputato, a quella del medico sul diritto alla salute o a quella dell'algoritmo di Uber o Deliveroo sui diritti di chi

lavora; ma si pensi anche – sebbene sia meno intuitivo – all'impatto che gli algoritmi dei motori di ricerca di informazioni sul *web* possono avere sulla libertà di scelta politica o di voto dell'utente).

Per tutte queste ragioni, in molti casi le decisioni algoritmiche finiscono per chiamare in causa la dimensione costituzionale dell'ordinamento giuridico.

Vorrei qui soffermarmi, in particolare, su un profilo di questa dimensione: il superamento della distinzione tra dimensione giuridica privata e pubblica.

2. *Il progressivo cambio di paradigma nei rapporti tra potere pubblico e poteri privati*

«Nel *Metaverso*, sarai in grado di fare quasi tutto ciò che puoi immaginare: stare insieme ad amici e familiari, lavorare, imparare, giocare, fare acquisti, creare, nonché realizzare esperienze completamente nuove che eccedono quello che pensiamo dei computer o dei telefoni oggi». Così, nell'ottobre 2021 Mark Zuckerberg ha presentato il futuro di Facebook, il social media da lui creato e che ha letteralmente rivoluzionato Internet e le relazioni sociali, diventando, così, una delle aziende più ricche del pianeta [1]. La "terra promessa" proposta dal CEO di Facebook è un non-luogo nel quale non ci sono malattie (i *virus* sono solo informatici), non c'è il duro condizionamento della realtà e soprattutto non c'è la dolorosa fatica di sopportare sé e i propri limiti. Ognuno potrà scegliere il proprio *avatar* e con quello presentarsi a tutti (gli altri *avatar*).

Sembra avverarsi così il più radicale degli ideali marxisti [2] e la profezia del più visionario pensatore del movimento del cosiddetto "Sessantotto", Herbert Marcuse: quella di liberare l'uomo dai lavori faticosi e ripetitivi [3].

---

[1] Nella *Founder's Letter* del 28 ottobre 2021, Zuckerberg ha annunciato che «The next platform will be even more immersive — an embodied internet where you're in the experience, not just looking at it. We call this the metaverse, and it will touch every product we build. […] In the metaverse, you'll be able to do almost anything you can imagine — get together with friends and family, work, learn, play, shop, create — as well as completely new experiences that don't really fit how we think about computers or phones today».

[2] "In tutte le rivoluzioni sinora avvenute non è mai stato toccato il tipo dell'attività, e si è trattato soltanto di un'altra distribuzione di questa attività, di una nuova distribuzione del lavoro ad altre persone, mentre la rivoluzione comunista si rivolge contro il modo dell'attività che si è avuto finora, sopprime il lavoro". Così K. MARX, F. ENGELS, *L'ideologia tedesca*, Roma, 1975, p. 29, ma anche cfr. pp. 56-57, 187.

[3] H. MARCUSE, *One-dimensional man: studies in the ideology of advanced industrial society*, con

Il punto è che non si tratta solo di uno scenario futuribile, più o meno distopico. È solo un passo – l'ultimo in ordine di tempo – di una trasformazione che si è avviata a partire dagli anni '90 e che sembra travolgere irresistibilmente i nostri assetti sociali, economici ed istituzionali.

La diffusione impetuosa e pervasiva delle nuove tecnologie nel settore dell'informazione e delle comunicazioni [4] rende i sistemi tecnologici indispensabili per lo svolgimento delle nostre attività quotidiane. Dalle funzioni più semplici, legate alle preferenze della singola persona, a quelle più complesse, riguardanti la gestione di interessi collettivi, fino al governo di intere popolazioni; un numero sempre maggiore di funzioni – pubbliche e private – è realizzato attraverso strumentazioni di natura tecnica.

In particolare, questo sta accadendo nel settore che può essere considerato la dimensione più recente e promettente dell'evoluzione tecnologica: quello dell'Intelligenza Artificiale, intendendo con questo termine generalmente un sistema algoritmico in grado di generare "contenuti, previsioni, raccomandazioni o decisioni" [5].

Come abbiamo visto all'inizio del paragrafo precedente, l'impiego delle tecniche di Intelligenza Artificiale nel campo delle decisioni è in aumento e altrettanto crescente è il suo influsso nelle scelte adottate dagli esseri umani.

In effetti, questa considerazione, in sé, potrebbe non essere sorprendente: l'evoluzione è nient'altro che il frutto di una costante relazione tra l'umano e la tecnologia [6]. La caratteristica che rende, però, peculiare il tempo che vivia-

---

introduzione di D. Kellner, II ed., Boston, 1991, p. 3 ss. dove afferma: «una confortevole, levigata, ragionevole, democratica non-libertà, prevale nella civiltà industriale avanzata, segno di progresso tecnico. In verità, che cosa potrebbe essere più razionale della soppressione dell'individualità nel corso della meccanizzazione di attività socialmente necessarie ma faticose (…)».

[4] Ovvero tecnologie, di uso generale, riguardanti i sistemi integrati di telecomunicazione, che a partire dagli anni Novanta del secolo scorso hanno posto le basi per la Quarta Rivoluzione industriale. Cfr. K. SCHWAB, P. PYKA, *Die Vierte Industrielle Revolution*, München, 2016.

[5] Cfr. la definizione contenuta all'art. 3, par. 1, n. 1, della Proposta di regolamento sull'Intelligenza Artificiale presentata dalla Commissione Europea il 21 aprile 2021 che recita: «"sistema di intelligenza artificiale" (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o *decisioni* che influenzano gli ambienti con cui interagiscono» (nostro il corsivo).

[6] Cfr. l'intervista a Carlo SINI, *La cosa in sé: una superstizione moderna* in *http://www.inattuale.paolocalabro.info/2012/03/la-cosa-in-se-una-superstizione-moderna.html, ultima consultazione 04/02/2019*); G. BUCCELLATI, *All'origine della politica. La formazione e la crescita dello Stato in Siro-Mesopotamia*, Milano, 2013; A. LEROI-GOURHAN, *Evoluzione e tecniche*, Milano, 1993.

mo, riguarda, da un lato, il *tipo* di cultura tecnica impiegata – quella nata a seguito della cosiddetta rivoluzione *cibernetica*[7] – cultura che implica *intrinsecamente* un riflesso sull'ordine politico[8]; dall'altro, la *trasversalità* di questa strumentazione tecnologica che, producendo anche decisioni – e non solo *mezzi* per eseguire decisioni – può applicarsi a qualsiasi ambito della esistenza umana.

Ad acutizzare questo quadro già estremamente significativo, è intervenuta la pandemia da Covid-19, accelerando ancor più visibilmente questa già evidente forma di dipendenza tecnologica. Recuperando l'efficace espressione del filosofo Hartmut Rosa, la pandemia potrebbe in realtà rivelarsi una delle molte forme di "decelerazione (acceleratoria) funzionale"[9] che hanno costellato la storia della modernità e che in ultima analisi hanno reso possibile il progresso tecnologico[10]. In altre parole, lo *shock* determinato dalla crisi innescata dalla pandemia ha accelerato processi di cambiamento già in corso, rendendo "improvvisamente obsoleto" ciò che già era vecchio e "improvvisamente indispensabile" ciò che era considerato come nuovo.

Oggi moltissime dotazioni tecnologiche rappresentano l'architettura essenziale di servizi di interesse generale. Si pensi, nel corso della pandemia, a quanti diritti costituzionali (salute, istruzione, lavoro) sono stati garantiti *solo* grazie a grandi piattaforme digitali *private* che hanno consentito, ad esempio, il tracciamento dei contatti, la didattica a distanza o il cosiddetto *smart-working*[11]. Ma altrettanto potremmo dire per la gestione delle telecomunica-

---

[7] N. WIENER, *Cybernetics or Control and Communication in the Animal and the Machine*, Cambridge, 1948; cfr. anche V. FROSINI, *Cibernetica: diritto e società*, Milano, 1968; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1/2019, p. 63 ss.

[8] H. MARCUSE, *One-dimensional man: studies in the ideology of advanced industrial society*, con introduzione di D. KELLNER, II ed., Boston, 1991, p. 3 ss. il brano citato sopra prosegue «Che questo ordine tecnologico comporti anche un coordinamento politico ed intellettuale è uno sviluppo che si può rimpiangere, ma che è tuttavia promettente» (nostra la traduzione).

[9] H. ROSA, *Accelerazione e alienazione. Per una teoria critica del tempo nella tarda modernità*, Torino, 2015.

[10] Cfr. C. VISENTIN, *Accelerazione sociale e pandemia: sulla teoria di Hartmut Rosa*, in *Pandora Rivista*, 14 luglio 2020, disponibile al seguente *link*: *https://www.pandorarivista.it/articoli/accelerazione-sociale-e-pandemia-sulla-teoria-di-hartmut-rosa/#_ftnref17*.

[11] Cfr. E. CREMONA, G. DI MEO, G. IANNIELLO, M. PANDOLFI, R. SETOLA, *Infrastrutture digitali strategiche per il paese, tra pubblico e privato*, in A. PAJNO, L. VIOLANTE (a cura di), *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, vol. III, *Pandemia e tecnologie. L'impatto su processi, scuola e medicina*, Bologna, 2021, pp. 76-82.

zioni, dell'energia [12], dei trasporti [13], dei sistemi giudiziari [14], degli apparati militari [15]. E ancor più profonda è la dipendenza tecnologica del sistema economico, sia nella dimensione produttiva (la cosiddetta industria 4.0), che nei servizi (si pensi ai settori bancario, finanziario, assicurativo), tanto da aver suggerito la nota definizione di "capitalismo di sorveglianza" [16].

La sola narrazione di questi fatti può già suggerire una prima chiave di lettura del fenomeno: dimensione pubblica e dimensione privata sono oggi profondamente sfidate nella loro storica distinzione [17]; nella pratica della società digitale queste dimensioni sono costantemente mescolate, soggetti privati assumono volontariamente funzioni tradizionalmente proprie dei pubblici poteri, mentre i soggetti pubblici sono spesso *costretti* a rivolgersi a privati (e non volontariamente li scelgono) per poter continuare ad assolvere le proprie funzioni.

La ragione profonda per cui siamo diventati così vistosamente dipendenti da queste nuove tecnologie sia nel settore pubblico che in quello privato, è complessa e richiederebbe altro approfondimento, ma in questa sede possiamo limitarci a osservare che essa deve essere ricercata in due direzioni: quella della *velocità* e della *convenienza*.

Oggi, grazie a sistemi di calcolo sempre più sofisticati è possibile elaborare quantità mai sperimentate prima di informazioni. Esiste una legge empirica [18]

---

[12] Si veda l'attacco *hacker* sferrato il 7 maggio 2021 alla *Colonial Pipeline*, oleodotto di quasi 9.000 chilometri che trasporta 3 milioni di barili di carburante al giorno da Houston a New York. Vd. *https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html*.

[13] Si pensi all'uso di sistemi di intelligenza artificiale nel settore dei trasporti, nei servizi di volo o nel settore nautico.

[14] Per una valutazione dell'impatto delle nuove tecnologie digitali sul processo si veda E. LONGO, *La giustizia nell'era digitale*, in corso di pubblicazione nel volume degli atti del convegno dell'Associazione Gruppo di Pisa dal titolo *Il diritto costituzionale e le sfide dell'innovazione tecnologica* (Genova 18-19 giugno 2021). Il riferimento è, in particolare al processo telematico introdotto nella giustizia civile e amministrativa, nonché a quello di prossima introduzione nella giustizia penale. Cfr. anche M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, 3, 2018, pp. 872-893.

[15] Cfr. C. CUCCO, D. MAURI, *Omicidi mirati a mezzo drone: brevi riflessioni a margine del caso "Lo Porto" tra diritto penale e diritto internazionale*, in *Diritto penale contemporaneo*, 5/2018, p. 65 ss.

[16] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, *passim*.

[17] Per una ricostruzione in chiave storica sulla distinzione tra diritto pubblico e diritto privato, cfr. B. SORDI, *Diritto pubblico e diritto privato*, Bologna, 2020.

[18] È la cosiddetta *Legge di Moore*. Si veda la Voce nell'Enciclopedia britannica, al seguente link: *https://www.britannica.com/technology/Moores-law.*

secondo la quale ogni diciotto mesi la complessità e le *performances* dei microprocessori raddoppia. Ovviamente questo dato di fatto produce un vantaggio incomparabile in termini di efficienza rispetto alla variabile sinora ritenuta indipendente nelle funzioni umane: quella temporale. Poter compiere la stessa quantità di operazioni in tempi sempre più ridotti è diventato un indicatore certo dell'efficienza di un sistema.

La seconda direzione è quella della *convenienza* pratica. L'automazione dei processi decisionali, da quelli più semplici (come cercare il tragitto più breve per raggiungere una località in auto), a quelli più complessi (prevedere se una persona che ha commesso un reato, lo ricommetterà), solleva gli esseri umani da un'attività estremamente complessa e faticosa: quella di riflettere, valutare e decidere; attività che, in certe situazioni, oltre ad essere impegnativa, può diventare anche rischiosa e potenzialmente, costosa, se nelle decisioni sono coinvolti profili di responsabilità [19].

Di qui l'ulteriore spinta alla diffusione di queste tecnologie tra le attività di natura pubblica e privata. Ovviamente, quando questi sistemi funzionano correttamente, non ne percepiamo l'esistenza; semplicemente, in maniera consapevole o meno, li utilizziamo e ne traiamo vantaggio; ma quando qualcuno di questi apparati tecnologici s'inceppa, mal funziona o, addirittura, viene sabotato [20], allora ci accorgiamo della loro esistenza. È proprio in queste situazioni che ci rendiamo conto del *potere* che questi dispositivi esercitano sulle nostre vite. Così realizziamo le conseguenze che possono derivare dall'avere o meno accesso a questi mezzi [21], ovvero quali effetti negativi possono derivare per la

---

[19] Cfr. C. CASONATO, *AI and Constitutionalism: The Challenges Ahead*, in B. BRAUNSCHWEIG, M. GHALLAB (a cura di), *Reflections on Artificial Intelligence for Humanity*, Cham**,** 2021, pp. 138 ss. Vari inoltre sono sul punto i contributi contenuti in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

[20] Ne è un esempio l'attacco hacker ai server della Regione Lazio, che ha impedito per alcuni giorni la possibilità di prenotare il vaccino contro il Covid-19; cfr. *https://www.regione.lazio.it/notizie/attacco-hacker*. Questa notizia di cronaca è solo una delle più eclatanti dei tempi recenti, a testimonianza di un fenomeno crescente e conosciuto come *cyber-crime*. Il termine è entrato ormai nel lessico comune tanto che l'Enciclopedia Treccani lo ha inserito nel suo dizionario *online* con questa definizione: «*Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo (rispettivamente, si parla di computer as a tool e computer as a target)*». La voce è inserita nel *Lessico del XXI secolo* dell'Enciclopedia. Cfr. *https://www.treccani.it/enciclopedia/cybercrime_%28Lessico-del-XXI-Secolo%29/#:~:text=cybercrime%20s.,e%20computer%20as%20a%20target*).

[21] Sia consentito rinviare a A. SIMONCINI, *L'uso delle tecnologie nella pandemia e le nuove diseguaglianze*, in L. VIOLANTE, A. PAJNO, *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, Bologna, 2021, p. 225 ss.

nostra vita se questi strumenti non funzionano correttamente ovvero se sono usati intenzionalmente in maniera lesiva.

La conclusione è che ci troviamo, dunque, dinanzi ad una nuova forma di potere, intendendo con questo termine la capacità, di natura pubblica o privata, di produrre unilateralmente effetti rilevanti nella sfera giuridica di un soggetto[22]. Effetti che possono essere liberamente voluti o accettati dal soggetto stesso, oppure subìti; possono ampliare la sua sfera di libera autodeterminazione ovvero restringerla[23].

Ad ogni modo, questi poteri tecnologici dalla natura mutevole, tanto pubblica quanto privata, possono contribuire alla realizzazione e all'ampliamento delle libertà fondamentali della persona, ovvero, per la stessa potenza "pratica", possono causare gravi lesioni o restrizioni[24]. È quel carattere "ambiguo" della modernità che Zygmunt Bauman ha da tempo messo in luce[25].

Questa *ambivalenza* si proietta sul mondo del diritto, spingendo verso il superamento della classica distinzione "pubblico" – "privato". Norberto Bobbio, alla voce *pubblico/privato* redatta per l'Enciclopedia Einaudi nel 1981, parlava al proposito di una «grande dicotomia», di una distinzione idonea a «dividere l'universo in due sfere, congiuntamente esaustive […] e reciprocamente esclusive»[26].

---

[22] Sulla distinzione tra le categorie di potere e potestà nel diritto pubblico e nel diritto privato, cfr. A. LENER, *Potere*, in *Enciclopedia del diritto*, XXXIV, 1985, p. 610 ss.

[23] A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI, *Diritti e libertà in internet*, Firenze, 2017, p. 19 ss.; G. DE MINICO, *Towards an Internet Bill of Rights*, in *Loy. L.A. Int'l & Comp. L. Rev*., 37, 1, 2015, p. 27 ss.; ID., *Internet. Regola e anarchia*, Napoli, 2012, p. 191 ss.; F. MODUGNO, *Diritti dei consumatori come diritti di terza generazione?*, in G. COCCO (ed.), *Diritti dell'individuo e diritti del consumatore*, Milano, 2010, p. 53 ss.; S. RODOTÀ, *Tecnologie e diritti,* Bologna, 1995, p. 122 ss.

[24] Ampiamente sul tema, H.-W. MICKLITZ, O. POLLICINO, A. REICHMAN, A. SIMONCINI, G. SARTOR, G. DE GREGORIO, *Constitutional Challenges in the Algorithmic Society*, Cambridge, in corso di pubblicazione.

[25] Z. BAUMAN, *Modernità e ambivalenza*, Bollati Boringhieri, Torino, 2010.

[26] N. BOBBIO, *Pubblico/privato*, in *Enciclopedia*, vol. XIII, Torino, 1981, ora in ID., *Stato, governo, società. Per una teoria generale della politica*, Torino, 1985, p. 3, cit. in B. SORDI, *Verso la grande dicotomia: il percorso italiano*, in G.A. BENACCHIO, M. GRAZIADEI, *Il declino della distinzione tra diritto pubblico e diritto privato, atti del IV Congresso nazionale SIRD, Trento, 24-26 settembre 2015*, Napoli 2016, p. 3. Procedendo *à rebours*, Federico Carlo di Savigny, passando in rassegna "l'intero diritto" afferma, nel suo Sistema del diritto romano attuale, che si distinguono in esso due rami: lo *Staatsrecht* e il *Privatrecht*. Il primo "ha per oggetto lo Stato", il secondo «l'insieme dei rapporti giuridici, in cui ciascun individuo esplica la propria sua vita»; Immanuel Kant, allo stesso modo, dimidia i suoi Principi metafisici della dottrina del diritto tra diritto privato, che disciplina il possesso, l'acquisto e il contratto, e il diritto pubblico, che comprende il diritto dello Stato, il diritto dei popoli e il diritto cosmopolitico. E così via, «senza so-

Oggi, dinanzi a queste nuove piattaforme tecnologiche capaci di condizionare in maniera così radicale le relazioni sociali, la scenografia disegnata da Bobbio negli anni '80 va ripensata. Non c'è più la stessa certezza né sui soggetti, né sulle attività. L'ordinamento pare ormai orientato verso una nozione «funzionale e cangiante»[27] di "pubblico", predominante nel dibattito dottrinale e giurisprudenziale, secondo la quale il criterio da utilizzare per tracciarne il perimetro non è sempre uguale a sé stesso, ma muta a seconda dell'istituto o del regime normativo che deve essere applicato e della *ratio* ad esso sottesa.

In questo contesto "liquido", nel quale soggetti privati soggiacciono a regimi di diritto pubblico e soggetti pubblici seguono le norme di diritto comune, si innesta il problema tecnologico: sia sotto il profilo della *funzione assolta* (privata o pubblica?), sia sotto il profilo della *regolazione* (privata o pubblica?).

Un potere tecnologico come quello che si esprime attraverso l'intelligenza artificiale chiama direttamente in causa, come visto all'inizio di questo contributo, il diritto pubblico e costituzionale. Il costituzionalismo, infatti, quantomeno nella sua versione moderna[28], nasce proprio con lo scopo di porre un limite giuridico ai poteri (dapprima quelli privati[29] e poi anche quelli pubblici[30]) al fine di proteggere in maniera effettiva i diritti e le libertà fondamentali della persona.

Il diritto pubblico – e quello costituzionale in particolare – ha da sempre trovato nella *normazione* lo strumento principale per fissare tali limiti, ovverosia, per creare un ordine legale al quale ricondurre i rapporti di natura giuridica che si vengono a creare all'interno di un determinato contesto sociale.

---

stanziali mutamenti» (ancora Bobbio), si giunge fino ad Ulpiano, secondo il quale «Huius studii duae sunt positiones, publicum et privatum. Publicum ius est quod ad statum rei Romanae spectat, privatum quod ad singulorum utilitatem pertinet», Dig. I, 1,1,2. Inst., I, 1, 4. E ancora una lunga, completa rassegna del rapporto tra diritto pubblico e diritto privato in B. SORDI, *Diritto pubblico e diritto privato*, cit., 2020.

[27] Così Cons. Stato, sez. VI, 26 maggio 2015, n. 2660, che ha dato corso ad un seguitissimo filone giurisprudenziale, tutt'oggi largamente prevalente.

[28] Sul tema si veda il classico B. CONSTANT, *La libertà degli antichi paragonata a quella dei moderni*, trad. it. e cura di L. ARNAUDO, Macerata, 2001.

[29] Il cosiddetto primo costituzionalismo nasce per limitare i poteri del re. Si prenda per tutti ad esempio l'art. 16 della *Dichiarazione dei diritti dell'uomo e del cittadino* del 1789: «Ogni società in cui la garanzia dei diritti non è assicurata, né la separazione dei poteri stabilita, non ha una costituzione». Cfr. M. FIORAVANTI, *Costituzionalismo: percorsi della storia e tendenze attuali*, Roma-Bari, 2009.

[30] Il cosiddetto secondo costituzionalismo, quello novecentesco, nasce invece per limitare il potere dello Stato. Cfr. per tutti P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984.

Per tale ragione, dinanzi all'"erompere" di questi nuovi poteri[31] oggi si ripropone una grande questione di natura costituzionale: *quali* fonti normative utilizzare e *che tipo* di regolazione può efficacemente delimitare l'esercizio del potere tecnologico, in particolare quando esso coinvolge le libertà o i diritti delle persone?

La risposta a queste domande richiede un approccio di diritto costituzionale – altrove è stato definito un *mindset*[32] – "ibrido", capace cioè di utilizzare diverse forme di propulsione, così come un linguaggio ed un metodo di analisi comprensibili sia dal regolatore che dal regolato.

Tutte le dimensioni fondamentali del paradigma pubblicistico, infatti, sono coinvolte.

Per un verso, il modo con il quale il potere tecnologico interferisce con la libertà attiene alla dimensione della "*forma di Stato*", intesa come la risoluzione che un dato ordinamento costituzionale dà alla tensione tra autorità e libertà[33]. Come abbiamo ricordato, queste nuovi sistemi tecnici, producono compressioni delle libertà fondamentali di natura del tutto nuova: si sta consolidando una forma di *dipendenza informativa* dalla tecnologia sempre più rilevante, by-passando, sempre più spesso, quelle agenzie educative che da sempre hanno avuto lo scopo consentire alle persone a sviluppare un proprio senso critico responsabile nell'uso delle informazioni.

Allo stesso tempo, aumenta l'uso di sistemi di intelligenza artificiale in grado di sostituire gli esseri umani nelle loro decisioni; dunque, o perché forniscono le informazioni necessarie per decidere, o perché del tutto sostituiscono le decisioni del soggetto, queste nuove tecnologie finiscono per comprimere la libertà umana, per così dire, *dall'interno* della volontà.

A tale scenario in trasformazione, va poi aggiunta una ulteriore considerazione che riguarda la dimensione economica dei soggetti che oggi producono e commerciano questi prodotti o servizi tecnologici capaci di interferire con le nostre libertà.

Stiamo parlando dei principali *players* economico-finanziari del nostro pianeta, in grado di aggregare capitali e risorse economiche di gran lunga superiori a quelle di molti Stati del mondo. Circostanza, questa, che deve indurre

---

[31] Cfr. E. CREMONA, *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in *Osservatorio sulle fonti*, 2/2021, numero speciale su *Autorità amministrative indipendenti e regolazione delle decisioni algoritmiche*, pp. 879-907.

[32] A. SIMONCINI, *Il costituzionalismo come "forma mentis". Un'ipotesi di ricerca*, in *Scritti in onore di Gaetano Silvestri*, Torino, p. 2260 ss.

[33] Per tutti, P. CARETTI, U. DE SIERVO, *Diritto costituzionale e pubblico*, Torino, 2020, p. 19 ss.

una ulteriore attenta ulteriore riflessione sulla natura (ancora?) solo privata di queste società [34].

Per altro verso, porsi la domanda sulle forme di limitazione normativa di questi poteri privati, aggiunge alla dimensione della forma di Stato sopra citata, anche quella della "*forma di Governo*", intesa come la distribuzione fondamentale dei poteri all'interno di un dato assetto costituzionale.

È evidente che, in sistemi costituzionali a forma di governo "parlamentare" quali il nostro, il compito della normazione deve spettare innanzitutto, ed in prima battuta almeno, agli organi il cui potere deriva direttamente dal popolo. Ma, anche in questo caso, come nella dimensione della forma di Stato, le caratteristiche proprie del potere tecnologico sono tali da mettere in crisi questa tradizionale attribuzione.

La normazione primaria "classica" – quella che si realizza attraverso la legge parlamentare, a cui si affiancano in vario modo i poteri legislativi del governo – oggi risulta essere inadeguata ed insufficiente a creare un ordine giuridico-normativo effettivamente espressivo dei principi costituzionali.

Non è un caso che proprio nell'area tecnologica stiamo vedendo fiorire negli ultimi decenni strumenti regolativi di nuova generazione, quali, ad esempio, la cosiddetta *soft-law* ovvero l'adozione di codici etici o di strumenti normativi quali, le linee guida o le c.d. *best-practices*: fonti sicuramente di struttura ed efficacia diversa rispetto alle fonti primarie tipiche dello strumentario costituzionale. Tutto questo richiede, per chi deve scrivere questo tipo di norme, un tasso di conoscenze tecniche ovvero il possesso di una quantità di informazioni che i classici procedimenti di regolazione centrati sull'organo rappresentativo della sovranità popolare, normalmente non hanno.

3. *Verso un diritto costituzionale delle* smart cities?

Nel contesto della *smart city* tutti i temi appena delineati assumono concretezza e si intersecano vicendevolmente. I servizi offerti ai cittadini in forma "*smart*" sono infatti nella maggior parte dei casi forniti da società private che attraverso diversi assetti giuridici offrono beni e servizi alla Pubblica Amministrazione [35].

Vi sono diverse amministrazioni locali nelle quali il paradigma "*smart city*"

---

[34] M. SCOTT, *Coronavirus crisis shows Big Tech for what it is – a 21st century public utility*, in *www.politico.eu*, 25 marzo 2020; W. LIU, *Coronavirus has made Amazon a public utility so we should treat it like one*, in *The Guardian*, 17 aprile 2020.

[35] E. MOROZOV, F. BRIA, *Ripensare la Smart city*, Torino, 2018.

viene declinato in forme più o meno intense e più o meno complesse [36]. Anche per questa ragione, più che ad un singolo modello da realizzare ci si potrebbe riferire correttamente ad un percorso [37] verso una sempre più efficace applicazione delle nuove tecnologie nei contesti urbani, al fine di migliorare la qualità della vita dei cittadini e delle persone fisiche che per svariate ragioni popolano quelle aree. Questo avverrà attraverso l'elaborazione di politiche *data-driven* e la fornitura di servizi ottimizzati grazie alla analisi e all'utilizzo dei *big data* [38].

Ciò che preme rilevare in conclusione di questa disamina introduttiva degli aspetti costituzionali della Città intelligente riguarda dunque il fatto che una *smart city* completamente realizzata non esista: essa è piuttosto un modello a cui ispirarsi ed aspirare. Un modello che in quanto tale può spingersi anche oltre i limiti che la realtà di un singolo ordinamento giuridico, in un determinato momento storico, possa consentire.

È perciò dirimente che lo sviluppo di una *smart city* sia saldamente ancorato al sistema di principi e di valori costituzionali nei quali la comunità si identifica.

Vi sono alcuni aspetti che pare opportuno porre in evidenza. Il primo attiene alla necessità, per evitare che l'utilizzo non meditato dei sistemi di Intelligenza artificiale sia estremizzato sino a porre in dubbio la garanzia dei diritti e delle libertà costituzionali, che venga sempre posto in essere un bilanciamento tra fattore umano e fattore tecnologico. L'Intelligenza artificiale, dunque, non può essere scissa dall'elemento umano non solo in termini di supervisione o di controllo umano sulla decisione [39], ma in termini di un più ampio equilibrio, nel contesto urbano, della componente naturale e di quella artificiale.

Secondariamente mi pare importante porre in evidenza la necessità che tut-

---

[36] E. FERRERO, *Le smart city nell'ordinamento giuridico*, in *Il foro amministrativo*, 4/2015, p. 1267 ss.

[37] Una "*smart transition*", cfr. lo studio *Social approach to the transition to smart cities*, European Parliamentary Research Service, Panel for Future of Science and Technology, February 2023.

[38] S. RANCHORDAS, A. KLOP, *Data-Driven Regulation and Governance in smart cities*, in *University of Groningen Faculty of Law Research Paper Series*, 7/2018, p. 2.

[39] Ci si riferisce qui all'art. 22 del GDPR, che prevede il diritto, per il destinatario di una decisione algoritmica, di ottenere l'intervento umano da parte del titolare del trattamento, e all'art. 14 della proposta di *Artificial Intelligence Act*, norma che prevede la sorveglianza umana sull'utilizzo di sistemi di Intelligenza artificiale ad alto rischio, al fine di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali. Si vedano A. SIMONCINI, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 26 ss.; A. SIMONCINI, *Quale modello per la regolazione dell'Intelligenza artificiale? L'Europa al bivio*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto dottorale di Alta Formazione in Scienze Giuridiche, Ca' Foscari Venezia 25-26 novembre 2021*, Milano, 2022, pp. 256-258.

ti i processi tecnologici, che comportano il trattamento di dati e che attengono alla fornitura di servizi alla collettività siano tutelati da una solida protezione dal punto di vista della sicurezza cibernetica [40]. Non solo gli attacchi *hacker*, ma anche interruzioni dei servizi a causa di consistenti guasti alle reti potrebbero infatti causare danni di gravità inestimabile.

Per porre la giusta attenzione su tutti gli aspetti citati appare di prioritaria importanza il ruolo di Autorità indipendenti ed Agenzie coinvolte per competenza [41]. Infatti la velocità con cui i cambiamenti tecnologici si impongono nella quotidianità richiede di poter far riferimento ad organi dedicati, che svolgano funzioni di sorveglianza, regolazione, informazione.

Da ultimo, appare quanto mai opportuno, ragionando di progressiva costruzione della *smart city*, ovvero di una città umana e tecnologica, incorporare in questa costruzione i principi costituzionali [42]. Mutuando il principio sancito dal GDPR della *privacy by design*, potremmo dire che la progettazione della città intelligente dovrebbe fin dalle prime fasi tener conto degli aspetti tecnologici, della sicurezza cibernetica, del giusto equilibrio tra uomo e macchina, ma prima di ogni altra cosa la *smart city* dovrebbe esser pensata come città dei valori etici e dei diritti, in cui la tutela delle libertà costituzionali possa esser garantita anche nei nuovi contesti e nei nuovi assetti che l'utilizzo della tecnologia, ed in particolare dell'Intelligenza artificiale nei contesti urbani sta delineando. Sarà così possibile per il diritto contribuire a promuovere il pieno sviluppo del potenziale dell'IA, evitando al contempo abusi ed utilizzazioni contrarie ai diritti delle persone [43].

---

[40] Si pensi ai servizi essenziali che rientrano nel Perimetro nazionale di sicurezza cibernetica, cfr. d.l. 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e d.P.C.M. 30 luglio 2020, n. 131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica.

[41] Mi riferisco in prima battuta alla Agenzia per la Cybersicurezza Nazionale, istituita con d.l. 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109 e al Garante per la protezione dei dati personali. Sulla base dell'art. 7 par. 5 del d.l. n. 82/2021 Agenzia ed Autorità garante hanno di recente stipulato un protocollo di intesa al fine di agevolare l'intervento coordinato su questi temi.

[42] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1/2019, p. 87.

[43] Così C. CASONATO, *Potenzialità e sfide dell'Intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 1/2019, p. 179.

INTELLIGENZA URBANA E TUTELA DEI DIRITTI FONDAMENTALI. ANTINOMIA O COMPLEMENTARITÀ NELLA NUOVA STAGIONE ALGORITMICA?

di *Federica Paolucci* e *Oreste Pollicino* [*]

1. *Introduzione*

Le città sono sempre più popolate tanto da esseri umani [1], quanto da strumenti tecnologici. Dati, intelligenza artificiale e sensori stanno componendo un'inedita dimensione della *urbs* in cui i modelli tradizionali della città (e del vivere umano) sono chiamati a coesistere con la rete. Questa nuova sfera dello spazio urbano prende il nome di *smart city*: un termine ad ombrello con il quale si suole intendere la nuova integrazione tra spazio digitale e spazio reale. Al di là di ogni distopico scenario che tale contesto è in grado di generare e far immaginare, l'analisi di questo fenomeno deve sull'*humus* che sta consentendo l'intersecazione tra spazio urbano e rete: i dati. Difatti, gli incessanti flussi di

[*] Ancorché il presente scritto costituisca il frutto della riflessione dei due autori, sono da attribuirsi a Federica Paolucci i paragrafi 1, 3 e 3.1; a Oreste Pollicino i paragrafi 2 e 2.1. Il paragrafo 4 è ascrivibile congiuntamente a entrambi gli autori.

[1] Come evidenziano numerosi studi, tra il 2000 e il 2015, le città sono cresciute dell'1,5% all'anno in termini di superficie. La crescita della superficie coperta dalle città è stata maggiore nei Paesi a basso reddito (2,6%), che in quelli a reddito medio (2,6%), rispetto ai Paesi a medio reddito (1,9% nei Paesi medio-bassi e 1,5% nei Paesi medio-alti) o ai Paesi ad alto reddito (1%) (EC OECD, 2020). Si faccia riferimento al *Population data booklet* elaborato dallo UN Department of Economic and Social Affairs, UN Habitat.

informazione che dalla Siberia alla Terra del fuoco consentono al mondo contemporaneo di funzionare in ogni sua forma[2] sono il cuore della città del futuro, sicché il suo funzionamento si radica nella combinazione di *Internet of Things* (IoT)[3], *big data*[4], *ubiquitous computing*[5] e *cloud*[6]. Tutti questi elementi sono le vere e proprie architetture su cui poggia la città (ideale) intelligente, ed hanno il compito di rendere la macchina urbana ottimizzabile e, soprattutto, controllabile. Osservando singolarmente ogni componente della *smart city* si può notare come il comun denominatore non sono solo i dati, ma anche i rischi alla tutela dei diritti fondamentali degli individui[7]. Difatti, è nelle vulnerabilità di queste singole architetture che si sostanziano le questioni aperte sulla regolazione della *smart city*. In altre parole, si ritiene che il punto d'indagine non debba condannare la tecnologia per avere modificato gli spazi urbani e aver esposto i cittadini a ulteriori rischi. Questi ultimi sono ben radicati nelle singole tecnologie, tutt'oggi in commercio, rintracciabili nelle case e negli uffici di molti, che consentono a ben vedere il funzionamento della città intelligente. D'altro canto, gli elementi virtuali non sostituiscono e non sostituiranno

---

[2] Il ruolo che il contesto digitale ha assunto negli ultimi anni è quanto mai evidente alla luce del cruciale supporto che l'intera rete è stata in grado di fornire nei momenti più bui della pandemia da Covid-19.

[3] Si veda, *ex multis*, L. ATZORI, A. IERA, G. MORABITO, *Understanding the Internet of Things: Definition, Potentials, and Societal Role of a Fast-Evolving Paradigm*, in *Ad Hoc Networks*, vol. 56, 2017, pp. 122-140.

[4] Come noto, i *big data* sono identificabili attraverso le c.d. "tre v": volume, varietà, velocità. L'analisi dei *big data* consiste nell'elaborazione automatizzata in cui grandi insiemi di dati vengono analizzati da algoritmi in modi nuovi e imprevisti per trovare modelli e correlazioni tra gli insiemi di dati, producendo così nuove conoscenze e informazioni su individui, gruppi o società in generale e informazioni su individui, gruppi o sulla società in generale. Si veda in part. R. KITCHIN, G. MCARDLE, *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets*, in *Big Data & Society*, vol. 3.1, 2016.

[5] Concetto utilizzato dalla letteratura per indicare la capacità assertiva e osservativa degli oggetti interconnessi con e nella vita degli individui. Tale struttura può essere identificata con il nome di «*everyware*», come descritto *ante litteram* in W.J. MITCHELL, *E-Topia: «Urban Life, Jim—But Not As We Know It»*, Cambridge, MA, 1999.

[6] Definito dal National Institute of Standards and Technology (NIST) in *Final Version of NIST Cloud Computing Definition Published*, 25 ottobre 2021 «*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*».

[7] A tal riguardo, si rimanda anche alla puntuale analisi di Lilian Edwards, che muove, appunto, da una considerazione dei singoli rischi associati agli IoTs e al *cloud* per profilare gli aspetti di maggiore criticità per la *privacy* degli individui. L. EDWARDS, *Privacy, Security and Data Protection in smart cities,* in *European Data Protection Law Review,* vol. 2, n. 1, 2016, pp. 28-58.

l'esperienza fisica. «*I flussi non sostituiscono gli spazi e i bit non rimpiazzano gli atomi*»[8], proprio perché si sta assistendo alla creazione di uno spazio ibrido, a cavallo tra digitale e reale. Difatti, in questo "non luogo" dove tecnologia e spazi fisici si incontrano, i cittadini vengono posti al centro di una vera e propria rivoluzione in cui si interfacciano non solo con la dimensione prettamente atomica, ma anche con gli elementi digitali che a mano a mano popolano la città del futuro. Orbene, il processo evolutivo della *smart city* non riguarda solamente l'urbanizzazione, ma tocca nel profondo il cittadino, il quale, già fortemente contaminato dalle moderne tecnologie digitali, si trova a vivere il contesto urbano in modo differente[9].

Alla luce di quanto premesso, è evidente che la corsa alla digitalizzazione dello spazio urbano stia coinvolgendo ogni settore, pubblico e privato, portando alla luce una serie di riflessioni che concernono sicuramente il mercato, ma anche il nuovo assetto di poteri. In questo contesto, è richiesto al costituzionalista di interrogarsi su talune tematiche che discendono dall'interazione con questo nuovo spazio, dove digitale e reale sono posti su piani quanto meno paralleli. Difatti, è innegabile che la città, così come ogni altro aspetto legato alla quotidianità degli individui, abbia subito una forte influenza derivata e causata dalla digitalizzazione grazie alla costituzione di un sistema in cui gli algoritmi sono utilizzati per raccogliere, collezionare e organizzare i dati dei cittadini al fine di prendere ogni tipologia di decisione[10]. Le problematiche legate alla realizzazione, nonché alla regolazione, della città intelligente non fanno altro che amplificarne delle altre che guardano in senso ancor più ampio alla traduzione nello spazio digitale delle garanzie tradizionalmente godute dagli individui nel mondo reale.

Dunque, si profila una problematica di bilanciamento tra due perni, la protezione dei diritti e gli interessi di investimento, tra protezione della riservatezza e incoraggiamento alla circolazione dei dati. In questo dualismo, che a ben vedere ha sempre caratterizzato il sistema normativo comunitario della protezione dei dati personali[11], si inseriscono anche le ultime proposte norma-

---

[8] C. RATTI, *La città di domani. Come le reti stanno cambiando il futuro urbano,* Torino, 2017, spec. 17.

[9] Si veda nel merito S. RANCHORDÁS, *Nudging citizens through technology in smart cities*, in *International Review of Law, Computers & Technolo*gy, vol. 34, n. 3, 2020, pp. 254-276.

[10] J. DANAHER, *The Threat of Algocracy: Reality, Resistance and Accommodation,* in *Philosophy & Technology*, vol. 29, n. 3, 2016, pp. 245-268.

[11] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Si veda, in particolare, il Considerando 7.

tive del legislatore europeo che, anche attraverso il *Digital markets act* [12], e il *Data Act* [13] sta muovendo da un sistema tutto incentrato sul controllo e sull'*accountability*, a uno più aperto, che possa favorire e incrementare la circolazione dei dati. In questo nuovo sistema, che sarà la necessaria benzina per permettere alle città intelligenti di ulteriormente svilupparsi, come si evidenzierà nella seconda parte di questo contributo, si stanno impiantando una serie di diritti e obblighi che erano già state inserite nel Regolamento 2016/679 [14], come la portabilità, e che, sulla base di determinati presupposti, riguarderanno sia i dati personali sia quelli non personali. Il loro *flow* è immenso e sostanzia la principale infrastruttura della città *smart.* Inoltre, come si premetteva, da questo quadro emergono delle chiare problematiche di sicurezza dei dati raccolti e di garanzia di protezione da interferenze esterne. Pertanto, la profilazione dei cittadini, la protezione della loro riservatezza, la creazione di un sistema di *governance* attuale che sia consapevole dei rischi ma anche delle opportunità, sembrano le principali sfide che si ritiene necessario affrontare per salire consapevolmente sul treno dell'innovazione. Muovendo da un'analisi delle sfide poste alla riservatezza degli individui, si cercheranno elementi di complementarità tra la città di domani e la città di oggi nell'ottica di delineare varchi in cui possano essere garantiti ed evoluti i diritti fondamentali di ciascuno anche nella città progredita dalla tecnologia e dalla diffusione delle reti.

2. *Quale riservatezza nella città intelligente: spunti di riflessione*

Da un punto di vista prettamente definitorio, la città intelligente indica una serie di 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, alimentando una crescita economica sostenibile, attraverso una sapiente gestione delle risorse naturali e

[12] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[13] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Brussels, 23.2.2022 COM(2022) 68 final.

[14] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). Qui di seguito GDPR.

ricorrendo ad una *governance* partecipativa[15]. È indubbio il fatto che l'innovazione e la tecnologia rappresentano degli importantissimi alleati nella lotta al cambiamento climatico[16], nell'ottimizzazione degli spazi urbani, nello sviluppo ed utilizzo sostenibile di tutte le fonti di energia, nonché nella garanzia di maggiore sicurezza. Ebbene, si ritiene che ciò debba imprescindibilmente passare attraverso un ripensamento dell'assetto rubano, della mobilità dei cittadini[17] e delle infrastrutture ICT. Detto passaggio può avvenire mettendo in relazione le infrastrutture materiali con il capitale umano, intellettuale e sociale, facendo sì che quest'ultimo assuma un ruolo centrale nel modello di pianificazione urbana intelligente. Infatti, almeno astrattamente, le *smart city* sono città in cui uno strato tecnologico viene sovrapposto all'intelaiatura urbana esistente, consentendo ai suoi cittadini e utenti di connettersi alla rete, interagire tra loro e con altri attori, quali la pubblica amministrazione, fornitori di beni e servizi e soggetti privati. Nello specifico, il fine delle città intelligente è quello di condurre ad un generale innalzamento della qualità dei servizi offerti al cittadino, quali il trasporto (pubblico e non), la distribuzione energetica, la cura della persona, la salute, il monitoraggio dell'ambiente, la risposta alle emergenze e le attività sociali e, più in generale, per le imprese coinvolte, la realizzazione di nuovi modelli di *business* sempre più efficaci e mirati sulla figura del cittadino-utente-cliente. In sostanza, le fasi del processo di raccolta dei *big urban data* dovrebbero creare meccanismi di sviluppo virtuosi sia in relazione ai servizi che alla riprogettazione della città del futuro[18].

Come si premetteva, lo spazio urbano *smart* è considerato un punto di incontro tra mondo virtuale e mondo materiale, tra digitale e analogico, all'interno del quale interagiscono sia soggetti biologici che artificiali[19]. Nonostan-

---

[15] F. TONI, *Smart city: innovazione e sostenibilità*, in *EAI Energia, Ambiente, Innovazione*, vol. 5, 2013, pp. 35-40.

[16] A tal riguardo, si rimanda ai *17 UN Sustainable Goals*, ossia una serie di iniziative che l'Organizzazione delle Nazioni Unite intende intraprendere per provocare un cambiamento entro il 2030, nella prospettiva di realizzare un futuro migliore per gli individui. Peraltro, numerose organizzazioni tra cui la AI For Good hanno evidenziato come ciascun obiettivo può essere effettivamente realizzato e accelerato grazie all'impiego di tecnologie automatizzate e AI, nel particolare. Si veda *https://ai4good.org/ai-for-sdgs/,* consultato in data 25 marzo 2022.

[17] Nelle parole di Musa, «*the goal of building a smart city is to improve the quality of life by using technology, to improve the efficiency of services and meet residents' needs.* [...] *The purpose of building smart cities is to make the lives of the residents easier and safe»,* S. MUSA, *Smart Cities – A Roadmap for Development*, in *J. Telecommun. Syst. Manage,* vol. 5, n. 3, 2016.

[18] G. PEDRAZZI, *Big Urban Data nella smart city*, in G.F. FERRARI (a cura di), *La prossima città*, Milano, 2017, spec. pp. 557-576.

[19] A tal riguardo, si rimanda a L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta tra-*

te, dunque, le menzionate opportunità, occorre chiedersi se un tale assetto sia in grado di essere non solo funzionale, ma anche tutelante dei diritti fondamentali dei cittadini, permettendo loro di vivere e partecipare liberamente alla vita cittadina [20].

Difatti, è possibile notare che l'opera di espansione dei diritti nel digitale [21] raggiunge la sua pienezza nel contesto della città intelligente. Come è già stato possibile osservare in riferimento ad altri spazi virtuali, quali, ad esempio, i *social network*, questi ultimi hanno acquisito un ruolo eminentemente pubblico, assimilabile a quello che le piazze esercitavano nella dimensione atomica [22]. Ed è, peraltro, attraverso di essi che si realizzano i diritti democratici dei cittadini, come nel caso del diritto di riunione o di assemblea. Nella *smart city*, al contrario, ogni aspetto tende invece a essere governato "digitalmente" da soggetti privati o da tecnologie sviluppate da quest'ultimi, facendo di quegli spazi essenzialmente pubblici, degli «*pseudo private places*» [23]. In questo inedito contesto, dunque, i diritti che per loro natura rappresentano la massima garanzia statale, – e, precipuamente, il diritto all'informazione; il diritto di libertà di

---

sformando il mondo, Milano, 2012*,* in part. a p. 106, chiarisce che «*stiamo lentamente accettando l'idea per cui non siamo agenti newtoniani isolati e unici, ma organismi informazionali, inforg, reciprocamente connessi e parte di un ambiente informazionale (infosfera), che condividiamo con altri agenti informazionali*».

[20] A tal proposito, si veda l'analisi di P. CARDULLO, C. DI FELICIANTONIO, R. KITCHIN (a cura di), *The right to the smart city*, Bingley (UK), 2019, spec. p. 27.

[21] A tal riguardo, si rimanda all'annoso dibattito guidato da F.H. EASTERBROOK, *Cyberspace and the Law of the Horse,* in *University of Chicago Legal Forum,* vol. 207, 1996. Peraltro, detto dibattito è alimentato da amplissima e anche recente letteratura, circa la necessità di creare, ovvero, d'altro canto, adattare la compiutezza dei diritti tradizionalmente garantiti alle nuove sfide del digitale.

[22] Giova menzionare il dibattito anche statunitense sul tema nell'ambito del quale la qualificazione giuridica dei social network «*costituisce un nodo da cui dipende l'effettività della tutela garantita dal Primo Emendamento*», M. BASSINI*, Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione,* in *Rivista Italiana di Diritto dell'Informatica*, vol. 2, 2021. Peraltro, la recente pronuncia nel caso Joseph Biden, Jr., President of the United States, *et al.*, v. Knight First Amendment Institute at Columbia University, *et al*., 593 U. S. BBBB (2021), e, in particolare, la *concurring opinion* di Justice Thomas, è stata in grado di portare alla luce un'idea di social network intesi come "*common carrier*", ossia "*essential facilities*". In altre parole, vengono intesi come infrastrutture essenziali per l'esercizio e l'alimentazione del dibattito pubblico, considerando spazi come Twitter, non solo "semplici" piattaforme private ma "public forum". Su tale tema, si rimanda anche a A. MORELLI, O. POLLICINO, *Metaphors, Judicial Frames, and Fundamental Rights in Cyberspace*, in *The American Journal of Comparative Law,* vol. 68, n. 3, 2020, pp. 616-646.

[23] D. MAC SITHIGH, *Virtual walls? The law of pseudo-public spaces*, in *International Journal of Law in Context*, vol. 8, n. 3, 2012, pp. 394-412.

espressione; il diritto alla cultura; il diritto all'identità e all'autonomia; il diritto all'autogestione; il diritto ai servizi pubblici e non pubblici; il diritto alla *privacy* – sono materialmente mediati dai soggetti privati. Tale aspetto, seppur non nuovo, in quanto tematica che emerge anche dai profili legati alla c.d. "*società algoritmica*" [24], profila per il costituzionalista una serie di sfide legate non solo alla garanzia di diritti fondamentali all'interno delle città, ma anche alla risoluzione del delicato rapporto attori pubblici e attori privati. Infatti, è necessario comprendere sia come permettere anche tramite strumenti normativi la reale partecipazione del cittadino, sia come mitigare e regolare l'ingerenza dell'attore privato nei progetti di pianificazione e rigenerazione urbana. In particolare, è necessario chiedersi: in una città che tutto vede, tutto processa, come può darsi il diritto all'identità e all'autonomia il diritto all'autogestione, il diritto alla *privacy*? È inevitabile che l'individuo stesso diventi parte integrante dell'ambiente ibrido assumendo allo stesso tempo, il ruolo di *user*, cliente e cittadino, peraltro, non sempre consapevolmente [25]. Per tale ragione, è necessario trovare un bilanciamento, in quanto l'integrazione di intelligenze artificiali e robotica nel tessuto urbano per fini di *governance* implica la necessaria adozione di cautele estreme, onde evitare, la creazione di uno sregolato sistema di sorveglianza a scapito dei diritti dei singoli [26]. La sfida non ricade solamente sull'attore privato nel progettare sistemi tecnologici rispettosi dei diritti umani, ma anche sul legislatore, che viene chiamato a dotarsi di un nuovo sistema di *governance,* come si dirà nella seconda parte di questo contributo.

Scendendo nel merito delle problematiche legate alla protezione dei dati personali, come si anticipava, un notevole valore viene dato alla *privacy* in ambito Europeo, il cui percorso costituzionale ha compiuto un ulteriore passo con l'adozione del Regolamento UE 2016/679 [27]. Il primo obiettivo è stato quello di garantire il diritto alla protezione dei dati personali in quanto diritto fondamentale degli interessati. Nonostante l'elevato grado di salvaguardia di cui questi godono nel panorama comunitario, vale la pena evidenziare come

---

[24] Cfr. J. DANAHER, *op. cit.*

[25] L. TAYLOR, C. RICHTER, S. JAMESON, C. PEREZ DE PULGAR, *Customers, users or citizens? Inclusion, spatial data and governance in the smart city. Inclusion, Spatial Data and Governance in the smart city,* in *SSRN*, 2016.

[26] Per l'appunto, senza specifiche regole si rischia, di «*alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere*». Indicativo in questo senso è l'allarme lanciato dal presidente dell'Autorità garante per la protezione dei dati personali italiano che nell'ambito dei modelli di *smart city* ha addirittura paventato il pericolo di un "*nuovo totalitarismo digitale*", A. SORO, *Discorso del Presidente Antonello Soro*, *Relazione 2018*, Garante per la Protezione dei Dati Personali, 2019, p. 5.

[27] Cfr. nota 14.

questo diritto non goda di una tutela assoluta ma che «*de[bba] essere considerato in relazione alla sua funzione nella società e bilanciato con altri diritti fondamentali, conformemente con il principio di proporzionalità*»[28]. Infatti, tali diritti possono essere limitati per proteggere altri diritti costituzionali o per scopi legittimi. Taluni dei principi cardine del GDPR soggiacciono ad alcune considerazioni di rischio, o di cautela, nell'affrontare trattamenti di dati personali che possano eccessivamente limitare le libertà degli individui. A tal proposito, il Considerando 39 stabilisce il principio della minimizzazione[29]. Come suggerisce lo stesso termine, è richiesto di ridurre non solo in termini quantitativi, ma anche qualitativi, i confini del trattamento del dato personale, ma anche di adoperare delle cautele, attraverso misure come la pseudonimizzazione per diminuire la facilità con cui i dati possono essere collegati agli individui. Almeno in astratto, dunque, la *smart city* mal si presta a un contesto improntato alla minimizzazione. La raccolta di dati attraverso IoT, la modalità di trattamento automatizzata di grandi quantità di informazioni attraverso tecniche di *big data analytics* e la conservazione ubiquitaria su *cloud* sono solo alcuni degli elementi che mettono in crisi il sistema del GDPR all'interno della città intelligente[30].

È, difatti, proprio nella facoltà di aggirarsi liberamente per lo spazio urbano, senza il rischio di eccessive intrusioni nella sfera privata[31], che si sostanzia l'ancillare concezione della *privacy*, così come venne intesa da Warren e Brandeis[32]. Sebbene vi siano delle proposte su come creare un bilanciamento tra esposizione e riservatezza, tra intrusione e *privacy*[33], queste non appaiono del

---

[28] GDPR, Considerando 4.

[29] Considerando 39: «*È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento*».

[30] Per una maggiore riflessione sull'argomento, G. VOJKOVIĆ, T. KATULIĆ, *Data Protection and smart cities,* in J.C. AUGUSTO (a cura di), *Handbook of smart cities,* Berlin, 2021.

[31] M. HIROSE, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review*, vol. 49, n. 5, 2017, p. 1591.

[32] S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review,* vol. 4, 1890.

[33] K. FINCH, O. TENE, *Smart Cities: Privacy, Transparency, and Community*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *Cambridge Handbook of Consumer Privacy*, Cambridge, 2018. Accanto alle questioni legate alla *data protection*, si profilano anche le problematiche che interessano i *bias* algoritmici e i rischi di discriminazione, derivanti dalla creazione di algoritmi non sempre trasparenti.

tutto convincenti, poiché ancora relegate su un piano di *compliance* che poco tiene in considerazione l'impatto sui diritti fondamentali. Proporre come soluzione un *data protection impact assessment* su larga scala, non appare logico rispetto alla dimensione tanto quantitativa quanto qualitativa della città intelligente. Al contrario, è importante stressare la necessità di riflettere, da un lato, sulle singole situazioni di rischio condotte dai singoli elementi tecnologici che si affastellano nello spazio urbano (del presente) e del futuro; dall'altro, occorre ripensare taluni principi della *data protection*, e, in particolare, il sistema di cui all'art. 6 del GDPR, e la raccolta del consenso dell'interessato [34]. Pertanto, ciò impone una riflessione organica che guardi all'interezza del diritto alla *privacy* e alla protezione dei dati personali in un ambiente sempre più complesso, in cui il tessuto urbano si trasforma, al fine di limitare *ex ante* fenomeni di sorveglianza e controllo indiscriminati.

A tal riguardo, questa operazione trasformativa travolge a pieno la riservatezza e la permeabilità dei requisiti che l'hanno elevata a «*Europe's First Amendment*». Difatti, in questo novellato contesto anche la tenuta degli standard precedentemente applicati è aspetto di rilevante importanza se si vuole assicurare la replicabilità delle garanzie ai diritti individuali. La fortezza europea della *privacy* è, dunque, ancora una volta assediata da nuove sfide che mettono in discussione la replicabilità interna ed esterna, nonché la sua complementarità rispetto alle sempre nuove sfide della tecnologia. Difatti, il mondo cui ci si sta affacciando – e le iniziative europee sembrano andare in questa direzione –, che, peraltro, è l'unico mondo in cui possa esistere una vera e propria *smart city*, reclama la circolazione dei dati, la portabilità e l'interoperabilità come suoi cardini.

Conclusi questi brevi cenni, occorre iniziare a rispondere alla domanda che, seppur non ancora esplicitata, necessariamente sorge, una volta compresa la dimensione d'indagine: è lo standard europeo in grado di farsi portatore di un sistema globale, replicabile nel contesto della *smart city*? A tale complesso quesito si tenterà di rispondere nel prossimo paragrafo.

2.1. (Segue) *La fortezza europea della* privacy *alla prova della* smart city

La *privacy* degli individui e la protezione della loro riservatezza sono due delle sfide cardinali dell'epoca moderna. L'esposizione alla raccolta di massa di dati personali è un aspetto notissimo, così come le garanzie che ovunque,

[34] G. DE GREGORIO, *Città, cittadino e diritti digitali*, in G.F. FERRARI (a cura di), *Smart city. L'evoluzione di un'idea*, Milano, 2020, pp. 493-527.

ma soprattutto in Europa [35], sono state messe in atto per assicurare uno dei diritti fondamentali protetti dalla Carta di Nizza [36]. Pertanto, è importante considerare come e se tale diritto possa trovare applicazione nella *smart city*. La *datafication* è una caratteristica centrale di ogni città intelligente, indipendentemente dalla prospettiva che si adotta per definirla e progettarla. L'incessante raccolta e trattamento di dati che provengono da molteplici fonti mette a rischio la protezione dei dati personali e la loro confidenzialità. In secondo luogo, si rinviene un problema di *privacy* biometrica rispetto alla propria salute, alle caratteristiche fisiche in grado di identificare il cittadino; ma anche una *privacy* "territoriale", ossia riguardante lo spazio personale, gli oggetti e la proprietà. Infine, si rileva un problema di *privacy* delle comunicazioni e delle transazioni. Queste preoccupazioni sorgono perché le città intelligenti collocano sensori nell'arredo urbano, dai cestini dei rifiuti ai lampioni, tracciano gli identificatori telefonici e i sistemi di mobilità intelligente, basandosi su ampi apparati di geolocalizzazione [37]. Perché, dunque, è rilevante parlare di *privacy* della *smart city*, anziché di *privacy* degli IoT, o degli *smart objects*? La risposta è necessariamente che la città intelligente rappresenta una sommatoria di tutte queste circostanze, come si premetteva in introduzione.

La *smart city* diventa un perfetto strumento di raccolta dei dati comunicati e condivisi dai cittadini, ove i dati non vengono solo venduti per interessi commerciali, ma vengono anche utilizzati per plasmare i comportamenti e il carattere dell'essere umano [38]. Sostanzialmente, nella città intelligente, i sistemi di sorveglianza, come circuiti di telecamere sempre funzionanti, diventano parte integrante dello sfondo urbano integrandosi nella quotidianità del cittadino [39].

---

[35] Si fa riferimento, in particolare, a quella cultura della *privacy* che ruota attorno all'importanza assegnata a questo diritto nelle scelte di *policy* delle istituzioni comunitarie. Peraltro, Bilyana Petkova ha brillantemente riassunto tale paradigma costituzionale nell'espressione «*privacy as EU First Amendment*», proprio a sancire la centralità della protezione dei dati personali in Europa. B. PETKOVA, *Privacy as Europe's First Amendment*, in *European Law Journal*, vol. 25(2), 2019, pp. 140-154.

[36] Art. 7 e art. 8 Carta dei Diritti Fondamentali dell'Unione Europea (2000/C 364/01).

[37] Si veda S. RANCHORDAS*, Cities of God: Smart Cities and Surveillance,* in *VerfBlog,* 2021.

[38] J. SADOWSKI, F. PASQUALE, *The Spectrum of Control: A Social Theory of the Smart City*, in *U. of Maryland Legal Studies Research Paper*, vol. 26, 2015.

[39] Come si vedrà, non sorreggono, peraltro, nemmeno i limiti imposti dal Regolamento UE 2016/679 in quanto non tutti i dati raccolti nelle città intelligenti saranno qualificabili come dati personali, poiché molti di essi si riferiscono alla gestione della folla, ai dati urbani o ambientali (ad esempio, i livelli di inquinamento atmosferico, la densità del traffico, il livello dell'acqua). Inoltre, parte dei dati raccolti diventerà disponibile sotto forma di dati aperti che consentiranno molteplici miglioramenti urbani. E, inoltre, le città intelligenti non raccolgono solo dati sulla città e i suoi arredi (ad esempio, i sondaggi delle lampade) ma anche sui loro cittadini. Di questi

Dunque, occorre quanto meno soffermarsi sulle *externalities* che vengono in evidenza dal momento in cui si basa il funzionamento della vita – e, dunque della città – smart sul flusso e sul trasferimento dei dati in *input* e in *output*. Le architetture che assicurano l'*onlife*[40], almeno in Europa, sono ancorate alla disciplina a protezione dei dati personali che, com'è noto, in questo contesto va ben oltre il diritto derivato, in quanto è tutelata anche come diritto fondamentale o quasi "costituzionale" ai sensi della Carta dei diritti fondamentali dell'Unione Europea[41]. In particolare, gli artt. 7 e 8 della Carta prevedono, in modo unico, due diritti distinti, ossia la protezione della vita privata (*privacy*) e la protezione dei dati personali: una novità rispetto ai tradizionali strumenti di tutela dei diritti umani e, soprattutto, la prima volta in cui la protezione dei dati ha acquisito lo status di diritto fondamentale a sé stante nell'ambito degli strumenti normativi internazionali esistenti[42].

Bisogna, dunque, domandarsi: quale standard di tutela verrà applicato nella città digitale? E, soprattutto, vivendo in un mondo globalizzato, quale standard di protezione viene assicurato alla persona fisica e digitale nella città *smart*? Domande che sono tutt'altro che banali se si tiene in considerazione l'immensa problematica che tutt'ora soggiace al trasferimento dei dati personali verso paesi terzi e la nota casistica che ha soprattutto coinvolto gli Stati Uniti d'America, dove il conflitto si è giocato proprio sul livello di protezione che viene assicurato agli individui da illecite interferenze nella loro vita privata. Tale aspetto viene ivi in rilievo non solo con riguardo alla programmazione delle architetture-fondamenta della *smart city*, ma appare logico immaginarne una criticità anche con riguardo all'utilizzo fisico di tali detti strumenti e la loro interazione con gli utenti-cittadini nello spazio fisico. Ebbene, in questa cornice la *privacy* e lo standard applicato – più orientato verso uno *ius excludendi alios*, o verso un *habeas data* – nell'ottica di garantire l'esercizio e l'*enforcement* dei diritti fondamentali nella nuova *onlife.* Chiarire lo standard e l'adeguatezza delle tutele ha una cruciale significanza nell'ambiente della città tecnologica sotto molteplici punti di vista. La necessità di chiarire quale standard di protezione applicare è inerentemente connessa dapprima ai dati con cui gli

---

ultimi non sono raccolti solamente i dati personali, bensì anche i c.d. metadati, ossia quelle informazioni che non sono riconducibili a un interessato identificato o identificabile, ma che forniscono ad ogni modo preziosi dettagli sul cittadino.

[40] L. FLORIDI, *The onlife manifesto: Being human in a hyperconnected era*, Berlin, 2015.

[41] Charter of Fundamental Rights of the European Union.

[42] YORDANKA IVANOVA, *The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World,* in *SSRN,* 2020). Volendo anche O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, New York, 2021.

elementi architettonici della città *smart* funzionano; in secondo luogo, dal livello di tutela assicurato, discende altresì la possibilità di poter azionare detti diritti e reclamarli in via diretta dinanzi a un *provider* o a un organo giudiziario. Pertanto, le problematiche che ancora permangono con riguardo al trasferimento dei dati personali verso paesi terzi è un aspetto che acquista un'importanza sostanziale non solo a livello di *compliance,* ma proprio nell'ottica di garantire la protezione orizzontale dei diritti degli individui.

Ebbene, anche se un livello di protezione adeguato non richiede necessariamente che i Paesi terzi adottino standard identici, le persone fisiche devono comunque godere di un grado di protezione che sia "sostanzialmente equivalente" a quello offerto dal diritto dell'UE[43]. L'equivalenza nel grado di protezione è richiesta, secondo la Corte, in virtù di un'interpretazione della Direttiva 95/46 alla luce della Carta di Nizza. Giova, quindi, rammentare che, nel contesto europeo, la Carta, anche a grazie all'opera creativa della Corte di Giustizia, è lo strumento giuridico utile per l'avanzamento del livello di tutela richiesto dal diritto dell'UE attraverso un'interpretazione elastica del parametro di "adeguatezza". Questo approccio è tutt'altro che retorico in quanto la CGUE era ispirata dall'entrata in vigore della Carta di Nizza a rivisitare le norme contenute nella direttiva sulla protezione dei dati personali e a rinnovarne l'interpretazione. Pertanto, il significato delle norme della direttiva andava mutando e, coerentemente, il livello di protezione accordato ai dati personali divenne molto più ampio anche prima dell'adozione del GDPR.

Per rispondere alla domanda che è stata precedentemente posta, ossia la replicabilità delle tutele assegnate all'individuo dalla normativa sulla protezione dei dati personali in altre giurisdizioni, occorre necessariamente guardare

---

[43] Si vedano in tal senso anche le Conclusioni dell'A.G. in *Maximillian Schrems c Data Protection Commissioner (Schrems I)*, ECLI:EU:C:2015:627. In particolare, al par. 141 argomenta: «*è per questo motivo che ritengo che la Commissione possa constatare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione*». Pertanto, è stato in primo luogo l'Avvocato Generale a manipolare l'interpretazione della direttiva. Dopo aver fatta sua questa argomentazione cruciale, peraltro, l'AG sostiene al paragrafo 142: «*Benché il termine inglese "adequate" possa essere inteso, dal punto di vista linguistico, nel senso che esso designa un livello di protezione appena soddisfacente o sufficiente, ed avere pertanto un campo semantico diverso dal termine francese "adéquat", si deve osservare che il solo criterio che deve guidare l'interpretazione di tale termine è l'obiettivo consistente nel conseguimento di un livello elevato di protezione dei diritti fondamentali, come richiesto dalla direttiva 95/46*».

all'estensione del campo di applicazione del diritto dell'UE, secondo l'interpretazione della Corte di Giustizia.

Tale aspetto è di assoluto rilievo nelle notissime sentenze *Google Spain*[44] e *Schrems I*[45], ove la CGUE applicò le norme dell'Unione, alla luce dei diritti fondamentali tutelati dalla Carta di Nizza, al di là dei confini europei, affermando così la propria sovranità digitale. In *Google Spain*, attraverso un'interpretazione espansiva della nozione di stabilimento, la Corte limitò il potere dei gestori di motori di ricerca, come attori privati, di condurre le loro attività economiche su scala globale senza essere soggetti alle normative dei Paesi in cui essi operano[46]. Similmente, in *Schrems I*, la valutazione effettuata dalla CGUE con riferimento alla *Safe Harbour Decision* era mossa eminentemente dalla necessità di assicurare che la nozione formale di territorio e giurisdizione non minassero sostanzialmente l'effettiva protezione dei diritti fondamentali nell'ecosistema digitale.

Ciò detto, occorre considerare se l'attivismo giudiziario possa mutare alla luce dell'ambito di applicazione territoriale del GDPR. In questa prospettiva, è interessante considerare una decisione della Corte Suprema della Columbia Britannica del 2014[47], resa prima che la CGUE, in *Google c. CNIL*[48], adottasse una nuova posizione chiarificatrice del fatto che il diritto all'oblio contenuto nell'art. 17 GDPR non può essere applicato al di fuori dell'UE. Nella sua decisione, la Corte Suprema della Columbia Britannica – menzionando espressamente il caso *Google Spain* – si occupò del problema dell'applicazione extraterritoriale della protezione accordata a livello domestico ai dati personali e, più in generale, della mancanza soluzioni efficaci elaborate su base meramente locale (e non necessariamente nazionale).

L'attore aveva richiesto un'ingiunzione provvisoria che proibisse a Google di mostrare i risultati di ricerca connessi al sito web accusato di violare i diritti di proprietà intellettuale dell'attore stesso. Google aveva obbedito all'ordine, anche se la rimozione aveva riguardato soltanto la versione canadese del mo-

---

[44] C-131/12 *Google Spain SL e Google Inc c Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317.

[45] C-362/14, *Maximillian Schrems c Data Protection Commissioner (Schrems I)*, ECLI:EU:C:2015:650, para. 38.

[46] Sulle conseguenze di queste decisioni si veda C. DOCKSEY, *The EU Approach to the Protection of Rights in the Digital Environment: Today and Tomorrow – State Obligations and Responsibilities of Private Parties – GDPR Rules on Data Protection, and What to Expect from the Upcoming ePrivacy Regulation*, in Consiglio d'Europa (a cura di), *Human Rights Challenges in the Digital Age: Judicial Perspectives*, Strasburg, 2020, p. 47 ss.

[47] *Equustek Solutions Inc v Jack* [2014] BCSC 1063.

[48] C-507/17 *Google c CNIL*, ECLI:EU:C:2019:772.

tore di ricerca (*google.ca*). Pertanto, i link al sito in questione erano ancora forniti da altri motori di ricerca non canadesi operati da Google. La Corte Suprema Canadese della Columbia Britannica, di conseguenza, ordinò a Google di rimuovere le pagine di alcuni siti web dai risultati della ricerca su base globale e non meramente nazionale. Il caso, pertanto, concerneva un ordine di rimozione a livello mondiale, il che costituiva in tutta probabilità un tentativo di rispondere al problema della frammentazione della protezione giuridica, inerentemente connessa alla natura locale delle giurisdizioni impegnate nell'applicazione dei diritti fondamentali in gioco.

La Corte d'Appello della Columbia Britannica rigettò l'appello di Google, sostenendo che la Corte aveva giurisdizione territoriale a rilasciare quella decisione non solo in Canada, ma altresì al di fuori del suo territorio [49]. Google argomentò in particolare che, poiché operava *online*, la giurisdizione territoriale della corte canadese non doveva applicarsi a Internet. Qui, in particolare, è interessante osservare come la corte si sia basata sulla sentenza *Google Spain*, ove la stessa argomentazione addotta da Google non era stata accolta dalla CGUE. La Corte d'Appello della Columbia Britannica concluse infatti che, sebbene Google sostenesse di offrire un sito meramente passivo ai residenti della Columbia Britannica che vogliano operare una ricerca su Internet e che i suoi programmi generino in automatico i risultati della ricerca senza che Google sia attivamente coinvolto nel processo, in realtà i siti di ricerca su Internet gestiti da Google non erano in realtà veramente siti passivi di informazione. Infatti, non appena un utente inserisce alcune lettere o una parola nella barra di ricerca, Google anticipa la richiesta e offre un menù a tendina contenente alcuni suggerimenti di possibili *query*. Google inoltre vendeva pubblicità ai clienti residenti nella Columbia Britannica: anzi, aveva stipulato precipuamente un contratto di pubblicità con i convenuti e aveva pubblicizzato i loro prodotti fin all'udienza stessa [50].

Avendo stabilito le ragioni per cui la corte canadese era competente a decidere della controversia in questione, la Corte d'Appello della Columbia Britannica si concentrò sulla questione dell'extraterritorialità. In maniera simile a *Google Spain*, il problema concerneva la necessità di fornire un'effettiva tutela dei diritti dell'attore e di prevenire il rischio che la legge venisse aggirata attraverso il ricorso all'ambiente *online*. Se in *Google Spain* l'obiettivo era propriamente quello di proteggere i diritti dei cittadini dell'UE, le corti canadesi si concentrarono invece su considerazioni legate all'equità [51]. Secondo la Corte

[49] *Equustek Solutions Inc v Google Inc* [2015] BCCA 265.

[50] *Ivi* para. 47-48 e 50.

[51] L'argomentazione delle corti della Columbia Britannica si basava sulla sez. 39 del *Law and*

la soluzione adottata da Google era del tutto insoddisfacente dal punto di vista degli attori. Al posto dei siti Internet deindicizzati, una quantità di nuovi siti era andata a sostituirli, avanzando in termini di *ranking*. I siti, argomentò la Corte, possono essere generati automaticamente, cosicché gli attori possono trovarsi a dover continuamente identificare nuovi URL da indicare a Google per chiederne la rimozione. Pertanto, uno schema di tutela che si basi sulla rimozione del singolo URL risultava inefficace. Di conseguenza, la Corte ritenne essere in suo potere la possibilità di emanare un'ingiunzione contro terze parti, quand'anche stabilite in Paesi terzi, laddove le circostanze lo richiedano. Il fatto che un'ingiunzione di siffatto tipo non fosse mai stata emanata nei confronti di un gestore di un motore di ricerca, quale Google, richiedeva di procedere con cautela, ma non ostava alla competenza della corte canadese in tale materia[52].

Nonostante Google avesse argomentato che le corti canadesi non avevano il potere di imporre una deindicizzazione dei risultati delle ricerche a livello globale, poiché Google avrebbe potuto trovarsi nella situazione di violare norme straniere, la Corte Suprema della Columbia Britannica rigettò altresì questo ragionamento, dimostrando una piena comprensione di come funzioni l'ambiente *online*. Essa osservò che, anche se Google gestisce un sito per ciascun Paese che viene utilizzato di default all'interno di quel Paese, è tuttavia possibile per gli utenti aggirare tale sistema e accedere ai siti Google di Paesi terzi. Pertanto, se anche i siti dei convenuti fossero stati rimossi dalle ricerche condotte attraverso *www.google.ca*, gli utenti canadesi avrebbero comunque potuto ricorrere ai siti *www.google.co.uk* o *www.google.fr* per accedere a tali siti[53].

Google tentò di argomentare, tra l'altro, che le corti godono di una limitata giurisdizione entro i propri territori e che non possano imporre ordini aventi portata extraterritoriale ai gestori di motori di ricerca. Inoltre, sostenne più in generale che un ordine avente rilievo globale potesse violare il principio di cortesia internazionale e la libertà di espressione. Focalizzandosi in particolare sulla possibilità che le corti imponessero ordini con efficacia internazionale, seguendo un percorso simile alle corti della Columbia Britannica, la Corte Suprema del Canada spiegò perché un tale ordine potesse essere giustificato sulla base delle circostanze specifiche del caso. In particolare, essa sostenne che il

---

Equity Act. Secondo questa legge, le ingiunzioni possono essere emanate in tutti i casi in cui la Corte ritenga giusto o conveniente emanare l'ordine, sulla base dei termini e delle condizioni che la Corte stessa ritenga giuste.

[52] *Equustek Solutions Inc v Jack*, cit., para. 72 e 133.

[53] *Ivi*, para. 148.

problema trattato all'interno del caso in questione avesse luogo *online* e a livello globale[54]. Poiché Internet non ha confini, e il suo habitat naturale è globale, l'unico modo per assicurare che un'ingiunzione interlocutoria raggiunga i suoi obiettivi è che essa si applichi nel luogo in cui opera Google – e cioè a livello globale. Tra l'altro, la maggioranza delle vendite operate dai siti dei convenuti avveniva proprio all'estero, cosicché, se l'ingiunzione fosse stata ristretta nel suo campo al solo territorio canadese o al sito google.ca, come richiesto da Google, il rimedio sarebbe stato incapace di prevenire un danno irreparabile. Secondo la Corte Suprema canadese, pertanto, non vi era alcuna equità nell'ordinare un'ingiunzione interlocutoria che non avesse alcuna prospettiva realistica di prevenire un danno irreparabile[55]. Innanzitutto, la Corte osservò che la violazione del principio di cortesia internazionale era soltanto teorica in quanto Google non aveva fornito prove sufficienti dell'impatto di una deindicizzazione globale sugli ordinamenti giuridici di Stati terzi. In secondo luogo, il diritto alla libertà di espressione non poteva giustificare la facilitazione della commissione di attività illecite in rete.

Queste furono le due ragioni principali che condussero la Corte Suprema canadese a concludere che, in assenza di una base probatoria, e considerato il diritto di Google a chiedere una rettifica nell'ordine, sembrava tutt'altro che equo negare all'attore un'ingiunzione che avesse efficacia extraterritoriale in linea con le sue necessità, oppure anche solo imporre ad esso l'onore di dimostrare in ogni Paese che tale ordine fosse lecito. Avendo a che fare con Internet, il giudizio di bilanciamento doveva tenere in piena considerazione l'inevitabile scenario globale comportato dalla richiesta di un'ingiunzione a carico di un attore quale Google. Inoltre, la Corte sottolineò come l'ordine in questione non aveva lo scopo di rimuovere alcuna espressione rilevante, *prima facie*, per i valori della libertà in questione: si trattava invero di un ordine di deindicizzazione di siti che violavano diversi ordini giudiziali. In tal senso, la Corte ritenne che non fosse accettabile il principio in base al cui la libertà di espressione richieda di ammettere la facilitazione della vendita di beni illeciti[56].

---

[54] G*oogle Inc v Equustek Solutions Inc* [2017] SCC 34.

[55] *Ibid*. para. 41. In questo caso, l'imposizione dell'ingiunzione mirava quindi a evitare un danno irreparabile derivante dai flussi di dati facilitati dai servizi offerti da Google. Concentrandosi sul principio di cortesia internazionale e sulla libertà di espressione, Google lamentò che l'imposizione di un ordine extraterritoriale potesse violare il primo poiché Google sarebbe stato obbligato in alcuni casi a violare il diritto di altri Stati. Anche con riferimento alla libertà di espressione, Google osservò che questo tipo di ingiunzione rischiava di compromettere la libertà di parola in rete. Tuttavia, la Corte Suprema del Canada rigettò anche queste argomentazioni.

[56] *Ivi*, para. 47-48.

Tutto questo *excursus* appare utile per comprendere il margine di replicabilità di detti diritti nel contesto della città *smart*, ove il confine tra azione *online* e azione reale semplicemente non esiste. Inoltre, l'ambito di applicazione extraterritoriale del GDPR codifica attualmente i tentativi della CGUE di assicurare un'effettiva protezione per i diritti dei propri cittadini sotto il profilo transnazionale. In particolare, l'art. 3(2) GDPR può essere considerato il risultato di uno standard di protezione di alto livello per la *privacy* in Unione Europea, che, nella società dell'informazione, non può più essere limitato esclusivamente al territorio europeo ma deve essere assicurato a livello globale[57].

La conseguenza di tale norma è duplice. In primo luogo, essa concerne il problema della giurisdizione. In particolare, tutti i casi di trattamento di dati personali che ricadano nell'ambito di applicazione dell'art. 3(2) GDPR saranno soggetti alla giurisdizione dell'Unione. Questo approccio permette di superare la dottrina dello stabilimento elaborata dalla CGUE in *Google Spain*, in quanto persino quegli enti che non siano stabiliti in UE potranno essere soggetti al GDPR. Ancora più importante è tuttavia la seconda conseguenza, ovverosia l'estensione delle regole euro-unitarie sulla *privacy* al contesto globale – e questa è, piuttosto una questione di sovranità digitale. Se, come sottolineato sopra, la CGUE in *Schrems I* si è occupata degli standard di protezione presenti nel sistema statunitense atti a governare il trattamento di dati personali di cittadini dell'UE, ora il parametro operativo di riferimento potrà essere direttamente quello europeo, come definito dal GDPR.

Dunque, la natura transnazionale degli strumenti digitali, di cui la città *smart* appare essere un amplificatore, sembra essere incompatibile con i tentativi di "regionalizzazione", non solo della *privacy*, ma anche della tecnologia tout court, sicché questo processo deve tendere verso l'aumento di un sufficiente grado di tutela dei diritti fondamentali. Questo processo di regionalizzazione, che rappresenta il riflesso dell'amplificazione di un impulso regolativo da parte delle corti, potrebbe verosimilmente risultare in una frammentazione e, forse, balcanizzazione tecnologica e dei relativi strumenti giuridici che governano suddetti sistemi[58].

---

[57] In particolare, l'art. 3(2) GDPR recita: «il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure (b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione».

[58] Un problema che si manifesta anche nell'ambito del *cloud computing,* come *supra* si accennava. Difatti, nell'ambito di questo servizio, l'esercizio di sovranità digitale dell'Unione Eu-

È evidente che il contrasto tra i limiti territoriali alla giurisdizione dei legislatori e delle corti, e la natura globale dei servizi digitali potrebbe comportare il rischio di una gara al ribasso nella protezione dei diritti in gioco e a una ridotta efficacia dei relativi meccanismi di tutela. Ciò rappresenta un ulteriore riflesso del conflitto tra diritto locale e diritto globale che caratterizza la globalizzazione del ruolo delle corti. L'analisi della giurisprudenza di cui sopra rivela una migrazione di idee giuridiche (o costituzionali) da un lato all'altro dell'Atlantico[59]. Finora, tale migrazione è stata quasi esclusivamente unidirezionale. I giudici europei "esportano" le idee europee al di fuori dell'Europa. In altre parole, le decisioni delle corti europee, che sono ampiamente citate al fine di corroborare la legittimità e persuasività delle loro stesse decisioni, ispirano e influenzano i giudici non europei, come accaduto per esempio in Canada. Attualmente, qualsiasi procedimento inverso sembra lungi dall'avvenire. Le corti europee sembrano essere più inclini a "insegnare" piuttosto che "imparare" quando si tratti di discutere della protezione, *erga omnes*, di valori costituzionali europei, anche al di là dei confini europei. Chiudendo su questo punto, è opportuno sottolineare che l'estensione del potere dei paradigmi europei, che stanno rendendo l'Europa, quasi paradossalmente, una fortezza per la protezione dei dati, non considera gli impatti politici e giuridici che esso ha sulle relazioni con i Paesi terzi. Questa scelta politica dell'UE può essere letta come un tentativo di codificare il diritto alla *privacy* digitale. Ciononostante, il ruolo delle corti in relazione alla tutela transnazionale della *privacy* e della protezione dei dati è solo ai suoi inizi.

---

ropea appare ancora agli albori, mancando di quel necessario focus sulla tutela dei diritti considerati in senso ampissimo, tenuto conto delle problematiche già emerse con riguardo alla disciplina a protezione dei dati personali. A tal proposito, appare necessario guardare alle spinte globali che interessano il *cloud* e il *free flow* di dati, anche non personali. Ebbene, considerando altre esperienze, come, ad esempio quella statunitense e cinese, emerge un atteggiamento volto all'adozione di misure difensive del proprio patrimonio digitale. D'altro canto, i *big players,* tra cui Google e Amazon, che, nell'ottica di adeguarsi a tali approcci limitati e limitanti, hanno sempre più regionalizzato e localizzato le loro risorse. Ancora una volta preoccupa come la scelta di proteggere o meno i propri clienti da accessi desiderati o indesiderati, sia se previsti dal CLOUD Act, sia se previsti dalle iniziative del governo cinese, ricadano su attori privati che, alla base di tali scelte cruciali, non pongono la *rule of law,* ma le più convenienti logiche di *business.*

[59] K. KOWALIK-BAŃCZYK, O. POLLICINO, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, in *German Law Journal,* vol. 17, n. 3, 2016, spec. p. 315.

3. *La città tra pubblico e privato*

La sovranità e l'applicazione del modello europeo di protezione dei dati non coinvolge solamente i rapporti tra Stati e l'emersione di corrispondenti modelli di tutela. L'inevitabile contributo degli attori privati nel *design*, produzione, commercializzazione di quelle che abbiamo identificato come le architetture della *smart city,* rende i soggetti detentori di queste ultime in grado di esercitare una grande influenza sui cittadini [60]. Il profilo che riguarda il controllo e la sorveglianza massivi desta negli interpreti forti preoccupazioni sulla capacità di garantire l'applicazione dei diritti fondamentali. Da ciò, nasce l'esigenza di definire una nuova dimensione del diritto alla riservatezza, nonché di quello all'autonomia e alla libera determinazione anche in relazione agli spazi pubblici.

La giurisprudenza della Corte europea dei diritti dell'uomo ha interpretato l'art. 8 della Convenzione europea sui diritti dell'uomo nel senso di ricomprendervi il diritto di ciascuna persona una propria "*vita sociale privata*" [61]. Sebbene in un contesto pubblico, sussiste una zona di interazione dei cittadini con gli altri, nella quale si estrinseca un'aspettativa alla *privacy* [62]. Un'accezione che fa da eco al concetto di Quarto Emendamento e a quella *"expectation of privacy"* elaborata dal giudice statunitense nella decisione del notissimo caso Katz v. US del 1967 [63], già ripresa da diverse Corti americane [64], le quali hanno

---

[60] *Ex multis,* su questo argomento, si cita C. O'NEIL, *Weapons of math destruction: How big data increases inequality and threatens democracy*, Washington D.C., 2016.

[61] Si vedano, tra altri precedenti, *Botta c. Italia*, 24 febbraio 1998, *Reports of Judgments and Decisions*, 1998-I*; Barbulescu c. Romania*, [GC], n. 61496/08, CEDU 2017.

[62] Si vedano, tra altri precedenti, *Peck c. Regno Unito,* n. 44647/98, CEDU 2003-I; *Von Hannover c. Germania* (n. 2), [GC], nn. 40660/08 e 60641/08, CEDU 2012; *Uzun c. Germania*, [GC], n. 61496/08, CEDU 2017; *Altay c. Turchia* (n. 2), n. 11236/09, 9 aprile 2019.

[63] Ivi il giudicante si esprimeva in questi termini: «[t]*he Fourth Amendment cannot be translated into a general constitutional 'right to privacy'. That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States ... For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection*», in *Katz v United States* 389 US 347 (1967) par. 350.

[64] In particolare, ci si riferisce a diverse importanti decisioni, come in *United States v. Jones,* 565 U.S. 400 (2012); *Riley v. California,* 573 U.S. 373, (2014) e in *Carpenter v. United States,* 585 U.S*.,* (2018).

avuto modo di chiarire che «*advances in technology can increase the potential for unreasonable intrusions into personal privacy*»[65].

Pertanto, anche e soprattutto nella *smart city*, la *privacy* deve essere una condizione infrastrutturale che permette il pieno esercizio dei diritti fondamentali e lo sviluppo dell'autonomia e della libera determinazione degli individui sia in spazi privati che in spazi pubblici. A tal proposito, va ricordato come il diritto alla *privacy* nella società digitale non possa limitarsi al non subire interferenze esterne nell'esercizio dei propri diritti individuali. Per esser davvero efficace, il diritto alla riservatezza e alla protezione dei dati personali deve connettersi in modo esplicito e rigoroso alla costruzione d'uno spazio comune di salvaguardia della dignità, delle libertà e della sicurezza delle persone[66].

Tuttavia, si rileva che la realizzazione di una simile condizione infrastrutturale all'interno delle città intelligenti non passa solo attraverso le decisioni dell'attore pubblico, bensì è subordinata anche alle volontà e intenti dei soggetti privati, detentori delle tecnologie più innovative. Infatti, deve ricordarsi come i modelli di *smart cities* finora proposti vedano l'utilizzo di sistemi ICT essenzialmente e quasi sistematicamente basati su partenariati pubblico-privati. Dal momento che le tecnologie utilizzate nelle città intelligenti hanno la capacità di aumentare il controllo e il grado di sorveglianza su ogni aspetto della vita dei cittadini, ne discende che, inevitabilmente, tale potere sarà ancora una volta appannaggio anche dei soggetti privati. Basti pensare, ad esempio, al ruolo che già ricoprono società come Amazon, Uber, AirBnB, le quali offrono servizi a vario titolo alle amministrazioni cittadine. Queste realtà, consce del binomio informazione-potere, sono massimamente attratte dalle incredibili opportunità che l'utilizzo di dati personali e informazioni dei cittadini può creare. Ciò, non tanto e non solo per aumentare la precisione dei propri spazi pubblicitari, ma soprattutto al fine di alimentare i loro algoritmi di intelligenza artificiale, impiegati a loro volta nei modelli di *smart cities*.

Un esempio di quanto ivi accennato è la crisi che questo spazio *uber* pubblico provoca all'esercizio della libertà di manifestazione del pensiero. Come già ampia letteratura ha messo in evidenza[67], l'attuale esercizio di questa liber-

---

[65] *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. 2019).

[66] Infatti, come indicò Stefano Rodotà nella sua relazione introduttiva alla ventiseiesima Conferenza internazionale sulla protezione dei dati: «noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro».

[67] Il riferimento ricade, in particolare, sull'analisi di J. M. BALKIN, *Free speech is a triangle*, in *Colum. L. Rev.*, vol. 118, 2018, p. 2011.

tà è sostanzialmente mediato da una serie di infrastrutture, tra cui i *social network,* che, attraverso il sistema di moderazione dei contenuti e dei filtri, dirige e amministra la formazione delle opinioni e delle idee nonché la circolazione delle medesime [68]. La commercializzazione e la diffusione di sistemi automatizzati non hanno delle ricadute solamente sull'esercizio passivo della libertà d'espressione, ossia il non incappare in bolle filtro o *thread* di disinformazione, ma vi sono delle importanti conseguenze con riguardo al profilo attivo, ossia la possibilità garantita al cittadino di manifestare liberamente il proprio pensiero.

Ebbene, anche da recente giurisprudenza della Corte Europea dei Diritti dell'Uomo e dall'interpretazione dell'art. 10 della Convenzione [69], è possibile evincere che la dimensione attiva abbia un'immensa centralità, non solo in rispetto al *medium* tecnologico, ma anche nella sua dimensione atomica [70]. Proprio in questo contesto, dunque, il pacifico esercizio della libertà d'espressione viene posto in crisi dalla presenza di *always-on devices,* come quelli sopra descritti, che popolano la città del futuro. Sebbene una parte della letteratura ritenga che tali meccanismi possano persino aumentare la partecipazione dei cittadini – si pensi alla circolazione di piattaforme di *e-voting* – d'altro canto preoccupano le possibili intrusioni e l'inasprimento di perduranti situazioni iniquità e discriminazione.

Il far passare l'esercizio delle libertà democratiche attraverso strumenti digitalizzati porta alla luce un grave problema di *digital literacy*, da un lato, e, dall'altro, la creazione dei c.d. *chilling effects.* In particolare, allo stato del-

---

[68] Il tema è stato ampiamente approfondito in O. POLLICINO, *Judges and Freedom of Expression: From Atoms to Bits Across the Atlantic*, in *Judicial Protection of Fundamental Rights*, Oxford (UK), 2021, pp. 51-98.

[69] Si veda, ad esempio, la decisione della Corte Europea dei Diritti dell'Uomo, 13ª sezione, Stern Taulats and Roura Capellera v. Spain, Application no. 51168/15 e 51186/15; Decisione della Corte Europea dei Diritti dell'Uomo, 5ª Sezione, Z.B. v. France, Application no. 46883/15, decisione del 2 settembre 2021.

[70] Questo concetto emerge nella pronuncia *Stern Tautlas v. Spain*, ove al par. 30 la Corte si è espressa in questi termini: «*La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun. Sous réserve du paragraphe 2 de l'article 10 de la Convention, elle vaut non seulement pour les "informations" ou les "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent: ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratique" (Handyside c. Royaume-Uni, 7 décembre 1976, § 49, série A no 24, et Lindon, Otchakovsky-Laurens et July c. France [GC], nos 21279/02 et 36448/02, § 45, CEDH 2007-IV). Telle que la consacre l'article 10 de la Convention, la liberté d'expression est assortie d'exceptions qui appellent toutefois une interprétation étroite, et le besoin de la restreindre doit se trouver établi de manière convaincante*».

l'arte, l'educazione alla digitalizzazione è ancora un problema parzialmente irrisolto, così come l'accesso alle stesse e a Internet [71]. Lo stesso impiego di queste tecnologie, indipendentemente dal grado di connettività della popolazione, a causa della mancanza di equità degli algoritmi, può, come si premetteva, radicare ancor di più determinate disuguaglianze. Tali tecnologie, riflettendo inevitabilmente scelte etiche e politiche e tendenze storiche, effettuano dei giudizi di valore [72] col rischio di acerbare l'esclusione di minoranze, non solo dall'utilizzo del mezzo tecnologico, ma anche dalla partecipazione alla *res publica.* Di conseguenza, e con riguardo al secondo aspetto, la struttura stessa della città intelligente è in grado di provocare un *vulnus* alle libertà fondamentali di tipo, ad esempio, associativo. In particolare, si prefigura il rischio di c.d. *chilling effects* [73]: una modificazione delle abitudini individuali per evitare di sottostare all'occhio indiscreto di una telecamera, pur di tutelare la riservatezza personale. Peraltro, la sempre maggiore presenza di attori privati nel triangolo della libertà d'espressione complica ulteriormente il quadro, non solo nel lato passivo, ma anche attivo dell'esercizio di tali libertà. Pertanto, sebbene la rete costituisca una possibilità di sviluppo della *smart city* e di integrazione per il cittadino, quest'ultima pone, allo stesso tempo, diverse sfide per i diritti fondamentali per via della riduzione degli spazi privati dei cittadini che rischia di condurre ad uno sgretolamento della distinzione tra spazi pubblici e privati. Su tale aspetto dovrà imperniarsi l'intera sfida di *governance* statale che, oltre a tener conto dei rischi alla sicurezza e alla riservatezza, dovrà senza dubbio guardare all'impatto sui diritti e le libertà fondamentali nel redigere *policy* che siano in grado di traghettare il cittadino verso lo spazio urbano *smart.*

3.1. (Segue) *Una sfida per il legislatore europeo*

Alla luce della panoramica che si è data e che finora ha toccato la *privacy*, la protezione dei dati personali, e la libertà d'espressione, risulta che le sfide che il legislatore dovrà affrontare sono numerosissime e dovranno essere sostenute da un apparato di *policy* che tenda alla ricerca della complementarità

---

[71] A tal riguardo, si rimanda al ricco dibattito sul tema, alimentato, *ex multis,* da M.R. ALLEGRI, G. D'IPPOLITO (a cura di), *Accesso a Internet e neutralità della Rete, tra principi costituzionali e regole europee*, Roma, 2017.

[72] F. PASQUALE, *The Black Box Society,* Cambridge, MA, 2015.

[73] M. BÜCHI, *Chilling Effects of Profiling Activities: Mapping the Issues*, in *Computer Law & Security Review,* vol. 36, 2020.

della città intelligente con i principi fondamentali, onde evitare la creazione di antinomie. Quest'ultime preoccupano non solo dal punto di vista dei diritti individuali, ma anche per le conseguenze sul mercato digitale.

A tal proposito, come si menzionava all'inizio, l'Unione Europea ha attività delle iniziative anche in tal senso. Una di queste è il regolamento sui mercati digitali, o Digital market act (DMA), gemello del Digital service act[74]. Essa consiste in una iniziativa legislativa volta a garantire un mercato unico competitivo per i servizi digitali e, in particolare, mercati delle piattaforme equi e contendibili. Difatti, equità (*fairness*) contendibilità (*contestability*) dei mercati digitali sembrano essere le due parole chiave su cui si appunta l'intera normativa[75]. Nonostante il plauso con cui tale iniziativa è stata accolta, in quanto va a regolamentare l'incidenza fortissima dei *gatekeeper*[76], ossia quelle piattaforme *online*, affermatesi come elementi strutturali dell'economia digitale, divenendo intermediari tra consumatori e imprese, creando distorsioni di mercato prive di autocorrezione.

Il collegamento di questa normativa con il tema in oggetto è quanto mai tautologico. Come più volte si è detto, il ruolo dei dati e, dunque, delle imprese che hanno fatto di questi il loro *core business,* sono asset essenziali nella città *smart*[77]. D'altro canto, però, i medesimi possono rafforzare situazione di

---

[74] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[75] Si vedano i Considerandi 28 e 32.

[76] Art. 3, definizione di *gatekeeper*: «a. Un fornitore di servizi di piattaforma di base è designato come gatekeeper se: a) ha un impatto significativo sul mercato interno; b) gestisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; c) detiene una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro. 2. Si presume che un fornitore di servizi di piattaforma di base soddisfi: a) il requisito di cui al paragrafo 1, lettera a), se l'impresa cui appartiene raggiunge un fatturato annuo nel SEE pari o superiore a 6,5 miliardi di EUR negli ultimi tre esercizi finanziari, o se la capitalizzazione di mercato media o il valore equo di mercato equivalente dell'impresa cui appartiene era quanto meno pari a 65 miliardi di EUR nell'ultimo esercizio finanziario, e se esso fornisce un servizio di piattaforma di base in almeno tre Stati membri; b) il requisito di cui al paragrafo 1, lettera b), se fornisce un servizio di piattaforma di base che annovera nell'ultimo esercizio finanziario più di 45 milioni di utenti finali attivi mensilmente, stabiliti o situati nell'Unione, e oltre 10 000 utenti commerciali attivi annualmente stabiliti nell'Unione; ai fini del primo comma, con utenti finali attivi mensilmente si fa riferimento al numero medio di utenti finali attivi mensilmente nel corso della maggior parte dell'ultimo esercizio finanziario; c) il requisito di cui al paragrafo 1, lettera c), se le soglie di cui alla lettera b) sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari».

[77] Tale aspetto era stato inizialmente riconosciuto nel DMA nel Considerando 36. Il riferimento, tuttavia, non è sopravvissuto agli emendamenti del legislatore europeo.

monopolio che consentono il governo del mercato digitale e, per converso, della città digitale. Orbene, nonostante il legislatore europeo abbia dato avvio a quest'opera di regolazione, come evidenziano taluni commentatori[78] un aspetto di cruciale importanza è stato trascurato. Il DMA ragiona attorno a un concetto di internet fatto di persone e non di cose. In altre parole, manca di guardare oltre la staccionata dove vi sono importanti novità strutturali della rete, tra cui il 5G, le quali avranno un feroce impatto su taluni settori dell'internet delle cose, come l'*automotive,* che hanno bisogno di una rete infrastrutturale solidissima, anche dal punto di vista della cybersicurezza[79]. Difatti, uno dei principali aspetti della *smart city* riguarda proprio la gestione del traffico[80], su cui si basano i servizi che vengono già resi da taluni *player*, quale Google Maps. Ebbene, il fatto che il DMA non si interroghi sulla tenuta della struttura proposta rispetto al già annunciato avvento di nuovi servizi, nuove piattaforme e quindi nuovi *gatekeepers*, è un aspetto problematico che evidenzia la mancanza di una visione prospettica che possa declinare al futuro il paradigma europeo, non solo dei dati personali.

Inoltre, la proposta di Regolamento non contiene alcun riferimento a concetti quali la nuova generazione di reti-servizio di oggetti connessi, pur imponendo, però, la garanzia di interoperabilità e portabilità dei sistemi sulla falsariga di quanto già previsto dal GDPR[81]. In breve, tali soluzioni non permettono di soffermarsi adeguatamente sul controllo e sull'utilizzo effettivo dei dati, tema chiave nel mercato digitale, e, ancor più, nella città digitale. Dette problematiche, necessitano, anche alla luce dell'estesa ricostruzione che si è fatta del modello europeo della *privacy*, di essere esaminate nella prospettiva del potere digitale, ossia della sovranità tanto statale dei dati (e di coloro che li detengono). Il DMA, così come altre iniziative, non guarda al controllo dei dati. O meglio, pare esserci un conflitto tra controlli legittimamente reclamabili: da

---

[78] M. POLO, A. SASSANO, *Dma: Digital Markets Act o Digital Markets Armistice?*, in *Mercato Concorrenza Regole*, 3, 2021.

[79] H. OLUFOWOBI, G. BLOOM, *Connected cars: Automotive cybersecurity and privacy for smart cities,* in *Smart cities cybersecurity and privacy*, Elsevier, 2019, pp. 227-240.

[80] A tal riguardo, si rimanda all'esempio di Venezia, come analizzato da F. MENEGHETTI, C. CARLO ROSSI CHAUVENET, G. FIORONI, *Rapporto 3/2022 – SMART cities e intelligenza artificiale*, in *BioLaw*, 1, 2022.

[81] Non ci si può ivi soffermare sulla criticità di garantire portabilità e interoperabilità, già ampiamente riscontrate nel settore. Si rimanda a J. WONG, T. HENDERSON, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, in *International Data Privacy Law*, Vol. 9, No. 3, 2019, come pure a M. POLO, A. SASSANO, *Dma: Digital Markets Act or Digital Markets Armistice?,* cit.

un lato, quello dell'interessato sui propri dati personali, e, dall'altro quello delle imprese sui dati, spesso non personali, che consentono il loro funzionamento. Tali dati sono altresì espressivi della realizzazione di due diritti contrapposti: la protezione dei dati, e la libertà d'impresa.

Il conflitto tra controllo e circolazione, tra artt. 7 e 8, e 16 della Carta di Nizza, si inserisce nel tema della regolazione del mercato digitale, ma anche in quello dell'intelligenza artificiale. In definitiva, quel che manca è un ponte tra *governance* dei dati personali e quella dei dati non-personali, con la conseguenza di amplificare il conflitto tra interessi contrapposti e opposti. Allo stato dell'arte, i due sistemi sono "*lost in translation*" e questo ponte mancante minaccia direttamente i diritti umani delle persone e lo sviluppo sicuro dei sistemi di apprendimento automatico. Le leggi europee sulla protezione dei dati, astrattamente il miglior modello possibile, si rivelano spesso inadeguate a fornire in concreto una protezione adeguata e duratura.

Si crede, dunque, che sia questa la principale sfida che dovrà affrontare il legislatore europeo, non solo nello spirito di garantire un efficace sviluppo della *smart city*, a prova di diritti. Occorre altresì che tale sviluppo comprenda proprio tutti gli interessi in gioco e consenta la comunicabilità dei sistemi di *governance* che vengono tutti toccati dalla rivoluzione digitale. In secondo luogo, è richiesto l'individuazione di un sistema su cui basare tale nuova collaborazione tra gli attori pubblici e privati. Senza alcuna pretesa di esaustività, dato l'immenso dibattito sul tema [82], si ritiene quanto mai necessario incorporare i valori dei diritti costituzionali sin dalla fase di progettazione delle macchine, e, per estensione, della città *smart*. Per tal ragione, è richiesto al costituzionalista di avvicinarsi alle necessità del digitale e di creare una nuova dimensione in cui l'*humus* sostanziale sia quello dei diritti umani fondamentali tradotto nel linguaggio della tecnologia.

La mancanza di questo processo di ibridazione, è di tutta evidenza in alcuni, seppur importanti, sforzi della Commissione Europea, ove nella proposta di Regolamento dell'Intelligenza Artificiale ancora manca una comunicazione effettiva tra problematiche tecnologiche e accentramento del focus sulla figura umana [83]. Pertanto, la sfida si situa nella costruzione di una cornice normativa che sia in grado di sostenere gli obiettivi del mercato unico e, d'altro canto,

---

[82] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, vol. 19, n. 1, 2020, pp. 41-70; M.F. Cuéllar, A.Z. Huq, *Toward the Democratic Regulation of AI Systems: A Prolegomenon*, in *U. of Chicago, Public Law Working Paper*, n. 753, 2020.

[83] L. Floridi, *The European Legislation on AI: A brief analysis of its philosophical approach*, in *Philosophy & Technology*, vol. 34, n. 2, 2021, pp. 215-222.

che sia tutelante dei valori europei, quali il principio della *rule of law*, la protezione dei diritti fondamentali, la dignità umana.

L'Europa sembra aver compiuto alcuni passi al fine di trovare un bilanciamento tra innovazione e tutela dei diritti. Favorendo, dunque, lo sviluppo di un tale modello, si potrebbe fondare una catena preziosa, capace di spingere verso un mercato del digitale che ricomprenda la scala valoriale dell'UE. Infatti, dall'entrata in vigore del GDPR, l'Unione Europea si è imposta nel settore come un importante attore, consentendo all'*acquis* comunitario di definire proporre un modello del quale la *privacy* rappresenta il Primo Emendamento [84].

Accanto alla collaborazione e alla *policy* «*by education* [85]», è necessario pensare a modelli pratici di interazione. Queste misure assomiglieranno meno agli strumenti di *policy* coercitiva del ventesimo secolo e più ai modelli di prevenzione e controllo apparentemente consensuale che si trovano anche nella *soft law*. Poiché molti degli strumenti di *policy* delle *smart city* saranno stati sviluppati con la collaborazione dei privati, in uno spazio in cui è sempre più difficile distinguere tra ciò che non è pubblico e ciò che lo è, ci saranno maggiori difficoltà nel mantenere una visione della *policy* urbana imposta e non ragionata [86]. Si ritiene, in conclusione, che la *data driven regulation* [87] debba essere continuamente assistita da un'analisi di impatto che abbia il suo fondamento nei diritti fondamentali dei cittadini [88]. Una realtà la cui concretizzazione si au-

---

[84] B. PETKOVA, *Privacy as Europe's First Amendment: A Brief Analysis of its Philosophical Approach*, cit.

[85] A. SIMONCINI, E. LONGO, *Fundamental Rights and the Rule of Law in the Algorithmic Society,* in H.-W. MICKLITZ, O. POLLICINO, A. REICHMAN, A. SIMONCINI, G. SARTOR, G. DE GREGORIO, *Constitutional Challenges in the Algorithmic Society*, Oxford (UK), 2021.

[86] E. JOH, *Policing the Smart City*, in *International Journal of Law in Context*, vol. 15(2), 2019, pp. 177-182.

[87] S. RANCHORDAS, A. KLOP*, Data-Driven Regulation and Governance in smart cities*, in A. BERLEE, V. MAK, E. TJONG TJIN TAI (a cura di), *Research Handbook on Data Science and Law*, Groningen, 2018.

[88] Si veda, a tal proposito, la Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adottata dal Council of Europe l'8 aprile 2020, ove al punto 14 si legge che: «*the design, development and ongoing deployment of algorithmic systems involves many actors, including software designers, programmers, data sources, data workers, proprietors, sellers, users or customers, providers of infrastructure, and public and private actors and institutions. In addition, many algorithmic systems, whether learning or non-learning, operate with significant levels of opacity, sometimes even deliberately. Even the designer or operator, who will usually establish the overarching aim and parameters of the system, including the input data, the optimisation target and the model, will often not know what information the system relies upon to make its decision, and is likely to encounter uncertain-*

spica non attenda la posa della prima pietra della città intelligente, ma che possa essere recepita nel design delle tecnologie, in particolare, quelle automatizzate, già ampiamente presenti nella realtà atomica e digitali dell'oggi.

4. *Conclusione*

La *smart city* rappresenta l'unione di una serie di difficoltà cui il diritto costituzionale, e, per converso, la protezione delle libertà fondamentali sono già ampiamente sottoposte nell'ambito della digitalizzazione. A partire, dunque, da una cornice generale ove si è cercato di porre in evidenza come i diritti individuali vengono messi ulteriormente in discussione nell'assetto della città intelligente, l'analisi ha riguardato nel particolare la sfida posta al sistema della *privacy* europeo, guardando precisamente all'estensione di questo modello anche al di fuori dell'ambito comunitario. In secondo luogo, alla luce delle difficoltà emerse, si è osservato come in questo spazio dove i confini tra pubblico e privato sono sempre più labili, il legislatore è chiamato ad assumere un ruolo prospettico, onde evitare una stagnazione in modelli normativi e tecnologici che faticano a stare al passo dell'evoluzione del digitale. Si tratta di uno "stress test" provocato dall'annessione di sensori e tecnologie intelligenti nell'ambiente urbano, cui il giurista è chiamato a rispondere con una straordinaria capacità di adattamento che tenga conto delle necessità di un ambiente in cui pubblico e privato sono necessariamente posti su piani inediti.

A ben vedere, sono argomenti che si inquadrano nel più ampio spettro delle problematiche provocate dalla digitalizzazione e con cui il diritto ha avuto a che fare negli ultimi dieci anni. In quest'ottica, la *smart city,* se ben regolata per tempo, non rappresenta assolutamente un'antinomia per il diritto, potendosi ben individuare nuovi sistemi di *governance,* ove pubblico e privato devono necessariamente collaborare. La *compliance* imposta dall'uno a scapito dell'altro non dovrà sostanziarsi in un sistema unilaterale di limiti, ma dovrà bensì guardare all'integrazione e all'innovazione di differenti sistemi bilanciando rischi e opportunità. In definitiva, sarà necessario sviluppare modelli di *smart city* idonei a garantire una *governance* trasparente, inclusiva, capace di sviluppare una visione chiara e condivisa del benessere, della qualità della vita e della sostenibilità [89].

---

ty about the direct and indirect effects of the system on users and the broader environments in which these systems are intended to operate».

[89] F. TONI, *Smart city: innovazione e sostenibilità*, cit.

«*Siamo chiamati a essere costruttori non vittime del futuro*», scriveva Fuller [90]. Volendo far tesoro di questo monito, si crede che l'Europa, più di altri attori, appaia assolutamente in grado di poter guardare al futuro e poter guidare la creazione di un nuovo modello regolatorio [91], non solo con riguardo al tema della *smart city*, ma senza commettere l'errore di ricadere in modelli stagnanti. Assumendo come faro la dignità umana e il rispetto di principi e diritti fondamentali, si potrà realizzare un ambiente in cui prevale la complementarità tra tecnologia e diritto, tra innovazione e protezione.

[90] R. BUCKMINSTER FULLER, K. KUROMIYA, *Cosmography. A posthumous scenario for the future of humanity,* New York, 1992, p. 8.

[91] In tal senso, si ricorda non solo il menzionato AI Act, ma anche la European Data Strategy, di cui il nodo centrale è rappresentato dal *Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data*, meglio noto come Data Act (COM(2022) 68, proposta pubblicata il 23 febbraio 2022), norma con la quale si andranno a rivedere anche taluni aspetti della Database Directive, ossia la Direttiva 96/9/EC. Tali proposte *policy* vanno, per l'appunto, nella direzione di stabilire un unico quadro di *governance* intersettoriale per l'uso di dati, sia da parte dei privati sia da parte degli attori pubblici.

PARTE II
POLITICHE E ISTITUZIONI

IL SERVIZIO PUBBLICO NELL'AMBITO DELLA CITTÀ INTELLIGENTE: CRISI DI UN CONCETTO TRADIZIONALE?

di *Nicolò Acquarelli*

SOMMARIO: 1. Considerazioni introduttive. – 2. La *smart city*: elementi costitutivi della fattispecie. – 3. Il "servizio pubblico" all'interno della *smart city*. Criticità. – 4. Conclusioni: il ruolo (centrale) delle istituzioni pubbliche nella città intelligente.

1. *Considerazioni introduttive*

Il modello di sviluppo urbano legato ai canoni della *smart city* implica, per la sua attuazione, interventi diretti anche alla riorganizzazione dei servizi pubblici. Difatti, una città intelligente, per dirsi tale, deve tendere a migliorare la qualità della vita umana anche mettendo a disposizione dei suoi cittadini servizi sostenibili e innovativi, erogati attraverso il ricorso alle tecnologie dell'informazione e della comunicazione (TIC) e calati sui bisogni specifici degli utenti [1]. Un nuovo approccio al tema dei servizi pubblici che deve essere posto in relazione con l'idea classica di pubblico servizio, per come storicamente affermatasi nel panorama del diritto amministrativo [2].

---

[1] Si legge, sul sito istituzionale della Commissione Europea, che la *smart city* «*is a place where traditional networks and services are made more efficient with the use of digital solutions for the benefit of its inhabitants and business*» (la pagina *web* è disponibile all'indirizzo: *https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en*).

[2] Il servizio pubblico rappresenta, del resto, un "concetto tradizionale" del diritto amministrativo. Rilevano D. SORACE, S. TORRICELLI, *Diritto delle amministrazioni pubbliche. Una introduzione*, Bologna, 2021, p. 105 che «*già dalla fine del secolo XIX il concetto di* service public *era stato associato dalla giurisprudenza al diritto amministrativo (con la sentenza Blanco del Tribunale dei conflitti del 1873) e poi, per l'influenza avuta dal pensiero di grandi giuristi come Duguit, all'idea stessa di Stato in senso costituzionale*».

L'obiettivo delle osservazioni che seguono sarà, allora, quello di verificare se possa trovare spazio, all'interno della *smart city*, il "servizio pubblico", inteso in senso tradizionale, come insieme di prestazioni tendenzialmente standardizzate (salva l'ipotesi dei servizi sociali[3]), organizzate dalla pubblica amministrazione e messe a disposizione della platea degli utenti senza discriminazioni e interruzioni[4].

Per far ciò sarà necessario individuare, in primo luogo e seppur sommariamente, gli elementi che concorrono alla definizione del concetto di *smart city*, pur consapevoli che, rispetto alla città intelligente, non si individua una definizione che possa dirsi realmente condivisa.

Dopo aver delineato la fattispecie sarà possibile verificare se la nozione tradizionale di "servizio pubblico" appena sintetizzata sia conciliabile con i canoni della città intelligente o se non si registrino, all'opposto, alcuni profili di incompatibilità. Saranno, invero, questi ultimi a emergere, sino a investire anche la figura dell'utente che, all'interno della città *smart*, vede mutare il proprio ruolo, passando da destinatario passivo di servizi erogati da terzi a soggetto attivamente coinvolto nell'attività di prestazione.

Proprio la rinnovata veste assunta dalla persona fisica dell'utente all'interno della *smart city* consentirà di condurre una riflessione conclusiva sul ruolo riservato, nella città *smart*, alle istituzioni pubbliche, ruolo di indubbio rilievo, nell'ottica di evitare che lo spazio urbano intelligente, piuttosto che tendere a incrementare la qualità di vita di chi lo abita, inneschi dinamiche escludenti e discriminatorie.

2. *La* smart city*: elementi costitutivi della fattispecie*

Come anticipato, la *smart city* sconta una certa incertezza definitoria, anche in ragione di un formante normativo che ancora non ha chiarito quali debbano essere i suoi tratti caratterizzanti[5]. Nondimeno, al fine di verificare se il

[3] I cui elementi caratterizzanti sono, all'opposto, l'individualizzazione e la personalizzazione degli interventi (v., *ex multis*, A. ALBANESE, *Diritto all'assistenza e servizi sociali. Intervento pubblico e attività dei privati*, Milano, 2007, spec. p. 137 ss.; V. MOLASCHI, *Sulla nozione di servizi sociali: nuove coordinate costituzionali*, in *Dir. econ.*, 2004, p. 95 ss.).

[4] Secondo i principi di *égalité* e *continuité* che, unitamente al canone della *mutabilité*, danno corpo alla c.d. "*lois de Rolland*" (v. L. ROLLAND, *Précis de droit administratif*, Paris, 1957, p. 18).

[5] Sono invece richiamate (ma, comunque, non definite) le "*comunità intelligenti*", all'art. 20, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221.

"servizio pubblico" sia in grado di integrare gli elementi costitutivi della città *smart*, si possono isolare alcuni aspetti ritenuti dalla dottrina identificativi del fenomeno [6].

Anzitutto, la città intelligente utilizza le nuove tecnologie nella fornitura dei servizi alla platea degli utenti. L'uso delle TIC rappresenta, anzi, il minimo comune denominatore di tutte le iniziative che confluiscono nell'ambito operativo della *smart city* [7], sicché l'attività di prestazione che prescinda dal loro impiego è del tutto estranea al fenomeno della città intelligente.

In secondo luogo, la città *smart* postula una generazione dal basso delle iniziative che vi confluiscono [8], incentrandosi, in buona sostanza, sul principio di sussidiarietà orizzontale di cui all'art. 118, comma 4, Cost. [9]. Nella *smart city* si dovrebbe [10], dunque, assistere a un processo di innovazione ascensionale (*bottom-up*) innescato dall'iniziativa degli operatori privati, con le istituzioni pubbliche tenute, esclusivamente, a dettare la cornice normativa al cui interno contenere questo "moto dal basso".

Infine, la città intelligente sposa la logica della condivisione, per il tramite della messa in comune di spazi, prestazioni, tecnologie e, soprattutto, di un complesso di informazioni.

Impiego delle TIC, sussidiarietà orizzontale e condivisione rappresentano, dunque, gli architravi su cui si fonda la *smart city* e rispetto ai quali è necessario verificare la compatibilità, con il paradigma della città intelligente, del concetto di "servizio pubblico".

---

[6] Sul punto cfr., tra gli altri, G. DELLE CAVE, *«Comunità intelligenti», enti locali, mobilità sostenibile: le* smart city *al cospetto del potere pubblico*, in *Dir. econ.*, 2021, p. 385 ss.; P. PANTALONE, M. PIACENTINI, *Smart city, tecnologia e mercato: quale ruolo per i pubblici poteri?*, in *diritto24.it*, 2020.

[7] F. FRACCHIA, P. PANTALONE, *Smart City: condividere per innovare (e con il rischio di escludere?)*, in *federalismi.it*, 22/2015, p. 10.

[8] G. DELLE CAVE, «*Comunità intelligenti*», cit., p. 386.

[9] V. diffusamente sul punto G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, in *Ist. fed.*, 2019, p. 463 ss. che accosta l'aggettivo "intelligente" esclusivamente alla città che, attraverso gli strumenti tecnologici, consente la partecipazione in chiave sussidiaria dei cittadini.

[10] L'impiego del condizionale tradisce la distanza tra l'idealtipo che si sta descrivendo e la realtà, ove, all'approccio *bottom-up* tipico dei paesi anglosassoni, si affianca un diverso modello di attuazione della città *smart* (*top-down*) tipico dei paesi europei. In quest'ultimo caso, è il potere pubblico a ricoprire un ruolo centrale nel determinare le linee di intervento necessarie per garantire ai consociati un ecosistema *smart*. Sulla contrapposizione tra questi due modelli v., per tutti, F. GASPARI, *Città intelligenti e intervento pubblico*, in *Dir. econ.*, 2019, p. 71 ss., spec. p. 75 ss.

3. *Il "servizio pubblico" all'interno della* smart city. *Criticità*

Alla luce del quadro appena tratteggiato è possibile, in verità, registrare alcuni disallineamenti che rischiano di mettere in crisi il pubblico servizio calato all'interno dello spazio urbano intelligente.

Una prima frizione riguarda l'organizzazione pubblica del pubblico servizio. È ben noto come quest'ultima si articoli in una prima fase, l'assunzione, frutto della decisione politica di farsi carico del soddisfacimento di particolari bisogni dei cittadini che il mercato non riesce a soddisfare, cui segue la regolazione del servizio e, infine, la sua gestione da parte della pubblica amministrazione o di soggetti a essa estranei [11].

All'interno della *smart city*, però, non si chiede al potere pubblico di mettere a disposizione della cittadinanza un'offerta di prestazioni, quanto, piuttosto, di consentire alle iniziative nate in seno alla società di esprimersi al meglio per soddisfare i bisogni dei consociati. Si prenda il caso della domanda di trasporto. Se, per soddisfarla, l'amministrazione organizza un servizio pubblico di linea, si fuoriesce dal perimetro della città intelligente per come tratteggiato in precedenza. Ciò non accade, invece, nel caso in cui la p.a., al fine di rispondere alla domanda di mobilità, incentivi, per esempio, l'iniziativa di soggettivi privati che organizzano servizi riconducibili alla c.d. *shared mobility*, magari limitandosi a regolarne l'esercizio per evitare un impatto negativo sulla circolazione stradale o sulla sicurezza urbana [12].

Un secondo disallineamento ha per oggetto le prestazioni che danno corpo al servizio pubblico.

Si è già visto che il pubblico servizio, tradizionalmente inteso, e salva l'ipotesi dei c.d. "servizi alla persona", si compone di un complesso di prestazioni di natura standardizzata, erogate per soddisfare esigenze sufficientemente omogenee degli utenti.

---

[11] Cfr., al riguardo, M. CLARICH, *Manuale di diritto amministrativo*, Bologna, 2022, spec. p. 365 ss. Sull'assunzione, regolazione e gestione del pubblico servizio v. anche il parere del Cons. Stato, sez. I, 7 maggio 2019, n. 1389.

[12] Come accaduto nel caso affrontato dalla sentenza del TAR Lombardia, Milano, sez. III, 3 luglio 2020, n. 1274. Il giudice amministrativo ha escluso che servizi di mobilità *in sharing* con dispositivi per la micromobilità elettrica potessero integrare la figura del "servizio pubblico", mancando il fondamentale momento dell'assunzione, ossia l'intento politico di soddisfare il bisogno dei cittadini di spostarsi sul territorio tramite l'uso di *hoverboard*, *segway*, monopattini elettrici e *monowheel*. L'amministrazione comunale aveva, infatti, ritenuto necessario regolare l'attività di noleggio di questi dispositivi solo in ragione dell'aumentare dei soggetti privati che spontaneamente avevano iniziato a erogare il servizio in modalità *free floating*, per evitare un suo svolgimento in maniera pericolosa o disordinata.

Nell'ambito della città *smart* questo paradigma muta.

Le potenzialità offerte dall'impiego delle nuove tecnologie nell'erogazione dei servizi consentono di calare sempre di più le prestazioni sui reali bisogni degli utenti, marcando una netta differenza rispetto alla richiamata idea di pubblico servizio come insieme di misure standard da garantire alla totalità dei fruitori. È emblematico, a tal proposito, il caso delle reti intelligenti (c.d. *smart grids* [13]) riferibili, soprattutto, ai servizi energetici e idrici [14]. Queste ultime, oltre a permettere agli utenti di produrre energia da fonti rinnovabili per l'autoconsumo o lo scambio in rete, consentono la trasmissione ai fornitori del servizio, mediante i contatori intelligenti (c.d. *smart meters*), delle informazioni relative al fabbisogno dei singoli fruitori, sì da consentire un'offerta personalizzata ed efficiente [15]. Naturalmente, il prezzo da pagare per avere accesso a un servizio del genere è la fornitura di una ingente mole di dati personali che rischiano di compromettere il diritto alla riservatezza di ogni singolo utente, se solo si pensa che le informazioni trasmesse dagli *smart meters* consentono di ricostruire, senza troppe difficoltà, le abitudini di vita dei destinatari del servizio (come impiegano il proprio tempo libero, quali apparecchi elettronici utilizzano, ecc.). È evidente che la questione si innesta nella più ampia problematica di garantire la corretta gestione dei dati personali in un contesto, quello della *smart city*, che non può prescindere – come visto – anche dalla condivisione delle informazioni [16].

Ulteriori profili di incompatibilità fra l'idea tradizionale di pubblico servi-

---

[13] Ossia «*qualsiasi attrezzatura, linea, cavo o installazione, a livello di trasmissione e distribuzione a bassa e media tensione, destinati alla comunicazione digitale bidirezionale, in tempo reale o quasi reale, al controllo e alla gestione interattivi e intelligenti della produzione, trasmissione, distribuzione e del consumo di energia elettrica all'interno di una rete elettrica in vista dello sviluppo di una rete che integri in maniera efficace il comportamento e le azioni di tutti gli utenti collegati a essa (produttori, consumatori e produttori-consumatori) al fine di garantire un sistema elettrico efficiente dal lato economico e sostenibile, che limite le perdite e offra un livello elevato di qualità e di sicurezza dell'approvvigionamento e della protezione*» (art. 2, par. 130, lett. a), Reg. UE n. 651/2014). Sul fenomeno delle *smart grids* v., per tutti, F. GIGLIONI, *La sfida dell'innovazione sulla regolazione pubblica. Il caso delle* smart grid, in *Munus*, 2013, p. 463 ss.

[14] Tutt'ora «enfatizzat[e] quale emblema della *smart city*» (così T. FAVARO, *Verso la* smart city*: sviluppo economico e rigenerazione urbana*, in *Riv. giur. edil.*, 2020, p. 117), le *smart grids* paiono, invero, non soddisfare pienamente il principio di sussidiarietà orizzontale nella misura in cui l'utilizzo delle reti si fonda su un previo provvedimento concessorio rilasciato al gestore.

[15] Si pensi, per esempio, alla possibilità offerta dalle *smart grids* di minimizzare sovraccarichi o, più in generale, variazioni della tensione elettrica.

[16] Sulla tutela dei dati personali all'interno della città intelligente cfr., in particolare, A. VENANZONI, *Smart cities e capitalismo della sorveglianza*, in *Forum di quaderni costituzionali*, 20 ottobre 2019; J. VALERO TORRIJOS, *Ciudades inteligentes y datos abiertos: implicaciones jurìdicas para la protección de los datos de carácter personal*, in *Ist. fed.*, 2015, p. 1025 ss.

zio e le prestazioni erogate all'interno della città *smart* si hanno, poi, rispetto alla fruizione senza discriminazioni del servizio e alla sua erogazione in modo continuativo.

Sul primo versante, l'impiego delle nuove tecnologie rischia di precludere l'accesso al servizio pubblico ai cittadini che non siano sufficientemente *smart*. È la nota problematica del *digital divide*, che concerne sia la carenza di adeguate competenze digitali da parte dei cittadini – la dimensione culturale del divario digitale –, sia la disponibilità della connessione o il ritardo nelle dotazioni digitali dovuto alle sfavorevoli condizioni economiche degli utenti (aspetti che si legano al profilo tecnico-economico del *digital divide*) [17]. Entrambe le richiamate dimensioni del fenomeno finiscono, dunque, per rappresentare una barriera nell'accesso ai servizi erogati tramite le TIC, sia per gli analfabeti digitali sia per quella parte della popolazione che, in ragione della scarsa copertura di rete o per motivazioni economiche, non può impiegare (o avere accesso a) i dispositivi elettronici [18].

Quanto, invece, alla continuità del servizio pubblico, si può osservare come questa possa essere potenzialmente pregiudicata dalla personalizzazione dell'offerta di servizio cui si è fatto in precedenza riferimento. La possibilità di rendere prestazioni adeguate agli specifici bisogni dei cittadini rende, difatti, più arduo il controllo sulla fornitura ininterrotta delle prestazioni, rispetto a quanto accade nel caso in cui un servizio sia erogato in modo rigido e centralizzato.

Si riprenda, per chiarire questo aspetto, il caso delle *smart grids*. La diffusione delle reti intelligenti consente al fruitore del servizio di avere un più ampio spettro di scelte circa le fonti di energia di cui approvvigionarsi (quella autoprodotta, quella messa a disposizione dai distributori, ecc.) e, conseguentemente, di beneficiare di prestazioni rispondenti alle proprie reali esigenze. Ciò, però, rischia di ostacolare la verifica in ordine alla continuità del servizio: la domanda diversificata degli utenti per la cui soddisfazione gli stessi possono

---

[17] Esamina i singoli aspetti caratterizzanti il *digital divide*, anche alla luce degli effetti prodotti dall'emergenza pandemica da Covid-19, P. ZUDDAS, *Covid-19 e* digital divide*: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio costituzionale*, 2020, p. 285 ss.

[18] Rischi amplificati dal confronto con i dati relativi al divario digitale in Italia. Per esempio, nel rapporto DESI (*Digital Economy and Society Index*) 2021, che rileva i progressi compiuti dai singoli Stati appartenenti all'Unione europea in punto di digitalizzazione, l'Italia si colloca al 20esimo posto fra i 27 Stati membri, con particolari criticità soprattutto rispetto alle competenze digitali. Si legge, difatti, che «*l'Italia è significativamente in ritardo rispetto ad altri paesi dell'UE in termini di capitale umano. Rispetto alla media UE, registra infatti livelli di competenze digitali di base e avanzate molto bassi*». Il *report* riguardante l'ordinamento italiano è disponibile al seguente link: *https://ec.europa.eu/newsroom/dae/redirection/document/80590*.

attingere a fonti di energia differenziate, non programmate e diffuse rende, difatti, più difficile controllare la fornitura del servizio da parte dei gestori della rete di distribuzione [19].

I profili di incompatibilità tra l'idea tradizionale di "servizio pubblico" e la *smart city* che l'analisi sin qui condotta ha messo in luce si riverberano pure sulla figura del destinatario del servizio, ossia la persona fisica dell'utente. Quest'ultimo, nel contesto della città *smart*, dismette i panni del mero *consumer* per rivestire quelli del *prosumer*, di un soggetto non più fruitore meramente passivo di prestazioni ma che, all'opposto, è tenuto ad attivarsi per poter beneficiare di un servizio, oltre a diventare esso stesso erogatore di prestazioni [20]. Il pensiero va, ancora una volta, alle *smart grids*, alla trasmissione di dati mediante gli *smart meters* per poter avere accesso a una prestazione personalizzata, e alla possibilità che le reti intelligenti offrono ai privati di scambiare in rete l'energia autoprodotta, dando vita a «*forme finora inusitate di economia circolare*» [21].

È naturale che, per ricoprire il ruolo di *prosumer*, si richieda al cittadino di essere *smart* come il servizio di cui beneficia, di essere in possesso di competenze e strumenti necessari per svolgere quel ruolo attivo nell'attività di prestazione cui si è fatto riferimento. Non è un caso, allora, che una parte della dottrina abbia evidenziato come, all'interno della *smart city*, si assista, perfino, a uno «*slittamento verso il fruitore del carattere intelligente inizialmente riferito alla comunità*» [22]: pieno godimento di servizi *smart* solo per chi si dimostri altrettanto "intelligente".

4. *Conclusioni: il ruolo (centrale) delle istituzioni pubbliche nella città intelligente*

Pare, però, evidente (e, in parte, è già emerso nella trattazione) che la dinamica cui si è appena fatto riferimento possa essere foriera di pericolose forme di marginalità ed esclusione, nei confronti, per esempio, di chi eserciti la

---

[19] Sottolinea questo aspetto F. GIGLIONI, in *Ist. fed.*, 2015, p. 1049 ss., spec. p. 1064.

[20] Osserva E. CARLONI, *Città intelligenti e agenda urbana: le città del futuro, il futuro delle città*, in *Munus*, 2016, p. 249, come il concetto di *smart governance* comporti «l'attivazione degli *stakeholder* (specialmente i cittadini) ed il loro coinvolgimento nei processi decisionali e di fornitura dei servizi, che è centrale nelle nuove dinamiche».

[21] T. FAVARO, *Verso la* smart city, cit., p. 116.

[22] F. FRACCHIA, P. PANTALONE, *Smart City*, cit., p. 10.

propria libertà alla non condivisione di informazioni o di chi non sia tecnologicamente preparato per ergersi al ruolo di *prosumer*[23]. Del resto, «una città *smart*, se tale aggettivo evoca principalmente, quando non esclusivamente, il paradigma tecnologico, non sempre è, di per sé, una città giusta»[24]. Ciò, tuttavia, cozza con l'attuale visione della *smart city*: superata una concezione esclusivamente legata alla dimensione infrastrutturale, si è, adesso, consapevoli che la città è "intelligente" se fa ricorso alle TIC anche per conseguire risultati di inclusione sociale[25]. Sono prova di questo cambio di passo, per esempio, i tentativi di inquadrare diversamente il fenomeno dal punto di vista semantico, passando dalla *smart city* al diverso concetto di *human smart city*[26] o di *smart community*[27].

Una simile vocazione inclusiva non può, dunque, tollerare che, all'interno della città intelligente, si verifichino fenomeni discriminatori come quelli poco sopra richiamati. Nell'ottica di prevenirne la manifestazione emerge il ruolo centrale dei pubblici poteri, in ragione della missione, loro attribuita dal principio di eguaglianza sostanziale, di attivarsi per eliminare le diseguaglianze materiali esistenti all'interno della cittadinanza[28]. Sarà, pertanto, compito delle istituzioni pubbliche contrastare, per esempio, il *digital divide* mediante una serie di azioni volte a curare l'educazione digitale dei cittadini o a mettere nella loro disponibilità le infrastrutture e la strumentazione necessarie per avere accesso ai servizi erogati mediante le TIC[29]. Ma l'attore pubblico dovrà, anche, adottare politiche di sensibilizzazione verso le innovazioni legate all'avvento della *smart city*, evidenziandone benefici e criticità,

---

[23] Osserva E. OLIVITO, *(Dis)eguaglianza, città e periferie sociali: la prospettiva costituzionale*, in *RivistaAic.it*, 2020, 49 che, nella città intelligente, «i cittadini sono inclusi a condizione che condividano gli obiettivi e gli esiti della *smart city* e sempre che siano in grado di avvalersi delle tecnologie dell'informazione; essi restano invece ai margini di essa, se non aderiscono a tale paradigma o non sono nella condizione di poter usufruire delle relative risorse».

[24] C. ACOCELLA, G. LANEVE, *Città intelligenti e diritti: nuove prospettive di consumo nel prisma della socialità*, in *P.A. Pers. e amm.*, 2020, p. 105 s., spec. p. 127.

[25] V., per tutti, E. OLIVITO, *(Dis)eguaglianza*, cit., spec. p. 44 ss.

[26] S. BOLOGNINI, *Dalla "smart city" alla "human smart city" e oltre. Profili epistemologici e giuspolitici nello sviluppo del paradigma "smartness oriented"*, Milano, 2018.

[27] V., al riguardo, le osservazioni di S.A. FREGO LUPPI, *Note minime in tema di nuove forme di cittadinanza attiva tra demarchia e beni comuni nel contesto della* smart city, in *Amministrazione in Cammino*, 2016, spec. p. 12 ss.

[28] Cfr., sul punto, G.U. RESCIGNO, *Principio di sussidiarietà orizzontale e diritti sociali*, in *Dir pubbl.*, 2002, spec. p. 44 ss.

[29] V. al riguardo le osservazioni di F. GASPARI, *Smart city, agenda urbana multilivello e nuova cittadinanza amministrativa*, Napoli, 2018, spec. p. 45 ss.

sì da permettere ai singoli cittadini di esercitare consapevolmente i propri diritti nell'ambito dello spazio urbano intelligente [30].

Resta, semmai, da verificare se un simile attivismo delle istituzioni pubbliche sia compatibile con uno degli "assi portanti" della città intelligente, ossia il principio di sussidiarietà orizzontale; del resto, il principio in questione «*sul piano politico […] è stato voluto e viene sostenuto da molti proprio in opposizione al principio di eguaglianza sostanziale*» [31] la cui attuazione chiama, invece, in causa i pubblici poteri.

Questa possibile frizione pare, in verità, superabile tramite un'interpretazione del principio di sussidiarietà orizzontale coerente con l'intero assetto costituzionale.

In linea generale, la declinazione orizzontale del principio implica una preferenza nei confronti delle attività svolte dai soggetti privati per la soddisfazione dei fini individuati dai pubblici poteri [32], legandosi «*a un principio di antica data, quello per cui l'intervento pubblico si legittima solo sul presupposto che, altrimenti, certi bisogni non potrebbero essere soddisfatti*» [33]. Letta alla luce del principio di eguaglianza in senso sostanziale, però, la sussidiarietà orizzontale «*fa scattare l'interruttore verso il potere pubblico*» [34] ogniqualvolta l'intervento del privato non porti a una reale diminuzione delle diseguaglianze esistenti tra i singoli cittadini. Alla luce di ciò, anche l'azione dei pubblici poteri nel contesto della città intelligente, piuttosto che contraddire l'elemento cardine della sussidiarietà, finirebbe per darne coerente attuazione, essendo diretta a contrastare fenomeni discriminatori che i soggetti privati non sarebbero in grado di fronteggiare autonomamente.

---

[30] Si pensi, ancora, alla scelta di aderire (o meno) alla logica della condivisione delle informazioni.

[31] G.U. RESCIGNO, *Principio di sussidiarietà*, cit., p. 44.

[32] La predeterminazione, a opera del soggetto pubblico, dei fini che i privati sono tenuti a soddisfare con il loro intervento insinua, semmai, il dubbio della compatibilità, con il dato costituzionale, del richiamato approccio *bottom-up* che dovrebbe caratterizzare, in linea teorica, la città intelligente.

[33] C. MARZUOLI, *Sussidiarietà e libertà*, in *Riv. dir. priv.*, 2005, p. 88.

[34] G.U. RESCIGNO, *Principio di sussidiarietà*, cit., p. 45.

UN NUOVO PARADIGMA DI *SMART CITY*: IL MODELLO SVEDESE

di *Silvia A. Carretta*

1. *Intelligenza artificiale urbana*

Il 22 aprile scorso ho avuto il piacere di essere invitata come ospite alla conferenza *Intelligenza artificiale e smart cities. Sfide e opportunità* svoltasi presso l'Università di Firenze. L'occasione è stata gradita per confrontarmi con i colleghi italiani su svariate tematiche giuridiche relative alle c.d. *smart city*. In particolare, lavorando in Svezia da oltre quattro anni, l'invito mi ha permesso di portare di fronte ai colleghi italiani il modello di città intelligenti svedesi e offrire alcuni elementi di confronto sull'uso dell'intelligenza artificiale (IA) nell'ambito delle realtà urbane del paese scandinavo.

Molte città intelligenti utilizzano una combinazione di IA, *Internet of Things* (IoT), realtà aumentata, servizi *cloud*, elaborazione dati in rete, *blockchain* e altre tecnologie innovative. Queste tecnologie emergenti vengono sempre più frequentemente utilizzate nei contesti urbani per la progettazione delle città, per contribuire alla pianificazione di servizi e nuove politiche a sostegno del cambiamento urbano, per ottenere una crescita sostenibile e migliore vivibilità.

Il presente contributo si propone di presentare un iniziale quadro teorico attorno all'emergenza di strumenti urbani di *smart city* (c.d. "IA Urbane") basati su sistemi di IA e sull'elaborazione dei c.d. *big data urbani*[1]. Successiva-

[1] La raccolta di numerosi dati sulle abitudini e scelte dei cittadini nelle nostre città, l'uso di

mente, attraverso l'analisi di alcuni casi di studio svedesi, vengono offerti spunti di riflessione per valutare quale possa essere il potenziale dell'utilizzo di queste nuove tecnologie e quali sono le principali questioni giuridiche da risolvere con imminenza. Alla luce di un confronto tra nazioni europee con politiche socio-economiche molto diverse, nonché geograficamente opposte, i principali temi di confronto riguardano l'innovazione e uguaglianza di genere, la transizione energetica, la sfida delle dinamiche politico-economiche alla base dell'IA, la prospettiva etica ed infine il tanto discusso argomento della *Accountability* dei sistemi di IA. Il tentativo è quello di raccogliere alcuni spunti di riflessione nell'evoluzione dell'IA urbane e dell'uso dei *big data* per una più autonoma gestione delle necessità politico-economiche, giuridiche e sociali.

Alla fine vengono delineate conclusioni e suggerimenti di cambiamento nelle politiche urbane attuabili grazie a queste moderne IA urbane.

1.1. *Partendo dall'incipit: una questione di definizioni*

Dopo aver esaminato numerose fonti – accademiche e non – è interessante notare *in primis* come il concetto di *smart city* non presenti una definizione consolidata (perlomeno a livello unitario) ma abbia ricevuto interpretazioni multiple sia in accademia che nell'industria privata. In secondo luogo, colpisce altresì l'assenza di una definizione condivisa delle principali tecnologie che compongono le città intelligenti (e.g. IA urbana, urbanistica intelligente, *big data urbani*, IoT, servizi *cloud*, e realtà aumentata). Ad esempio, la Commissione Europea, definisce le *smart city* come «*un luogo in cui le reti e i servizi tradizionali sono resi più efficienti con l'uso di soluzioni digitali a vantaggio dei suoi abitanti e delle imprese*»[2]. Alcuni autori le ritengono invece un concetto che abbraccia «*la maggior parte delle aree in cui operano i governi locali: trasporti, imprenditorialità civica, democrazia e trasparenza, energia pulita e fornitura di servizi*»[3].

---

tecniche di *data mining* in tempo reale, il rilevamento dei *pattern* tra i dati raccolti hanno aperto una nuova era nella ricerca e nella pianificazione delle politiche urbane. Ciò nonostante, rimane necessario tenere a mente anche i pericoli per la *governance* urbana. V. e.g. J. KANDT, M. BATTY, *Smart cities, big data and urban policy: Towards urban analytics for the long run*, in A. YEH, Q. LI, S. WILLIAMS, M. BATTY, X. YE (ed.), *Big Data and Urban Planning – Cities*, Vol. 109, February 2021.

[2] Traduzione dell'autore. v. sito della COMMISSIONE EUROPEA: *www.ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/City-initiatives/smart-cities_en.*

[3] E. ALMIRALL, J. WAREHAM, C. RATTI, P. CONESA, F. BRIA, A. GAVIRIA, A. EDMONDSON, *Smart Cities at the Crossroads: new tensions in city transformation*, in *California Management Review*, 59(1):2016, pp. 141-152.

Per lo scopo del presente contributo, le IA urbane vengono definite come un filone emergente di urbanistica intelligente, la quale fa uso di sistemi di IA e di *big data* per migliorare la pianificazione e implementazione di numerosi servizi nel panorama urbano contemporaneo, così come la *governance* urbana. Ad esempio, l'IA viene utilizzata per i servizi di trasporto urbano, il monitoraggio della mobilità, la raccolta dei rifiuti urbani, la gestione dei servizi per il cittadino, il tracciamento dei contatti (si pensi alla situazione endemica del virus Covid-19), il risparmio energetico e di acqua, l'ottimizzazione del riscaldamento urbano e così via.

Sebbene accademici e professionisti attingano ad un insieme omogeneo di idee ispirate a tecnologie emergenti (anche se a volte meno avanzate di quanto si voglia far credere) numerosi progetti di smart city effettivamente esistenti manifestano una serie di variazioni contestuali[4]. Come sostiene Picon, «*la smart city appartiene in parte all'immaginazione*»[5]: una condizione che rende difficile definire tutte le incarnazioni di questo ideale urbano. Ciò nonostante si può notare come emerga una comunanza: l'uso della tecnologia della comunicazione e informazione come meccanismo per rendere queste città "intelligenti".

L'emergere di IA urbane nelle città è un fenomeno complesso, sia dal punto di vista teorico che empirico. Più specificamente, queste IA urbane sono strumenti in grado di acquisire un'enorme quantità di dati dall'ambiente circostante, interpretarli, classificarli, per poi prendere una o più decisioni razionalmente, utilizzando le informazioni acquisite e secondo obiettivi predefiniti.

La peculiarità sta nella loro capacità di prendere autonomamente decisioni riguardo a complesse situazioni urbane e agire autonomamente al fine di svolgere compiti di gestione dei servizi urbani. Di conseguenza, le decisioni di pianificazione e gestione dei servizi si sposta sempre più dalle mani degli esseri umani a quelle "virtuali" delle macchine intelligenti, in grado di intraprendere decisioni autonomamente e in modo non supervisionato[6].

---

[4] E.g. N. ANGELIDOU, *Smart cities: a conjuncture of four force,* Cities, Vol. 47, September 2015, pp. 95-106; T. SHELTON, M. ZOOK, A. WIIG, *The 'actually existing smart City'*, in *Cambridge Journal of Regions, Economy and Society*, 8/2015, pp. 13-25; F. CUGURULLO, *The origin of the smart city imaginary: from the dawn of modernity to the eclipse of reason*, in C. LINDNER, M. MEISSNER (ed.), *The Routledge Companion to Urban Imaginaries*, London, 2018, pp. 113-124.

[5] A. PICON, *Urban infrastructure, imagination and politics: from the networked metropolis to the smart City*, in *International Journal of Urban and Regional Research*, 2018, p. 270 ss.

[6] I sistemi di IA possono essere tangibili, cioè incorporati all'interno di *robot*, droni o altri strumenti tecnici. Al contrario, possono anche essere in grado di agire pur senza essere "incar-

Queste decisioni possono potenzialmente innescare cambiamenti radicali nella città e pertanto è indispensabile che siano soggette a limiti di legge e ad una specifica regolamentazione. In particolare, vista l'enorme rilevanza che hanno i dati raccolti per il corretto apprendimento delle IA, è imperativo sviluppare un'apposita *governance* dei dati urbani ed una struttura giuridica che possa supportare l'avvalersi di questa tecnologia e al contempo limitare possibili abusi[7]

2. *Il modello svedese*

Dopo questa parentesi introduttiva, è possibile ora concentrarsi su soluzioni empiriche esistenti in Svezia, che si basano su sistemi di IA applicati specificamente ai contesti urbani.

La forte tendenza all'urbanizzazione in corso in Svezia offre nuove sfide e opportunità. Le città stanno diventando sempre più importanti per creare condizioni di crescita economica, efficienza energetica e delle risorse, benessere umano e sviluppo sostenibile della società nel suo insieme[8]. Poiché le città vengono sviluppate per soddisfare le crescenti sfide dovute dall'urbanizzazione, sono necessarie nuove soluzioni intelligenti.

La Svezia ha una lunga storia come pioniera nelle questioni relative all'ambiente e allo sviluppo sostenibile. Essa guida la strada grazie a soluzioni all'avanguardia in settori come la gestione dei rifiuti, la mobilità, il risparmio di acqua, un efficiente uso di corrente elettrica e del teleriscaldamento, la *governance* urbana e le politiche di parità di genere.

L'idea di riunire sotto un unico emblema le soluzioni di IA urbane svedesi ha preso vita nel 2016 con il progetto *Smart City Sweden*[9]. L'obiettivo è quello di sviluppare ed esportare in altri paesi dell'Unione soluzioni relative a nuove tecnologie per il miglioramento delle politiche di mobilità, clima, energia e ambiente. Nel 2019 il progetto è stato ampliato per includere altresì soluzioni intelligenti relative a urbanistica, digitalizzazione e sostenibilità sociale. Vari

---

nati" in un corpo tangibile, ma operare attraverso cosiddetti "agenti *software*". Si veda S.J. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach*. IV ed., Harlow, 2020.

[7] V. e.g. E. ALMIRALL, J. WAREHAM, C. RATTI, P. CONESA, F. BRIA, A. GAVIRIA, A. EDMONDSON, *op. cit*.

[8] FLANDER STATE GOVERNMENT - FLANDERS INVESTMENT & TRADE, *Market Survey: Smart Cities in Sweden*, 2020.

[9] V. sito Smart City Sweden: *www.smartcitysweden.com.*

progetti intelligenti vengono applicati oggigiorno in contesti differenti e contribuiscono allo sviluppo delle summenzionate cinque aree di interesse, offrendo un esempio di *best practices* da esportare e promuovendo l'attività di aziende pronte a portare le proprie soluzioni in nuovi mercati.

Un primo interessante esempio di pianificazione e gestione dei servizi abitativi urbani attraverso strumenti basati su sistemi di IA, e applicati ad un contesto urbano, arriva dalla più grande università tecnica svedese. Situato a Stoccolma, nel campus dell'università, il KTH Live-In Lab mira a contribuire a realizzare edifici sostenibili ed efficienti sotto il profilo delle risorse. La ricerca e il collaudo sono effettuati in edifici reali, consentendo non solo una valutazione del prodotto stesso ma anche una valutazione di come ogni componente (i.e. inquilino) contribuisca alle prestazioni dell'edificio nel suo insieme. Difatti, una peculiarità sta nel fatto che il Lab riceve dati da oltre 305 appartamenti per studenti nel campus universitario (e da un hotel), permettendo di analizzare i dati e prendere decisioni su come sviluppare ulteriormente il progetto sulla base delle effettive esigenze degli inquilini, valorizzando così una politica di uguaglianza e inclusione degli studenti universitari nel tessuto abitativo cittadino, nonché una politica di responsabilizzazione (rendendoli parte dell'iter decisionale) [10].

Il modello svedese esemplifica come una città intelligente vada oltre l'uso delle tecnologie digitali per un migliore utilizzo delle risorse e minor impatto ambientale. La creazione di un nuovo modello di *smart city* significa certamente la costruzione di reti di trasporto urbano più intelligenti, un migliore approvvigionamento idrico, modi più efficienti per illuminare e riscaldare gli edifici, e strutture moderne per lo smaltimento dei rifiuti. Ma significa altresì la creazione di un'amministrazione cittadina più interattiva e reattiva, che metta in primo piano i cittadini stessi e i loro bisogni, che soddisfi le esigenze di una popolazione che invecchia, che tenga in considerazione le differenze di genere, e la realizzazione di spazi pubblici più sicuri. Non da ultimo, questo nuovo modello significa anche ideare politiche socio-economiche che contrastino le dinamiche di disuguaglianza, discriminazione e disagio economico già esistenti nel tessuto sociale urbano (andando a limitare il forte potere economico di gruppi ridotti di persone, i quali beneficiano maggiormente dei frutti dell'innovazione tecnologica).

In quest'ottica, nelle prossime sezioni vengono introdotti alcuni casi di studio di IA urbane applicate nel contesto di *smart city* svedesi. Questi casi empiri-

[10] Questo caso di studio mi sta particolarmente a cuore, avendo vissuto anche io nel Lab il mio primo anno a Stoccolma, *www.liveinlab.kth.se*.

ci rappresentano strumenti intelligenti usati nel paese scandinavo per definire politiche a sostegno del cambiamento urbano. Il tentativo è quello di offrire spunti di riflessione sulle principali questioni giuridiche legate all'evoluzione di IA urbane e dell'uso dei *big data*, per avviare le necessarie discussioni circa le necessità politico, economiche e sociali legate alle *smart city*.

3. *Alcuni spunti di riflessione*

Nonostante la popolarità degli strumenti di IA e l'esteso uso di *big data* nel panorama urbano, rimane necessario mantenere un atteggiamento critico riguardo a questi strumenti.

In passato, la scienza e le nuove tecnologie sono spesso stati usati come espedienti retorici per legittimare la riproduzione delle relazioni di potere e di determinate ideologie, e per supportare esistenti politiche economiche, le quali riflettono gli squilibri e le discriminazioni già esistenti nella società. Di conseguenza, le *élite* che beneficiano maggiormente dei frutti dell'innovazione tecnologica rischierebbero di rimanere incontrastate [11].

Da una prospettiva politico-economica, l'IA può implementare programmi di crescita economica e diversificazione, come stabilito ad esempio in alcune agende urbane [12].Tuttavia, dall'altro lato essa può essere al contempo soggetta a sfide progettuali tipiche della sperimentazione *ex novo* di progetti urbani tecnologici, a costi elevati, e persino ad accettare rischiosi compromessi in termini di diritti umani e valori fondamentali [13]. Conscia di queste sfide, la Svezia ha studiato alcune applicazioni di IA urbane (*infra*) finalizzate ad un uso consapevole di questa tecnologia, per ottimizzarne gli aspetti positivi e contrastarne gli effetti collaterali. Tutto ciò, non in un'ottica di limitazione dell'uso della tecnologia, bensì con un atteggiamento di curiosità verso l'ignoto, di accettazione e di ausilio alla liberalizzazione dei servizi, sempre nel rispetto dei

[11] Come già rilevato in altri studi, "intelligente" e "sostenibile" non sono necessariamente sinonimi. v. H. AHVENNIEMI, A. HUOVILA, I. PINTO-SEPPÄ, M. AIRAKSINEN, *What are the differences between sustainable and smart cities?*, in *Cities*, 60:2017, pp. 234-245.

[12] B.N. TAYLOR, A. WHILE, *Competitive urbanism and the limits to Smart City innovation: The UK Future Cities initiative*, in *Urban Studies*, 54(2), 2017, pp. 501-519.

[13] E.g. M. GANDY, *Cyborg urbanization: Complexity and monstrosity in the contemporary city,* in *International Journal of Urban and Regional Research*, 29(1), 2015, pp. 26-49; S. MARVIN, *et al.*, *Urban Living Labs: Experimenting with city futures*, New York, 2018; A. LESZCZYNSKI, *Speculative futures: Cities, data, and governance beyond smart urbanism*, in *Environment and Planning*, 48(9):2016, pp. 1691-1708.

principi di trasparenza, uguaglianza e responsabilizzazione dei cittadini nelle politiche urbane.

3.1. Smart city*, innovazione e uguaglianza di genere*

Anche se può non apparire ovvio a prima vista, le città intelligenti, l'innovazione urbana e lo sviluppo tecnologico sono strettamente collegati alla questione della parità di genere. La parità di genere è un obiettivo fondamentale della politica dell'UE. La Commissione Europea ha posto questa parità in cima alla sua agenda politica e ha recentemente adottato un'ambiziosa strategia per il lustro 2020-2025 volta a raggiungere un'Europa in cui la parità di genere sia la regola [14]. Al contempo le Nazioni Unite definiscono la parità di genere un diritto umano fondamentale, spingendosi fino a definirla persino una condizione necessaria per un mondo prospero, sostenibile e in pace [15] .Tale impegno è comprovato dal fatto che questo diritto è stato inserito come quinto obiettivo per lo Sviluppo Sostenibile secondo l'Agenda 2030 [16].

Sfortunatamente, molte politiche urbane e i relativi servizi continuano a non tenere conto del fattore del genere, nonostante uomini e donne utilizzino la città e i suoi servizi in modo diverso. Si pensi ai servizi educativi, sanitari, familiari per l'infanzia e per i genitori, all'uso di alloggi popolari da parte di famiglie monogenitoriali o di quelle a basso reddito, ai trasporti pubblici, ai servizi a sostegno alle vittime della violenza di genere, all'uso di parchi pubblici e così via [17].

Dunque, una comprensione completa, sulla base di concreti *big data* urbani, di come il genere limiti o migliori le esperienze dei cittadini nei servizi pubblici è una parte integrante nella costruzione di una città intelligente paritaria nel genere, che offra una continua crescita sociale, economica e ambientale sostenibile. Attraverso processi di ricerca di soluzioni nuove e innovative

---

[14] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025,* COM/2020/152.

[15] ORGANIZZAZIONE DELLE NAZIONI UNITE, *Risoluzione dell'Assemblea Generale 25 Settembre 2015*, *Transforming our world: the 2030 Agenda for Sustainable Development*, A/RES/70/1, 2015.

[16] *Ibidem.*

[17] Si pensi ad esempio ad una rete intelligente di telecamere di sorveglianza, collegata a diversi database e in contatto con le autorità o ad un'app, che possano aiutare a individuare le strade più sicure e informare i famigliari sul percorso in tempo reale.

alle sfide urbane, le strutture di potere di genere possono essere messe in discussione e rese sistematicamente visibili.

Un esempio di risposta innovativa a questa questione arriva dalla città di Umeå, a nord della Svezia. Questo comune lavora da oltre 30 anni con le questioni di uguaglianza di genere in modo strategico e rivoluzionario. L'ambizione è quella di creare condizioni affinché donne e uomini abbiano lo stesso potere di influenzare le scelte sociali e ottenere servizi equivalenti, senza limiti dovuti a nozioni stereotipate di genere [18].

Nell'ambito del piano d'azione integrato che esplora questo problema, Umeå ha studiato il legame tra uguaglianza di genere, città intelligenti e innovazione urbana al fine di aumentare la consapevolezza e rendere sistematicamente visibili le strutture di potere di genere nei processi di innovazione [19]. Questo progetto mira a una più chiara comprensione sul perché e come includere un'analisi critica sul genere nell'innovazione urbana delle città intelligenti. Considerando la latitudine a cui si trova Umeå, per numerosi mesi all'anno la città rimane innevata e coperta da una coltre di neve e ghiaccio, e alle 2 pomeridiane è già buio. Soluzioni di IA urbane potrebbero far sentire le donne più sicure quando tornano dal lavoro al buio in questi mesi. E poiché spesso sono le donne a portare i bambini a scuola o ad usare la bici per recarsi al lavoro, lo sviluppo di un algoritmo di IA potrebbe altresì aiutare a predire esattamente il meteo e indicare la strategia più efficiente per pulire le strade dalla neve, partendo proprio dalle piste ciclabili, o per garantire che le strade che collegano le scuole siano più sicure [20].

Ulteriormente, in termini di soluzioni di *smart city*, la città di Umeå offre una serie di informazioni gratuite e accessibili (c.d. *Open Data*) per lo sviluppo di servizi intelligenti, provvede a raccogliere in maniere strutturata dati separati per genere, raccoglie altresì informazioni su chi necessità di questi dati, come vengono usati, quali dati nello specifico sono usati per addestrare l'IA e come vengono sviluppate nuove soluzioni [21].

---

[18] Nel 2019, nell'occasione dei 30 anni di impegno della città di Umeå per la parità di genere, è stato preparato un report che descrive i traguardi raggiunti. *www.umea.se/download/18.333c64e217718860a23ac/1611053814262/Jubileumsskrift%20j%C3%A4mst%C3%A4lldhet%20Ume%C3%A5%20kommun.pdf*.

[19] S. KNEESHAW, J. NORMAN, *Gender equal cities*, in *Urbact*, III, 2019, p. 37ss.

[20] Per approfondimenti v. sito del comune di Umeå: *www.umea.se/kommunochpolitik/manskligarattigheter*.

[21] Ad esempio, il progetto *Ruggedised* a Umeå per la creazione di un "distretto intelligente" supporta una serie di soluzioni tecnologiche tra cui una piattaforma decisionale *open-data*, una IA urbana per la gestione dei fabbisogni del campus universitario, connessioni "smart" a ener-

In un più ampio ragionamento riguardo le politiche di genere, alle città intelligenti e all'innovazione urbana è importante cercare di creare una comprensione della città come luogo in cui le strutture di potere di genere sono sempre presenti. La Svezia sembra aver colto con determinazione la sfida di individuare nuove politiche di genere come motore dell'innovazione e del progresso sociale, e di renderle sostenibili grazie all'uso di *big data* e IA urbane.

In conclusione, per rendere visibili, problematizzare, riformulare queste sfide, è opportuno promuovere uno scambio di idee e soluzioni per condividere le migliori pratiche tra le città europee. È necessario che i professionisti, i politici (sia a livello locale che nazionale) e le istituzioni si chiedano come sviluppare strumenti e approcci contestualizzati a livello locale per lavorare verso l'uguaglianza di genere nelle politiche, nella pianificazione e nei servizi urbani. La realizzazione di questi ultimi può essere facilitata dall'uso di sistemi di IA non discriminatori e più equi. Difatti, per ottenere soluzioni non solo *smart* ma anche eque servono *big data* che siano effettivamente rappresentativi delle diversità presenti nel tessuto sociale delle nostre città.

3.2. *Transizione energetica e Quadro 2030 per il clima e l'energia*

Nell'ambito del *Green Deal* europeo per il periodo 2021-2030[22], la Svezia ha preso l'impegno di compiere la transizione verso l'uso delle energie rinnovabili e ridurre le sue emissioni di CO^2 entro il 2030. La questione è un esempio oggi molto pertinente alla luce della crisi energetica che ha colpito l'Europa, e soprattutto il Belpaese, facendo rincarare il costo dell'elettricità[23].

La problematica principale che la Svezia sta affrontando per raggiungere tale obiettivo è come stimare la capacità necessaria della rete energetica e allo stesso tempo cercare di convincere le persone a ridurre il loro consumo di energia[24]. Una delle soluzioni proposte prevede l'uso di contatori intelligenti nella maggior parte delle case che possono rilevare quanta elettricità viene utilizzata e per che tipo di scopi. Ad esempio, nel 2018, la rete elettrica intorno al comune di Malå è stata dotata di un sistema intelligente di sorveglianza della

gia 100% rinnovabile; "gamification" per influenzare i modelli comportamentali; dell'utente finale, *www.ruggedised.eu/cities/umeaa*.

[22] COMMISSIONE EUROPEA, *Il Green Deal europeo*, COM(2019) 640.

[23] ISPI DATALAB, *Crisi energetica: l'Italia è diversa?*, in *www.ispionline.it,* 16 febbraio 2022.

[24] REGERINGSKANSLIET FAKTAPROMEMORIA, *Meddelande om en europeisk grön giv*, 2019/20:FPM13.

rete, che rileva e localizza guasti e deviazioni. Lo *Smart Grid Surveillance* di Exeri è dotato di sensori intelligenti, comunicazioni radio, algoritmi di IA e analisi avanzata dei *big data*[25]. Questa soluzione è un grande passo avanti nello sviluppo di reti intelligenti e offre importanti vantaggi in termini di monitoraggio, manutenzione proattiva, localizzazione dei guasti, tempi di fermo ridotti, funzionamento più efficiente e riduzione dei costi.

Un altro tema caldo nel dibattito sulla transizione energetica è la costruzione di nuove aree urbane. La questione qui riguarda l'opportunità di aumentare l'urbanizzazione e ridurre sempre di più l'ambiente naturale circostante le città (tema caro agli svedesi) a favore di nuovi alloggi e infrastrutture, energeticamente neutrali e dotati delle più moderne tecnologie di IA. Il quartiere di Norra Djurgårdsstaden (i.e. *Stockholm Royal Seaport*) a Stoccolma è la più grande area di sviluppo urbano della Svezia. È un quartiere sostenibile di recente realizzazione, costruito interamente su carta, efficiente in termini di risorse e privo di combustibili fossili. La città ha sviluppato un sistema intelligente di distribuzione dell'acqua piovana e di disgelo, in grado di fare previsioni sulle future esigenze idriche. Il sistema collega tetti verdi e giardini 'intelligenti' per lo studio di come la tecnologia intelligente possa rafforzare il dialogo tra le persone e la natura, specialmente quando quest'ultima è sotto pressione (e.g. durante i periodi di forti piogge e nelle estati calde e aride)[26].

Alla luce dell'odierna crisi idrica nel nord Italia, e del progressivo aumento della desertificazione sul territorio nazionale a causa del cambiamento climatico, questo esempio scandinavo potrebbe essere una fonte di ispirazione per una soluzione che possa essere riadattata anche alla realtà del nostro Paese. L'alternativa ad un'eccessiva urbanizzazione è la promozione di uno stile di vita più sostenibile, utilizzando maggiormente gli edifici e le infrastrutture già esistenti. Difatti, la costruzione di nuove case più efficienti dal punto di vista energetico e termico comporta una spesa economica non indifferente e ciò porterebbe ad inefficienze abitative e discriminazione verso coloro che non possono permettersi una nuova casa o che non vogliono trasferirsi nelle nuove aree urbane (spesso sovrappopolate).

La domanda principale è se sia corretto da un punto di vista etico e sociale, nonché ammissibile da un punto di vista giuridico, costringere i cittadini a trasferirsi in questi nuovi edifici, e più in generale ad essere soggetti all'uso di IA urbane e a fornire i propri dati per collezionare *big data*, offrendo in cambio protezione contro i cambiamenti climatici, gli impatti economici e sociali del-

[25] EXERI, *Smart Grid Surveillance*™, *www.exeri.se*, 2018.

[26] V. il sito dedicato: *www.norradjurgardsstaden2030.se/en/innovation-projects/smartergreenercities/*.

l'aumento del costo dei carburanti, dell'elettricità, dei beni alimentari e così via. Questa soluzione non sembra plausibile. Ci si dovrebbe invece domandare se ci siano altri modi per convincere le persone a vivere in modo più sostenibile e efficiente dal punto di vista energetico e sociale. È proprio qui che vengono in nostro aiuto i sistemi di IA urbane come quelli menzionati sopra e le nuove tecnologie intelligenti che consentono ad esempio una più corretta distribuzione dell'elettricità e delle risorse primarie, il riuso di acqua, il risparmio energetico, un più efficiente uso dei trasporti, e la riduzione dei consumi quotidiani.

È ormai troppo tardi per negare le conseguenze devastanti sull'economia e sulla società che stiamo vivendo a causa del cambiamento climatico [27]. La Commissione Europea sta lavorando da quasi due decenni per cambiare le cose a livello dell'Unione [28], e anche gli Stati Membri si stanno impegnando a introdurre politiche nazionali (la Svezia dai primi anni 2000 monitora con impegno gli effetti dei cambiamenti climatici sui suoi ecosistemi, sull'ambiente culturale e sulla salute umana) [29]. C'è ancora molto da fare per cambiare le abitudini dei cittadini ma questa apparente rinata consapevolezza spinge verso un cambiamento almeno nelle politiche urbane, attraverso l'uso di soluzioni intelligenti che permettano di semplificare la vita dei cittadini, automatizzare numerosi compiti e alleviare ulteriori impatti negativi sul clima. Solo così potremo abbracciare un cambiamento sociale che permetta di vincere la sfida della transizione energetica e combattere il cambiamento climatico.

3.3. *Sfidare le dinamiche politico-economiche alla base dell'IA*

Un ulteriore spunto di riflessione vuole rilevare il fatto che l'uso dei sistemi di IA rischi di non essere in grado di contrastare dinamiche politico-economiche più ampie, che stanno alla base della loro creazione. Anzi, si potrebbe quasi dire che, talvolta, questi sistemi non facciano altro che rinforzare il potere economico di gruppi ridotti di persone, i quali beneficiano maggior-

---

[27] Per un resoconto sulle conseguenze in Svezia v. THE LOCAL, *How climate change is changing northern Sweden and the people who live there*, 2021, in: *www.thelocal.se/20211025/how-climate-change-is-changing-northern-sweden-and-the-people-who-live-there/*

[28] Libro Verde della Commissione al Consiglio, al Parlamento Europeo, al Comitato economico e sociale europeo e al Comitato delle regioni – L'adattamento ai cambiamenti climatici in Europa – quali possibilità di intervento per l'UE, COM/2007/0354.

[29] SVENSKA REGERIGEN, STATENS MILJÖDEPARTEMENTET, *Sverige inför klimatförändringarna – hot och möjligheter*, SOU 2007:60.

mente dei frutti dell'innovazione tecnologica, lasciando così incontrastate le dinamiche di disuguaglianza, discriminazione e disagio economico già esistenti nel tessuto sociale urbano.

Nonostante la crescente preoccupazione pubblica e l'azione di vari legislatori per limitarne l'uso, gli algoritmi di riconoscimento facciale e altre tecnologie di IA ad alto rischio sono appena state circoscritte [30]. I cosiddetti progetti di "città intelligenti" negli Stati Uniti (ma non solo) hanno provato come questi consolidino sempre più il potere nelle mani di poche società *big tech* che operano a scopo di lucro, privando le città e la società civile di risorse economiche ma anche violando la *privacy* e diritti fondamentali dei loro cittadini.

Un evidente esempio è il progetto Sidewalk Labs di Google, in Canada. Questo progetto introduce «*il primo quartiere al mondo costruito da Internet in su*» e supporta la creazione di un punteggio di credito cittadino gestito da Google come parte del suo piano di collaborazione con la città di Toronto [31].Tale progetto è stato duramente criticato, tanto da essere alla fine dismesso, per la mancanza di trasparenza e di accesso pubblico agli algoritmi, per le lacune nella condivisione delle scelte sui requisiti di tale infrastruttura digitale pubblica, per il rigetto della proprietà pubblica dei dati, l'assenza di forme autentiche di partecipazione civica, di rispetto della *privacy* e di un serio reinvestimento dei guadagni in politiche di benessere sociale [32].

La questione principale qui è come bilanciare, da un lato, l'esigenza di aumentare l'uso delle soluzioni di IA sviluppate da società *tech* private e messe a disposizione della pubblica amministrazione (PA) per usufruire dei benefici e, dall'altro lato, assicurarsi che aziende private non inseriscano i propri interessi nelle soluzioni *smart* delle nostre città, ma garantiscano il rispetto dei valori dell'Unione e dei diritti umani fondamentali.

---

[30] COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2018; R. VAN NOORDEN, *The ethical questions that haunt facial recognition research*, in *Nature*, 587:2020; E.L. ANDREWS, *How flawed data aggravates inequality in credit*, Stanford University HAI center, *www.hai.stanford.edu/news/how-flawed-data-aggravates-inequality*-credit, 6 agosto 2021; M. BURGESS, *The lessons we all must learn from the A-levels algorithm debacle*, in *Wired*, *www.wired.co.uk/article/gcse-results-alevels-algorithm-explained,* 20 agosto 2020.

[31] *Google affiliate Sidewalk Labs abruptly abandons Toronto smart City project*, in *www.theguardian.com/technology/2020/may/07/google-sidewalk-labs-toronto-smart-City-abandoned*, 2020.

[32] B. WYLIE, *Debrief on Sidewalk Toronto Public Meeting #3 – A master class in gaslighting and arrogance*, in *Medium*, *www.medium.com/@biancawylie/debrief-on-sidewalk-toronto-public-meeting-3-a-master-class-in-gaslighting-and-arrogance-c1c5dd918c16*, 19 agosto 2018.

La risposta è insita in un notevole cambiamento concettuale: la PA non è più solo fornitrice di servizi direttamente ai cittadini, bensì ora facilita lo scambio di dati con i cittadini stessi. In altre parole, grazie all'IA e ai *big data* urbani, la PA facilita lo scambio di informazioni che essa stessa raccoglie dai cittadini, con quelle raccolte dall'industria privata, in modo da fornire servizi pubblici in un modo più efficiente e sostenibile. Un ottimo esempio è il laboratorio IA della città di Helsingborg: il *Smarter City Lab*[33]. Questa IA urbana è in grado di gestire grandi quantità di dati e può essere utilizzata dall'industria privata e dai cittadini per addestrare le proprie IA. Il Lab mira a rafforzare la cooperazione tra le imprese, il mondo accademico e la PA.

Per ottenere tale fine è necessario lavorare su nuovi modelli di business e un più accurato quadro giuridico. Come spiega Pilar Conesa, la PA dovrebbe progettare nuovi schemi giuridici, economici e di *governance* per richiedere alle società *tech* private di condividere i dati che raccolgono dai loro utenti e al contempo promuovere comportamenti collaborativi da parte dei cittadini per lo sviluppo di tecnologie intelligenti, che coinvolgono *big data* urbani e dati personali e sensibili[34].

Alla luce dell'esempio scandinavo, si evidenzia l'importanza di dare a tutti i cittadini la possibilità di usufruire delle soluzioni che la tecnologia offre, che siano a portata di cittadino e che siano il più possibile inclusive. Forti di un ampissimo diritto all'informazione – che in particolare include il principio di totale accesso ai documenti della PA – i cittadini svedesi godono di un rapporto con la PA che supporta un livello molto alto di trasparenza e accessibilità[35]. Grazie a tali valori e a innovative politiche di uguaglianza e parità (già dalla prima metà del 1900) è possibile prendere spunto dall'esempio scandinavo per lo sviluppo di IA urbane e nuove soluzioni intelligenti che contrastino le ricorrenti dinamiche politico-economiche che sono causa di disuguaglianza, discriminazione e disagio economico.

Le nuove *smart city* possono e devono essere usate per portare uno sviluppo paritario e di uguaglianza economica e sociale sul tessuto urbano, soprattutto in quartieri a diversa composizione etnica, sociale e culturale.

---

[33] V. il sito dedicato: *www.innovation.helsingborg.se/en/platforms/smarter-City-lab-more-testing-of-ai-in-the-City-all-businesses/*.

[34] E. Almirall, J. Wareham, C. Ratti, P. Conesa, F. Bria, A. Gaviria, A. Edmondson, *op. cit*., p. 143 ss.

[35] C.F. Bergström, M. Ruotsi, *Grundlag i gungning? En ESO-rapport om EU och den svenska offentlighetsprincipen. Rapport till Expertgruppen för studier i offentlig ekonomi 2018:1*, Stockholm, 2018.

3.4. *Una prospettiva etica spinosa*

Il sempre più esteso accesso ai *big data* e la maggior implementazione di sistemi di IA autonomi hanno aperto una nuova era nella ricerca e nella pianificazione delle politiche e dei servizi urbani. Questi nuovi strumenti permettono un processo decisionale più agevole, un'urbanistica più intelligente e basata maggiormente sull'evidenza, e consentono una più agile implementazione di nuovi servizi nel panorama urbano.

Tuttavia, tali IA allontanano l'essere umano dalle decisioni di pianificazione e gestione dei servizi urbani. Si pone dunque di primaria importanza la spinosa questione dell'etica dell'IA. La *governance* urbana riguarda la responsabilità sociale e giuridica di decidere ciò che sia giusto o sbagliato, buono o cattivo, sostenibile o non sostenibile, per il bene della comunità e del singolo cittadino. Conseguentemente, rimane da stabilire come sia possibile che un'intelligenza non umana possa prendere decisioni su ciò che sia "giusto" per i cittadini, sostenibile per l'ambiente urbano o finalizzato al bene della comunità[36]. In altre parole, la domanda da porsi è come possa un sistema di IA distinguere tra cosa sia buono o cattivo, sostenibile o insostenibile, a vantaggio o non della comunità. Dalla risposta che si dà, dipenderà altresì la concezione di come possa essere considerata responsabile un'IA urbana, ovvero *Accountable* (v. *infra*) per le proprie decisioni ed eventuali conseguenze dovute a scelte non etiche o illecite.

Il bilanciamento tra lo sviluppo di visioni dipendenti da questa tecnologia, il priorizzare il benessere dei cittadini e l'assicurarsi che le *smart city* siano più eque piuttosto che più efficienti è molto fragile da ottenere. Ad esempio, la stessa IA potrebbe occasionalmente dover prendere decisioni di natura etica. Si pensi allo *screening* dei passeggeri aeroportuali, alle decisioni a punteggio (*credit score*) sull'assegnazione di alloggi comunali o di altri servizi di assistenza sociale, o ancora all'uso di IA per la sorveglianza da parte delle forze dell'ordine, o a casi più estremi di un possibile incidente in cui il danno è inevitabile (c.d. *trolley problem*[37]). Come sceglierà l'IA di distribuire il danno, soprattutto se inevitabile?

L'impiego di un approccio algoritmico basato sull'evidenza per la *governance* della città sembra garantire apparentemente decisioni razionali, logiche

---

[36] F. CUGURULLO, *Urban Artificial Intelligence: From Automation to Autonomy in the Smart City,* in *Frontier in Sustainable Cities*, 2:38, 2020.

[37] Questo esperimento ipotetico coinvolge filosofia, psicologia ed etica. In uno scenario immaginario uno spettatore può scegliere di salvare 5 persone che rischiano di essere investite da un tram senza freni, ma deviando il carrello ucciderà lo stesso 1 persona.

e imparziali, grazie ad un processo decisionale più agevole e basato sull'evidenza e su *big data*. Tuttavia, esso fornisce a chi amministra la città una sorta di scudo protettivo da responsabilità per decisioni che sollevano problemi etici e morali, consentendo loro di dire: «*Non sono io, sono i dati!*»[38].

Nella città intelligente, quindi, la capacità dell'IA di prendere decisioni autonomamente innesca dilemmi morali ed etici che richiedono di porsi la domanda se queste macchine debbano possedere valori morali o personalità giuridica. Come osserva Bostrom, i valori, gli ideali e gli obiettivi di un'IA potrebbero essere notevolmente diversi da quelli dei suoi creatori, semplicemente perché un'intelligenza non umana non può pensare esattamente come quella umana[39]. L'ampia discussione su queste questioni va rimandata ad altra sede. È sufficiente invece rilevare in questa sede che quando si tratta di città intelligenti, non basta valutare come l'IA possa impattare le dinamiche politico-economiche. Occorre, invece, tenere a mente altresì le questioni etiche relative all'uso di queste tecnologie e al loro impatto sui diritti fondamentali dei cittadini.

Alla luce di questi rischi morali, etici e giuridici, ci si potrebbe domandare se la soluzione migliore sia quella di bloccare l'uso di ogni tecnologia innovativa che ponga rischi – più o meno elevati – per la prosperità dei cittadini. Una risposta così intransigente non può certo essere quella adatta. Non è reprimendo l'innovazione e l'uso di tecnologie emergenti che la società potrà muoversi verso un futuro migliore, che offra nuove opportunità di benessere per i cittadini. Una soluzione, invece, potrebbe essere lo sviluppo di IA urbane in condivisione tra le varie PA, o tra queste e le istituzioni governative, al fine di unire le forze per ottenere soluzioni intelligenti finalizzate al primario benessere dei cittadini, che siano *Accountable* l'uno verso l'altro (v. *infra*) e che offrano tutele e garanzie di legge.

Richiamando l'esempio del paese scandinavo, la maggior parte dei comuni svedesi fa parte di un'alleanza regionale – la *Stadshubbs Alliansen* – composta da un numero crescente di *City Hub* (i.e. gruppi di città) i quali lavorano insieme sia dal punto di vista commerciale che tecnico per fornire un'infrastruttura *wireless* solida e competitiva per l'IoT. Poiché ogni comune dispone di reti in fibra aperte, attraverso una tecnologia d'avanguardia (*wireless standard Long Range* – LoRaWAN™), la Stadshubbs Alliansen ha creato un mercato per realizzare il potenziale della digitalizzazione: una piattaforma tecnica e commerciale tra città per la fornitura di soluzioni di comunicazione digitale.

---

[38] Come ben evidenziato in: U. HAQUE, *What is a city that would be 'Smart'?*, in *City in a Box*, vol. 34, 2012.

[39] N. BOSTROM, *Superintelligence*, Oxford, 2017.

Ciò significa che chiunque abbia bisogno di comunicare con i sensori LoRaWAN può farlo facilmente senza dover costruire o gestire la propria infrastruttura e avendo accesso ad un enorme database di *big data* urbani multirappresentativi, a cui altrimenti non avrebbe accesso [40].

Dunque, lo sviluppo di città intelligenti esige che chi le amministra si impegni a tenere un approccio aperto e multidisciplinare alle esigenze dei cittadini e all'uso di tecnologie emergenti, per offrire tutte le garanzie che la legge richiede. Al contempo, i legislatori nazionali e europei sono responsabili di imporre loro volta una chiara e omnicomprensiva visione sull'uso e i limiti delle IA urbane e dei *big data* urbani (e non solo), nel rispetto dei valori etici, dei diritti fondamentali dei cittadini e soprattutto della protezione dei dati personali [41].

3.5. *La quadratura del cerchio:* Accountability *dei sistemi di IA*

Un'ultima considerazione si dimostra necessaria alla luce di quanto detto finora. Abbiamo detto che i sistemi di IA presenti nelle *smart city* sono sempre più intelligenti (cioè in grado di prendere decisioni in maniera autonoma). Fare ricorso sempre più a IA urbane e delegare loro le decisioni nel contesto della pianificazione dei servizi e dell'innovazione urbana significa al contempo essere fondamentalmente consapevoli degli effetti che questa tecnologia ha sulle persone e sulla società, sulle nostre capacità decisionali e incolumità psicofisica.

Dunque, è indispensabile assicurarsi che le decisioni prese dalle IA urbane soddisfino un'ampia serie di requisiti etici e giuridici. *In primis* occorre che questa tecnologia, e le sue decisioni autonome, rispettino i valori fondamentali dell'Unione e i diritti umani intransigibili, nonché limitino al minimo qualunque effetto potenzialmente negativo sulla vita dei cittadini.

Prendendo spunto dagli *Orientamenti etici per un'IA affidabile* [42] emessi nel 2018 dal gruppo europeo di esperti ad alto livello sull'IA, questi ultimi hanno

---

[40] Un'interessante applicazione di questa tecnologia ha permesso alla città di implementare un sistema intelligente di equipaggiamenti di salvataggio lungo le coste svedesi, *www.stadshubbsalliansen.se/livboj*.

[41] Questo è quanto la Commissione Europea sta portando avanti con le proposte di regolamento sull'IA (COM/2021/206) e i due Digital Services Act (COM/2020/825) and Digital Markets Act (COM/2020/842).

[42] GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, *Orientamenti etici per un'IA affidabile*, 2019.

individuano 7 requisiti per un'IA affidabile. Tra questi requisiti ce n'è uno che merita particolare attenzione: l'*Accountability*.

Premesso che questa parola anglofona potrebbe essere tradotta in italiano con 'responsabilità' [43], occorre sin da subito chiarirne l'uso in questa sede. Nonostante il termine *Accountability* abbia un'origine latina (*ad+computare*), nella nostra lingua sembra essere assente una parola davvero equivalente al termine inglese, che ne comprenda estensivamente tutti i concetti ivi inclusi. Difatti, «*il senso di accountability non è identico a quello di responsabilità […]. La accountability è la qualità di chi è responsabile non solo in blocco e in modo indifferenziato ("se sbaglio, pago"), ma anche passo per passo, nel senso di essere fin dall'inizio pronto a fornire spiegazioni per ogni aspetto che compone il proprio agire complessivo*» [44].

Ciò posto, data la complessità dell'argomento in questione, si potrebbe dedicargli un intero contributo. Tuttavia, in questa sede, mi limito a sollevare brevemente l'attenzione su tre elementi da tenere indispensabilmente in considerazione. Primo, è fondamentale la consapevolezza degli esseri umani coinvolti nel ciclo di vita di un'IA per contribuire a una ripartizione corretta della responsabilità tra i diversi professionisti e per sviluppare sistemi di IA efficaci, etici e inclusivi. In altre parole, è indispensabile garantire sempre la presenza di un coinvolgimento umano nel ciclo di vita dell'IA, con un controllo efficace sullo sviluppo, l'implementazione e l'uso dei sistemi. Questo permette di determinare quale/i tra i numerosi professionisti è incaricato dei compiti di supervisione e manutenzione di ogni fase del ciclo di vita e, pertanto, di intraprendere un'azione correttiva proattiva [45]. Segnatamente, in caso di danni – e.g. patrimoniali o non, biologici o morali – occorre implementare meccanismi per individuare su chi cada la responsabilità di fornire spiegazioni per ogni aspetto che compone il proprio agire o quello del sistema, e di porre rimedio ai danni.

Secondo, l'*Accountability* dell'IA – e di riflesso degli esseri umani coinvolti "*in-the-loop*" [46] – per qualsiasi potenziale risultato dannoso del processo decisionale cambia durante l'intero ciclo di vita del sistema. Queste decisioni er-

---

[43] Tuttavia il testo italiano delle linee guida mantiene la dicitura inglese. V. *ivi*, p. 16.

[44] *Come possiamo tradurre accountability?*, in *www.accademiadellacrusca.it*, 2022.

[45] L'esecuzione inaccurata di un qualsiasi passaggio all'interno del ciclo di vita dell'IA si tradurrà in modelli fuorvianti o con *bias* intrinseche e risultati discriminatori.

[46] Il concetto di '*human-in-the-loop*' viene comunemente identificato con lo sviluppo di una soluzione per un problema tecnologico che includa le persone nella progettazione di detta soluzione. In altre parole, un operatore umano è una componente cruciale all'interno del processo automatizzato poiché introduce il controllo di supervisione umano. V. e.g. T.B. SHERIDAN, *Telerobotics, automation, and human supervisory control*, Cambridge, 1992.

ronee dipendono fortemente dalla fase in cui si trova l'errore nel modello, o dai dati usati per i vari *training*, o dal professionista (e dalle sue responsabilità) che era coinvolto nelle diverse fasi di progettazione, sviluppo e utilizzo del sistema di IA.

Terzo, come menzionato *supra*, queste IA urbane possono intraprendere azioni autonomamente. In un processo decisionale ibrido, è per lo più possibile spiegare la decisione dell'IA e ricollegarla all'azione di un professionista preposto o ai dati scelti e usati da quest'ultimo. Invece, nel caso di un processo decisionale completamente autonomo e non supervisionato (i.e. *deep learning*), questo processo di determinazione diventa più complesso. Qui è difficile anche per gli sviluppatori del sistema capire il ragionamento alla base del risultato dell'IA. Risulta quindi più arduo individuare il momento esatto in cui è sorto l'errore, in quale fase del ciclo di vita del sistema, o esattamente quali dati utilizzati per addestrare il modello sono alla base della deduzione o decisione errata dell'IA. In conclusione, per garantire l'*Accountability* delle IA urbane e dei loro risultati – sia prima che dopo la loro attuazione – nonché dei professionisti coinvolti, è imperativo mettere in atto adeguati meccanismi che minimizzino gli effetti sfavorevoli. Questi meccanismi devono tener conto dei tre elementi summenzionati, nonché della specifica legislazione applicabile all'industria di riferimento (si pensi alle differenti normative tra il settore pubblico e privato, o a settori regolamentati come il medicale) e a ogni elemento del caso concreto.

4. *Rilievi conclusivi*

Questi spunti di riflessione non vogliono presumere di essere un punto di arrivo, bensì un punto di partenza per stimolare ulteriori discussioni e individuare risposte opportune alle domande poste *supra*.

Come menzionato, le soluzioni intelligenti basate su sistemi di IA e *big data* urbani presentano un enorme potenziale per ottenere uguaglianza di genere e facilitare la transizione energetica, nonché per contrastare le dinamiche politico-economiche di disuguaglianza e discriminazione sul tessuto urbano. Esse sono in grado di offrire una più agile pianificazione e gestione dei servizi urbani e possono contribuire ad una crescita sostenibile e al miglioramento della vita dei cittadini.

Tuttavia, trattandosi di problemi complessi, le riflessioni di cui sopra non si adeguano a soluzioni univoche. Esse esigono invece un approccio multidisciplinare e adattabile ai rapidi mutamenti a cui la tecnologia è soggetta. Difat-

ti, l'IA è una tecnologia poliedrica ed in costante evoluzione. È pertanto difficile ricollegarla ad una sola disciplina o definirla sotto un'unica categoria che ne includa tutte le funzionalità e gli usi.

Alla luce di ciò, occorre dunque che anche i giuristi siano coinvolti in primo piano nelle discussioni relative all'uso, ai limiti da porre, e a come regolamentare i sistemi di IA, accanto a *data scientist*, ingegneri, filosofi, sociologi e gli altri professionisti necessariamente coinvolti.

Segnatamente, è indispensabile che questi ultimi e le IA urbane da loro sviluppate siano soggetti ad un'apposita *governance* e a meccanismi giuridici che ne garantiscano l'*Accountability* e che minimizzino gli effetti negativi delle eventuali decisioni illecite che possono innescare cambiamenti radicali nella città.

Infine, si è detto come non è reprimendo l'innovazione e l'uso di tecnologie emergenti che potremo muoverci verso un futuro migliore, che offra nuove opportunità di benessere per i cittadini. Bensì, occorre un quadro normativo chiaro e un approccio multidisciplinare che tolga la tecnologia dal fulcro della discussione e rimetta al centro i bisogni, le necessità e i diritti dei cittadini.

In conclusione, è indispensabile impegnarsi per sviluppare una struttura giuridica come meccanismo di controllo dell'IA urbana, la quale al contempo ne supporti l'uso per il miglioramento delle politiche sociali, ne limiti gli abusi e i potenziali rischi per i cittadini, e ne garantisca l'*Accountability* per qualsiasi conseguenza avversa.

SMART CITIES E DIMENSIONI DELLA SOLIDARIETÀ

di *Matteo Giannelli*

SOMMARIO: 1. Solidarietà e doveri dopo la pandemia. – 2. Società digitale e solidarietà: un rapporto in via di definizione. – 3. Tra pubblico e privato: immagini del tortuoso percorso italiano della solidarietà digitale. – 4. Solidarietà digitale e cultura della condivisione. Dimensione locale e dimensione globale.

1. *Solidarietà e doveri dopo la pandemia*

Nell'affrontare il tema delle nuove declinazioni del principio di solidarietà nella società digitale è necessario partire dalla constatazione che le conseguenze socio-economiche della pandemia da SARS-CoV-2 abbiano creato disuguaglianze ed emarginazioni riguardanti, in primo luogo, soggetti di fatto già discriminati [1]. In un simile contesto le *smart cities* – rappresentando l'archetipo dell'applicazione dell'innovazione tecnologica alla vita delle comunità – possono identificare una politica di contrasto alle diseguaglianze ma, allo stesso tempo, veicolare l'emersione di inedite diseguaglianze. Un punto di partenza che deve esser ben evidenziato dedicato al rapporto tra *smart cities* e dimensioni della solidarietà.

Durante il primo *lockdown* e nelle fasi immediatamente successive – come normalmente accade durante i periodi di emergenza – il principio di solidarietà è stato richiamato in più occasioni nella narrazione operata sia da parte dei pubblici poteri che dai principali mezzi di informazione [2]. Si è trattato, tutta-

[1] Cfr. in particolare, i contributi contenuti nel volume A. PAJNO, L. VIOLANTE, *Biopolitica, pandemia e democrazia*. Rule of law *nella società digitale*, vol. II, *Etica, comunicazione e diritti*, Bologna, 2021, e, in particolare, A. SIMONCINI, *L'uso delle tecnologie nella pandemia e le nuove disuguaglianze*, p. 225 ss.

[2] Sul ruolo di questi ultimi nella pandemia e sulla loro natura di poteri privati o sociali, v.

via, di un appello vago, in mera funzione anti-individualistica, limitato a forme di solidarietà nel *lockdown* e del tutto disinteressato a quanto ci fosse da realizzare *a seguito* del *lockdown*, correndo così il rischio di apparire come puramente ideologico.

Una riflessione giuridica sul «risveglio della solidarietà»[3], e sulle sue declinazioni riferite alla *smart city*, non può, dunque, prescindere, dalle dimensioni enunciate dall'art. 2 della Costituzione – solidarietà politica, economica e sociale – e da una conseguente e precisa individuazione dei diversi soggetti ai quali sono riferibili i doveri costituzionali[4]. Ciò equivale a chiedersi se le diseguaglianze emerse nel corso della pandemia impongano, o meno, un nuovo modo di pensare a questi, ben al di là di alcune, più o meno recenti, contrapposizioni tra "età dei diritti" ed "età dei doveri"[5].

Sul punto, peraltro, non si può fare a meno di riconoscere che nella storia repubblicana la cultura dei doveri – o, per alcuni, delle responsabilità – sia rimasta in secondo piano[6]. Il coordinamento sistematico tra diritti e doveri, infatti, è stato sviluppato solo in parte dalla giurisprudenza[7] e dalla dottrina costituzionalistica[8], anche se, negli ultimi anni, è possibile registrare una certa inversione di tendenza[9] con la pubblicazione di studi e lavori volti innanzitutto a ri-

---

G.E. VIGEVANI, *Sistema informativo e opinione pubblica al tempo della pandemia*, in *Quaderni costituzionali*, 2020, p. 779 ss.

[3] Per utilizzare l'espressione di E. MORIN (con la collaborazione di S. ABOUESSALAM), *Changeons de voie. Les leçons du coronavirus*, Éditions Denoël, Paris, 2020 (trad. it. R. PREZZO, *Cambiamo strada. Le 15 lezioni del coronavirus*, Milano, 2020, p. 33 ss.).

[4] Evidenziato da A. MORELLI nei numerosi lavori dedicati al tema: di recentesi veda l'editoriale *Doveri costituzionali e principio di solidarietà*, in *Diritto costituzionale*, 2/2019, p. 5 ss.

[5] Per una proposta di lettura dell'art. 2 che abbia come riferimento la considerazione che la "Repubblica dei doveri inderogabili" e la "Repubblica dei diritti inviolabili" sono due gambe dello stesso corpo, le quali o stanno insieme o vengono fatalmente meno entrambe cfr. M. FIORAVANTI, *Art. 2*, Bari, 2017, p. 22.

[6] Basti pensare a quanto affermato da Noberto Bobbio in un dialogo con Maurizio Viroli: «se avessi qualche anno, che non avrò, sarei tentato di scrivere L'età dei doveri», così in N. BOBBIO, M. VIROLI, *Dialogo intorno alla Repubblica*, Roma-Bari, 2001, p. 40.

[7] Su cui cfr. E. LONGO, *Corte costituzionale, diritti e doveri*, in F. DAL CANTO, E. ROSSI (a cura di), *Corte costituzionale e sistema istituzionale. Giornate di studio in ricordo di Alessandra Concaro*, Torino, 2011, p. 339 ss.

[8] Lo nota M. OLIVETTI, *Diritti fondamentali*, Torino, 2018, p. 14.

[9] Per questa affermazione E. ROSSI, *Relazione introduttiva*, in F. MARONE (a cura di), *La doverosità dei diritti: analisi di un ossimoro costituzionale?*, Napoli, 2019, p. 9 ss., cui si rinvia per i numeri riferimenti bibliografici, anche risalenti (a partire da G. LOMBARDI, *Contributo allo studio dei doveri costituzionali*, Milano, 1967), che non è possibile riportare in questa sede. Sul versante della giurisprudenza della Corte costituzionale si segnala la sentenza n. 114/2019 in cui

costruire i fondamenti teorici del principio solidaristico, la loro compatibilità con il tema dei diritti e, perfino, la necessità di una "riscoperta" dei doveri per la vita democratica, in modo da dare nuova linfa al concetto di etica repubblicana [10].

L'individuazione dell'oggetto e della latitudine dei doveri rappresenta, dunque, un problema persistente. Un processo reso ancora più complesso dalla svalutazione e dalla conseguente crisi del principio di solidarietà su cui essi si fondano [11], specie alla luce di quei tentativi che sembrano confinarlo in un terreno meramente altruistico [12].

2. *Società digitale e solidarietà: un rapporto in via di definizione*

Uno degli obiettivi principali della dimensione costituzionale della solidarietà, nella sua congiunzione con l'eguaglianza, è rappresentato dall'inclusione. Un fine ancora più arduo da raggiungere in un mondo "dilatato", come quello emerso durante la pandemia, in cui alla relazione si è sostituita la connessione [13]. Un contesto in cui sembra bruscamente svanire uno spazio fisico, come quello rappresentato generalmente dalle città: luoghi vocati, per le loro dimensioni e articolazioni, a costruire tessuti sociali rendendo così possibile la garanzia dei diritti attraverso concetti chiave come sussidiarietà orizzontale, eguaglianza e sostenibilità [14].

Proprio a partire da questa cornice muove la riflessione sulla solidarietà digitale come forma di relazionalità che implica un *diverso* modo di pensare ai doveri costituzionali e di reagire alle diseguaglianze.

---

viene esplicitato il legame tra garanzia dei diritti e adempimento dei doveri («nell'architettura dell'art. 2 Cost. l'adempimento dei doveri di solidarietà costituisce un elemento essenziale tanto quanto il riconoscimento dei diritti inviolabili di ciascuno»).

[10] Su cui. M. VIROLI, *Repubblicanesimo*, Roma-Bari, 1999.

[11] Così A. APOSTOLI, *La svalutazione del principio di solidarietà*, Milano, 2012, spec. p. 141 ss.

[12] Mette in luce il rapporto tra carità, assistenza e solidarietà S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014, p. 57 ss.

[13] Ancora A. SIMONCINI, *L'uso delle tecnologie nella pandemia e le nuove disuguaglianze*, cit., pp. 225-226.

[14] Sul punto cfr. F. FRACCHIA, P. PANTALONE, *Smart City: condividere per innovare (e con il rischio di escludere?)*, in *Federalismi*, 22/2015, spec. p. 17 ss. Sulla città come «autentico luogo paradigmatico della contemporaneità e delle sue continue trasformazioni» cfr. C. ACOCELLA, G. LANEVE, *Città intelligenti e diritti: nuove prospettive di consumo nel prisma della socialità*, in *P.A. Persona e Amministrazione*, 2/2021, pp. 105 ss., spec. p. 119, anche per la citazione riportata nel testo.

Gli autori che hanno riflettuto in maniera sistematica sul concetto di solidarietà digitale e sulle sue possibili declinazioni sono partiti dalla considerazione che questa potesse rappresentare una delle direttrici su cui lavorare per creare una via d'uscita dalla crisi economica e, in particolare, dai suoi inevitabili riflessi sociali, capaci di confinare i singoli nelle proprie individualità [15].

Nel 2013 il sociologo Felix Stalder si è servito del sintagma solidarietà digitale legandolo alla nozione di condivisione e alla rivalutazione del concetto di beni comuni *online* ("*digital commons*") al fine di teorizzare una forma di interconnessione in grado di fornire un potenziale strutturale al concetto stesso di solidarietà [16]. Evgeny Morozov, per altro verso, ha ricordato che le stesse infrastrutture tecnologiche possono esser utilizzate per creare democrazia o consumo, citando, a tal proposito, l'esempio della Cina dove il *Social Credit System* promuove la convivenza sociale con regole in linea con il controllo statale [17]. Morozov sottolinea come le disuguaglianze siano accentuate dai giganti digitali, ragion per cui risulta necessario trovare il modo per democratizzare la *ricchezza* e ridare slancio al ruolo dello Stato: il rischio che si corre, altrimenti, è quello di un'esplosione sociale causata dagli squilibri creati a livello globale dal mondo digitale [18].

Particolarmente significative sono le riflessioni sulle città come laboratori digitali per la democrazia e la sostenibilità, pur nella consapevolezza dell'impossibilità di una soluzione locale a problemi nazionali e globali. Un modello che, in ogni caso, appare in grado di formare reti e coalizioni sociali attraverso la sperimentazione di una serie di tecnologie che consentano la gestione di alcune politiche pubbliche (da quelle riguardanti i trasporti pubblici fino alle questioni abitative, passando per la sanità e l'istruzione) in una logica di solidarietà [19]. Una simile declinazione del concetto di *smart cities*, dunque, po-

---

[15] Inevitabile il confronto con il pensiero di Émile Durkheim per il quale un fattore cruciale della solidarietà è rappresentato dall'"effervescenza collettiva", ossia quel sentimento che si prova a far parte di un gruppo che ci porta fuori dalla nostra individualità. Cfr. É. DURKHEIM, *De la division du travail social*, Paris, 1893 (trad. it. F. AIROLDI NAMER, *La divisione del lavoro sociale*, Milano, 1971, p. 231 ss.).

[16] F. STALDER, *Digital solidarity*, London, 2013, spec. p. 31 ss.

[17] Risale al 2011 il contributo in cui il sociologo bielorusso aveva constatato l'assenza di virtù palingenetiche della rete ed espresso le sue posizioni critiche, cfr. E. MOROZOV, *The Net Delusion: The Dark Side of Internet Freedom*, New York, 2011.

[18] E. MOROZOV, *Digital Socialism? The Calculation Debate in the Age of Big Data*, in *New Left Review* 116/117 (March-June), 2019, p. 33 ss., spec. 54. Di recente cfr. ID., *The tech 'solutions' for coronavirus take the surveillance state to the next level*, in *The Guardian*, 15 April 2020.

[19] In termini ampi cfr. E. OLIVITO, *Dis)eguaglianze, città e periferie sociali: la prospettiva costituzionale*, in *Rivista AIC*, 1/2020, pp. 1 ss., spec. p. 44 ss.

trebbe essere un veicolo attraverso cui istituzionalizzare forme di solidarietà anzitutto economica ma, allo stesso tempo, un'occasione per «mantenere la promessa di ridare alle città una dimensione adatta alle persone, e ciò significa anche democratizzare la proprietà e l'accesso alle tecnologie digitali»[20].

Al termine di questa breve rassegna, dovrebbe risultare evidente, che, pur nelle molteplici e possibili declinazioni, l'eventualità di riconoscere una dimensione giuridica vincolante al concetto di solidarietà digitale si connette, inscindibilmente, con l'individuazione dei destinatari di tale dovere[21]. Il tema è stato affrontato dal punto di vista giuridico – e, dunque, della sua capacità di tradursi in precise regole all'interno di singole disposizioni legislative o altre fonti – con riferimento ai rapporti tra privati che si realizzano nell'ambito degli *Smart contracts*, dove si è sostenuto che la solidarietà contrattuale debba lasciare spazio alla solidarietà digitale, idonea anzitutto a ricreare una forma di relazione tra i soggetti coinvolti[22].

Da un punto di vista del diritto costituzionale è, in primo luogo, necessario ricostruire i termini del rapporto tra pubblico e privato: è evidente che il ruolo primario dello Stato (e delle Regioni e degli enti locali) non potrà fare a meno di relazionarsi con le grandi società transnazionali.

La solidarietà digitale si traduce, infatti, in un principio capace di rivolgersi sia ai poteri pubblici sia, soprattutto, ai poteri privati. Se i primi, sia a livello nazionale che sovranazionale, possono – anzi devono – attuare delle azioni che abbiano come obiettivo primario il superamento il *digital divide* e la realizzazione delle condizioni per una vera e propria cittadinanza digitale, più incerti sembrano i contenuti giuridici degli obblighi di cui possono esser destinatari i secondi.

---

[20] Così il Rapporto sull'investimento delle infrastrutture sociali in Italia (ricerca coordinata da E. TREVIGLIO), *Rilanciare le infrastrutture sociali in Italia*, promosso dalla Fondazione ASTRID e dalla Fondazione Collegio Carlo Alberto della Compagnia di San Paolo, e in particolare il par. 5.5 dedicato al caso di studio Barcellona. Sul punto v. anche F. BRIA, E. MOROZOV, *Rethinking the Smart City. Democratizing Urban Technology*, January 2019, New York, 2018; con riferimento alla teoria del *nudge*, S. RANCHORDÁS, *Nudging Citizens through Technology in Smart Cities*, in *International Review of Law, Computers & Technology*, vol. 33, 2019, disponibile in SSRN: *https://ssrn.com/abstract=3333111*.

[21] Nella consapevolezza che l'impostazione legislativa dei doveri non esaurisca la sfera della solidarietà: per il riferimento alla dimensione costituzionale della "solidarietà spontanea" cfr. F. GIUFFRÈ, *I doveri di solidarietà sociale*, in R. BALDUZZI, M. CAVINO, E. GROSSO, J. LUTHER, *I doveri costituzionali: la prospettiva del Giudice delle leggi*, Torino, 2007, p. 42.

[22] F. GHODOOSI, *Digital Solidarity: Contracting in the Age of Smart Contracts*, September 7, 2019, disponibile in SSRN: *https://ssrn.com/abstract=3449674*; che rinvia allo studio di D. MARKOVITS, *Arbitration's Arbitrage: Social Solidarity at the Nexus of Adjudication and Contract*, 59 *Depaul l. Rev*. 431, 469 (2009).

Tuttavia, sono proprio questi ultimi, in quanto detentori dei dati, a poter dare un contributo imprescindibile per il raggiungimento delle medesime finalità di interesse pubblico, in un'ottica capace di richiamare la dimensione orizzontale della sussidiarietà e, quindi, di incidere con forza maggiore proprio sulla dimensione locale. In altre parole, la trasformazione digitale della società, unitamente al suo carattere trasversale rispetto a prospettive di regolazione sia nazionali che sovranazionali, richiede un cambio di paradigma anche rispetto ai soggetti destinatari dei doveri.

3. *Tra pubblico e privato: immagini del tortuoso percorso italiano della solidarietà digitale*

L'interpretazione che intendeva come destinatario dell'obbligo di solidarietà il solo potere pubblico deve oramai ritenersi superata[23]. Tale obbligo, che si concreta, innanzitutto, in una rimozione degli ostacoli digitali, non riguarda esclusivamente lo Stato, e le sue articolazioni, ma concerne tutti i soggetti e gli operatori coinvolti nell'utilizzo di tecnologie e servizi digitali, a partire dalle grandi multinazionali dell'innovazione tecnologiche (le c.d. *Big Tech*). Queste realtà sono, infatti, potenze economiche e digitali sempre più capaci di determinare e di orientare politiche, stili di vita e di lavoro, condizioni culturali e sociali.

Il rapporto che si verrà a creare tra questi poteri non dovrà, tuttavia, assumere le forme della beneficenza e generosità, da un lato, e della riconoscenza, dall'altro. Una simile costruzione del legame tra pubblico e privato si rinviene, invece, nel concetto di "solidarietà digitale" promosso, o per meglio dire *pubblicizzato*, dal Ministero per l'Innovazione tecnologica e la digitalizzazione italiano a partire dalla prima fase della pandemia nella primavera del 2020.

Questa iniziativa, che assumeremo come paradigmatica, ci aiuta a riflettere sul rapporto tra gratuità e solidarietà, tra spirito di liberalità e lo spirito di solidarietà e, in definitiva, sull'«agire non egoistico come deviazione da un modello di comportamento non razionale»[24]. Con essa i grandi monopoli privati (Amazon, Microsoft, Google, ecc.) offrono, attraverso una piattaforma pubblica[25], dei contenuti e dei servizi che sono solo apparentemente gratuiti, ma

[23] Ci si sofferma con attenzione G. SCOTTI, *Alla ricerca di un nuovo costituzionalismo globale e digitale: il principio di solidarietà "digitale"*, in *Forum di Quaderni Costituzionali*, 2, 2021, p. 415 ss.

[24] Sul punto v. G. RESTA, *Gratuità e solidarietà: fondamenti emotivi e irrazionali*, in *Rivista critica del diritto privato*, 2014, p. 39 ss.

[25] Consultabile al link: *https://solidarietadigitale.agid.gov.it/*.

che, in realtà, rappresentano un'importante occasione di raccolta e utilizzo dei dati, per di più in ambiti cruciali – basti pensare alle cinque categorie individuate: connettività, *e-learning*, *smart working*, informazione e svago, supporto ai cittadini [26] – e senza la consapevolezza necessaria da parte degli utenti coinvolti.

In sintesi, si è trattato di un tentativo meritevole di attenzione dal punto di vista meramente formale della collaborazione tra istituzioni pubbliche e soggetti privati durante il *lockdown*. Il rapporto tra solidarietà privata e solidarietà pubblica, infatti, si pone come tema centrale, anche alla luce, della formulazione dell'art. 118 della Costituzione che ha aperto nuovi e inediti spazi per quanto riguarda la realizzazione di doveri inderogabili nell'ambito di talune attività di interesse generale [27].

Il principio di solidarietà, tuttavia, anche qualora si tratti di una solidarietà digitale, richiede primariamente un'azione positiva delle istituzioni pubbliche, nella specifica prospettiva dell'art. 3, comma 2, della Costituzione, che sia in grado di orientare e determinare la formazione di una serie di regole giuridiche, provenienti anche da soggetti privati. Per questa ragione, di pari passo con la promozione dei servizi offerti, il Governo italiano avrebbe dovuto stipulare, specie in assenza di codici deontologici, alcuni protocolli capaci di individuare e tutelare i dati sensibili delle persone, delle istituzioni e delle imprese coinvolte. È interessante notare come, al contrario, non vi fosse traccia di questi aspetti: alle aziende interessate veniva richiesto, in un'ottica di carattere puramente commerciale, di eliminare l'obbligo di rinnovo al termine del periodo dell'offerta (la cui descrizione non doveva esser redatta «in tono promozionale»), la diffusione della stessa su tutto il territorio nazionale, o su una o più regioni, e la creazione di un canale di adesione appositamente dedicato all'iniziativa [28].

---

[26] Per un'analisi dei contenuti e dei servizi cfr. P. ZUDDAS, *Covid-19 e* digital divide*: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio AIC*, 3/2020, p. 302 ss.

[27] Così G. TARLI BARBIERI, *Doveri inderogabili*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 2072.

[28] Solo nella c.d. "fase 2" della solidarietà digitale – in cui la richiesta si è concentrata sulla ripartenza delle attività didattiche attraverso l'offerta di soluzioni innovative e servizi digitali a supporto dell'istruzione scolastica – sono stati definiti dei requisiti di partecipazione maggiormente stringenti: nell'allegato all'Avviso pubblico diffuso dal Ministero per l'Innovazione tecnologica e la digitalizzazione erano contenuti requisiti di partecipazione che facevano riferimento ai concetti di "sicurezza, affidabilità, scalabilità e conformità alle norme sulla protezione dei dati personali, nonché divieto di utilizzo a fini commerciali e/o promozionali di dati, documenti e materiali di cui gli operatori di mercato entrano in possesso per l'espletamento del servizio". Cfr. *https://innovazione.gov.it/assets/docs/Didattica_Digitale_Avviso_Manifestazione_interesse_2020_09_28.pdf* e *https://innovazione.gov.it/assets/docs/Allegato%20A_Avviso__Pubblico_Didattica Digitale.pdf.*

Allo stesso modo anche a livello locale, la città intelligente può essere un formidabile strumento di inclusione e di partecipazione[29], mettendo i suoi "utenti" al riparto dal concreto rischio di propagare fattori di discriminazione socio-spaziale, che incidono sulla «distribuzione di risorse e di opportunità per chi non abbia le indispensabili abilità o propensioni tecnologiche»[30].

La *smart city*, come detto, rappresenta l'archetipo dell'applicazione dell'innovazione tecnologica alla vita della comunità: digitalizzazione, *e-government*, cittadinanza digitale, open data, industria 4.0, *smart* e *green mobility*, nuove forme di istruzione e di lavoro, sicurezza, salute. Una dimensione nella quale sussidiarietà verticale ed orizzontale possono realizzarsi secondo geometrie inedite, mentre vengono sperimentate nuove forme di partenariato pubblico-privato e di *governance*.

In essa emergono anche nuovi rischi, che in parte riproducono e acuiscono dinamiche già note: l'utilizzo malevolo delle informazioni, con gravi pregiudizi per i diritti e le libertà delle persone fisiche e per il corretto funzionamento del sistema democratico; le distorsioni del mercato, con i giganti del mondo tecnologico che accrescono costantemente i loro oligopoli; le questioni etiche legate all'utilizzo sempre più consistente dei sistemi di *machine-learning*.

Unione europea, Governi nazionali, enti locali, Università e centri di ricerca, Autorità di controllo ed Agenzie, sono chiamati a collaborare virtuosamente per rispondere alle innumerevoli questioni emergenti e per contribuire al migliore utilizzo delle nuove tecnologie al servizio delle comunità, anche al fine di rafforzare il *Digital Single Market* e di assicurare la competitività europea a livello globale.

4. *Solidarietà digitale e cultura della condivisione. Dimensione locale e dimensione globale*

La solidarietà digitale potrà, dunque, tradursi in un veicolo di regolazione solo qualora si dimostri capace di assumere un contenuto giuridico che determini, innanzitutto, nuove forme di partecipazione. Una solidarietà non fine a sé stessa, solitaria, ma determinata a creare fiducia reciproca e a incide-

[29] Su cui in termini critici, anche con riferimenti alle varie declinazioni, E. SPILLER, *Citizens in the loop? Partecipazione e Smart city*, in F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), *La città e la partecipazione tra diritto e politica*, Torino, 2019, p. 289 ss.

[30] Così E. OLIVITO, *Dis)eguaglianze, città e periferie sociali: la prospettiva costituzionale*, cit., p. 49.

re sulla declinazione attuale del concetto stesso di cittadinanza [31].

Da più parti, spesso in maniera retorica, si è sottolineato che, una volta superata la pandemia da Covid-19, non si potranno e non si dovranno ripetere le azioni passate. I termini di questo cambiamento, tuttavia, non sono stati chiariti, rimanendo vaghi e indefiniti.

Un'inversione di rotta sarà possibile, innanzitutto, attraverso una politica europea delle reti capace non solo di contrastare e regolare efficacemente il dilagare delle piattaforme digitali c.d. *Over The Top* [32] ma anche di porre una grande questione di controllo democratico sull'accesso ai dati e una finalità sociale delle tecnologie digitali [33]. Temi che sembrano attualmente assenti nel dibattito pubblico [34] e che, invece, sono stati richiamati dal Garante europeo per la protezione dei dati personali nel piano strategico per il quadriennio 2020-2024 [35]. Il paradosso della solidarietà digitale è, infatti, messo in luce dall'esperienza cinese, già richiamata, del *Social credit system*, dove l'accesso alla rete è sintomo di controllo sociale.

Negli ambiti chiave dell'istruzione e del lavoro, in cui si sono verificati le disuguaglianze più evidenti, la solidarietà digitale dovrebbe tradursi anzitutto in forme di consapevolezza critica nell'uso degli strumenti messi a disposizioni durante l'emergenza: accanto alle questioni infrastrutturali vi sono anche quelle, altrettanto fondamentali, delle competenze digitali. Inoltre, le istituzioni pubbliche dovrebbero sviluppare dei *software open source* [36]: un investimento im-

---

[31] Cfr. ancora l'opera di S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., p. 115 ss.

[32] A partire dagli interventi che costituiscono la *Strategia europea per il digitale*. Si pensi all'impatto che potranno avere il *Digital services act* (DSA) e il *Digital Markets Act* (DMA) sulle piattaforme *online*, specie in termini di trasparenza e responsabilità dei processi algoritmici.

[33] Di recente per una prospettiva critica estesa al GDPR e, in particolare, all'eccessiva attenzione posta sulla protezione dei dati, definita come "religione", e non al loro uso, si veda il pamphlet V. MAYER-SCHÖNBERGER, T. RAMGE, *Access Rules. Freeing information to stop Big Tech, revive innovation, and empower society*, Berkeley, 2020 (trad. it. E. CIANCO, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, Milano, 2021).

[34] Si pensi al caso italiano della rete unica verticalmente integrata, su cui cfr. *Rete unica per sostenere Telecom Italia, una chiave di lettura*, in *HDblog.it*, 6 ottobre 2020; *Tim e Open Fiber: aspettiamo a seppellire la concorrenza*, in *Il Sole 24ore*, 22 settembre 2020, disponibile all'indirizzo: *https://www.econopoly.ilsole24ore.com/2020/09/22/tim-open-fiber-concorrenza/*.

[35] Dove si sottolinea la necessità di un approccio pan-europeo al contrasto della pandemia di Covid-19 basato sulla solidarietà digitale e sulla condivisione dei principi di protezione dati a tutela, innanzitutto dei soggetti più vulnerabili, *https://edps.europa.eu/press-publications/press-news/news#news_5895*.

[36] Sul concetto di "*free software*" e sulla sua necessaria declinazione in termini di trasparenza e conoscibilità cfr. L. LESSIG, *Foreword to the First Edition*, in *Free Software, Free Society: Selected Essays of Richard M. Stallman*, III ed., Boston, 2015, p. vii, per cui «Free software is con-

portante finalizzato a creare maggiore cognizione nell'utilizzo di questi strumenti, sulla scorta di coloro che hanno segnalato come l'impiego di programmi simili possa consentire una maggiore trasparenza come forma di democrazia digitale[37].

L'assenza di consapevolezza è tuttora una delle fonti da cui si alimenta il *digital divide* e ha reso le piattaforme di cui oggi disponiamo delle mere infrastrutture di consumo individualizzato, non di condivisione e assistenza reciproca.

Lo sviluppo dell'infrastruttura tecnologica e la promozione di una cultura digitale rappresentano, dunque, lo spazio in cui possono muoversi le ragioni della solidarietà digitale. Due orizzonti chiave, da un punto di visto politico-democratico, per realizzare quella «piena appartenenza a una comunità»[38] che conferisce significato al concetto di cittadinanza e al cui interno non può mancare quello spirito di solidarietà che "è, e deve essere, alla base del rapporto permanente fra i cittadini e la collettività espressa e rappresentata dalle istituzioni pubbliche"[39].

La riflessione sulla solidarietà digitale, tuttavia, non può esser limitata al solo contesto locale ma deve esser condotta anche nel contesto globale e, per questo, deve misurarsi con gli attori che lo popolano. La trasformazione digitale, con i suoi caratteri di universalità, e trasversalità, impone un punto di vista che sia riferito al potere esercitato dalle grandi multinazionali cui si è fatto riferimento.

La proiezione delle dimensioni della solidarietà oltre i confini dello Stato nazionale è, dunque, un ulteriore terreno su cui poter verificare le effettive possibilità della solidarietà digitale.

Sul punto può esser utile tornare alla primavera del 2020, al primo *lock-*

---

trol that is transparent, and open to change, just as free laws, or the laws of a "free society," are free when they make their control knowable, and open to change».

[37] Nella dottrina italiana v. G. ZICCARDI, *Democrazia elettronica e libertà dei dati tra sistemi elettorali e WikiLeaks*, in *Ciberspazio e diritto*, 1/2011, p. 8 ss.; M.F. DE TULLIO, *Solidarietà e Covid-19*, in G. DE MINICO, M. VILLONE (cura di), *Stato di diritto – Emergenza – Tecnologia*, e-book disponibile su *Consulta Online*, 2020, p. 156 ss. Infine, con riferimento alle riforme della p.a. italiana e, in particolare, alla legge n. 124/2015, B. CAROTTI, *L'amministrazione digitale e la trasparenza amministrativa*, in *Giornale di diritto amministrativo*, 5/2015, p. 627.

[38] Così T.H. MARSHALL, *Citizenship and social class, and other essays*, Cambridge, 1950 (tr. it. S. MEZZADRA, *Cittadinanza e classe sociale*, Roma-Bari, 2002, p. 10). la cui riflessione sulle forme della cittadinanza risulta imprescindibile. Nella letteratura italiana P. COSTA, *Civitas. Storia della cittadinanza in Europa*, vol. 4, *L'età dei totalitarismi e della democrazia*, Roma-Bari, 2001, spec. p. 483 ss.

[39] Così V. ONIDA, *Costituzione e corona virus. La democrazia nel tempo dell'emergenza*, Milano, 2020, p. 37.

down, quando Apple e Google hanno condiviso pubblicamente i dati sulla mobilità, mostrando il traffico di persone in vari contesti sociali: sulla base di tali dati i decisori politici hanno potuto trarre alcune importanti indicazioni sul rispetto delle misure di contenimento e gestione dell'epidemia da essi introdotte. In seguito alla pubblicazione di questi *Community Mobility Reports*, anche Facebook attraverso il suo programma "Data for Good" ha lanciato un'iniziativa per condividere i dati aggregati e anonimizzati in suo possesso con istituzioni, università e centri di ricerca in una serie di Paesi, tra cui l'Italia. L'obiettivo, in questo caso, era la formulazione di un modello predittivo di diffusione del contagio da coronavirus e la creazione di una mappa dei sintomi, in relazione alla presenza di persone in un determinato territorio.

Queste iniziative *open data* di alcune delle *Big Tech* costituiscono un potenziale indice di una rinnovata sensibilità sociale. Un atteggiamento che, tuttavia, va valutato attentamente: se da un lato può identificare la consapevolezza che il potere delle informazioni in loro possesso comporta un elevato livello di responsabilità nei confronti della società e, allo stesso tempo, qualifica come insufficienti le azioni volontarie finora intraprese; dall'altro potrebbe trattarsi di una mera donazione a fini tattici per «generare qualche articolo positivo sui giornali» e accontentare il decisore politico [40].

Una preoccupazione che sembra fondata ma che, in via generale, sembra aver in qualche misura posto un aggravio di responsabilità «all'uso delegato e oscuro dei dati di terzi» dalla quale non ci si dovrebbe poter sottrarre se non con la prova di aver fatto quanto era nelle proprie possibilità [41]. Una ricostruzione in cui il vincolo di solidarietà sociale, l'etica d'impresa, sia *off-line* o *online*, acquistano una loro dimensione autonoma e prevalente sulla finalità lucrativa così come richiesto dalla gerarchia costituzionale dei valori [42].

Il comportamento delle *Big Tech* – si potrebbe citare a mero titolo di esempio il noto caso delle *app* di tracciamento – illustra chiaramente come il controllo sulle informazioni in un mondo guidato dai dati si sia spostato a favore di coloro che generano, archiviano e analizzano i flussi delle informazioni sulle loro piattaforme digitali.

Il concetto di solidarietà digitale si lega, quindi, inscindibilmente con la tematica della condivisione dei dati. Se nella prospettiva della regolazione non sembra possibile, o addirittura pensabile, rompere i monopoli delle informa-

---

[40] È la posizione espressa da V. MAYER-SCHÖNBERGER, T. RAMGE, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, cit., pp. 309-310.

[41] Sul punto, anche per la citazione che precede, cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche*. Privacy *e* lex mercatoria, in *Dir. pubbl.*, 2019, p. 97.

[42] *Ibidem*.

zioni, risulta quantomai necessario ricavare degli spazi in cui stabilire degli obblighi: il caso dei dati sanitari anonimizzati e relativi alla ricerca, per esempio, potrebbe esser paradigmatico di una libera circolazione, condivisione e utilizzo a fini sociali. Il tutto in un contesto in cui oltre l'80% dei dati raccolti non viene usato nemmeno una volta [43] e che, dunque, anche per ragioni – per certi versi paradossali – connesse al valore dei dati medesimi, impone lo sviluppo di una nuova disciplina volta a estendere, promuovere e tutelare l'accesso libero ai dati accumulati da soggetti privati di grandi dimensioni da parte dei soggetti pubblici interessati a servirsene per obiettivi sociali o di informazione [44].

In conclusione, è proprio in un simile panorama che risulta imprescindibile collocare la realtà delle *Smart Cities*, intese innanzitutto come modello dello sviluppo urbano [45] e veicolo, attraverso la loro dimensione tecnologica, di solidarietà ed eguaglianza sostanziale.

[43] V. MAYER-SCHÖNBERGER, T. RAMGE, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, cit., p. 203.

[44] Su cui in questo volume cfr. G. RESTA, *Le* smart cities *e il rilievo sociale dei dati*, p. 201 ss., con particolare riguardo alle evoluzioni della disciplina europea.

[45] Sul punto G.F. FERRARI, *Smart City: l'evoluzione di un'idea,* in ID. (a cura di), *Smart City. L'evoluzione di un'idea*, Milano, 2020, 13 ss.

POLIZIA PREDITTIVA E *SMART CITY*: VECCHIE E NUOVE SFIDE PER IL DIRITTO PENALE

di *Giulia Tavella*

SOMMARIO: 1. Introduzione. – 2. Polizia predittiva. – 3. Il quadro normativo attuale. – 4. Polizia predittiva e *smart city*. – 5. Vecchie e nuove sfide per il diritto penale.

1. *Introduzione*

Nel mondo si fa sempre più avanti l'idea della *smart city*, archetipo di città intelligente e interconnessa, capace di implementare soluzioni tecnologiche per i bisogni della società [1].

È stato osservato che la crescita del fenomeno *smart city* si ripercuote inevitabilmente sullo sviluppo della polizia predittiva e viceversa: se, da un lato, la città "intelligente" permette di incrementare i dati a disposizione dei *software* di polizia predittiva, dall'altro, questi ultimi ne condividono la strategia di efficienza, cercando di prevenire e/o contrastare la criminalità [2].

Invero, secondo un approccio di tipo prettamente economico, mentre fenomeni quali la raccolta della spazzatura o la gestione delle luci sono direttamente proporzionali all'efficienza della città, la criminalità, al contrario, ne è inversamente proporzionale, in quanto la sua presenza incide sull'economia del nucleo urbano. I software di polizia predittiva, pertanto, permetterebbero

[1] Sebbene non ci sia una definizione unanime del concetto di *smart city*, come tale generalmente si intende un'area urbana in cui le reti e i servizi tradizionali sono resi più efficienti attraverso l'uso di tecnologie digitali e di telecomunicazione, a beneficio degli abitanti e delle imprese. Ciò comporta, ad esempio, reti di trasporto urbano più intelligenti, forniture d'acqua migliorate e strutturate per lo smaltimento dei rifiuti, modi più efficienti per illuminare e riscaldare gli edifici, così come un'amministrazione cittadina più interattiva e spazi pubblici più sicuri. La definizione è ripresa dal sito *https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smartcities_en.*

[2] V. E.E. JOH, *Policing the Smart City*, in *International Journal of Law in Context*, 15/2019.

il raggiungimento di un "ottimo paretiano", consentendo di migliorare le performance investigative, nonché di allocare le risorse in maniera più efficiente.

Ciò sembra confermato anche da un recente studio che ha dimostrato come l'utilizzo dei sistemi di polizia predittiva migliori la produttività delle forze dell'ordine in termini di repressione del crimine, mantenendo un ottimo rapporto costi-benefici. In particolare, l'autore ha esaminato la relazione empirica tra l'utilizzo del software *Keycrime* e la produttività dei pattugliamenti di polizia misurata dalla probabilità che gli autori dei reati siano arrestati, utilizzando dati relativi a rapine a danno di esercizi commerciali e banche sul territorio di Milano lungo un arco temporale di due anni e mezzo [3].

Non sono mancate, tuttavia, voci discordanti, che non solo hanno ritenuto non dimostrata la maggiore capacità dei software predittivi di prevedere e contrastare i reati [4], ma ne hanno evidenziato anche il *vulnus* che da questi potrebbe derivare in termini di tutela dei cittadini e garanzia dei loro diritti [5].

Ad ogni modo, il contributo trasformativo delle nuove tecnologie sembra ormai innervare ogni campo dell'esistenza costringendo ad una costante riflessione anche sul piano giuridico. Il presente scritto, dopo una breve ricostruzione della pratica di polizia predittiva e del quadro normativo attuale in cui opera, evidenzia due aspetti derivanti dalla sua intersezione con il discorso organizzativo della *smart city*. Il primo profilo attiene all'ingente aumento di dati raccolto dai sensori sparsi sul territorio cittadino, i quali potranno essere successivamente impiegati dai sistemi di polizia predittiva che su questi si basano. Il secondo concerne la possibilità che l'attività di prevenzione venga incorporata nella stessa architettura urbana, con la conseguenza che più le città diven-

---

[3] Cfr. G. MASTROBUONI, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *The Review of Economic* Studies, Vol. 87, Issue 6, 2020, pp. 2727-2753. *V. anche,* L. GIRALDI, *Intelligenza artificiale e predictive policing nella rinnovata fase di indagine*, in A. MASSARO (a cura di), *Intelligenza artificiale e giustizia penale*, Caltanissetta, 2020, pp. 39-92, p. 48. Secondo l'autore, tale maggiore efficienza è dovuta principalmente al fatto che le risorse, anche se limitate, e i dati in possesso delle autorità vengono sfruttati in maniera ottimizzata rispetto al passato. Da un lato, infatti, un simile impiego delle risorse permette il raggiungimento, *mutatis mutandis*, di un "ottimo paretiano" investigativo; dall'altro, concede alla polizia giudiziaria, intesa in senso lato, di organizzare strategie operative e decisionali più efficienti.

[4] V. S. TULUMELLO, F. IAPAOLO, *Policing the future, disrupting urban policy today. Predictive policing, Smart City and urban policy in Memphis (TN)*, in *Urban Geography*, 2019.

[5] Sul punto, *ex plurimis*, A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *BioLaw Journal,* 2019; G. CONTISSA, G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 4/2019; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

gono *smart*, connesse vigili, più l'attività di polizia potrebbe diventare un aspetto meno visibile e più integrato dell'ambiente urbano. In entrambi i casi appare necessario vagliarne la compatibilità con i principi del diritto penale, mettendo in luce fin da subito che ciò potrebbe scalfirne – quantomeno in via potenziale – qualche certezza.

2. *Polizia predittiva*

Con l'espressione "*polizia predittiva*" (*predictive policing*) si intende l'utilizzo di tecniche analitiche, e in particolare quantitative, per identificare possibili *target* per l'intervento della polizia, prevenire la commissione di reati futuri [6] e risolvere crimini passati facendo uso di metodi statistici sia nella fase di prevenzione che investigativa [7]. Tale "previsione" [8] si basa sulla rielaborazione pro-

[6] Secondo la tesi degli "ottimisti", gli scenari della giustizia algoritmica permetterebbero addirittura il superamento del diritto penale per il raggiungimento dei propri scopi. Ciò in quanto, se gli algoritmi, come da più parti prefigurato, si rivelassero davvero in grado di predire con assoluta infallibilità – e dunque di prevenire – la commissione di determinati reati, gli strumenti del diritto penale perderebbero in radice la propria utilità. Tali entusiasmi, tuttavia, non possono essere condivisi: l'utilizzo degli algoritmi nel campo della giustizia penale deve essere esaminato ed analizzato con attenzione, specialmente in considerazione delle evidenti tensioni con i diritti fondamentali. Sul punto, v. V. MANES, *Intelligenza artificiale e giustizia penale*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'Intelligenza Artificiale*, Torino, 2021, p. 281.

[7] Secondo Perry *et al.*: «*Predictive policing is the application of analytical techniques — particularly quantitative techniques — to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions […] Another term used to describe the use of analytic techniques to identify likely targets is forecasting. Although there is a difference between prediction and forecasting, for the purposes of this guide, we use them interchangeably*»; cfr. W.L. PERRY, B. MCINNIS, C.C. PRICE, S.C. SMITH, J.S. HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, 2013, p. xiii. V. anche F. BASILE, *Intelligenza artificiale e diritto penale; quattro possibili percorsi di indagine*, in *Dir. pen. Uomo*, 2019; M. PAPA, *Future Crimes: intelligenza artificiale e rinnovamento del diritto penale*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale,* Pisa, 2020.

[8] Il verbo "predire" rappresenta la traduzione italiana più comune sia del termine inglese "*to forecast*" che di quello "*to predict*", entrambi relativi al concetto di anticipazione del futuro. Tuttavia, c'è una differenza tra i due: mentre "*to forecast*" fa riferimento ad una previsione oggettiva, scientifica, riproducibile e libera da distorsioni ed errori individuali, "*to predict*" presenta un'accezione maggiormente soggettiva, prevalentemente intuitiva, non riproducibile e soggetta, invece, a distorsioni individuali. In linea con questa distinzione, benché nella lingua italiana non si riscontrino conseguenze pratiche, nella lingua inglese sarebbe più corretto utilizzare il verbo "*to forecast*" e non "*to predict*", e gli aggettivi a questo conseguenti. Nella comunità scien-

babilistica di una serie di dati che riguardano sia la commissione di reati, sia i loro autori. Tra questi si annoverano i dati relativi a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi teatro di ricorrenti azioni criminali e alle loro caratteristiche, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati; talora, inoltre, vengono utilizzate anche informazioni circa l'origine etnica, il livello di scolarizzazione, le condizione economiche, le caratteristiche somatiche [9], riconducibili a soggetti appartenenti a determinate categorie criminologiche [10].

L'obiettivo di "predire" *chi* potrà commettere un reato, o *dove* e *quando* potrà essere commesso, pone necessariamente il fenomeno in una prospettiva *ante delictum*, limitata quindi alla fase antecedente l'esercizio dell'azione penale, in linea con l'approccio predittivo delle odierne alternative algoritmiche che compongono quello che taluni hanno rinominato "sistema oracolare *legaltech*" [11].

La pratica di polizia predittiva si è sviluppata negli Stati Uniti alla fine del secolo scorso e trova il suo fondamento nelle teorie della criminologia ambientale, secondo le quali è possibile prevedere la commissione di un fatto criminoso in base alla considerazione che un individuo tenderà a commettere un delitto ogni qual volta vi sia l'opportunità e i benefici da questo derivanti siano altamente desiderabili [12].

---

tifica, tuttavia, è più diffuso il termine *predictive policing* (e non *forecast policing*). Sul punto, cfr. W.L. PERRY *et al.*, *Predictive Policing*, cit., p. 1.

[9] Con il rischio di un "Lombroso 2.0", secondo la felice espressione di A. GIANNINI, *Lombroso 2.0: On AI and Predictions of Dangerousness in Criminal Justice*, in *Riv. it. dir. pen.*, Vol. 29, Issue 1, 2021.

[10] F. BASILE, *Intelligenza artificiale e diritto penale*, cit., p. 10.

[11] L'espressione è di V. MANES, *L'oracolo algoritmico e la giustizia penale*, cit., p. 553. Sul punto, v. anche G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen.*, 3/2019; F. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4/2020.

[12] Più diffusamente: «*questa opportunità [di commettere un reato] è legata alla presenza di una serie specifica di fattori, definiti dalle teorie razionali del crimine ed, in particolare, dalla "teoria delle attività di routine": la presenza di un autore motivato (motivated offender) e di obiettivi/bersagli che suscitino "interesse" nell'offender (suitable targets), nonché, contestualmente, l'assenza di quello che viene definito "guardiano capace" (capable guardian), cioè di una persona – o di un sistema, ad esempio una serie di telecamere – che sia in grado di impedire che il crimine venga portato a compimento, o che quantomeno ne disincentivi il tentativo di realizzazione*», cfr. R. PELLICCIA, *Polizia predittiva: il futuro della prevenzione criminale?*, in *www.cyberlaws.it*, 9 maggio 2019, il quale, a sua volta, fa riferimento a F.P. WILLIAMS, M.D. MC SHANE, *Devianza e criminalità*, Bologna, 2002.

Invero, tale attività di analisi e mappatura delle attività criminali in un'area geograficamente determinata non è nuova. Da tempo, infatti, i fattori sociali, demografici, economici, ambientali, nonché quelli derivanti da precedenti penali, rappresentano indici rilevanti quantomeno ai fini dell'allocazione delle risorse di polizia. Ciò che appare oggi innovativo, invece, è la capacità di analizzare in tempi molto brevi un enorme quantitativo di dati grazie allo sviluppo esponenziale delle tecnologie e alla loro capillare diffusione, nonché di estrarre, mediante algoritmi di *data mining*, dei *pattern* prima invisibili [13].

La principale utilità della polizia predittiva, infatti, giace nella scoperta di similitudini e analogie ricavate a seguito dell'analisi e comparazione di variabili che si relazionano costantemente fra loro [14]. A ciò si aggiungono due ulteriori vantaggi in termini di efficienza: i *software* predittivi contribuiscono a una migliore gestione del *know how* delle forze dell'ordine in un'area geografica specifica, svincolandone la conservazione dalla presenza fisica e competenza dei singoli agenti, e migliorano le performance investigative in condizioni di limitate risorse umane, consentendo una allocazione più proficua delle stesse [15].

A seconda dello scopo per il quale sono utilizzati, i sistemi di polizia predittiva sono classificabili in due macrocategorie [16]:

– sistemi volti ad individuare le c.d. "*zone calde*" (*hotspot*): luoghi che, secondo calcoli statistici, costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati (*crime mapping*). Tali previsioni permettono di intensificare i controlli proprio su territori "ad alto rischio". Esempi di si-

---

[13] Per *data mining* si intende *l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di informazioni da grandi quantità di dati, attraverso metodi automatici o semi-automatici, e l'utilizzo scientifico, aziendale, industriale o operativo delle stesse. In particolare, il data mining produce una nuova conoscenza, in quanto evidenzia correlazioni e regolarità non apparenti dai dati in sé dissociati. Queste informazioni possono tradursi in pattern*, idonei all'applicazione, sul presupposto che dati riferiti al passato possono rivelare schemi di azioni utili circa attività future. Sul punto, C. SARRA, *Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 41 ss.; v. anche S.H. LIAO, P.H. CHU, P.Y. HSIAO, *Data Mining Techniques and Applications – A decade review from 2000 to 2011*, in *Expert Systems and Applications*, 39/2012.

[14] L. GIRALDI, *Intelligenza artificiale e predictive policing*, cit., p. 48.

[15] G. CONTISSA *et al.*, *Quando a decidere in materia penale sono (anche) algoritmi e IA*, cit., p. 621.

[16] La distinzione è ripresa da F. BASILE, *Intelligenza artificiale*, cit., p. 11. Tale classificazione è stata proposta anche da W.L. PERRY *et al.*, *Predictive Policing,* cit., pp. 19 ss. Sul punto, v. anche L. GIRALDI, *Intelligenza artificiale e predictive policing*, cit., pp. 59 ss.

stemi di questo tipo sono *Risk Terrain Modeling* (RTM), specializzato nella predizione di reati di spaccio di sostanze stupefacenti in individuate aree urbane [17], e *PredPol*, un software sviluppato dalla collaborazione tra il dipartimento di polizia di Los Angeles e la UCLA [18], entrambi diffusi negli Stati Uniti. In Italia, si rammenta *X-LAW*, sviluppato dalla Polizia di Napoli e utilizzato nel campo della prevenzione dei reati c.d. "*predatori*" [19];

– sistemi volti ad individuare gli autori di crimini seriali (*crime linking*). Tali previsioni permettono, attraverso un meccanismo di profilazione, di individuare l'autore di un precedente reato ovvero di prevedere dove e quando un

[17] «*I ricercatori hanno elaborato questo sistema sottoponendo all'algoritmo RTM dati inerenti ai fattori ambientali e spaziali più frequentemente connessi alla commissione dei reati suddetti: presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, di fermate di mezzi pubblici, di stazioni ferroviarie, di snodi di strade ad alta percorribilità, di bancomat, di compro-oro, di parcheggi scambiatori, infine, di scuole. Ciò ha consentito di elaborare una vera e propria "mappatura" di alcune grandi aree metropolitane al fine di individuare le "zone calde" dove più elevato risulta il rischio di spaccio di sostanze stupefacenti, con conseguenti benefici in termini di programmazione e attuazione di interventi di prevenzione della delinquenza connessa allo spaccio*», cfr. F. BASILE, *op. cit*., p. 11, che, a sua volta, rinvia a J.M. CAPLAN, L.W. KENNEDY, J.D. BARNUM, E.L PIZA, *Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis to Explore the Dynamics of Criminogenic Behaviour Setting*, in *Journal of Contemporary Criminal Justice*, n. 33(2)/2017, pp. 133 ss.; a J.M. CAPLAN, L.W. KENNEDY, *Risk Terrain Modeling: Crime Prediction and Risk Reduction*, in *Univ. of California Press*, 2016; J.M. CAPLAN, L.W. KENNEDY, J.D. BARNUM, E.L PIZA, *Risk Clusters, Hotspots and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, in *Journal of Quantitative Criminology*, 2010, pp. 339 ss**.** Per maggiori informazioni sul sistema, si visiti il sito *https://www.riskterrainmodeling.com/*.

[18] «*PredPol grew out of a research project between the Los Angeles Police Department and UCLA. The chief at the time, Bill Bratton, wanted to find a way to use COMPSTAT data for more than just historical purposes. The goal was to understand if this data could provide any forward-looking recommendations as to where and when additional crimes could occur. Being able to anticipate these crime locations and times could allow officers to pre-emptively deploy officers and help prevent these crimes. Working with mathematicians and behavioral scientists from UCLA and Santa Clara University, the team evaluated a wide variety of data types and behavioral and forecasting models. The models were further refined with crime analysts and officers from LAPD and the Santa Cruz (California) Police Department. They ultimately determined that the three most objective data points collected by police departments provided the most accurate input data for forecasting: 1. crime type; 2. crime location; 3. crime date and time*», cfr. *https://www.predpol.com/*.

[19] «*X-Law è un trovato tecnologico e metodologico ideato e implementato per sperimentare, per la prima volta in Italia, l'applicazione della Polizia Predittiva per la Sicurezza Urbana, (…) si basa sulla possibilità di poter prevedere, con l'impiego d'Intelligenza Artificiale, scippi, rapine, furti, borseggi, truffe e altri delitti di tipo cosiddetto "predatorio" che normalmente avvengono nelle nostre bellissime città. Il trovato nel suo insieme consiste in un protocollo tecnico e metodologico configurato per generare e impiegare strategicamente allarmi Predittivi georeferenziati di possibili crimini, elaborati secondo un esclusivo modello previsionale di Machine Learning*», cfr. *https://www.xlaw.it/presentazione/*; v. anche E. LOMBARDO, *Sicurezza 4P. Lo studio alla base del software X-law per prevedere e prevenire i crimini*, Venezia, 2019.

determinato soggetto ne commetterà un altro[20]. I risultati forniti da questi *software* potrebbero, inoltre, essere usati anche per ricostruire la carriera criminale del soggetto profilato, ossia per imputargli non solo il reato in occasione del quale egli è stato individuato, ma anche quelli precedenti costituenti la serie criminale ricostruita grazie all'archiviazione e all'elaborazione dei dati. A tale categoria appartiene il software italiano *Keycrime*, impiegato in materia di rapine a danno di esercizi commerciali e banche[21]. Altri *software* parimenti ispirati all'idea di *crime linking* sono *Precobs* in Germania[22] e *Harm Assessment Risk Tool* (HART) in Inghilterra[23].

---

[20] Questi software cercano di profilare il possibile autore della serie criminale attraverso la raccolta e l'incrocio di una gran mole di dati, provenienti da varie fonti (immagini riprese da una telecamera o informazioni relative a precedenti analoghi reati, ecc.) e prevederne eventuali futuri reati. L'idea di fondo è che alcune forme di criminalità si manifestano in un arco temporale e in una zona geografica molto circoscritti (c.d. *near repeat crimes*, o reati a ripetizione ravvicinata). Ad esempio, la commissione di una rapina sembrerebbe essere associata ad un elevato rischio di commissione di una nuova rapina, da parte degli stessi autori e in una zona geografica assai prossima al luogo del primo delitto, entro le successive 48 ore e, sia pur con un tasso di rischio decrescente, fino a tutto il mese successivo; v. F. BASILE, *Intelligenza artificiale*, cit., p. 12. V. anche A.G. FERGUSON, *Predictive Policing and Reasonable Suspicion*, in *Emory Law Journal*, Vol. 67, Issue 2, 2012.

[21] Il software *Keycrime* è utilizzato dal 2008 sul territorio del Comune di Milano e dal 2009 su tutta la provincia del capoluogo lombardo. Originariamente elaborato presso la Questura di Milano e poi divenuto di proprietà di un'azienda privata, *Keycrime* nasce per individuare gli autori seriali di rapine a danno di esercizi commerciali e banche sul presupposto che è stato dimostrato che il 70% delle rapine di questo tipo sia riconducibile a condotte seriali. Recentemente è stata iniziata una ulteriore sperimentazione anche per i furti in appartamento. L'algoritmo utilizza dati di *input* riguardanti prevalentemente le caratteristiche fisiche dell'autore (corporatura, colore di capelli, età, sesso, etnia, ecc.) e le circostanze in cui si è esplicata la condotta criminosa (utilizzo di armi da fuoco, tipo di esercizio rapinato, metodo di fuga, veicolo, ecc.). Questi dati, così come avviene nel corso delle indagini preliminari, vengono acquisiti dalla polizia giudiziaria in sede di sommarie informazioni testimoniali ovvero attraverso l'acquisizione di immagini e/o video degli impianti di sorveglianza. Ciò che cambia attiene alla fase successiva, poiché i dati vengono trasferiti nel software che procede alla loro elaborazione e li confronta con gli altri dati contenuti nei *dataset*. A fronte dei dati di *input*, il sistema fornisce quale *output*: il collegamento fra reati (il *crime link* appunto), individuando la serie ascrivibile al medesimo autore, e le previsioni sul suo prossimo reato, ossia su quando, dove e come questi dovrebbe commetterlo. Sul punto, v. M. VENTURI, *KeyCrime – La chiave del crimine*, in *PrimoPiano*, 12/2014, disponibile su *www.onap-profiling.org*; R. PELLICCIA, *Polizia predittiva,* cit.; L. GROSSI, *Software predittivi e diritto penale*, cit., pp. 162-170; G. MASTROBUONI, *Crime is Terribly Revealing*, cit., *https://keycrime.com/*. Sul punto, v. anche C. PARODI, V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Dir. pen. cont.*, 6/2019, p. 56.

[22] K. SEIDENSTICKER, F. BODE, F. STOFFEL, *Predictive Policing in Germany*, Projekt SKALA, 2018, disponibile all'indirizzo *http://nbn-resolving.de/urn:nbn:de:bsz:352-2-14sbvox1ik0z06.*

[23] La polizia del Durham, in collaborazione con l'Università di Cambridge, ha messo a pun-

Da questa breve ricostruzione appare evidente come si stia diffondendo l'utilizzo degli algoritmi nell'ambito delle attività di polizia di prevenzione e come tale pratica sia destinata ad assumere sempre maggiore rilevanza in futuro.

3. *Il quadro normativo attuale*

Fino ad epoca recente, l'utilizzo degli strumenti di polizia predittiva, e più in generale dei sistemi di intelligenza artificiale[24], non è stato oggetto di specifica disciplina, demandando le condizioni e le modalità del loro impiego, nonché la valutazione e la valorizzazione dei loro risultati, alla sola iniziativa degli operatori di polizia e alla prassi.

Un primo passo verso la regolamentazione si è registrato nel dicembre 2018 con l'adozione della *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e in ambiti connessi* da parte della Commissione Europea per l'efficacia della giustizia del Consiglio d'Europa (CEPEJ)[25]. Tale documento, esempio emblematico di *soft law*, cristallizza cinque principi che devono rappresentare la cornice imprescindibile di qualsiasi futura disciplina in materia: il rispetto dei diritti fondamentali (e in particolare del diritto di accesso alla giurisdizione e del diritto ad un processo equo), il principio di non discriminazione, il principio di qualità e sicurezza nell'analisi dei dati e

---

to il sistema HART con l'obiettivo di promuovere processi decisionali che permettano di realizzare interventi mirati a ridurre il rischio di recidiva. In realtà, più che al *genus* dei sistemi di polizia predittiva, sembrerebbe più corretto ricondurre il sistema HART ai c.d. *risk assessment toools,* ossia a quegli strumenti computazionali in grado di calcolare se un soggetto si sottrarrà al processo o commetterà ulteriori reati, che operano in una fase successiva rispetto a quella di prevenzione e indagine. D'altra parte, è inevitabile che queste categorie, dai confini ancora sfocati, possano talvolta sovrapporsi. Cfr. M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.,* 2019, pp. 10 ss.

[24] La proposta di Regolamento della Commissione Europea indica con il termine "intelligenza artificiale" (IA) una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali. Il documento è reperibile all'indirizzo *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.*

[25] Per un'attenta disamina della Carta etica europea per l'utilizzo dell'intelligenza artificiale, si rinvia a S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penalistiche e informatiche*, in *Leg. Pen.*, 2018.

delle decisioni giudiziarie (ossia l'utilizzo di fonti certificate e dati intangibili, attraverso modelli concepiti in modo multidisciplinare, in un ambiente tecnologico sicuro), il principio di trasparenza e imparzialità (declinato nelle forme di accessibilità, comprensibilità e verificabilità esterna dei processi computazionali), e l'inderogabile possibilità di controllo da parte dell'utente (il c.d. *under user control*).

Nell'aprile 2021, la Commissione Europea ha presentato la proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale[26]. Nella proposta non viene regolata l'intelligenza artificiale in quanto tale, ma il suo ingresso nel mercato, la messa in uso e l'utilizzo nell'ambito dell'Unione Europea dei sistemi che contengono tale tecnologia (i c.d. SIA, Sistemi di Intelligenza Artificiale[27]), nel tentativo di mantenere quanta più neutralità nei confronti della tecnologia in discussione e per non rischiare una veloce obsolescenza definitoria. La proposta classifica i SIA in base al rischio di impatto negativo sui diritti fondamentali: più il prodotto è suscettibile di mettere in pericolo tali diritti, più severe sono le misure adottate per eliminare o mitigarne l'impatto, fino a vietare determinati prodotti ritenuti incompatibili. In particolare, il Regolamento identifica: SIA proibiti (Titolo II), SIA ad alto rischio (Titolo III) e SIA che richiedono una specifica regolamentazione (Titolo IV); si ipotizza la possibilità di una ulteriore categoria di SIA residuali[28].

Nell'ambito della giustizia penale, la categoria prevalente sembra essere rappresentata dai SIA ad alto rischio, ossia non proibiti in quanto tali, ma soggetti a requisiti aggiuntivi (specificati nei Capitoli 2-6); tra questi, infatti, rientrano quelli utilizzati per l'identificazione biometrica e la categorizzazione di individui (escludendo i SIA inquadrati come "proibiti"[29]), nonché, più in generale, quelli utilizzati dalle forze di polizia e nell'amministrazione della giustizia.

---

[26] Il documento è reperibile all'indirizzo *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.*

[27] «*Per "sistema di intelligenza artificiale" (sistema di IA) si intende un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*», cfr. art. 3, n. 1 Regolamento.

[28] Per un'analisi dei profili di criticità emersi fin dalla bozza di Regolamento, v. A. LAVORGNA, G. STUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*, in *Dir. pen. cont.*, 2/2021.

[29] Tra i SIA proibiti, invece, rientrano i sistemi di identificazione biometrica "a tempo reale" da remoto in spazi pubblici per funzioni di polizia, se utilizzati ai fini di sorveglianza indiscriminata. La proposta, tuttavia, prevede varie eccezioni che sembrano ammetterne l'uso sulla ba-

Con riguardo al profilo della gestione e protezione dei dati necessari per l'utilizzo dei *software* in questione, deve, invece, farsi riferimento al *Data protection reform package*, costituito dal Regolamento 2016/679/UE (GDPR) e dalla Direttiva 2016/680/UE, che sostituiscono, rispettivamente, la Direttiva 95/46/CE e la Decisione quadro 2008/977/GAI [30]. In particolare, la Direttiva 2016/680/UE, che costituisce una *lex specialis* rispetto al Regolamento, mira a stabilire norme minime relative alla «*protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica*» [31].

A livello nazionale, la Direttiva 2016/680/UE è stata attuata con d.lgs. 18 maggio 2018, n. 51 [32], il cui art. 8, riprendendo l'art. 11 della Direttiva, stabilisce il divieto di decisioni basate unicamente su trattamenti automatizzati (il c.d. criterio di non esclusività del dato algoritmico) [33]. Ne consegue che l'im-

---

se di una valutazione "caso per caso" e mediante il ricorso a criteri di proporzionalità (art. 5, nn. 2-4 Regolamento). Nei SIA considerati a rischio inaccettabile rientrano anche alcune casistiche del riconoscimento facciale, specialmente laddove sia un'autorità pubblica ad utilizzarle, salvo eccezioni (art. 5, n. 1d Regolamento). Cfr. A. LAVORGNA, G. STUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza*, cit., pp. 92-93.

[30] Sul punto, P. DE HERT, V. PAPAKONSTANTINOU, *The new Police and Criminal Justice Data Protection Directive. A first Analysis*, in *New Journal of European Criminal Law*, 1/2016, pp. 7 ss.

[31] Cfr. art. 1, par. 1, Direttiva.

[32] «*1. Il presente decreto attua nell'ordinamento interno le disposizioni della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio. 2. Il presente decreto si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. 3. Il presente decreto non si applica ai trattamenti di dati personali: a) effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea; b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione europea*», cfr. art. 1 d.lgs. n. 51/2018.

[33] Sull'interpretazione dell'espressione "*decisione basata unicamente su un trattamento automatizzato*", v. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., p. 16, che, a sua volta, richiama J. SAJFERT, T. QUINTEL, *Data Protection Directive (EU) 2016/680 for police and criminal justice authorities*, in M. COLE, F. BOHEM (a cura di), *Commentary on the General Data Protection Regulation,* Cheltenham, 2018, pp. 10 ss.

piego di software di polizia predittiva, laddove non limitati all'allocazione delle forze di polizia sul territorio ma utilizzati anche ai fini dell'individuazione della responsabilità penale, non potrà costituire l'unico elemento sul quale basare la decisione in sede di giudizio. In particolare, quando entra in gioco la libertà personale dell'imputato, l'art. 8 deve essere letto congiuntamente agli artt. 5 e 6 CEDU e all'art. 6 CDFUE, con l'effetto che il tradizionale diritto di accesso al giudice deve oggi essere declinato nel diritto dell'interessato a che sul suo *status* si pronunci un giudice "in carne ed ossa" [34], il quale dovrà tenere conto anche di elementi di prova ulteriori rispetto all'*output* del *software* predittivo [35].

D'altronde, tale esito interpretativo poteva già desumersi dalla normativa esistente. *In primis*, l'art. 192, comma 2, c.p.p. stabilisce che l'esistenza di un fatto non può essere desunta da indizi a meno che questi siano gravi, precisi e concordanti, con la conseguenza che l'*output* del *software* si presenta come solo uno dei tanti elementi che possono fondare il giudizio di responsabilità. Inoltre, i risultati dell'attività predittiva devono essere assunti nel rispetto della disciplina codicistica e, pertanto, tenendo conto dei divieti di utilizzabilità stabiliti dall'art. 191 c.p.p. e dal divieto di perizia criminologica di cui all'art. 220, comma 2, c.p.p. Il tutto, infine, deve essere letto nella cornice dell'art. 533 c.p.p., che impone al giudicante la valutazione di condanna al di là di ogni ragionevole dubbio, la cui connotazione di ragionevolezza è difficilmente riconducibile all'interno di un algoritmo [36] e, pertanto, "calcolabile" [37].

---

[34] V. G. UBERTIS, *Intelligenza artificiale*, cit., p. 83, il quale, riprendendo una nozione elaborata nell'ambito del dibattito internazionale sviluppatosi in seno all'ONU sulle armi autonome, parla di: «*controllo umano significativo*».

[35] Quanto all'impiego in sede processuale di elementi di prova ottenuti mediante l'utilizzo di *software* di polizia predittiva e, più in generale, di dati generati automaticamente – attraverso algoritmi e modelli computazionali –, il cui vaglio di attendibilità si scontra con il tradizionale diritto probatorio, v. S. QUATTROCOLO, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3/2020. V. anche, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale,* cit., p. 17; C. PARODI *et al.*, cit., pp. 61 ss.; G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale,* in *Sistema penale*, 8 gennaio 2021.

[36] Come ben sintetizzato da Canzio: «*la legge (art. 101, co. 2 Cost.) e la ragione (art. 111, co. 6 Cost.) costituiscono presidi della razionalità del giudicare e fonti di legittimazione della giurisdizione e dei giudici*»; cfr. G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., p. 2.

[37] Per una riflessione in merito al tema del diritto "calcolabile", v., *ex plurimis*, N. IRTI, *Per un dialogo sulla calcolabilità giuridica,* in *Riv. dir. proc.*, 2016. Sul punto, v. anche A. CARLEO (a cura di), *Calcolabilità giuridica*, Bologna, 2017.

4. *Polizia predittiva e* smart city

Come anticipato, condizione indispensabile per l'elaborazione di strategie efficienti e previsioni attendibili da parte dei software di polizia predittiva è la disponibilità di dati e, in particolare, di *big data*[38]; di questi, una parte ingente viene catturata mediante i c.d. sensori (telecamere, microfoni, sensori di quantità fisiche, ecc.) distribuiti nelle città[39].

La trasformazione dei centri urbani in *smart city* determina un incremento di sensori sul territorio cittadino, secondo la nota dinamica del c.d. *Internet of Things* (IoT)[40], e, conseguentemente, un aumento della raccolta di dati che possono essere successivamente – ma anche *real-time*[41] – impiegati dai *software* predittivi.

In altre parole, tecnologie disegnate per raccogliere e manipolare dati al fine di migliorare l'efficienza della gestione di una città potranno essere sfruttate anche per le attività di polizia predittiva[42]. Ad esempio, un semaforo dotato di sensori per cui all'avvicinarsi di una macchina e in assenza di altri veicoli in attraversamento faccia scattare il verde permette la costante sorveglianza di

---

[38] Sull'utilizzo di *big data* da parte delle forze dell'ordine nell'utilizzo di tecniche di polizia predittiva, v. A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3/2018.

[39] I dati catturati dai sensori sono solo una parte del *dataset* a disposizione dei *software* di polizia predittiva. Si pensi alla mole enorme di dati ottenuti dal *social media mining*, ossia mediante l'estrazione di enormi quantità di dati grezzi sui *social network* per identificare tendenze comportamentali. Per uno studio circa l'utilizzo di Twitter al fine della predizione di reati, v. M. S. GERBER, *Predicting crime using Twitter and kernel density estimation*, in *Decision Support Systems*, Vol. 61, 2014.

[40] Sul punto, v. N. CLIMER, *Il cloud e l'Internet delle cose*, in J. AL-KHALILI (a cura di), *Il futuro che verrà*, Torino, 2017.

[41] Per esempio, la città di Natal (Brasile) ha aderito alla *IEEE Smart City Initiative* con l'obiettivo di trasformarsi in una *smart city* attraverso lo sviluppo di sistemi e applicativi per rinforzare l'uso delle tecnologie e migliorare la qualità della vita dei cittadini. All'interno di questa iniziativa è stata sviluppata ROTA, una piattaforma volta a migliorare la sicurezza pubblica mediante la raccolta, l'integrazione, l'analisi e la condivisione di informazioni riguardanti gli eventi che si verificano e i veicoli delle pattuglie di polizia. In particolare, i suoi due moduli (ROTA-PSM e ROTA PVM) sono applicazioni mobili utilizzate per monitorare la posizione delle pattuglie sul territorio e per supportarle nelle loro operazioni in tempo reale. V. A. ARAUJO, N. CACHO, A.C. THOME, A. MEDEIROS, J. BORGES, *A Predictive Policing Application to Support Patrol Planning in Smart Cities,* 2017 International Smart Cities Conference (ISC2), 2017, disponibile all'indirizzo *https://www.researchgate.net/publication/321236214*.

[42] E.E. JOH, *Policing the Smart City*, cit., p. 180. L'autrice definisce le funzionalità delle *smart cities* come "*dual-use technologies*".

quella specifica strada; ancora, un cestino che si auto-monitora per segnalare ai servizi di igiene urbana quando deve essere svuotato potrebbe allo stesso tempo raccogliere informazioni circa la tipologia di rifiuti e la frequenza con cui vengono gettati.

Non solo. La trasformazione in *smart city* potrebbe determinare un'ulteriore conseguenza, ossia che l'attività di prevenzione venga incorporata nella stessa architettura urbana [43]. Ciò significa non solo che strade, marciapiedi, palazzi, veicoli conterranno sensori capaci di raccogliere dati, ma che questi potrebbero anche essere capaci di fornire una immediata risposta automatica a comportamenti indesiderati. Ad esempio, si potrebbe precludere l'accesso a determinati luoghi a coloro che vengono identificati mediante un meccanismo di riconoscimento facciale come autori di precedenti reati; oppure un veicolo, interagendo con i sensori stradali, potrebbe impedire al guidatore di superare il limite di velocità consentito, di passare con il rosso, o, più in generale, di trasgredire una norma del Codice della strada [44]. Tornando agli esempi precedenti, il semaforo dotato di sensori potrebbe interagire direttamente con il veicolo impedendo la trasgressione, mentre il cestino che si auto-monitora potrebbe allertare autonomamente le forze dell'ordine laddove rilevi un pacco sospetto.

Quindi, più le città divengono *smart*, connesse e vigili, più la polizia potrebbe risultare meno visibile e più integrata nell'ambiente urbano.

Risulta dunque evidente la stretta sinergia esistente tra *smart city* e polizia predittiva, la cui genealogia parte da un presupposto comune: il tentativo di rendere la città oggetto del pensiero razionale, del calcolo di dati e del controllo [45]. Entrambe le dimensioni, infatti, condividono il focus sull'anticipazione e sulla gestione del futuro quale soluzione per risolvere i problemi presenti, e la concettualizzazione del problema urbano come una questione di soluzioni tecnologiche e tecnocratiche.

5. *Vecchie e nuove sfide per il diritto penale*

Rinviando ad altra sede l'analisi delle molteplici perplessità circa l'attendi-

[43] *Ibidem*. Secondo l'autrice, il *policing* è "*inerente*" alla *smart city*: man mano che le città divengono più *smart*, l'attività di *policing* è sempre più incorporata nell'infrastruttura urbana.

[44] Per un approfondimento in materia di *self-driving cars*, si rimanda al contributo di A. CAPPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. pen. cont.*, 2/2019.

[45] S. MATTERN, *Mission control: A history of the urban dashboard*, in *Places Journal*, 2015.

bilità dei sistemi di polizia predittiva [46] e le preoccupazioni da questi sollecitate con riguardo alle garanzie fondamentali e alla tutela dei principi costituzionali [47], vogliono qui evidenziarsi due ricadute critiche del binomio *smart city*/polizia predittiva sulla materia penale.

La prima attiene alla compatibilità di tale ricostruzione con i principi di materialità e di offensività, nonché con la finalità rieducativa della pena, e concerne i sistemi di polizia predittiva in generale, il cui utilizzo – come precedentemente evidenziato – è incrementato dall'ingente quantitativo di dati raccolti dai sensori delle *smart city*.

Nel racconto di Philip Dick "*The Minority Report*" la prevenzione del reato si spinge a punire un fatto non ancora commesso, ma che è stato "previsto"

---

[46] In particolare, si rammenta il rischio del c.d. *confirmation feedback loop*, ossia il rischio di innescare circoli viziosi. I *software* predittivi sono sistemi che si auto-alimentano con i dati prodotti dal loro stesso utilizzo: ad esempio, se un sistema individua un determinato *hotspot*, aumenteranno i controlli della polizia, con la conseguenza che aumenterà il tasso dei reati rilevati in quella zona, che diventerà, a sua volta, ancora più "calda". Le zone non considerate "calde", invece, in ragione del minor dispiego di forze dell'ordine, rischiano di rimanere, o di diventare, zone franche per la commissione di reati. Il problema si lega indissolubilmente con la tendenza degli algoritmi ad essere discriminatori. Infatti, sebbene le nuove tecnologie mettano a disposizione dell'investigatore un ampio patrimonio informativo disponibile per orientare l'attività operativa in maniera selettiva e proficua, allo stesso tempo possono essere basati su pregiudizi, che, a loro volta, tendono ad auto-avverarsi: se si vigila con più attenzione su determinate categorie, si scovano per ciò stesso più reati, anche se il tasso di criminalità non è realmente superiore alla media. Cfr. F. BASILE, *Intelligenza artificiale e diritto penale*, cit., p. 13; P. SORBELLO, *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in *Dir. pen. cont.*, 2/2019, p. 386; F. UBERTIS, *Intelligenza artificiale*, cit., pp. 10-11; v. anche K. LUM, W. ISAAC, *To Predict and Serve?,* disponibile all'indirizzo *https://doi.org/10.1111/j.1740-9713.2016.00960.x*; A.G. FERGUSON, *Predictive Policing and Reasonable Suspicion*, cit., p. 322.

[47] Le critiche avanzate nei confronti degli strumenti di polizia predittiva sono molteplici. *In primis*, tali *software* sollevano delle perplessità circa il rispetto del principio di uguaglianza (art. 3 Cost.); come ben sintetizzato da Manes: «*l'algoritmo – per antonomasia – è anti-egualitario, perché considera alcuni fattori di rischio e non altri (età, genere, ma anche luogo di residenza, back-ground socioeconomico, abitudini di vita, tendenze sessuali o "morali", data di commissione del primo precedente, etc.), e su queste basi non solo suggerisce l'allocazione di maggiori risorse di polizia in alcuni contesti urbani piuttosto che in altri, ma pone una presunzione di maggior pericolosità in relazione ad alcuni soggetti e non ad altri*», cfr. V. MANES, *L'oracolo algoritmico*, cit., p. 559. In secondo luogo, si pone il problema della tutela dei dati e del diritto alla *privacy*; sul punto, v. M.F. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Pol. dir.*, 2016, p. 662. Infine, non si deve trascurare la circostanza che la maggior parte di questi software sono coperti da brevetti depositati da aziende private, i cui detentori tendono a non disvelare i propri segreti industriali e commerciali. Ciò determina una maggior difficoltà nella comprensione dei meccanismi del loro funzionamento, con evidente pregiudizio delle esigenze di trasparenza e di verifica della qualità e affidabilità dei risultati da essi prodotti, v. E.E. JOH, *Policing the Smart City*, cit., pp. 179-180.

da tre soggetti con sviluppate capacità cognitive impiegati a tale scopo da un immaginario dipartimento di polizia; per tale giustizia predittiva, infatti, anche la mera intenzione costituisce reato e determina delle conseguenze in punto di sanzione.

Questo scenario distopico non sembra realizzabile in un diritto penale liberale a base oggettivistica che richiede, ai fini della pena, la commissione di un fatto materiale di reato – così come sancito dall'art. 25, comma 2, Cost. – che, a sua volta, si sostanzi nell'effettiva offesa di un bene giuridico [48].

Sotto questo profilo, la prima categoria di sistemi predittivi, ossia quelli volti ad individuare i c.d. *hotspot*, non pongono particolari problemi, in quanto il loro utilizzo è circoscritto alla fase di allocazione delle risorse di polizia o, al più, all'individuazione di particolari zone dove potrebbe essere commesso un reato. In questo caso, la polizia si reca nel luogo indicato ed eventualmente impedisce la commissione di un reato o la "limita" alla forma del tentativo. Ne consegue che la responsabilità penale sarà ancorata al fatto commesso dall'agente, se pur limitato allo stadio del tentativo.

Lo stesso non può dirsi con riferimento ai sistemi di *crime linking*, che hanno lo scopo di individuare l'autore di un precedente reato ovvero di prevedere dove e quando un determinato soggetto ne commetterà un altro. In questo caso si assiste ad uno spostamento del baricentro dall'accertamento del fatto di reato ad una verifica avente ad oggetto esclusivamente, o comunque eminentemente, il suo autore.

Riprendendo le considerazioni svolte altrove in tema di *risk assessment tools* [49], ciò rischia di determinare un passaggio dal "diritto penale del fatto" ad un "diritto penale d'autore" (o "del tipo criminologico dell'autore"), posto che il giudizio di responsabilità andrebbe a fondarsi non sul parametro oggettivo del fatto di reato commesso dall'agente, bensì su una valutazione della sua personalità [50]. Peraltro, tale valutazione si fonderebbe su statistiche, schemi

---

[48] F. MANTOVANI, *Diritto penale. Parte generale*, XI ed., Padova, 2020. Si rammentano anche le voci autorevoli di N. MAZZACUVA, *Il disvalore di evento nel diritto penale*, Milano, 1983; F. PALAZZO, *La recente legislazione penale*, Padova, 1985; F. SGUBBI, *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, Bologna, 1990.

[49] M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale,* cit., pp. 19 ss.

[50] Come è noto, la formula "*diritto penale d'autore*" evoca la circostanza per cui non si punisce più il reato, ma il reo e, nello specifico, per "quello che è" non per "quello che fa", in contrasto con un sistema improntato sul diritto penale del fatto e della colpevolezza. La letteratura sul tema è vasta; *ex plurimis*, L. FERRAJOLI, *Il diritto penale del nemico e la dissoluzione del diritto penale*, in *Questione giustizia*, 2006; M. DONINI, M. PAPA (a cura di), *Diritto penale del nemico. Un dibattito internazionale*, Milano, 2007; F. PALAZZO, *Contrasto al terrorismo, diritto penale del nemico e diritti fondamentali*, in *Questione giustizia*, 2/2006. Quanto alla declinazione del

comportamentali generali e decisioni riferite a determinati gruppi di individui, ossia su un *tipo* di individuo e non sul *singolo* che riceverà la punizione, in evidente tensione con il principio di individualizzazione del trattamento sanzionatorio, e conseguentemente con la funzione rieducativa della pena garantita dall'art. 27, commi 1 e 3 Cost.

Se, dunque, il principio di materialità appresta un limite insuperabile alla responsabilità penale e la finalità rieducativa non consente di strumentalizzare l'individuo per fini generali di politica criminale, l'utilizzo di tale secondo gruppo di strumenti predittivi non è facilmente conciliabile con l'idea di giustizia penale. La trasformazione del centro urbano in *smart city*, sebbene non introduca un nuovo problema, ne consolida uno già esistente.

Il secondo profilo di interesse – per certi versi più innovativo – si presenta quale diretta conseguenza della tesi secondo cui l'avvento delle *smart city* potrebbe determinare l'incorporazione dell'attività di prevenzione dei reati direttamente nell'architettura urbana[51].

Ciò potrebbe comportare due conseguenze. La prima è che, così facendo, l'algoritmo vada ad affiancare ed integrare la legge anche in materia penale[52], secondo la nota formula "*code is law*", per cui il diritto e la sua applicazione sono sostituite – se non in toto, almeno in parte – da una corrispondente in-

"diritto penale d'autore" con riferimento al formante algoritmico, cfr. G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, cit., p. 10.; V. MANES, *L'oracolo algoritmico e la giustizia penale,* cit., p. 559.

[51] La centralità dell'architettura nel fenomeno della regolamentazione è evidenziata anche da Lessig, il quale considera nel modello pre-Internet quattro diversi vincoli ai comportamenti degli individui: la legge, il mercato, le norme sociali e – appunto – l'architettura. Come primo vincolo l'individuo trova innanzitutto la legge, che prevede diritti, obblighi e sanzioni nel caso di inosservanza delle regole imposte. In secondo luogo, l'individuo è vincolato dalle norme sociali che influiscono sul modo di comportarsi, condannando colui che violi una regola ad una pena inflitta non dallo Stato, ma dalla comunità. Il terzo tipo di vincolo è costituito dalle leggi del mercato. Infine, l'ultimo vincolo è rappresentato dall'architettura, cioè dal mondo fisico e dalle condizioni simultanee dettate dall'ambiente naturale, che possono influire sul comportamento individuale, ma questa, diversamente dalle leggi e dalle norme sociali, non vincola attraverso sanzioni *ex post.* Cfr. L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999; v. anche E. MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Il Mulino Riv. web*, 1/2017.

[52] Nel settore civile, tale fenomeno sembra già in atto. Si fa riferimento ai c.d. *smart contract*; protocolli informatici basati sulla tecnologia *blockchain* che eseguono in modo automatico o semi-automatico i comandi stabiliti in sede di programmazione corrispondenti alle clausole negoziali stabilite dalle parti durante la contrattazione. Sul punto, v. S. HASSAN, P. DE FILIPPI, *The expansion of algorithmic governance: From code is law to law is code*, in *Field Actions Science Report*, Special Issue 17, 2017. Per un'efficace sintesi della letteratura sul tema, v. V. DWIVEDI, V. PATTANAIK, V. DEVAL, A. DIXIT, A. NORTA, D. DRAHEIM, *Legally Enforceable Smart-Contract Languages: A Systematic Literature Review*, in *ACM Computing Surveys*, Vol. 54, 5/2020.

frastruttura informatica [53]. Invero, la disciplina dei fenomeni attinenti al sistema penale si avvia a essere regolata tramite codici algoritmici al punto che il primato delle norme incriminatrici disposte dalla legge viene sostituito dalle norme che regolano l'applicazione del *software* [54], con evidenti ricadute sul principio di legalità e sui corollari del nostro diritto penale "tradizionale" [55].

In secondo luogo, si apre la prospettiva di uno spostamento del paradigma penalistico dalla logica della sanzione alla logica della prevenzione e della *compliance* [56], generando «*il progressivo appannamento della distinzione fra pre-*

---

[53] Il sintagma "*code is law"* esprime l'idea che con l'avvento delle nuove tecnologie il codice informatico possa arrivare a regolare il comportamento di coloro che le utilizzano. Cfr. L. LESSIG, *Code is law. On Liberty in cyberspace,* in *Harvard Magazine*, 2000, e già prima *Code and Other Laws of Cyberspace*, cit.; v. anche S. HASSAN *et al.*, *The expansion of algorithmic governance*, cit. Secondo alcuni autori, l'informatica e la digitalizzazione del diritto modificano non soltanto i mezzi di diffusione della legge, ma, più profondamente, la sua stessa elaborazione e il rapporto con il mondo. La scrittura numerica si inserisce nella produzione della norma e la giustizia predittiva (o giustizia digitale) va intesa come una fonte alternativa di normatività giuridica. Cfr. A. GARAPON, J. LASSEGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, 2018; E. FRONZA, "*Code is Law". Note a margine del volume di Antoine Garapon e Jean Lasségue, Justice digitale. Révolution graphique et rupture anthropologique, PUF, Paris, 2018*, in *Dir. pen. cont.*, 11 dicembre 2018. Hildebrandt parla di "*technological normativity*" in contrapposizione alla "*legal normativity*", cfr. M. HILDEBRANDT, *Legal and technological normativity: more (and less) than twin sisters*, in *Techné: Research in Philosophy and Technology*, 12/2008; v. anche, M. HILDEBRANDT, *Code driven law. Freezing the future and scaling the past*, in C. *MARKOU*, S. DEAKIN (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, London Borough of Camden, 2020.

[54] «*L'algoritmo tende a sostituire la legge. Al punto che il primato delle norme incriminatrici disposte dalla legge viene sostituito dalle norme che regolano l'applicazione del software: e ciò potrebbe accadere sia nel giudizio di fatto attinente alla individuazione di innocenza e colpevolezza dell'imputato, sia nel giudizio di diritto circa la definizione del confine tra lecito e illecito. Dunque, il testo della fattispecie incriminatrice diventa soltanto uno degli elementi che entrano nella piattaforma digitale per la gestione della governance giudiziaria*», cfr. F. SGUBBI, *Il diritto penale totale*, Bologna, 2019, pp. 41 ss.

[55] È, tuttavia, innegabile che il nostro diritto penale "tradizionale", e in particolare il suo principale strumento concettuale ossia la fattispecie incriminatrice, stia conoscendo un momento di forte crisi poiché è in crisi la possibilità di ordinare il mondo in base all'aspetto delle cose. Dinnanzi a tale crisi, si tratta di capire quale possa essere il possibile contributo delle nuove tecnologie, ossia se possiamo immaginare che queste ci conducano a un rinnovamento della fattispecie incriminatrice, a concepirne e svilupparne una nuova tipologia, che presenti nuove modalità di descrivere, comunicare il precetto penale. Cfr. M. PAPA, *Future crimes*, cit., p. 4. Più diffusamente, M. PAPA, *Fantastic voyage. Attraverso la specialità del diritto penale*, II ed., Torino, 2019; *M.* PAPA*, La fattispecie come sceneggiatura dell'ingiusto: ascesa e crisi del diritto penale cinematografico*, in *Criminalia*, 2019.

[56] Cfr. C. BOUCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. ita. dir. e proc. pen*., 4/2019; secondo l'autore, l'intelligen-

venzione e accertamento dei reati»[57]. In altre parole, se fino ad ora il diritto penale ha garantito la tutela dei beni giuridici in modo normativo e controfattuale, dunque intervenendo solo una volta commesso il fatto di reato, i sistemi di polizia predittiva – e di intelligenza artificiale in generale –, specie se incorporati nell'infrastruttura urbana, perseguono nel lungo periodo l'obiettivo della pratica impossibilità o almeno della sostanziale minimizzazione delle lesioni ai beni giuridici[58].

Tuttavia, una tale impostazione richiede anche una consapevole scelta politico-criminale, in quanto la costante sorveglianza nei confronti dei cittadini derivante dall'incorporazione della prevenzione nell'architettura urbana, che rende i fatti di reato *eo ipso* o *de facto* impossibili[59], ne comprime indefettibilmente la libertà di "determinarsi altrimenti", con il rischio di una rottura con il tradizionale diritto penale liberale, nonché di una deriva verso forme di c.d. "*paternalismo tecnologico*"[60].

---

za artificiale a è un costrutto sociale la cui prassi è in grado di trasformare le nostre basilari concezioni di ordinamento sociale e giuridico fino a decretare la fine del diritto penale per come noi lo conosciamo.

[57] G. ILLUMINATI, *Editoriale*, in *Rev. italo-española der. proc.*, 1/2019, p. 1.

[58] Con evidenti ripercussioni sulle funzioni della fattispecie incriminatrice e, in particolare, della funzione comando. La fattispecie, infatti, è capace di orientare il comportamento dei cittadini ancora prima, e a prescindere, dalla minaccia della pena; cfr. M. PAPA, *Fantastic voyage*, cit., pp. 108 ss. V. anche C. BOUCHARD, *L'intelligenza artificiale come fine del diritto penale?*, cit., p. 1934.

[59] Secondo Brennan-Marquez, il *policing* produce «*a social order – a surveillance society – in which people constantly monitor and curate the data-trails they leave behind in everyday life*», cfr. K. BRENNAN-MARQUEZ, *Big Data Policing and the Redistribution of Anxiety*, in *Ohio State Journal of Criminal Law,* 2018, p. 487. «*L'ambizione della legaltech è diventare essa stessa la giustizia, tramite una rivoluzione numerica che rende mondi eterogenei compatibili fra loro, mettendo in comunicazione il diritto e la realtà mutevole del fatto. Il sogno segreto è di un mondo dove i rapporti sociali non saranno più gestiti dalla politica e dal diritto, bensì dalla tecnica, partendo dalla consapevolezza che l'opinione pubblica è più rassicurata da una decisione tecnica, che da una decisione umana, pur se presa nel rispetto di tutte le garanzie. La giustizia fatta dagli uomini rischia di venire considerata arbitraria, fallace, un dato storico superato. Si è così messo in moto, dunque, un processo di desimbolizzazione della fragile umanità del diritto e del giudice e una resimbolizzazione in termini scientifici*», cfr. E. FRONZA, "*Code is Law". Note a margine del volume di Antoine Garapon e Jean Lasségue, Justice digitale,* cit.

[60] Tanto più si producono previsioni comportamentali volte alla prevenzione del crimine basate sul diffuso impiego di dati, tanto più è favorita l'internalizzazione da parte dei singoli soggetti del progetto stesso di prevenzione del crimine. L'individuo, infatti, impegnandosi nel progetto tecnologico-informatico di inibizione del crimine attraverso il monitoraggio del rischio altrui, lo fa a costo di monitorare se stesso, accetta tutto questo come proprio e diventa così l'esecutore delle strutture di potere alla base di questo progetto di sorveglianza, cfr. C. BOUCHARD, *L'intelligenza artificiale come fine del diritto penale?*, cit., p. 1937.

In conclusione, è opinione di chi scrive che le conseguenze prospettate, per la rilevanza e incidenza sui principi e sulle fondamenta stesse del nostro diritto penale, meritino un'adeguata attenzione nel discorso *smart city*/polizia predittiva, in quanto, a fronte degli innegabili vantaggi in termini di efficienza e di prevenzione e/o repressione del crimine, potrebbero verificarsi anche imprevisti e indesiderati cambi di paradigma.

PARTE III
CRITICITÀ E OPPORTUNITÀ

SMART CITY E SICUREZZA INFORMATICA. LA *CYBERSECURITY* COME *ASSET* FONDAMENTALE DELLE CITTÀ DEL FUTURO

di *Stefano Aterno*

SOMMARIO: 1. Nell'era delle *smart city* quanto è importante la *Cybersecurity*? – 2. La sicurezza informatica come *asset* fondamentale di un sistema iper-connesso in quanto parte integrante della Sicurezza di un Paese. – 3. La *Cybersecurity* nei suoi aspetti normativi.

1. *Nell'era delle* smart city *quanto è importante la* Cybersecurity*?*

Lo "*spazio cibernetico*" in un mondo complesso come quello delle *smart city* rappresenta un nuovo dominio, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale), nel quale gli esseri umani, e nel prossimo futuro verosimilmente anche le intelligenze artificiali, possono agire e interagire a distanza.

Un dominio di importanza strategica per lo sviluppo economico, sociale e culturale dei diversi Paesi ma al contempo un nuovo "spazio virtuale" luogo di competizione economica e geopolitica.

Grazie ai progressi delle tecnologie di comunicazione e l'impiego diffuso di dispositivi elettronici e di monitoraggio si intrecciano quotidianamente nello spazio cibernetico miliardi di interconnessioni, si scambiano conoscenze a livello globale e viene raccolto un gigantesco numero di dati e di informazioni compresi quelli di natura personale e sensibile (c.d. *big data*).

La dimensione cibernetica è pertanto generata dalla ramificata rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mettono in contatto tra loro un crescente numero di esseri umani e permettono loro di attivare e controllare da ubicazioni remote macchine e apparati in tutto il mondo.

Un ecosistema complesso nel cui ambito gli esperti della materia sono soliti distinguere i seguenti tre livelli essenziali: il livello fisico infrastrutturale, rap-

presentato dalle macchine (le architetture delle reti, i computer, i router...); il livello logico informativo rappresentato dal volume dei dati gestiti dalle macchine (database, file, ma anche *software* gestiti dalle macchine); il livello sociale cognitivo, ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei *social network*, gli indirizzi IP delle macchine).

Da un punto di vista ambientale lo spazio cibernetico, soprattutto in una *smart city*, si presenta come un ambiente virtuale, privo di confini fisici nel senso tradizionale del termine, uno spazio indefinito nel cui ambito non esiste divisione tra pubblico e privato, tra la sfera militare e civile. Un ambiente in cui pressoché tutto è duale e dove tutto può essere preso dalla parte civile e portato verso la parte militare: sistemi operativi, *off the shelf*, *storage*, una serie di *software* che controllano anche indirettamente sistemi anche di comando e controllo di tipo militare dove l'anello più debole è come sempre lo *human factor* e dove pertanto l'elemento umano, a prescindere dalla resistenza della piattaforma di sicurezza implementata, costituisce il tallone d'Achille sfruttato dagli attaccanti.

In quanto dominio creato dall'uomo lo spazio cibernetico è, inoltre, in continua evoluzione e implementazione, in connessione con la rapidità e pressoché ininterrotta evoluzione delle tecnologie dell'informazione e della comunicazione (*Information, and Communication Technology*, ICT) grazie alle quali vengono erogati in misura crescente servizi essenziali per la collettività e strategici per il Paese.

A questo proposito la dottrina che da tempo si occupa del tema della sicurezza cibernetica invita a riflettere sulla vastità dei settori che nelle moderne società si avvalgono dei servizi digitali.

Non esiste «un settore in questo momento – anche molto lontano, come l'agricoltura o altri – che non si poggi pesantemente sul cyber space».

Servizi economici e finanziari, sistemi di comando e controllo militare, sistemi di fornitura di energia elettrica o acqua, l'assistenza sanitaria, le telecomunicazioni, dispositivi fisici con cui interagiamo giornalmente sono controllati da sistemi informatici.

Una *smart city* è un luogo in cui le reti e i servizi tradizionali sono resi più efficienti con l'uso di soluzioni digitali a beneficio dei suoi abitanti e delle imprese. Una città intelligente che vive e prospera grazie alle reti di connessione ultraveloce e ad oggetti e servizi (Tv, lampadine, posti auto, fermate autobus, semafori, uffici pubblici, servizi pubblici e privati, recapito dei pacchi e della posta) completamente automatizzati e informatizzati.

Una città intelligente va oltre l'uso delle tecnologie digitali per un migliore utilizzo delle risorse e minori emissioni di aria cattiva. Vuol dire reti di traspor-

to urbano intelligenti, impianti di approvvigionamento idrico e di smaltimento dei rifiuti migliorati e modi più efficienti per illuminare e riscaldare gli edifici. Significa un'amministrazione cittadina più interattiva e reattiva, spazi pubblici più sicuri e un migliore soddisfacimento delle esigenze di una popolazione che se è vero che da una parte invecchia, dall'altra vede crescere i propri giovani in un ambiente tecnologico sano.

La *smart city* è, in definitiva, una città che gestisce le risorse pubbliche e private in modo intelligente, mira a diventare economicamente sostenibile ed energeticamente autosufficiente, ed è attenta alla qualità della vita e ai bisogni dei propri cittadini. È, insomma, uno spazio territoriale che sa stare al passo con le innovazioni e con la rivoluzione digitale, ma anche sostenibile e attrattiva. Le *smart city* sono più competitive della media delle altre città e rappresentano un volano importante per l'economia di un Paese.

Nelle *smart city* – almeno in quelle ideali teorizzate dalla letteratura sul tema– è presente un elevato livello di connettività e i milioni di sensori di cui è costellata sono in grado di raccogliere ingenti masse di dati, le strade sono percorse da auto elettriche e a guida autonoma, gli incroci sono regolati da semafori intelligenti, gli oggetti si scambiano informazioni tra di loro grazie all'*Internet of Things* (IoT). Ma ci sono anche ampi spazi verdi, il traffico è fluido ed è possibile praticare una mobilità sostenibile fatta di *bike sharing*, *car sharing* e auto ibride o elettriche. Per tutti questi motivi la *smart city* è costellata di sensori che generano una grande quantità di dati, i quali possono alimentare servizi più evoluti ed in tempo reale, e permettere alle amministrazioni una gestione sempre più efficiente, con poche file perché i servizi pubblici sono tutti a portata di App e di accessi *online*.

L'emergenza sanitaria scaturita dall'attuale pandemia ha messo a dura prova le grandi città, le cosiddette "*global cities*" in cui si concentrano i quartier generali delle grandi multinazionali e i centri finanziari, dove interi distretti dirigenziali e tutte le attività accessorie hanno subito gli effetti del *lockdown*. Nei centri urbani il ritorno alla situazione precedente sarà strettamente correlato al cambio di paradigma che riguarderà i processi lavorativi nel mondo ibrido delle *smart city* in cui lavoreremo in parte da casa e in parte in ufficio e dove per forza di cose assisteremo a un mutamento degli assetti, degli equilibri geografici ed urbani.

In questo scenario di un futuro prossimo pertanto la diffusione di oggetti tra loro interconnessi, di reti di connessione sempre più veloci e potenti, di registri distribuiti in grado di registrare e gestire transazioni di vario tipo (*Blockchain*), di criptovalute (come *Bitcoin*, *Lite Coin*, *Ether* e *Ripple*), di sistemi di *Artificial Intelligence* (AI) e di apparecchiature e macchine robotizzate contribuirà ad un ulteriore ampliamento del dominio cibernetico e quindi

delle superfici sulle quali perpetrare attacchi informatici su vasta scala grazie alla complicità della moltiplicazione esponenziale delle vulnerabilità cibernetiche.

In quanto dominio artificiale il dominio cibernetico presenta, delle "vulnerabilità" ovvero dei punti di debolezza attraverso i quali è possibile acquisire illegalmente dati e informazioni che "transitano" nello spazio cibernetico ovvero compromettere in tutto o in parte il funzionamento di servizi e sistemi digitali.

Le vulnerabilità del dominio cibernetico rappresentano pertanto il rovescio della medaglia del progresso tecnologico ed informatico.

Di difficile individuazione e classificazione tali "fratture" del sistema informatico possono dipendere sia da fattori tecnici congeniti al *software* applicativo, sia dal mancato o non corretto funzionamento dei sistemi di protezione o da vizi e vulnerabilità (colpose o dolose) degli hardware o comunque dei supporti informatici. Da tempo in sede istituzionale si sottolinea l'esigenza di disporre di materiali tecnologicamente certificati più facilmente controllabili e monitorabili, con particolare riferimento alla fornitura di materiale militare o dedicata alle infrastrutture critiche.

In tutti i principali contesti nazionali, europei ed internazionali nei quali si analizzano le principali sfide alla stabilità, alla sicurezza e alla crescita dei popoli la minaccia cibernetica viene da tempo considerata come una minaccia assai significativa, mutevole nei suoi tratti essenziali, in continua evoluzione, rapida rispetto al bersaglio da aggredire e capace di produrre effetti a distanze non raggiungibili con gli ordinari strumenti di attacco.

Gli attacchi cibernetici possono, infatti, originare da qualsiasi punto della rete globale e per le loro peculiarità sono idonei a determinare rilevanti conseguenze sul funzionamento e l'integrità della rete informatica di un Paese.

Al riguardo viene di sovente ricordato che le operazioni nello spazio cibernetico si svolgono con una velocità di oltre 20.000 volte maggiore di quelle nello spazio fisico, di oltre 200.000 volte maggiore di quelle nell'aria, e di 10 milioni di volte maggiore di quelle in terra ed in mare. Con l'IoT, l'uso dell'intelligenza artificiale e l'utilizzo di sistemi robotici a supporto delle *smart city* questi valori numerici sono destinati a moltiplicarsi.

Gli attacchi informatici sono generalmente a carattere asimmetrico in quanto i mezzi a disposizione del soggetto attaccante sono allo stato delle conoscenze attuali nettamente superiori alle capacità di difesa del soggetto attaccato. La difficile tracciabilità degli attacchi rende inoltre estremamente complesse le attività preventive, investigative e di contrasto.

L'uso di Artificial Intelligence anche negli attacchi informatici decuplicherà la forza dei prossimi attacchi. Nel contesto della sicurezza informatica,

l'utilizzo efficace dell'AI facilita il livello della comprensione delle minacce ed integra rapidamente il know-how dei 'difensori' per combattere alla pari (o quasi). Invece di fare affidamento su attacchi storici per individuare quelli nuovi, l'AI difensiva apprende ciò che è normale per un'organizzazione ed è in grado di rilevare attività anomale e potenzialmente pericolose non appena si manifestano anche se mai individuate in precedenza.

Con riguardo poi agli effetti dell'aggressione informatica in diversi documenti ufficiali pubblicati sia a livello nazionale che internazionale, si sottolinea la capacità degli attacchi cibernetici di produrre danni sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali e si sottolinea la necessità di predisporre capacità operative difensive al fine di preservare la sicurezza del "Sistema Paese" e di rafforzare la tenuta delle strutture politiche, economiche e sociali.

A livello nazionale da tempo le Relazioni sulla politica dell'informazione per la sicurezza trasmesse dal Governo (Presidenza del Consiglio dei ministri) al Parlamento ai sensi dell'art. 38 della legge n. 124/2007 pongono particolare attenzione all'accresciuto livello di complessità e sofisticatezza della minaccia cyber e all'eterogeneità del profilo soggettivo dell'attaccante.

Emerge, in proposito, una variegata gamma di attori che si muovono nel *cyber space* con finalità ed obiettivi diversi, tutti di difficilissima identificazione che vanno dall'*hacker* individuale che agisce a scopo di lucro, all'organizzazione criminale, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici.

Dal punto di vista della pericolosità si passa, quindi, dal vandalismo cibernetico alla vera e propria guerra cibernetica.

In futuro, osservano gli analisti, nuove tipologie di attacco saranno probabilmente elaborate anche in conseguenza del sempre più diffuso utilizzo dell'innovazione tecnologica dell'IoT (*Internet of Things*) in diversi ambiti industriali, domestici e lavorativi. L'elenco potrebbe partire dalle piattaforme e dai sistemi informatici e in *Cloud* delle aziende, ai televisori di ultima generazione o alle consolle dei giochi elettronici a certi giocattoli per bambini, passando per le telecamere di sorveglianza attivabili da remoto, fino ad arrivare ai nostri smartphone collegati a sistemi di domotica domestica o lavorativa spesso anche collegati a sistemi di sicurezza.

In questi contesti sfruttando i richiamati dispositivi collegati in rete, sarà possibile a soggetti ostili acquisire illegalmente, con maggiore facilità rispetto agli attuali metodi intrusivi, informazioni riguardanti la vita privata e lavorativa della vittima, ovvero prendere il controllo di dispositivi e macchinari altrui, dirottandone l'azione, visionare dati riservati (telefonici, di posta elettronica, ecc.) oppure distruggere memorie o sequestrarle a scopo di ricatto (rendendole indisponibili al legittimo titolare).

La tematica è di particolare interesse anche nel campo della Difesa dove l'evoluzione delle tecnologie dell'informazione ha da un lato permesso di velocizzare i processi decisionali ai vari livelli di comando grazie all'ausilio di sistemi informativi di comando e controllo automatizzati che permettono la memorizzazione e lo scambio di enormi quantità di dati ed informazioni in "tempo reale", dall'altro lato l'utilizzo di tali strumenti tecnologici ha tuttavia reso le Forze Armate particolarmente vulnerabili ai rischi afferenti alla sicurezza dei sistemi e delle informazioni ivi contenute provenienti da minacce interne ed esterne all'organizzazione militare.

Da qui la necessità, avvertita dai Paesi maggiormente evoluti sul piano militare, di definire adeguate misure di difesa cibernetica rispetto a eventi di natura volontaria o accidentale che potrebbero compromettere o alterare dati e servizio fondamentali nell'ambito dell'organizzazione della Difesa.

Da diversi anni il tema della sicurezza cibernetica costituisce oggetto di analisi nell'ambito delle Relazioni sulla politica dell'informazione per la sicurezza, predisposte dal Governo (Presidenza del Consiglio dei ministri) e trasmesse al Parlamento ai sensi dell'art. 38 della legge n. 124/2007, recante disposizioni concernenti il Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto e in questi anni la legislazione si è senza dubbio rafforzata. La legge n. 124/2007 prevede, infatti, che entro il mese di febbraio di ogni anno il Governo trasmetta al Parlamento una relazione scritta, riferita all'anno precedente, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti. Alla relazione è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica. Con una certa lungimiranza si cercò fin dal 2007 di prevedere un'attenzione importante anche agli aspetti della sicurezza informatica che già in quegli anni interessavano le infrastrutture critiche e non solo.

In relazione a questo tema è possibile osservare come già nelle Relazioni sulla politica dell'informazione per la sicurezza degli ultimi anni la *Cybersecurity* veniva definita come un fondamentale campo di sfida per l'intelligence un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione.

A questa prima analisi hanno fatto seguito nelle Relazioni presentate al Parlamento negli anni successivi ulteriori riflessioni, che secondo un livello crescente di intensità hanno considerato la minaccia cibernetica come una «*sfida crescente per le politiche di sicurezza degli Stati*», un «*obiettivo informativo prioritario dell'attività intelligence nazionale*», «*la sfida più impegnativa per il sistema Paese*». Tale valutazione viene motivata in considerazione dei suoi peculiari tratti caratterizzanti che attengono tanto al dominio digitale nel quale

viene condotta, quanto alla sua natura diffusa e transnazionale, quanto ancora agli effetti potenziali in grado di produrre ricadute peggiori di quelle ipotizzabili a seguito di attacchi convenzionali e di incidere sull'esercizio di libertà essenziali per il sistema democratico.

Negli ultimi anni si è notato un innalzamento della qualità e della complessità di alcune tipologie di attacco. Sul fronte delle infrastrutture di attacco, i gruppi responsabili di azioni di *cyber-espionage* hanno proseguito nell'impiego di servizi IT commerciali (domini web, servizi di *hosting*, ecc.), forniti da *provider* localizzati in diverse regioni geografiche, anche per rendere difficoltoso il processo di individuazione attribuzione. Attenzione viene inoltre rivolta anche alla c.d. minaccia ibrida, considerata quale impiego combinato di strumenti convenzionali e no, le cui traduzioni operative sono risultate (e saranno sempre più) amplificate grazie alla digitalizzazione di intere città e regioni in ogni settore e che sta interessando ogni aspetto della vita sociale, arrivando ad esplicitarsi anche in operazioni di influenza/ingerenza attuate per condizionare il corretto svolgimento di fondamentali dinamiche dei processi democratici.

A seconda del diverso grado di offensività gli attacchi cibernetici vengono tradizionalmente ricondotti ad atti di cyber criminalità, cyber spionaggio, cyber terrorismo e cyber guerra. In alcune analisi scientifiche è frequente il richiamo all'*hacktivism* per indicare gli attacchi cyber motivati ideologicamente.

Ciascuna delle richiamate fattispecie presenta al suo interno molteplici sfaccettature, così come un'operazione malevola complessa nello spazio cibernetico può essere il risultato di una pluralità di azioni intrusive di natura diversa.

Lo spionaggio cibernetico di frequente precede le altre forme di minaccia con intensità crescente e le accompagna nella loro evoluzione. In tale ambito non sempre è possibile riconoscere una chiara distinzione tra queste categorie.

Al di là delle singole peculiarità caratteristica comune di tutte le tipologie di attacchi criminali è la difficile individuazione degli autori degli atti ostili, la loro provenienza geografica e, talvolta, la stessa finalità dell'attacco cyber anche per la presenza, come detto di finalità plurime e interessi convergenti di due o più parti committenti. Nelle *smart city* le misure di sicurezza dei sistemi, degli strumenti e dei servizi rappresentano uno dei punti più importanti. L'adeguatezza delle misure rispetto alle diverse tipologie di rischio, il continuo aggiornamento delle analisi di prevenzione, la capacità di resilienza devono costituire una costante e un vero e proprio valore aggiunto per l'esistenza stessa delle *smart city*. Parafrasando un principio caro alla normativa in tema di trattamento dei dati si potrebbe dire che per crescere bene una moderna *smart city* del futuro deve fondarsi sul principio di *Security by design*.

2. *La sicurezza informatica come* asset *fondamentale di un sistema iper-connesso in quanto parte integrante della Sicurezza di un Paese*

Ad onor del vero, a prescindere dalle *smart city*, la sicurezza informatica è diventata negli ultimi anni un tema fondamentale. In un sistema iper-connesso essa è parte integrante della sicurezza stessa di un Paese, potremmo dire è parte integrante della sicurezza nazionale. Per troppo tempo chi avanzava esigenze di sicurezza lo faceva cercando di comprimere diritti di libertà.

Nell'ultimo decennio, soprattutto davanti a periodi di emergenza e di compressione (a volte limitata a volte meno dei diritti) è stato necessario parlare di sicurezza e anche di sicurezza informatica sforzandosi soprattutto di ricercare il giusto equilibrio tra esigenze di sicurezza e diritti di libertà. Un concetto di *Security* non contrapposto alle libertà bensì esso stesso diritto di libertà nel rispetto anche dei diritti personali.

La sicurezza concepita non più in contrapposizione con la libertà, quasi che la lievitazione dell'una necessariamente debba comportare una conseguente diminuzione o attenuazione dell'altra, ma va accreditata come espressione, invero una delle molteplici espressioni, del diritto di libertà.

Una sicurezza, quindi, da percepire come diritto di libertà, uno dei tanti diritti di libertà consacrati esplicitamente e implicitamente dalla nostra Costituzione. Un diritto da vivere non soltanto nella dimensione individuale tipica di ogni libertà, ma da esercitare preliminarmente nella caratterizzazione collettiva propria dei diritti sociali che vanno garantiti a tutti oltreché ai singoli.

Una sicurezza, conseguentemente, che proprio la connotazione libertaria consente di evidenziare come altamente democratica in quanto contiene in sé i valori e i limiti propri di ciascun diritto di libertà, primo fra tutti quello di non poter negare sé stessa.

Laddove ciò dovesse accadere, verrebbe infatti a configurarsi una sicurezza diversa, non più democratica e costituzionalmente garantita, ma una sicurezza deviata rispetto alla sua essenza, espressione di un'impostazione derivante da un regime autoritario abituato, questo sì, a negare la libertà.

La sicurezza deve essere intesa come una delle molteplici espressioni del diritto di libertà, uno dei tanti, che come la riservatezza e al pari di essa sia consacrato esplicitamente e implicitamente nella nostra Costituzione. Una sicurezza quindi conseguentemente democratica che contiene in sé, come la *privacy*, i valori ed i limiti propri di ciascun diritto di libertà. Nuovi concetti della sicurezza quindi. Concetti di sicurezza e privacy adeguati ai tempi e strettamente legati tra loro in quell'indissolubile legame che deve esistere tra diritti sociali e diritti di libertà.

Il ruolo della *privacy* e della sua legislazione assume in questo ambito un ruolo di garanzia e di controllo in funzione di quel giudizio di responsabilità che deve esistere affinché questa apparente dicotomia si mantenga sempre nel giusto equilibrio.

Lo spionaggio, la sorveglianza e la conseguente aggressione alla *privacy* dei cittadini e di interi stati sovrani fa sempre più spesso notizia. Il concetto di sicurezza e di sorveglianza sono da decenni in totale evoluzione. La sicurezza è diventata una caratteristica costante e fondamentale del mondo moderno. Un mondo moderno che, per dirla come Bauman, è diventato un mondo liquido. Si parla di modernità liquida, intendendola come individualizzata, privatizzata, incerta, flessibile, vulnerabile. Cittadini, lavoratori, consumatori, navigatori della Rete sono sempre in movimento spesso privi di certezze ma accettano il rischio che i loro movimenti vengano monitorati, tracciati, localizzati e profilati.

Anche l'esigenza di sicurezza e la necessità di *privacy* scivolano lentamente verso uno stato fluido. L'esigenza di sicurezza e l'aumento della capacità di sorveglianza sui dati personali e sugli individui per farli sentire più sicuri (o dargli la sensazione di esserlo). Un tempo la sorveglianza era solida, stabile in qualche modo, garantita da principi giuridici certi e da punti di riferimento indiscutibili. Oggi la sorveglianza tende a farsi liquida soprattutto nei momenti in cui frammenti di dati personali, trattati per determinate finalità, divengono facilmente utilizzabili per altri scopi.

Prima di affrontare il problema centrale, che voglio porre alla vostra attenzione, occorre premettere che ormai quando parliamo di *privacy* dei nostri dati abbiamo di fronte un concetto di riservatezza che si muove su un "doppio binario": da un lato, il trattamento dei dati dei consumatori, la profilazione delle nostre abitudini a fini di *marketing* e di studio del comportamento umano e dall'altro il trattamento e la conservazione dei dati per finalità di accertamento, prevenzione e repressione dei reati nonché per esigenze di sicurezza nazionale.

In quest'ultimo ambito molte sono le deroghe ai principi generali. Riguardo alla prima tipologia di trattamento e al suo rapporto con il diritto alla riservatezza è da tempo chiaro a tutti che la *privacy* non gode di ottima salute ed è alla ricerca di un riscatto sociale.

Senza cercare altrove fantomatici colpevoli è sufficiente che ciascuno di noi si guardi allo specchio: siamo noi per nostra volontà a mandare al massacro il nostro diritto alla *privacy*. Nella migliore delle ipotesi, spesso con una colpa che definirei "una colpa cosciente" consentiamo di fare uno scambio con la nostra *privacy* perché lo consideriamo un costo ragionevole da pagare in cambio dei meravigliosi servizi che ci vengono offerti.

Con lo stesso atteggiamento colpevole rifiutiamo di leggere le condizioni di

contratto dei servizi e le informative su "app" e *software* che scarichiamo sui nostri palmari o personal computer e non ci rendiamo conto di quanto è importante ai fini della sicurezza informatica (Cybersicurezza) del nostro *smartphone*. Al limite tra la colpa cosciente e il dolo eventuale stiamo uccidendo la nostra *privacy*, la nostra sicurezza informatica e quella dei nostri dati spesso sensibili, finanziari o molto personali. Moltissimi adolescenti in relazione ad "app" e *social network* usano il proprio *smartphone* come una sorta di "confessionale elettronico portatile" e forse non solo gli adolescenti. Negli ultimi anni infatti traspare che tutte queste novità raccolgono l'attenzione di tutti i soggetti a prescindere dalla fascia d'età.

L'alto livello di sicurezza (con compressione e affievolimento della riservatezza dei cittadini) e il rispetto della *privacy* degli stessi possono coesistere, possono operare in sinergia e tenersi in equilibrio se alla base vi è un costante richiamo al senso e al dovere di responsabilità. Se è vero come è vero che Libertà è innanzitutto Responsabilità (art. 2 Cost.) il richiamo a quest'ultima deve essere molto più forte e presente nella normativa di settore di quanto non lo sia ora. Ma soprattutto deve essere un punto fermo culturale.

Oggi siamo già in ritardo, è diventata imprescindibile una nuova e più profonda cultura della sicurezza dei dati e della *privacy* finalizzata a permeare non solo gli addetti ai lavori, ma ogni individuo e ogni titolare del trattamento dei dati.

È necessario che ciò avvenga proprio oggi, in un momento in cui l'esigenza di sicurezza rischia di affievolire alcuni tra i diritti fondamentali.

Occorre una sensibilità nuova, anche politica, che passi da una tutela della riservatezza dei dati e delle informazioni anche attraverso una maggiore cultura della Sicurezza informatica. L'equilibrio tra un diritto alla sicurezza e la sicurezza come diritto di libertà può essere sostenibile e può essere garantito dalla presenza, anche di maggiore *Accountability*, non solo da parte di ogni titolare, ma anche di ogni cittadino.

Nel linguaggio di tutti i giorni, le parole *dato* e *informazione* rischiano di essere confuse. I dati sono numeri, testo, immagini che si riferiscono a fatti non organizzati oppure sono dati personali in quanto informazioni riferibili direttamente o indirettamente ad una persona fisica.

Le informazioni sono dati organizzati in modo da essere utili all'utente. Una mappa di un aeroporto militare è un'informazione (riservata), la geolocalizzazione di un dipendente è un dato personale, la geolocalizzazione di un ristorante è un'informazione. La geolocalizzazione di un soggetto (nome e cognome o e-mail) che cerca un ristorante su Google Maps è un dato personale.

Anche le informazioni che non sono dati personali meritano talvolta la medesima sicurezza degli altri.

Ogni azienda o Ente pubblico o privato ha una sua percezione di cosa si intende per "sicurezza delle informazioni"; per esempio: segretezza dei progetti innovativi e dei propri clienti, accuratezza di tutti i dati economici e di produzione, disponibilità dei sistemi informatici, riservatezza dei dati sensibili, particolari e giudiziari.

Il termine sicurezza, però, nasconde in sé una contraddizione. Sicurezza, infatti, fa venire in mente qualcosa di assoluto e inconfutabile, cioè qualcosa di impossibile che si realizzi nella realtà almeno nella sua completezza e assolutezza. Si dice che Fort Knox, dove si trovano le riserve monetarie degli USA, è uno dei luoghi più sicuri al mondo: sofisticati sensori, barriere perimetrali e allarmi sono tutti ai massimi livelli. Come se non bastassero, è sede di un comando di Marines pronti a intervenire per qualsiasi problema. Fort Knox è riconosciuto come sinonimo di luogo sicuro.

Ma come reagirebbe la struttura a un impatto imprevisto con un meteorite di un chilometro di diametro che centra in pieno Fort Knox? Se non previsto e preventivato attraverso un monitoraggio dello spazio con un sistema di trasferimento sicuro del denaro prima dell'impatto il denaro sarebbe perso. Non si riuscirebbero a salvare le riserve auree americane. Questo è chiaramente un esempio per dire che non ha senso parlare di sicurezza in senso assoluto, ma solo in senso relativo. Fort Knox non è infatti resistente ad un grosso meteorite. Per questo motivo bisogna diffidare di chiunque offre prodotti o soluzioni sicuri al 100%. Una tale affermazione classifica subito la persona come scarsamente competente o come un imbonitore che vuole vendere qualcosa. Deve essere individuato il livello adeguato di sicurezza che si vuole ottenere attraverso la valutazione del rischio. Il livello di sicurezza deve essere raggiunto attraverso opportune azioni di trattamento. Nel caso in cui quel livello non possa essere raggiunto, le carenze devono essere analizzate e, se il caso, accettate.

Nel tempo, la valutazione deve essere ripetuta per verificare se il livello di sicurezza desiderato e quello attuato siano ancora validi. Queste attività di valutazione, azione o accettazione e ripetizione costituiscono la gestione del rischio (*Risk Management*).

Da questo ragionamento risulta che, quando si parla di sicurezza delle informazioni, non ci si limita alla sicurezza informatica, ossia relativa alle informazioni in formato digitale e trattate dai sistemi dell'*Information and Communication Technology*, ma a tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e distruggere le informazioni. Questo è uno dei motivi per cui si preferisce parlare di "informazioni" e non di "dati": il termine, intuitivamente, ha una valenza più ampia.

Più rigorosamente, la sicurezza delle informazioni include quella dei dati, come si deduce dalle quattro tipologie di rappresentazione della conoscenza:

– dati: insieme di singoli fatti, immagini e impressioni;
– informazioni: dati organizzati e significativi;
– conoscenza: informazioni recepite e comprese da un singolo individuo;
– sapienza: conoscenze tra loro connesse che permettono di prendere decisioni.

La Sicurezza delle informazioni (*Information security*) è definita come preservazione della riservatezza, integrità e disponibilità delle informazioni:

– Riservatezza (*Confidentiality*): proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;
– Integrità (*Integrity*): proprietà di accuratezza e completezza;
– Disponibilità (*Availability*): proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

Ci si riferisce spesso a queste proprietà come parametri (RID) approfonditi in modo più completo nei libri sulla certificazione ISO 27001 o altri del settore.

Si parla di sicurezza informatica quando ci si limita alla sicurezza delle informazioni sui sistemi informatici.

Con il termine *Cybersecurity*, molto in uso in questo periodo, s'intende la stessa sicurezza informatica, solo con un nome ritenuto più suggestivo. Esso è tratto dal termine *cyberspace*, inventato da William Gibson nel 1986 nell'ambito della letteratura cyberpunk forse perché il termine "Internet" non era abbastanza diffuso. Lo stesso Gibson ha ammesso di avere usato il termine greco "*cyber*" (timone, da cui è anche tratto anche il termine italianizzato e forse più corretto di "cibernetica") senza saperne il significato ma solo perché interessante.

In ambito informatico si estremizza dicendo che "il computer sicuro è il computer spento o, meglio, rotto", oppure che "l'unico sistema realmente sicuro è un sistema spento, affogato in un blocco di cemento, sigillato in una stanza con pareti schermate col piombo e protetto da guardie armate; e anche in questo caso, si potrebbero avere dei dubbi".

È evidente che questo approccio non considera la disponibilità delle informazioni. La riservatezza è spesso associata alla segretezza, però la necessità di mantenere riservate le informazioni non implica la necessità di non rivelarle ad alcuno, ma di stabilire chi ha il diritto ad accedervi.

Non è semplice stabilire le caratteristiche di riservatezza di ogni informazione e chi può accedervi, come dimostra l'esempio di un'azienda in cui i dati sul personale sono sicuramente riservati, ma persone diverse devono accedervi per motivi di continuità lavorativa e spesso per adempimenti legislativi: il me-

dico competente, l'amministrazione, i dirigenti, certi uffici pubblici, il commercialista e l'ufficio legale. Ciascuno non dovrebbe accedere a tutti i dati, ma solo ad una parte di essi: l'amministrazione alla sola busta paga, il medico ai soli dati sanitari, l'ufficio legale solo ai dati utili ai fini della difesa in sede giudiziaria o per adempimenti legislativi, l'amministratore di sistema solo ai fini di manutenzione.

I metodi e le tecniche utilizzati per accedere illegalmente ai sistemi informatici altrui sono complessivamente definiti *hacking*; chi utilizza questi metodi e tecniche è detto *hacker* anche se spesso i veri *hacker* lo fanno per denunciare e sottolineare falle e vulnerabilità nei sistemi di sicurezza. Il vero hacker è un profondo conoscitore dell'informatica, che non accetta le regole e giochetti e interessi economici presenti nel mondo dei computer e di Internet. L'*hacker* che si definisce Etico (*ethical hacking*) quando riesce a entrare in un sistema protetto, non causa, in genere, danni o non usa quei dati e informazioni per lucrare grandi somme di denaro, ma lascia un segno della sua visita, a volte comunicando il modo in cui è riuscito a superare i sistemi di sicurezza, così che l'azienda o l'ente possano evitare che questo riaccada in futuro. Ecco, nel fare questo occorre prestare molta attenzione perché il limite tra le condotte possibili in questi frangenti e la configurabilità di alcuni reati è molto sottile. È necessario limitarsi davvero, senza la volontà di accedere in modo illecito o danneggiare i sistemi informatici, a denunciare le vulnerabilità o le falle dei sistemi e senza proporsi in prima persona per risolvere il problema. Ciò al fine di evitare che tale richiesta di "consulenza" assuma i contorni di un ricatto o una estorsione: "ti dico questo e di dico come fare per risolverla solo se ti vorrai avvalere di me". Ancora in Italia manca la cultura in questo settore soprattutto da parte delle aziende, all'esterno esistono veri e propri accordi contrattuali, i c.d. *Ethical hacking agreement* con i quali stabilire vincoli, limiti ed eventualmente compensi tra le parti. In quest'ultimo caso si parla di hacking etico, così come quando sono le stesse aziende a commissionare l'uso di tecniche di *hacking* per testare la sicurezza dei propri sistemi e delle proprie reti rivolgendosi ad imprese esperte nel settore. Quando, invece, si accede a sistemi informatici altrui per acquisire i dati, trarne profitto o semplicemente per danneggiarli o distruggerli, si parla di *cracking* e chi lo pratica è detto cracker e commette senza alcun dubbio (i dubbi che si possono avere con il vero *Ethical hacker*) una serie di reati informatici come accesso abusivo, acquisizione e utilizzo illecito di codici di accesso, danneggiamento informatico (nelle sue diverse accezioni), utilizzo di programmi informatici malevoli, intercettazione illecita di dati o rivelazione di segreti aziendali.

Il fattore umano è veramente l'anello più debole della sicurezza, sosteneva tanti anni fa a ragion veduta Kevin Mitnick. La possibilità di ingannare esiste

perché esiste la possibilità di essere ingannati: la fallibilità e la debolezza cognitiva di ciascuno di noi, la fiducia che riponiamo nei principi comunicativi sono il presupposto dell'inganno. La possibilità dell'inganno è insita nella natura umana, e in particolare nel linguaggio, strumento primo di comunicazione umana. Che l'inganno sia una forma di interazione umana frequentissima, lo dimostra già la ricchezza di espressione a livello lessicale e la vastissima bibliografia che in ogni secolo se n'è occupata. Fatta eccezione dell'inganno intrinseco (lo scherzo, la rivalità) e delle cosiddette menzogne di cortesia non si inganna per il gusto di ingannare, ma con lo scopo di manipolare le conoscenze dell'altro in modo da influenzare i suoi comportamenti, ed indurlo ad agire in modo che noi possiamo perseguire i nostri scopi. Di conseguenza, quando l'inganno fa uso della comunicazione, esso non la stravolge: se infatti lo scopo della comunicazione è influenzare l'altro, l'inganno, come strumento di influenzamento, non può che definirsi a tutti gli effetti una forma di comunicazione. Ottenere quello che si vuole dagli altri, "convincerli", può essere perseguito in due modi: mediante la persuasione, oppure mediante una manipolazione prevaricatrice e quindi negativa. È una manipolazione psicologica, che mira a catturare l'attenzione del destinatario inducendolo a dire sì o comunque a rispondere alle richieste che gli vengono fatte fornendo informazioni che altrimenti non si rivelerebbero.

Anche nell'era delle *smart city* l'ingegneria sociale sarà un ibrido di persuasione e manipolazione. Nel futuro più che mai, quest'arte dell'inganno risulterà ancora ampiamente utilizzata in ambito informatico e propedeutica spesso all'intrusione nei sistemi, soprattutto per via della continua evoluzione dei sistemi di sicurezza sempre più performanti e resilienti.

Il *social engineering* in questo settore rappresenta un insieme di tecniche utilizzate dai cybercriminali per attirare gli ignari utenti ad inviare loro i propri dati riservati, infettare i loro computer tramite malware o aprire collegamenti a siti infetti. Inoltre, gli *hacker* approfittano della mancanza di conoscenza di un utente; grazie alla velocità della tecnologia, molti consumatori e dipendenti non si rendono conto del valore incondizionato dei dati personali e non sanno come proteggere al meglio queste informazioni.

Quasi tutti gli attacchi contengono una sorta di *social engineering*. Le classiche e-mail di "*phishing*" e i virus truffa, ad esempio, sono cariche di sfumature sociali. Le mail di *phishing* cercano di convincere gli utenti che esse provengono in realtà da fonti legittime, nella speranza di procurarsi anche pochi dati personali o aziendali. Nel frattempo, le e-mail che contengono allegati pieni di virus, fingono spesso di provenire da contatti fidati o offrono contenuti multimediali che sembrano innocui, come video "divertenti" o "carini". In alcuni casi, gli aggressori usano metodi più semplicistici di

social engineering per ottenere l'accesso alla rete o al computer. Ad esempio, un hacker potrebbe frequentare la mensa pubblica di un grande palazzo degli uffici, mentre gli utenti lavorano sui loro *tablet* o *laptop* e fare "*shoulder surf*". Ciò potrebbe comportare un elevato numero di *password* e nomi utente, il tutto senza inviare e-mail o scrivere nemmeno una riga di codice del virus. Alcuni attacchi, invece, si basano su una comunicazione effettiva tra attaccanti e vittime; in questo caso, l'attaccante spinge l'utente a permettere l'accesso alla rete con il pretesto di un problema serio che richiede attenzione immediata. La rabbia, il senso di colpa e la tristezza sono tutti utilizzati in egual misura per convincere gli utenti che il loro aiuto è necessario e non possono farne a meno. Infine, è importante fare attenzione al social engineering in quanto mezzo di confusione. Molti dipendenti e consumatori non si rendono conto che con solo poche informazioni (nome, data di nascita o indirizzo), gli *hacker* possono accedere a più reti, mascherandosi da utenti legittimi al personale di supporto IT.

Da qui, è semplice ripristinare le *password* e ottenere un accesso quasi illimitato. La protezione contro il *social engineering* inizia con l'istruzione: gli utenti devono essere istruiti a non fare mai clic su collegamenti sospetti e a proteggere sempre le credenziali di accesso, anche in ufficio o a casa. Tuttavia, nel caso in cui le tattiche sociali abbiano successo, il risultato più probabile è un'infezione da *malware*.

Per combattere *rootkit*, *trojan*, *ransomware* e altri ancora, è fondamentale utilizzare una soluzione di sicurezza Internet di alta qualità, in grado sia di eliminare le infezioni che di tracciarne l'origine. Ma soprattutto, i titolari del trattamento non potranno trascurare l'implementazione di ottimi sistemi e processi di *backup* su larga scala unitamente a sistemi di prevenzione degli attacchi informatici basati su sistemi predittivi che utilizzano l'Intelligenza Artificiale. Sistemi però che tutelino comunque e i dati e le informazioni e consentano alle *smart city*, le città del futuro, di crescere e fornire servizi tecnologici ai cittadini nel rispetto dei diritti personali.

3. *La* Cybersecurity *nei suoi aspetti normativi*

Nel corso degli ultimi anni sono stati adottati una serie di provvedimenti normativi volti a definire l'architettura strategica nazionale per la sicurezza cibernetica al fine di potenziare progressivamente le capacità di difesa cibernetica del Paese.

Nello specifico, nel 2013, con il c.d. "decreto Monti" (d.P.C.M. 24 gennaio

2013), l'Italia ha provveduto a definire le molteplici competenze di settore tra i diversi attori istituzionali delineando la governance nazionale in materia di *Cybersecurity*.

Il 17 febbraio 2017 è stato adottato il decreto del Presidente del Consiglio dei ministri recante la direttiva in materia protezione cibernetica e sicurezza informatica nazionali (c.d. "decreto Gentiloni") che ha interamente sostituito il precedente decreto del 2013 introducendo importanti innovazioni volte, in particolare, ad assicurare un maggiore coordinamento tra le diverse strutture istituzionali previste nel nuovo quadro strategico. Nel maggio 2018 con il d.lgs. n. 65/2018, di recepimento della Direttiva del 2016, n. 1148 (c.d. "Direttiva NIS") sono stati delineati ulteriori interventi di rafforzamento del sistema di sicurezza cibernetica del Paese. Dal 2018 trova, inoltre, applicazione il d.lgs. n. 101 adottato per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE del 2016, n. 679 (noto come "GDPR" *General Data Protection Regulation*) che impone a chi custodisce e tratta dati personali (soggetti pubblici e privati) l'adozione di standard di sicurezza più elevati rispetto al passato. A sua volta il Regolamento UE del 2019, n. 881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 *Cybersecurity Act* introduce una certificazione Europea della sicurezza cibernetica di hardware e software trasponendo in campo informatico gli stringenti standard già applicati alla sicurezza fisica dei beni prodotti nella UE. Responsabile delle certificazioni è l'Agenzia Europea per la sicurezza delle reti e dell'informazione (European Network and Information Security Agency, ENISA).

Da ultimo il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il decreto legge del 2019, n. 105 (pubblicato nella *Gazzetta Ufficiale* del 21 settembre 2019) che introduce disposizioni urgenti in materia di "perimetro" di sicurezza nazionale cibernetica.

Al riguardo, si ricorda che il 19 luglio 2019 il Consiglio dei ministri aveva approvato il disegno di legge sul «*perimetro di sicurezza nazionale cibernetica*» (A.S. 1448). Pochi giorni prima, in data 11 luglio 2019, era stato approvato dal Consiglio dei ministri il decreto legge del 2019, n. 64 (non convertito in legge) sull'estensione del Golden Power per garantire la sicurezza delle nuove infrastrutture di telecomunicazione con particolare riferimento a quelle 5G.

Completano, infine, l'impianto normativo e regolamentare una serie di ulteriori disposizioni normative adottate in ambito nazionale che hanno riguardato profili specifici del tema della sicurezza cibernetica con particolare riferimento alle modalità di contrasto al fenomeno *cyber crime* e alle relative attività di *intelligence*.

Negli ultimi anni abbiamo assistito ad una corsa legislativa senza precedenti verso la creazione di una infrastruttura legislativa e organizzativa in tema di

Cybersecurity. Molti provvedimenti normativi governativi hanno delineato e dato forma ad una architettura strategica nazionale in materia di sicurezza cibernetica con particolare riferimento alle competenze assegnate in tale ambito ai principali attori istituzionali.

Il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha approvato il d.l. n. 105/2019 (pubblicato nella *Gazzetta Ufficiale* del 21 settembre 2019) che introduce disposizioni urgenti in materia di "perimetro" di sicurezza nazionale cibernetica.

In particolare, il decreto fa riferimento ad amministrazioni pubbliche, nonché ad enti oppure operatori nazionali, pubblici e privati i cui sistemi informatici:

– sono necessari per l'esercizio di una funzione essenziale dello Stato;
– sono necessari per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
– il cui malfunzionamento, interruzione o uso improprio possono pregiudicare la sicurezza nazionale.

I soggetti che fanno parte del perimetro e i loro fornitori dovranno notificare gli eventuali incidenti "aventi impatto su reti, sistemi informativi e servizi informatici" e vengono stabilite le misure "volte a garantire elevati livelli di sicurezza".

In particolare, il comma 3 demanda ad un d.P.C.M. – da adottare entro dieci mesi dalla conversione del decreto legge – la definizione:

– delle procedure in base alle quali i soggetti del perimetro di sicurezza nazionale cibernetica segnalino gli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici (lett. a);
– delle misure volte a garantirne elevati livelli di sicurezza (lett. b).

All'elaborazione delle richiamate misure provvedono, secondo gli ambiti di competenza delineati dal medesimo decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

Per quanto riguarda le procedure di segnalazione degli incidenti su reti, sistemi informativi e sistemi digitali rientranti nel perimetro di sicurezza nazionale cibernetica, i relativi soggetti (amministrazioni pubbliche, nonché enti oppure operatori nazionali, pubblici e privati) devono notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano. Il CSIRT procede poi a inoltrare tempestivamente tali notifiche al Dipartimento

delle informazioni della sicurezza (DIS). Siffatta trasmissione è prevista anche qualora siano interessate attività demandate al Nucleo per la sicurezza cibernetica. A sua volta il DIS assicura una ulteriore trasmissione all'organo del Ministero dell'interno preposto alla sicurezza e regolarità dei servizi di telecomunicazioni; alla Presidenza del Consiglio dei ministri (se le notifiche degli incidenti giungano da un soggetto pubblico – o da un soggetto fornitore di servizi fiduciari qualificati o svolgente l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, ai sensi dell'art. 29 del Codice dell'amministrazione digitale, d.lgs. n. 82/2005) ovvero al Ministero dello sviluppo economico (se le notifiche giungano da un soggetto privato del perimetro di sicurezza nazionale cibernetica). Le misure di sicurezza – di cui alla lett. b) – esse devono assicurare elevati livelli di prevenzione e salvaguardia delle reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica.

Il testo integra ed adegua, inoltre, il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo, con particolare riferimento a quanto previsto dal d.l. n. 21/2012, in modo da coordinare l'attuazione del Regolamento UE del 2019, n. 452, sul controllo degli investimenti esteri, e apprestare idonee misure di tutela di infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione del d.l. n. 21/2012.

L'art. 4 modifica il d.l. n. 21/2012 in tema di poteri speciali del Governo nei settori ad alta intensità tecnologica (c.d. *golden power*). In particolare, viene ampliato il perimetro dei settori che possono essere individuati con regolamento ai fini dell'applicazione della disciplina, con riferimento alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico. Viene altresì stabilito che, fino all'adozione del regolamento che individua i settori rilevanti, è soggetto a notifica l'acquisto a qualsiasi titolo, da parte di un soggetto esterno all'Unione Europea, di partecipazioni in società che detengono beni e rapporti in specifici settori, fra i quali quelli legati alla Cybersicurezza, di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società. Il comma 2 prevede altresì che tali notifiche possano dar luogo all'esercizio di poteri speciali da parte del Governo, mediante l'imposizione di condizioni e impegni diretti a garantire la tutela degli interessi essenziali dello Stato nonché l'opposizione all'acquisto della partecipazione.

Le nuove norme, tra l'altro:

– istituiscono un meccanismo teso ad assicurare un procurement più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di *information and communication technology* (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti. Con

specifico riferimento al comparto della Difesa si prevede che per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, il Ministero proceda, attraverso un proprio Centro di valutazione in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza;

– prevedono che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate ai sensi del d.l. n. 21/2012, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard;

– rafforzano i poteri del Centro di valutazione e certificazione nazionale (il CVCN, istituito al Mise), che potrà imporre "test di hardware e software" in caso di "affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici" dei soggetti inseriti nel perimetro;

– attribuiscono al Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi, il potere di eliminare, ove indispensabile e per il tempo strettamente necessario, lo specifico fattore di rischio o di mitigarlo, secondo un criterio di proporzionalità, disattivando totalmente o parzialmente, uno o più apparati o prodotti impiegati nelle reti e nei sistemi".

Nello specifico, il decreto legge stabilisce in quattro mesi il termine per individuare le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati che entreranno a far parte del cosiddetto perimetro cibernetico, a tutela della sicurezza di reti e servizi definiti "strategici". Sempre in quattro mesi l'organismo tecnico di supporto al CISR, il Comitato Interministeriale per la Sicurezza della Repubblica, con un rappresentante della Presidenza del Consiglio dei ministri, dovranno stabilire i criteri in base ai quali i soggetti predisporranno e aggiorneranno "con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici sensibili di rispettiva pertinenza, comprensivo della relativa architettura e componentistica", che verrà poi diffuso agli organismi di competenza.

Con il d.l. n. 82/2021 sono state emanate alcune disposizioni urgenti in materia di Cybersicurezza tra le quali definizione dell'architettura nazionale di Cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza nazionale.

L'Agenzia viene istituita, a tutela degli interessi nazionali nel campo della

Cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico e stabilisce la sua sede in Roma.

Ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

Il direttore generale è nominato tra soggetti appartenenti a una delle categorie di cui all'art. 18, comma 2, della legge n. 400/1988, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni.

Il Direttore generale ed il vice direttore generale, ove provenienti da pubbliche amministrazioni di cui all'art. 1, comma 2, del d.lgs. n. 165/2001, sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza.

La creazione di questo nuovo ente era necessaria già da tempo. In una realtà in cui da diversi anni le vulnerabilità delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche di soggetti pubblici e privati vengono sfruttate al fine di provocare il malfunzionamento o l'interruzione, totali o parziali, di funzioni essenziali dello Stato e di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, nonché di servizi di pubblica utilità, con potenziali gravi ripercussioni sui cittadini, sulle imprese e sulle pubbliche amministrazioni, sino a poter determinare un pregiudizio per la sicurezza nazionale.

I recenti attacchi alle reti di interi paesi Europei e di importanti società internazionali hanno determinato effetti anche di natura sistemica oltre che di danno economico e sottolineano ulteriormente come il dominio cibernetico costituisca terreno di confronto con riflessi sulla sicurezza nazionale, sulle competenze in materia, sulla necessità di assicurare un più efficace coordinamento tra le forze in campo, di attuare misure tese a rendere il Paese più sicuro e resiliente anche nel dominio digitale, di disporre dei più idonei strumenti di immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza che coinvolgano profili di Cybersicurezza.

Il decreto nasce anche dall'urgenza di dare attuazione al Piano nazionale di ripresa e resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, che prevede apposite progettualità nell'ambito della Cybersicurezza, in particolare per l'istituzione di un'Agenzia di Cybersicurezza nazionale, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, ponendo la Cybersicurezza a fon-

damento della trasformazione digitale. L'urgenza di dover intervenire al fine di ridefinire l'architettura italiana di Cybersicurezza, ha portato ad istituire un'apposita Agenzia per la Cybersicurezza nazionale, per adeguarla all'evoluzione tecnologica, al contesto di minaccia proveniente dallo spazio cibernetico, nonché al quadro normativo Europeo, e di dover raccordare, altresì, pure a tutela dell'unità giuridica dell'ordinamento, le disposizioni in materia di sicurezza delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche.

Il decreto ha anche il pregio di definire e chiarire alcuni concetti chiave del settore, quali ad esempio:

– Cybersicurezza, come l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza;

– il c.d. decreto legge c.d. "perimetro": ovvero il d.l. n. 105/2019, convertito, con modificazioni, dalla legge n. 133/2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

– "il d.lgs. NIS" ovvero il d.lgs. n. 65/2018, di attuazione della Direttiva UE del 2016, n. 1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

– il CISR, il Comitato interministeriale per la sicurezza della Repubblica di cui all'art. 5 della legge n. 124/2007;

– DIS, il Dipartimento delle informazioni per la sicurezza di cui all'art. 4 della legge n. 124/2007;

– AISE, l'Agenzia informazioni e sicurezza esterna di cui all'art. 6 della legge n. 124/2007;

– AISI, l'Agenzia informazioni e sicurezza interna di cui all'art. 7 della legge n. 124/2007;

– COPASIR, il Comitato parlamentare per la sicurezza della Repubblica di cui all'art. 30 della legge n. 124/2007;

– Strategia Nazionale di Cybersicurezza, la strategia di cui all'art. 6 del d.lgs. NIS.

Il decreto attribuisce all'art. 2 le competenze del Presidente del Consiglio dei ministri attribuendogli in via esclusiva:

– l'alta direzione e la responsabilità generale delle politiche di Cyber– sicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;

– l'adozione della strategia nazionale di Cybersicurezza, sentito il Comitato interministeriale per la Cybersicurezza (CIC) di cui all'art. 4;

– la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la Cybersicurezza nazionale di cui all'art. 5.

È il Presidente del Consiglio dei ministri che, sentito il CIC, impartisce le direttive per la Cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la Cybersicurezza nazionale.

Egli è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate ai sensi del presente decreto e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse. Inoltre, presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la Cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di Cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

Questo Comitato ha diversi compiti di impulso e direttiva:

– propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di Cybersicurezza nazionale;

– esercita l'alta sorveglianza sull'attuazione della strategia nazionale di Cybersicurezza;

– promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla Cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della Cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di Cybersicurezza;

– esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la Cybersicurezza nazionale.

Il Direttore generale dell'Agenzia svolge le funzioni di segretario del Comitato.

Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, il direttore generale del DIS, il direttore dell'AISE, il direttore dell'AISI, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare. Questo Comitato svolge altresì le funzioni già attribuite al CISR dal decreto legge del perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'art. 5 del medesimo decreto legge del perimetro.

Il Direttore generale dell'Agenzia ha la rappresentanza legale ed è chiaramente la figura centrale per la strategia di Cybersecurity italiana. Egli è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia.

L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali.

Un regolamento interno disciplina l'organizzazione e il funzionamento dell'Agenzia, in particolare, l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse disponibili.

Sono organi dell'Agenzia il direttore generale e il Collegio dei revisori dei conti. Con il regolamento sono disciplinati:

– le funzioni del direttore generale e del vice direttore generale dell'Agenzia;
– la composizione e il funzionamento del Collegio dei revisori dei conti;
– l'istituzione di eventuali sedi secondarie.

Il regolamento è stato adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del decreto, con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'art. 17 della legge n. 400/1988, previo parere del COPASIR, sentito il CIC.

Il decreto indica specificatamente le funzioni dell'Agenzia per la Cybersicurezza nazionale. L'Agenzia assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge n. 121/1981, il coordinamento tra i soggetti pubblici coinvolti in materia di Cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'art. 4, comma 3, lett. l), della legge n. 124/2007 (servizi di sicurezza e di

intelligence), sia le competenze dell'Ufficio centrale per la segretezza di cui all'art. 9 della medesima legge n. 124/2007.

L'Agenzia predispone la strategia nazionale di Cybersicurezza svolgendo ogni necessaria attività di supporto al funzionamento del Nucleo per la Cybersicurezza, di cui all'art. 8. È una Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al d.lgs. NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal decreto.

L'Agenzia e l'Autorità nazionale di certificazione della Cybersicurezza ai sensi dell'art. 58 del Regolamento UE del 2019, n. 881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni relative.

Essa infatti accredita, ai sensi dell'art. 60, comma 1, del Regolamento UE del 2019, n. 881 del Parlamento Europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza. Delega, ai sensi dell'art. 56, comma 6, lett. b), del Regolamento del 1029, n. 881 del Parlamento Europeo e del Consiglio, il Ministero della difesa e il Ministero dell'Interno, attraverso le rispettive strutture accreditate di cui al punto 1), al rilascio del certificato Europeo di sicurezza cibernetica. Assume tutte le funzioni in materia di Cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

– al perimetro di sicurezza nazionale cibernetica, di cui al decreto legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto legge perimetro, le attività di ispezione e verifica di cui all'art. 1, comma 6, lett. c), del decreto legge del perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

– alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli artt. 16-*bis* e 16-*ter* del d.lgs. n. 259/2003, e relative disposizioni attuative;

– alla sicurezza delle reti e dei sistemi informativi, di cui al d.lgs. NIS;

– partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'art. 1, comma 8, del d.l. n. 21/2012, convertito, con modificazioni, dalla legge n. 56/2012;

– assume tutte le funzioni attribuite alla Presidenza del Consiglio dei mini-

stri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'art. 1, comma 6, lett. c), del decreto legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

– assume tutte le funzioni già attribuite al DIS dal decreto legge del Perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'art. 1, comma 19-*bis*, del decreto legge del perimetro;

– provvede, sulla base delle attività di competenza del Nucleo per la Cybersicurezza di cui all'art. 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'art. 5 del decreto legge del perimetro;

– assume tutte le funzioni in materia di Cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'art. 51 del d.lgs. n. 82/2005, nonché in materia di adozione di Linee Guida contenenti regole tecniche di Cybersicurezza ai sensi dell'art. 71 del medesimo d.lgs. L'Agenzia assume, altresì, i compiti di cui all'art. 33-*septies*, comma 4, del d.l. n. 179/2012, convertito, con modificazioni, dalla legge n. 221/2012, già attribuiti all'Agenzia per l'Italia digitale;

– sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'art. 8 d.lgs. NIS;

– partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

– cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della Cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la Cybersicurezza;

– coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della Cybersicurezza. Nell'ambito dell'Unione Europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni, ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di Cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di Cybersicurezza definite dal Presidente del Consiglio dei ministri;

– perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionale, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di Cybersicurezza;

– stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di Cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di Cybersicurezza, ferme restando le competenze del Ministero degli esteri e della cooperazione internazionale;

– promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della Cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di Cybersicurezza;

– svolge attività di comunicazione e promozione della consapevolezza in materia di Cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

– promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della Cybersicurezza, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati;

– per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri.

L'Agenzia è designata quale Centro nazionale di coordinamento ai sensi dell'art. 6 del Regolamento UE del 2021, n. 887 del Parlamento Europeo e del Consiglio del 2021, che istituisce il Centro Europeo di competenza per la Cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Con-

siglio di direzione del Centro Europeo di competenza per la Cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'art. 12 del Regolamento UE del 2021, n. 887.

La legge di istituzione dell'Agenzia ha modificato anche la collocazione del CSIRT italiano di cui all'art. 8 del d.lgs. NIS prevedendo il suo trasferimento presso l'Agenzia dove ha assunto la denominazione di CSIRT Italia.

Anche il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia. Sotto il profilo della tutela dei dati personali, nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

Presso l'Agenzia è costituito, in via permanente, il Nucleo per la Cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della Cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Il Nucleo per la Cybersicurezza è presieduto dal direttore generale dell'Agenzia o dal vice direttore generale da lui designato ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'AISE, dell'AISI, di ciascuno dei Ministeri rappresentati nel Comitato di cui all'art. 5 della legge n. 124/2007, del Ministero dell'Università e della Ricerca, del Ministro delegato per l'innovazione tecnologica e la transizione digitale e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri.

Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'art. 9 della legge n. 124/2007. I componenti possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della Cybersicurezza.

Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti, anche relativamente ai compiti di gestione delle crisi di cui all'art. 10 del decreto.

Tra le finalità del Nucleo per la Cybersicurezza si annoverano i seguenti compiti:

– può formulare proposte di iniziative in materia di Cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia;

– promuove, sulla base delle direttive di cui all'art. 2, comma 2, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto dall'art. 7-*bis*, comma 5, del decreto legge del 2015, n. 174, convertito, con modificazioni, dalla legge n. 198/2015;

– promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

– valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della Cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

– riceve, per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi, dal DIS, dall'AISE e dall'AISI, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno di cui all'art. 7-*bis* del d.l. n. 144/2005, convertito, con modificazioni, dalla legge n. 155/2005, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (Computer Emergency Response Team – CERT) istituiti ai sensi della normativa vigente;

– riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

– valuta se gli eventi di cui alle lett. e) e f) assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla situazione in atto e allo svolgimento delle attività di raccordo e coordinamento di cui all'art. 10, nella composizione ivi prevista.

Nelle situazioni di crisi che coinvolgono aspetti di Cybersicurezza alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia. Il Nucleo assicura il supporto al CISR e al Presidente del Consiglio dei ministri, nella materia della Cybersicurezza, per gli aspetti relativi alla gestione

di situazioni di crisi ai sensi del comma 1, nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure necessarie.

L'Agenzia Nazionale della Cybersecurity rappresenta in sostanza un primo passo importante per la realizzazione (insieme a tutti gli altri soggetti deputati alla sicurezza nazionale non solo cibernetica) di azioni comuni e trasversali volte a garantire la sicurezza e la resilienza delle infrastrutture critiche necessarie allo sviluppo digitale del Paese e delle città del futuro.

LE NUOVE TECNOLOGIE NEI MUSEI PER LO SVILUPPO DELLE CITTÀ

di *Paola Beccherle*

1. *Il ruolo del museo nella* smart city

La rivoluzione digitale sta portando cambiamenti radicali nell'economia e nella società. I nuovi sviluppi dei sistemi di *Artificial Intelligence*, assieme al cambio di prospettiva dall'attuale "*Web 2.0*"[1] al "*Web3*"[2], hanno favorito l'emergere di inedite economie e modi di vivere. In questo contesto, realtà fisica e digitale convergono sempre più. Conseguentemente, il concetto di territorio diventa multidimensionale[3]: le città acquisiscono una dimensione digitale, sia

[1] Caratterizzato da un uso interattivo dell'ambiente *online* attraverso social media, blog e piattaforme.

[2] Per cui l'ambiente *online* è concepito come un ecosistema decentralizzato. Sul concetto di Web3, V. SHERMIN. *Token Economy: How the Web3 reinvents the Internet*, vol. 2, Berlino, 2020.

[3] L. LAZZERETTI, *What is the role of culture facing the digital revolution challenge? Some reflections for a research agenda*, in *European Planning Studies*, 2020, pp. 1-21.

utilizzando le nuove tecnologie per rendere più efficienti le reti e i servizi tradizionali sia riflettendo la loro immagine nei contenuti condivisi *online*.

Le città che sviluppano strategicamente la loro dimensione digitale sono spesso riconosciute come "*smart cities*". Agli albori del concetto di città intelligente vi era un approccio fortemente tecno-centrico. Negli ultimi anni, il termine "*smart city*" ha assunto un orientamento maggiormente umano-centrico, ponendo l'attenzione sulla partecipazione, la qualità della vita e l'impegno civico delle persone che vivono ed operano nella città [4].

In questo contesto, le organizzazioni culturali, e in particolare le istituzioni museali, possono svolgere un ruolo cruciale nella *smart city*. Da una parte i musei possono contribuire alla trasformazione digitale della città attraverso l'adozione di nuove tecnologie per interagire con i visitatori e per attivare inediti modelli di business. Dall'altra, essi possono contribuire sostenendo le politiche locali, costituendosi come centri di riflessione e di elaborazione culturale nella città [5]. I musei mettono al centro della loro azione la partecipazione della comunità e l'impegno civico, fungendo da *hub* creativi per l'educazione e l'immaginazione [6]. Ciò è possibile attraverso strategie di sviluppo e coinvolgimento dell'*audience* che permettono di attirare, tramite i canali di comunicazione, anche i cosiddetti "non pubblici". Inoltre, attraverso la comunicazione *online*, i musei contribuiscono alla reputazione e al *brand* della città, attirando visitatori, talenti e investimenti e promuovendo la cultura e i valori della città [7].

I musei possono quindi svolgere un ruolo fondamentale per le *smart ci-*

---

[4] M. FOTH, A. HUDSON-SMITH, D. GIFFORD, *Smart cities, social capital, and citizens at play: a critique and a way forward*, in M. ZHEGU, F. OLLEROS (eds.), *Research handbook on digital transformations (Research Handbooks in Business and Management)*, Cheltenham, 2016, pp. 203-221.

[5] Sul tema, con esempi di esperienze innovative partecipative tra musei e comunità locali quali interpreti del patrimonio culturale si veda I. SALERNO, *Narrare il patrimonio culturale. Approcci partecipativi per la valorizzazione di musei e territori*, in *Rivista di scienze del turismo*, vol. 4, n. 1-2, 2013, doi: *10.7358/rst-2013-01-02-sale*.

[6] Sul tema dello sviluppo locale "dal basso", basato sulla valorizzazione del patrimonio territoriale come bene comune, si veda G. DEMATTEIS, A. MAGNAGHI, *Patrimonio territoriale e coralità produttiva: nuove frontiere per i sistemi economici locali*, in *Scienze del territorio*, 6, 2018, pp. 12-25, *https://doi.org/10.13128/Scienze_Territorio-24362*.

Sul museo come spazio informale dove sviluppare forme partecipate di educazione, S. OLIVA, L. LAZZERETTI, *Natural history museums and sustainable development: The role of education for humanistic tourism*, in M. DELLA LUCIA, E. GIUDICI, *Humanistic Tourism: Values, Norms and Dignity*, Londra, 2020, pp. 1-27.

[7] Sulle istituzioni museali come attrattori per le industrie creative e motori dello sviluppo economico nelle città si veda G. LORD, N. BLANKENBERG, *Museums, Cities and Soft Power*, Washington, 2015.

ties nella ricostruzione del passato della città e nella co-creazione di immaginari urbani futuri seguendo le visioni, le esperienze e i desideri dei cittadini [8].

Nonostante l'importanza delle nuove prospettive di sviluppo di internet e delle nuove tecnologie digitali, il dibattito sulle potenziali sinergie tra musei e città per sfruttare efficacemente le nuove opportunità offerte dal digitale per l'economia locale e la coesione sociale è ancora limitato.

In letteratura alcuni studi evidenziano da una parte il contributo della cultura per lo sviluppo regionale e urbano, e dall'altra il contributo della cultura per la trasformazione digitale.

Tali contributi fanno spesso riferimento alle politiche europee in ambito culturale, regionale e digitale, in quanto costituenti il quadro di riferimento per l'azione a livello locale, sia dal punto di vista della *governance* museale sia urbana. Tuttavia, in letteratura non vi sono contributi che analizzano simultaneamente le sinergie e i collegamenti tra le politiche culturali, di sviluppo regionale e urbano e digitali al fine di tracciare gli spazi di intersezione in cui musei e città possono agire coralmente per lo sviluppo urbano sociale, culturale ed economico attraverso l'impiego delle nuove tecnologie.

Allo stesso modo, nella letteratura nell'ambito dell'economia e del *management* della cultura i contributi sul ruolo dei musei nella *smart city* sono limitati.

La ricerca condotta e presentata al Convegno *Intelligenza artificiale e smart cities. Sfide e opportunità* intende analizzare l'interrelazione delle politiche europee per la cultura, per lo sviluppo regionale e urbano e per le nuove tecnologie al fine di delineare in che misura il dibattito a livello europeo considera la trasformazione digitale dei musei e delle città, aprendo alle nuove reciproche opportunità e sinergie che ne derivano.

Il presente articolo è strutturato come segue. Nel secondo paragrafo verrà illustrata la metodologia di ricerca utilizzata nel condurre lo studio. Nel terzo paragrafo verranno presentati i risultati dell'analisi delle politiche europee che mettono in luce il potenziale ruolo strategico inespresso dei musei nella *smart city*. Verranno illustrate le politiche che integrano le tre dimensioni considerate secondo tre temi principali emersi: la conservazione digitale del patrimonio culturale della città; la valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digitali; e il ruolo delle organizzazioni culturali per la partecipazione culturale nello spazio digitale.

---

[8] Sul tema, C. GRAJALES, M. FOTH, P. MITCHELL, G. CALDWELL. *The museum in the Smart City: the role of cultural institutions in co-creating urban imaginaries*, in K.S. WILLS, A. AURIGI (eds.), *The Routledge Companion to Smart Cities*, Londra, 2020, pp. 332-347.

Nel quarto paragrafo si presenterà il caso di studio selezionato per contribuire empiricamente all'indagine: le Gallerie degli Uffizi a Firenze. Nel quinto paragrafo verranno presentati i risultati preliminari dell'indagine. Infine, nel sesto paragrafo saranno delineate delle riflessioni conclusive.

2. *Metodologia di ricerca*

Lo studio è stato condotto in due fasi: dapprima sono state analizzate le politiche europee per indagare il contesto in cui musei e città si muovono nella loro reciproca trasformazione digitale; successivamente, è stato analizzato un caso di studio per contribuire empiricamente alla ricerca sul ruolo delle nuove tecnologie nei musei per lo sviluppo della città.

Per quanto riguarda la prima fase, lo studio è stato condotto esaminando gli atti giuridici dell'Unione Europea, come regolamenti, direttive, decisioni, raccomandazioni, pareri ma anche comunicazioni, programmi ed iniziative della Commissione Europea, del Consiglio Europeo e del Parlamento Europeo pubblicati sui siti web istituzionali [9]. Sono state considerate le politiche europee per la cultura, lo sviluppo locale e per il digitale, in quanto costituenti i tre principali ambiti riguardanti la trasformazione digitale di musei e città. Lo studio è stato condotto procedendo ad una revisione dei documenti con l'obiettivo di individuare i punti in cui i *policy-maker* europei hanno considerato la trasformazione digitale nell'ambito della cultura e delle città simultaneamente. Sono state analizzate le politiche sia attualmente in vigore sia le politiche afferenti a programmi non più attivi ma il cui effetto è ancora riscontrabile nell'azione quotidiana di musei e città.

Nell'analisi sono state considerate le politiche culturali europee dedicate in particolare al patrimonio culturale e riguardanti le organizzazioni *non-profit*, non comprendendo il più ampio argomento della creatività contemporanea e delle imprese culturali ad essa legate. Tale scelta è motivata dal fatto che, assieme alle città, il soggetto della presente ricerca sono i musei, organizzazioni *non-profit* che custodiscono e valorizzano il patrimonio storico-artistico delle città.

I risultati dell'analisi sono stati categorizzati secondo tre temi principali emersi: la conservazione digitale del patrimonio culturale della città; la valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digita-

[9] Principalmente, ma non esclusivamente, pubblicati sul sito *https://eur-lex.europa.eu/homepage.html.*

li; e il ruolo delle organizzazioni culturali per la partecipazione culturale nello spazio digitale.

Nella seconda fase della ricerca è stata condotta l'analisi di un caso di studio: le Gallerie degli Uffizi a Firenze. Il caso è stato selezionato per contribuire empiricamente all'indagine per tre motivi, attinenti sia le caratteristiche della città di Firenze sia le caratteristiche delle Gallerie: per prima cosa, perché Firenze è una città considerata "*smart*", che ha quindi intrapreso strategicamente un percorso di trasformazione digitale; poi, perché gli Uffizi sono uno dei complessi museali più rappresentativi della città di Firenze; infine, perché gli Uffizi si sono distinti per un uso quotidiano e pervasivo dei canali di comunicazione *online* e delle nuove tecnologie.

L'analisi del caso è stata condotta durante un periodo di ricerca presso le Gallerie degli Uffizi da dicembre 2021 ad aprile 2022. Per lo studio sono state impiegate fonti di dati primarie e secondarie. Riguardo alle prime, sono state condotte 15 interviste semi-strutturate con il personale delle Gallerie degli Uffizi, facente parte sia il Dipartimento Strategie Digitali sia altri Dipartimenti che utilizzano strumenti digitali; dall'altra, sono state analizzate fonti di dati secondarie sia fornite dalle Gallerie durante il periodo di ricerca sia pubblicate sui canali di comunicazione istituzionali della Gallerie [10] e del Ministero della Cultura.

Dall'analisi del caso di studio è emerso che le attività digitali delle Gallerie degli Uffizi riflettono i temi risultanti dallo studio delle politiche culturali europee, e per questo sono stati categorizzati secondo i tre temi individuati nella prima fase dello studio: le Gallerie degli Uffizi per la conservazione digitale del patrimonio culturale della città, per la valorizzazione dell'esperienza turistica in città e nei territori limitrofi e per la partecipazione alla cultura nello spazio digitale.

3. *Le sinergie tra politiche per la cultura, lo sviluppo locale e per il digitale a livello europeo*

Le sinergie e le complementarità tra le politiche culturali, di sviluppo regionale e urbano e digitali dell'Unione Europea sono state analizzate al fine di

[10] Sono stati raccolti report di attività annuali, schede di valutazione della performance, bilanci e dati sull'attività digitale principalmente tramite i siti web istituzionali delle Gallerie degli Uffizi *www.uffizi.it* e *www.trasparenza.uffizi.it* e i canali social Twitter, Facebook, Instagram, YouTube e TikTok.

tracciare gli spazi di intersezione in cui musei e città possono agire coralmente per lo sviluppo urbano sociale, culturale ed economico attraverso l'impiego delle nuove tecnologie.

Dall'analisi si evince che solo a partire dal 2014 è iniziata una riflessione integrata su questi temi. I punti di contatto tra tali politiche possono essere raggruppati in tre argomenti: la conservazione digitale del patrimonio culturale delle città; la valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digitali; e il ruolo delle organizzazioni culturali per la partecipazione culturale nello spazio digitale. Di seguito verranno presentati nel dettaglio.

3.1. *Conservazione digitale del patrimonio culturale delle città*

Il primo tema emerso riguarda la conservazione digitale del patrimonio culturale delle città.

Per quanto riguarda le politiche culturali, la *Nuova agenda per la cultura* (2018) [11], che costituisce un quadro di riferimento per la cooperazione culturale a livello europeo, sottolinea l'importanza della digitalizzazione dei monumenti storici a rischio nelle aree urbane.

Il *Quadro d'azione europeo sul patrimonio culturale* (2019) [12], che riguarda l'organizzazione comune tra gli Stati membri per le attività legate specificamente al patrimonio culturale a livello europeo, prende in considerazione l'uso di nuove tecnologie, come la modellazione 3D, per la conservazione e il restauro delle risorse culturali tangibili. Inoltre, il Quadro annuncia che dal 2019 il progetto *Copernicus*, dedicato all'osservazione della Terra tramite sistema satellitare, fornisce informazioni *open data* sul patrimonio culturale tangibile, come i monumenti storici e l'architettura. Ciò risulta utile alle città per monitorare lo stato di conservazione del loro patrimonio culturale.

Sullo stesso tema, le politiche di sviluppo regionale e urbano sostengono la conservazione digitale in particolare nel Fondo Europeo di Sviluppo Regionale (FESR), che mira a promuovere uno sviluppo equilibrato nelle diverse re-

[11] COMMISSIONE EUROPEA, *Final Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions A New European Agenda for Culture*, COM(2018) 267 {SWD(2018) 167 final}, 2018, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:267:FIN*.

[12] COMMISSIONE EUROPEA, *European Framework for Action on Cultural Heritage,* Commission Staff Working Document, 2019, *https://op.europa.eu/en/publication-detail/-/publication/5a9c3144-80f1-11e9-9f05-01aa75ed71a1*.

gioni europee, fornendo occasioni per colmare gli squilibri e rafforzare la coesione economica e sociale. Nel precedente periodo di programmazione, dal 2014 al 2020, il programma FESR ha sottolineato come l'uso di soluzioni digitali innovative possa promuovere la cultura, la conservazione e il restauro del patrimonio artistico al fine di rendere i luoghi attraenti [13].

Diversi progetti avviati nell'ambito dell'iniziativa *Cultural Heritage in Action* [14] implicano l'uso di piattaforme *online* e azioni di digitalizzazione per preservare e valorizzare il patrimonio culturale urbano materiale, immateriale e digitale. L'iniziativa è stata lanciata nel 2020 e, sebbene faccia formalmente parte delle politiche culturali, riguarda l'ambito dello sviluppo regionale e urbano, essendo un programma di apprendimento tra pari per i responsabili delle politiche regionali e locali.

Infine, tra le politiche per l'innovazione possiamo trovare riferimento alla conservazione digitale del patrimonio culturale urbano nel programma *Horizon Europe 2021-2027* [15], il quale finanzia azioni per lo sviluppo di strumenti digitali e nuove tecnologie a supporto del restauro e della protezione del patrimonio culturale.

3.2. *Valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digitali*

Il secondo tema emerso dall'analisi delle sinergie tra patrimonio culturale, sviluppo urbano e regionale e nuove tecnologie nelle politiche europee consiste nel riutilizzo dei contenuti culturali digitalizzati delle organizzazioni culturali locali per migliorare l'esperienza turistica nelle città.

Per quanto riguarda le politiche culturali, questo tema è citato nel *Piano di lavoro per la cultura (2015-2018)* [16]. In particolare, il piano incoraggia l'esplo-

---

[13] INTERACT, COMMISSIONE EUROPEA, *Connecting Cultures, Connected Citizens Inspiring examples of Interreg Cultural Heritage projects in the framework of the 2018 European Year of Cultural Heritage*, Bratislava, 2018.

[14] COMMISSIONE EUROPEA, *Urban agenda for the EU Multi-level governance in action*, Directorate-General for Regional and Urban Policy, 2019 *https://ec.europa.eu/regional_policy/sources/docgener/brochure/urban_agenda_eu_en.pdf*.

[15] COMMISSIONE EUROPEA, *Horizon Europe: strategic plan 2021-2024*, Directorate-General for Research and Innovation, Publications Office, 2021, *https://data.europa.eu/doi/10.2777/083753*.

[16] CONSIGLIO EUROPEO, *Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on a Work Plan for Culture (2015-2018)*, (2014/C 463/02), in *Official Journal of the European Union*, 2014, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XG1223(02)&from=EN*.

razione di modalità in cui la digitalizzazione dei servizi e dei contenuti culturali possono sostenere e potenziare lo sviluppo di itinerari e reti turistiche transeuropei. Allo stesso modo, il *Quadro d'azione europeo sul patrimonio culturale* (2019)[17] supporta l'accessibilità *online* e la digitalizzazione del patrimonio culturale, promuovendo il riutilizzo dei materiali digitalizzati in altri settori. Nello stesso documento è citato il programma COSME (*Europe's programme for small and medium-sized enterprises*)[18], attraverso il quale l'Unione Europea mira a premiare, tra le altre cose, le sinergie tra il turismo e le industrie culturali finanziando prodotti in grado di promuovere il turismo e il miglioramento dell'esperienza dei visitatori del patrimonio culturale attraverso l'uso delle tecnologie.

Tra le politiche regionali, l'Unione Europea sostiene il riutilizzo dei contenuti culturali digitalizzati per costruire itinerari turistici attraverso il *Recovery and Resilience facility* (2021-2026)[19]. In particolare, il piano sottolinea l'importanza di sviluppare nuovi *business model* e servizi per supportare la resilienza e la transizione digitale del settore culturale. Come mostrano due recenti report prodotti dalla Commissione Europea[20] e da *Culture Action Europe*[21], alcuni Stati più di altri hanno investito nella preparazione di contenuti culturali digitali per il settore del turismo, con il fine di coinvolgere il grande pubblico e riutilizzare i contenuti digitalizzati nell'economia oltre che nella ricerca e l'educazione: è il caso della Slovenia, dell'Italia e della Grecia.

Infine, il programma *Digital Europe* (2021-2027)[22] stimola il riutilizzo dei contenuti digitalizzati nel settore culturale per lo sviluppo del turismo sosteni-

---

[17] COMMISSIONE EUROPEA, *European Framework for Action on Cultural Heritage,* Commission Staff Working Document, 2019, *https://op.europa.eu/en/publication-detail/-/publication/5a9c3144-80f1-11e9-9f05-01aa75ed71a1.*

[18] Per maggiori informazioni sul programma COSME, si visiti la pagina web dedicata *https://ec.europa.eu/growth/smes/cosme_en.*

[19] PARLAMENTO EUROPEO, CONSIGLIO EUROPEO, *Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility*, in *Official Journal of the European Union*, 18.2.2021, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0241&from=EN.*

[20] COMMISSIONE EUROPEA, *Recovery and Resilience Scoreboard. Thematic analysis: Culture and Creative Industries*, aprile 2022, *https://ec.europa.eu/economy_finance/recovery-and-resilience-scoreboard/assets/thematic_analysis/scoreboard_thematic_analysis_culture.pdf.*

[21] CULTURE ACTION EUROPE, *Culture in the EU's national recovery and resilience plans*, novembre 2021, *https://cultureactioneurope.org/files/2021/11/NRRPs_analysed_digital.pdf.*

[22] PARLAMENTO EUROPEO, CONSIGLIO EUROPEO, *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240*, 2021, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0694&from=EN.*

bile, dell'istruzione e della *smart city*, fornendo *open data* su collezioni e siti monumentali. Tale obiettivo fa riferimento nello specifico alla call *DIGITAL-2022-CULTURAL-02*, che mira a stimolare la creazione di uno spazio comune europeo di dati per il patrimonio culturale per cogliere le opportunità offerte dalle tecnologie per migliorare la qualità, la sostenibilità, l'uso e il riutilizzo dei dati del settore culturale.

La rilevanza della valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digitali è stata ribadita anche nella recente *Raccomandazione della commissione per uno spazio comune europeo di dati per il patrimonio culturale*[23], la quale pone l'enfasi sulle opportunità offerte dalla digitalizzazione sia per il turismo e sia per la *smart city*.

3.3. *Il ruolo delle organizzazioni culturali per la partecipazione culturale nello spazio digitale*

Il terzo tema emerso riguarda il ruolo delle organizzazioni culturali per la partecipazione culturale nello spazio digitale. Le politiche europee sottolineano l'importanza di coinvolgere i pubblici fornendo accesso alla cultura, stimolando la cittadinanza attiva e la *governance* partecipativa del patrimonio culturale, anche nella dimensione digitale.

Tra le politiche culturali, gli ultimi due Piani di lavoro per la cultura, che costituiscono i piani d'azione della Nuova Agenda per la cultura, in particolare considerano il tema della *governance* partecipativa. Il *Piano di lavoro per la cultura* (2015-2018)[24] considera la *governance* partecipativa del patrimonio culturale digitale, auspicando la collaborazione tra il settore pubblico, gli *stakeholder* privati e la società civile, e la cooperazione tra le diverse aree politiche. Il *Piano di lavoro per la cultura* (2019-2022)[25] valorizza l'importanza di

---

[23] COMMISSIONE EUROPEA, *Raccomandazione (UE) 2021/1970 Della Commissione del 10 novembre 2021 relativa a uno spazio comune europeo di dati per il patrimonio culturale*, novembre 2021, *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021H1970&from=EN.*

[24] CONSIGLIO EUROPEO, *Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on a Work Plan for Culture (2015-2018)*, (2014/C 463/02), in *Official Journal of the European Union*, 23.12.2014, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XG1223(02)&from=EN.*

[25] COMMISSIONE EUROPEA, *Final Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions A New European Agenda for Culture*, COM(2018) 267 {SWD(2018) 167 final}, 2018 *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:267:FIN.*

coinvolgere i giovani come pubblico attivo delle organizzazioni culturali, che reinterpretano ed innovano il patrimonio culturale, stimolando la cittadinanza attiva, la loro futura occupabilità e l'inclusione sociale.

Per quanto riguarda le politiche di sviluppo regionale e urbano, diverse proposte ricevute nell'ambito delle *Azioni Innovative Urbane* (UIA)[26], che derivano dal già citato programma del Fondo Europeo di Sviluppo Regionale 2014-2020, hanno incluso le nuove tecnologie per migliorare l'accesso e la partecipazione alla cultura dei cittadini per il benessere sociale e fisico.

Infine, anche le politiche per il digitale pongono l'attenzione su questo tema. In particolare, il programma *Horizon Europe* (2021-2027) è contraddistinto per la prima volta da un cluster dedicato a *Cultura, creatività e società inclusiva* nell'ambito del Pilastro 2 *Sfide globali e competizione industriale europea*. Il programma riconosce l'importanza della democrazia diretta e partecipativa e della cittadinanza attiva anche nella dimensione digitale. Per fare questo, il programma sottolinea la necessità di proporre l'accesso ai contenuti culturali, aprendosi a nuovi modelli di gestione partecipativa del patrimonio culturale.

Oltre ai tre temi presentati, si ritiene di interesse riportare un quarto tema rilevato nell'ambito del programma *Horizon Europe* (2021-2027): l'utilizzo delle nuove tecnologie per la promozione e la riscoperta dell'artigianato tradizionale locale.

4. *Il caso delle Gallerie degli Uffizi a Firenze, città creativa e "*smart*"*

La città di Firenze è da sempre riconosciuta in Italia e nel mondo come città d'arte per eccellenza. Tuttavia, negli ultimi anni, Firenze ha conosciuto una transizione: al concetto di città d'arte si è affiancato il concetto di città creativa, come rilevato da Lazzeretti e Oliva (2018)[27]. Le autrici definiscono città creativa una città che concepisce la cultura come una risorsa creativa per l'innovazione. A Firenze il patrimonio culturale, insieme al sapere tradizionale e alle risorse umane creative, favoriscono l'innovazione e l'emergere di modelli di sviluppo della città *culture-driven*. Ciò rende la città dinamica e moderna[28].

[26] Per maggiori dettagli sull'iniziativa UIA, si veda: *https://www.uia-initiative.eu/en/culture-and-cultural-heritage.*

[27] In particolare, le autrici si soffermano sui rischi e le opportunità relative alla trasformazione economica locale secondo un approccio orientato alla cultura e alla creatività. L. LAZZERETTI, S. OLIVA, *Rethinking city transformation: Florence from art city to creative fashion city*, in *European Planning Studies*, 2(9), 2018, pp. 1-18.

[28] Gli autori approfondiscono in particolare il ruolo dell'industria della moda per un'im-

Allo stesso tempo, Firenze ha intrapreso un percorso che l'ha portata ad essere riconosciuta nel 2020, 2021 e 2022 città *Più smart d'Italia* dall'ICity Rank [29]. Per lo stesso report, Firenze si configura come Città Digitale, ovvero una città che «*Utilizza – in modo più diffuso, organico e continuativo – le nuove tecnologie nelle attività amministrative, nell'erogazione dei servizi, nella raccolta ed elaborazione dei dati, nell'informazione, nella comunicazione, nella partecipazione e per portare avanti processi di innovazione istituzionale, culturale ed organizzativa al fine di migliorare la qualità della vita e dei servizi funzionali, i livelli di occupazione e la competitività, come risposta ai bisogni delle generazioni attuali e future, garantendo la sostenibilità economica, sociale e ambientale dello sviluppo urbano*». Tale riconoscimento è frutto della realizzazione di un programma di trasformazione digitale di medio-lungo termine, cominciato nel 2015 con l'adozione dello *Smart City Plan* [30], un documento contenente le linee guida per lo sviluppo fino al 2030. Ciò che è interessante notare è che il *Firenze Smart City Plan* riconosce l'importanza dell'impiego delle ICT «*Considerando e anzi valorizzando il patrimonio artistico culturale che caratterizza Firenze*» e riconosce il ruolo fondamentale dei musei per l'innovazione nella città. In particolare, il Piano sottolinea come la tecnologia digitale consente di arricchire l'esperienza dei cittadini e dei turisti prima, durante e dopo la visita ai musei e di promuovere il patrimonio artistico della città. La città punta «*Ad accrescere la portata della trasmissione culturale ai cittadini in generale e alle nuove generazioni in particolare, e allo stesso tempo di facilitare l'accesso a musei, mostre, monumenti, offrendo un sostegno concreto alla valorizzazione dei beni culturali e del sapere umano*».

Le Gallerie degli Uffizi sono uno degli istituti museali più rappresentativi della città di Firenze, e tra i più antichi e importanti complessi museali del mondo. Nel 2020, 2021 e 2022, le Gallerie si sono posizionate al primo posto tra gli istituti museali statali italiani con più visitatori [31].

Dal 2016, gli Uffizi hanno adottato una strategia digitale con una forte

---

magine della città di Firenze competitiva. L. LAZZERETTI, F. CAPONE, P. CASADEI, *The role of fashion for tourism: An analysis of Florence as a manufacturing fashion city and beyond*, in N. BELLINI, C. PASQUINELLI, *Tourism in the City – Towards an Integrative Agenda on Urban Tourism*, Heidelberg, 2017, pp. 207-220.

[29] Si vedano i report pubblicati da Forum PA: FPA, *ICity Rank 2020*, 2020 *https://www.forumpa.it/icity-rank/; FPA. ICity Rank 2021, 2021 https://www.forumpa.it/icity-rank/.*

[30] Si veda il documento *Firenze Smart City Plan* del Comune di Firenze, 2015, consultabile al seguente link: *https://ambiente.comune.fi.it/sites/ambiente.comune.fi.it/files/2019-11/Smart_City_Plan_it.pdf.*

[31] I dati sui visitatori e la classifica dei musei statali più visitati sono pubblicati annualmente sul sito dell'Ufficio Statistica del Ministero della Cultura, accessibili dal seguente link: *http://www.statistica.beniculturali.it/Visitatori_e_introiti_musei.htm.*

spinta sulla comunicazione *online* attraverso il sito web e i *social media*. Per fare questo, l'istituto museale si è dotato di un Dipartimento di informatica e Strategie Digitali dedicato, composto dall'Area ICT e dall'Area Strategie Digitali. La strategia digitale ha portato gli Uffizi, nel 2021 e nel 2022, ad essere il museo italiano più seguito sui social media[32]. Sommando i seguaci su tutte le piattaforme in cui il complesso museale è presente, a dicembre 2022 gli Uffizi contavano più di 1 milione di *followers*[33]. Per i risultati conseguiti nella comunicazione digitale, gli Uffizi hanno ricevuto diversi premi, tra cui il *Brand Reporter Award* conferito dalla società di consulenza strategica Brand Reporter Consulting nel 2021[34] e il riconoscimento per la *Comunicazione responsabile* del Premio Aretè per le Digital Humanities nel 2022[35].

Attraendo e coinvolgendo pubblici nazionali e internazionali, le Gallerie degli Uffizi promuovono l'immagine di Firenze nel contesto *online* attraverso la dimensione digitale.

Dall'analisi delle iniziative digitali attivate degli Uffizi è stata riconosciuta una corrispondenza ai temi emersi dall'analisi delle politiche: gli Uffizi utilizzano le nuove tecnologie per la conservazione digitale dei beni culturali, per la valorizzazione dell'esperienza turistica in città attraverso contenuti culturali digitali, e per la partecipazione alla cultura nello spazio digitale. Si presenteranno di seguito nel dettaglio le iniziative messe in campo dall'Istituto museale.

4.1. *Le Gallerie degli Uffizi per la conservazione digitale del patrimonio culturale della città*

Le Gallerie degli Uffizi, oltre a pubblicare quotidianamente contenuti *online* come articoli, immagini, video e dirette *streaming* di conferenze, conservano digitalmente il patrimonio culturale che, in senso lato, costituisce parte del patrimonio della città di Firenze che ne testimonia la storia.

Il complesso museale rende le opere digitalizzate liberamente accessibili

---

[32] IL GIORNALE DELL'ARTE E THE ART NEWS NEWSPAPER, *La classifica mondiale delle mostre più visitate,* Il Giornale dell'Arte, Numero 427, aprile 2022, pp. 23-37.

[33] GALLERIE DEGLI UFFIZI. *I numeri degli Uffizi 2022*, Documento consultabile sul sito istituzionale: *https://www.uffizi.it/news/gallerie-degli-uffizi-i-numeri-del-2022*.

[34] GALLERIE DEGLI UFFIZI. *I numeri degli Uffizi 2021*, Documento consultabile sul sito istituzionale: *https://www.uffizi.it/news/numeri-2021#:~:text=Le%20Gallerie%20degli%20Uffizi%20tornano,Tutti%20i%20numeri%20del%202021&text=Dopo%20il%202020%2C%20l'anno,7%25%20rispetto%20a%20quello%20precedente.*

[35] GALLERIE DEGLI UFFIZI. *I numeri degli Uffizi 2022*, Documento consultabile sul sito istituzionale: *https://www.uffizi.it/news/gallerie-degli-uffizi-i-numeri-del-2022*.

sul sito web attraverso due sezioni dedicate: la sezione *Opere d'arte* contiene le schede di catalogo della collezione degli Uffizi in inglese e in italiano; la sezione *Archivi digitali* è composta da tre progetti: l'*Archivio fotografico*, il *Catalogo* e il *Progetto Euploos*. L'Archivio Fotografico offre oltre 600.000 immagini ad alta risoluzione provenienti dal Gabinetto Fotografico delle Gallerie, costituito da fotografie recenti ma anche da raccolte storiche, tra cui la documentazione dei danni bellici degli anni 1945-1946 e la documentazione di Firenze durante l'alluvione del 1966 e il salvataggio dello stesso archivio fotografico.

Il Catalogo contiene schede informative sulle collezioni della Galleria degli Uffizi, di Palazzo Pitti e del Giardino di Boboli.

Infine, il *Progetto Euploos – Gabinetto dei Disegni e delle Stampe* costituisce il catalogo del Gabinetto dei Disegni e delle Stampe delle Gallerie degli Uffizi e raccoglie oltre 180.000 voci di catalogo, realizzato con la collaborazione congiunta del Kunsthistorisches Institut in Florenz, del Max-Planck-Institut e della Scuola Normale Superiore.

4.2. *Le Gallerie degli Uffizi per la valorizzazione dell'esperienza turistica in città e nei territori limitrofi*

Le Gallerie degli Uffizi dal 2021 valorizzano la città di Firenze e il turismo sostenibile attraverso il progetto congiunto con la Fondazione CR di Firenze *Terre degli Uffizi*, facente parte del più ampio programma *Uffizi Diffusi*. Il progetto, della durata di cinque anni, mira ad offrire la visibilità degli Uffizi ai luoghi minori di Firenze con il fine di stimolare la scoperta di tali luoghi e di delocalizzare i turisti dal centro di Firenze ai territori limitrofi.

La valorizzazione digitale dei territori è perseguita attraverso la realizzazione di video che illustrano la cultura, il paesaggio, la storia artistica dei territori e la tradizione toscana e italiana, compresa quella enogastronomica. I video sono disponibili in una sezione dedicata del sito degli Uffizi e vengono promossi sui canali di comunicazione social istituzionali.

Nel 2021 sono state organizzate nove mostre, mentre nel 2022 otto.

Il progetto *Uffizi Diffusi* e il sotto-programma *Terre degli Uffizi* sono stati riconosciuti dalla stampa nazionale e internazionale per le iniziative tese a decentralizzare il turismo e a renderlo più sostenibile e in armonia con la comunità, ottenendo ampia visibilità. In particolare, nel 2021 il progetto *Uffizi Diffusi* è stato riconosciuto nel *Best in Travel 2022* di Lonely Planet[36], classifica

[36] LONELY PLANET, *Best in Travel 2022*, XVI ed., Torino, 2021.

nella quale Firenze è stata l'unica città italiana ad essere riconosciuta grazie al progetto delle Gallerie degli Uffizi. Nello stesso anno, il *Time Magazine* ha inserito la Toscana degli *Uffizi Diffusi* nei 100 luoghi più belli del mondo [37]. Il progetto *Terre degli Uffizi* è stato riconosciuto anche da *Apollo Magazine*, che lo ha incluso tra le sei migliori iniziative espositive dell'anno [38]. Infine, nel 2023 la rivista "The Economist" ha citato il progetto *Terre degli Uffizi* come un'innovazione che costituisce un modello da seguire per gli altri musei [39].

4.3. *Le Gallerie degli Uffizi per la partecipazione alla cultura nello spazio digitale*

Gli Uffizi forniscono ai cittadini di Firenze competenze e conoscenze attraverso attività di educazione al patrimonio culturale, anche nello spazio digitale.

Per quanto riguarda la collaborazione con le scuole, l'Area Scuola e Giovani degli Uffizi lavora a stretto contatto con le scuole primarie e secondarie di Firenze, anche attraverso strumenti didattici digitali. Per citare alcuni esempi, *Ambasciatori digitali dell'Arte* è un progetto di alternanza scuola-lavoro per le scuole superiori, che mira a stimolare la riflessione sulla collezione degli Uffizi su un tema specifico. Il risultato del progetto consiste nella creazione di video in cui gli studenti reinterpretano la collezione, i quali vengono poi pubblicati *online*.

Il progetto *Forza scuole... arrivano gli Uffizi!* consiste in video-lezioni a distanza per le scuole, con l'obiettivo di sostenere l'educazione al patrimonio culturale nelle scuole fiorentine e non solo. Nel 2021, sono state erogate 989 lezioni *online* per le scuole, e 42 incontri *online* per bambini e famiglie.

Gli Uffizi hanno poi avviato un progetto Erasmus, denominato *HEROES*, in collaborazione con il Museo di Atene sull'educazione museale, con l'Università di Pedagogia di Malaga, la Scuola Marco Polo di Firenze e il Centro Machiavelli di progettazione europea. L'obiettivo del progetto era quello di scambiare le conoscenze in merito a modelli innovativi di *peer education* applicati all'educazione culturale. Il progetto è stato portato avanti anche con

---

[37] J. BUCKLEY, *World's Greatest Places 2021: Tuscany, Italy, Uffizi on tour*, in *Time Magazine online*, 2021, *https://time.com/collection/worlds-greatest-places-2021/6079319/tuscany-italy/*.

[38] APOLLO MAGAZINE, *Exhibition of the Year: The Shortlists*, 2021, *https://www.apollo-magazine.com/exhibition-of-the-year-shortlist-apollo-awards-2021/*.

[39] THE ECONOMIST, *The Uffizi is taking its art to the people*, 2023 *https://www.economist.com/culture/2023/05/09/the-uffizi-is-taking-its-art-to-the-people*.

l'utilizzo di piattaforme di teleconferenza che hanno reso possibile il dialogo e l'apprendimento reciproco a distanza.

Per quanto riguarda il lavoro svolto dagli Uffizi con i cittadini adulti, le associazioni e altri enti di Firenze, vi sono diversi progetti orientati al *life-long learning*, all'inclusione, all'accessibilità e alla conservazione della memoria storica dei cittadini fiorentini.

L'Area Mediazione Culturale e Accessibilità, che si occupa di rendere accessibile la visita al museo, sia *online* che *offline*, collabora con associazioni ed enti fiorentini per offrire prodotti e servizi culturali digitali accessibili a cittadini e visitatori con disabilità. Nel 2021 sono state offerte ad adulti, con disabilità e non, 53 visite e lezioni *online* con 992 partecipanti.

Allo stesso tempo, l'Area coinvolge cittadini fiorentini provenienti da tutto il mondo nella reinterpretazione della collezione secondo i valori universali che la caratterizzano, realizzando video pubblicati *online* sui canali di comunicazione istituzionali. Tra le iniziative, vi è una mostra virtuale dedicata alle presenze africane nei dipinti delle Gallerie, e una mostra realizzata nel 2017 dal tema *Islam e Firenze*, che ha esplorato le connessioni tra la cultura islamica e quella fiorentina attraverso i dipinti delle gallerie degli Uffizi, e i cui risultati sono pubblicati sul sito web. Infine, si ritiene interessante citare la collaborazione delle Gallerie all'iniziativa *Diario popolare* di un'associazione locale, che mira a raccogliere i ricordi dei fiorentini su diversi luoghi della città per poi condividerli sul loro blog *online*.

Oltre ai temi già citati, è stato rilevato come gli Uffizi contribuiscano anche alla promozione dell'artigianato artistico fiorentino *online* attraverso l'*e-commerce* lanciato nell'aprile 2022. Tra le pubblicazioni e il *merchandise*, vi sono infatti anche oggetti artigianali realizzati a Firenze come scatole decorate a mano e cornici in legno.

5. *Risultati preliminari*

5.1. *Risultati dell'analisi delle politiche europee*

L'analisi delle politiche europee ha dimostrato che, il più delle volte, i *policy-maker* europei non considerano contemporaneamente la trasformazione digitale della cultura e delle città. Di conseguenza, i modelli di sviluppo, le opportunità e le sinergie reciproche tra queste dimensioni non sono ancora sufficientemente esplorati.

Si nota come le politiche e i programmi riportati, quando considerano il

patrimonio culturale urbano, spesso facciano riferimento alla conservazione tecnologica del solo patrimonio culturale architettonico o monumentale tangibile delle città escludendo, il più delle volte, il patrimonio tangibile conservato nei musei e il patrimonio intangibile, come la memoria della comunità. Se il tema della digitalizzazione del patrimonio culturale in tutte le sue forme è ampiamente preso in considerazione dalle politiche culturali dell'Unione Europea, esso tende a perdere vigore quando le politiche considerano la digitalizzazione del patrimonio delle aree urbane. Risulta quindi fondamentale esprimere con più forza la rilevanza per le città della digitalizzazione del patrimonio materiale, immateriale e digitale presente nell'area urbana al fine di alimentare un approccio olistico che porti musei e città a collaborare più strettamente.

È stato poi rilevato come, nelle politiche per la cultura e per lo sviluppo locale, è riconosciuto il contributo dei musei per la costruzione e il mantenimento del *brand* della città, per essere luoghi di interazione comunitaria e centri di conoscenza in grado di responsabilizzare i cittadini, attirando allo stesso tempo talenti e turismo e garantendo la coesione sociale. Tuttavia, in molte politiche non viene considerato come gli strumenti digitali e l'ambiente *online* possano moltiplicare le opportunità offerte dai musei a beneficio della città. È il caso, ad esempio, di come la comunicazione *online* dei musei possa contribuire alla promozione e alla reputazione *online* della città, oppure come possano essere messi a disposizione dai musei degli spazi digitali di dibattito per la cittadinanza sulle questioni sociali e politiche urbane tramite social media, siti web e piattaforme di *live streaming.*

Si può inoltre notare come l'enfasi delle politiche riguardo alla digitalizzazione del patrimonio culturale è spesso posta sull'aspetto conservativo, trascurando molte volte la valorizzazione digitale del patrimonio culturale cittadino. Sebbene, come si è visto, un tema emerso è quello del riutilizzo dei beni culturali digitalizzati in altri settori, tra cui quello turistico, la maggior parte dei finanziamenti e delle iniziative dell'Unione Europea sono volti alla protezione e conservazione digitale del patrimonio.

5.2. *Il caso delle Gallerie degli Uffizi: risultati preliminari*

Le Gallerie degli Uffizi, attraverso il Dipartimento di informatica e Strategie Digitali, dal 2016 utilizzano i canali di comunicazione *online* e le nuove tecnologie per rendere il patrimonio culturale sempre più accessibile e fruibile dai pubblici, sia *aficionados* sia i cosiddetti "non pubblici".

Le azioni delle Gallerie degli Uffizi in ambito digitale risultano in linea con

quanto emerso dall'analisi delle sinergie delle politiche europee in ambito culturale, urbano e digitale e con lo *Smart City Plan* della città di Firenze. Le Gallerie degli Uffizi, infatti conservano e valorizzano digitalmente il patrimonio della città rendendo accessibili al pubblico generale e specialistico gli archivi digitali delle opere custodite. Le Gallerie poi promuovono il turismo attraverso la creazione di contenuti culturali digitalizzati e fruibili sui loro canali digitali come il sito web e i *social media* al fine di valorizzare anche i luoghi meno conosciuti della città e della sua provincia. Gli Uffizi promuovono la partecipazione al patrimonio e al dialogo democratico *online* attraverso attività di educazione al patrimonio culturale. Tali attività coinvolgono le scuole locali, le associazioni e altri enti del territorio e il pubblico potenziale attraverso strategie di *audience development* ed *engagement* sui canali di comunicazione digitale, con un *focus* sul coinvolgimento dei giovani. Infine, le Gallerie degli Uffizi contribuiscono a promuovere la città di Firenze, valorizzando le specificità locali con contenuti digitali *online* come, ad esempio, l'artigianato.

Tuttavia, attraverso l'analisi delle azioni in ambito digitale degli Uffizi è stato rilevato come l'organizzazione museale offra al proprio pubblico una comunicazione *online* ancora prevalentemente unidirezionale. I contenuti proposti non sono spesso realizzati con il fine di aprire un dialogo con i pubblici *online,* ma con l'intento di comunicare attività e iniziative delle Gallerie. Questo è il caso anche del profilo TikTok che, seppure caratterizzato da un tono ironico e adatto ad un'audience giovane, non presenta iniziative atte a coinvolgere attivamente le audience attraverso, ad esempio, il lancio di sfide o audio da riutilizzare per contenuti generati dagli utenti della piattaforma. In futuro, le nuove tecnologie e i canali di comunicazione *online* potrebbero essere utilizzati per offrire al pubblico nuove forme di coinvolgimento più interattive e dialogiche per sfruttare appieno le potenzialità offerte dalle nuove tecnologie per lo sviluppo della città.

6. *Riflessioni conclusive*

I musei sono spazi in cui, negli ultimi anni, il coinvolgimento dei cittadini nella creazione di narrative urbane e nel dibattito sociale e politico della città sono diventati sempre più centrali. I musei sono infatti in grado di creare "*drammaturgie*" [40] capaci di attivare e coinvolgere i cittadini sui problemi ur-

[40] K. RIEMER, M. SCHWARZ, *Street Values: In the new Landscape of Societal Heritage Practices*, Amsterdam, 2017.

bani, la diversità e l'inclusione, l'architettura, lo sviluppo economico e la mobilitazione politica nelle città. Da questo punto di vista, la collezione del museo diventa strumento per innescare dibattito e nuove connessioni e relazioni [41], contribuendo al coinvolgimento della società e ad incoraggiare l'innovazione nel contesto urbano [42]. L'adozione di nuove tecnologie e canali di comunicazione da parte dei musei permette di raggiungere e coinvolgere pubblici nuovi, dialogando e creando connessioni con i cittadini e i visitatori della *smart city*. In questo modo, i musei sono in grado di generare immaginari urbani tramite strumenti digitali e *data-driven* [43], potenziando i loro visitatori *online* e *offline* a considerare il loro ruolo di "*co-makers*" attivi della città [44]. I musei si costituiscono così come spazi di generazione, promozione e anche legittimazione delle narrative legate alla *smart city* [45].

La ricerca qui presentata contribuisce al dibattito sulle *smart cities* tracciando gli spazi di intersezione nelle politiche dell'Unione Europea in cui musei e città possono agire insieme per lo sviluppo urbano sociale, culturale ed economico attraverso l'impiego delle nuove tecnologie.

Se la letteratura accademica sul tema dei musei nella *smart city* – sebbene ancora limitata – evidenzia il ruolo significativo dell'utilizzo delle nuove tecnologie nei musei per contribuire allo sviluppo della città, i risultati preliminari dell'analisi condotta sulle politiche europee per la cultura, lo sviluppo regionale e urbano e per il digitale in Europa mostrano come esse non considerino ancora sufficientemente tali potenzialità. Per questo, i *policy-maker* europei dovrebbero adattare la visione della cultura come patrimonio in grado di generare sviluppo economico, coesione sociale e creatività alla luce delle opportunità e delle sfide che i nuovi ambienti digitali stanno ponendo. In questo modo, il patrimonio culturale non solo potrebbe contribuire alla diversità culturale *online* promuovendo le specificità locali e a stimolare l'inclusione e il dialogo democratico sul web, ma potrebbe costituirsi anche come una risorsa in grado di inserirsi nelle nuove economie digitali.

---

[41] L. Solima, M. Tani, P. Sasso, *Social innovation and accessibility in museum: some evidence from the SoStare al MANN project*, in *Il capitale culturale*, 23, 2021, pp. 23-56.

[42] T. Giannini, J.P. Bowen, *Museums and Digital Culture*, London, 2019.

[43] Y. Ioannidis, K. Raheb, E. Toli, A. Katifori, M. Boile, M. Mazura, *One Object Many Stories: Introducing ICT in Museums and Collections Through Digital Storytelling*, Digital Heritage International Congress, 28 ottobre-1 novembre, Marsiglia, 2013, pp. 421, 424.

[44] N. Grincheva, *City museums in the age of datafication: could museums be meaningful sites of data practice in smart cities?*, in *Museum Management and Curatorship*, 2022.

[45] C. Grajales, M. Foth, P. Mitchell, G. Caldwell, *The museum in the Smart City: the role of cultural institutions in co-creating urban imaginaries*, in K.S. Wills, A. Aurigi (eds.), *The Routledge Companion to Smart Cities*, Londra, 2020, pp. 332-347.

Alla luce di tali risultati e della letteratura sul tema, si possono delineare alcune riflessioni specificamente in merito al *management* dei musei e alle politiche nella *smart city*.

Da una parte, vi è la necessità per i *policy-maker* delle *smart cities* di conoscere i propri cittadini e visitatori e le loro necessità tramite la raccolta di dati *online* e *offline*, in modo da formulare politiche e strategie di conseguenza. Le *smart cities* potrebbero poi attivare politiche per lo sviluppo della cultura e l'impiego delle nuove tecnologie al fine di attrarre lavoratori creativi che possano contribuire all'economia della città e al fine di promuovere l'inclusione sociale fornendo occasioni di dialogo, di fruizione culturale e di apprendimento per tutti i cittadini. Una delle più grandi sfide per le *smart cities* in questo contesto rimane quella di colmare i divari digitali che portano spesso all'esclusione di alcune fette di popolazione.

Dall'altra, si rende fondamentale per i musei implementare un tipo di comunicazione bidirezionale. Per fare questo, i musei devono conoscere i propri pubblici, soprattutto individuando le categorie non ancora coinvolte nelle attività culturali, al fine di stimolare ed estendere il dibattito sulla città. Per attrarre e raggiungere i pubblici, si rende necessario per i musei utilizzare le nuove tecnologie e i canali di comunicazione *online*, dotandosi di una strategia digitale che permetta di instaurare nuove relazioni e di creare attività *online* e *offline* partecipative. In questo modo i visitatori, siano essi residenti o turisti, potrebbero essere maggiormente coinvolti, riscoprendo le radici culturali della città, le sue trasformazioni nel tempo e nello spazio, e i modelli di sviluppo possibili per il futuro.

Dall'analisi condotta emerge come vi sia la necessità che città e musei lavorino a stretto contatto per assicurare la coesione sociale e il benessere dei cittadini, pensando ad uno sviluppo urbano che integri cultura e tecnologia. Le *smart cities*, collaborando con i musei, possono offrire agli "*smart citizen*" l'accesso *online* al patrimonio culturale per promuoverne la fruizione per fini di diletto e di studio, per sviluppare nuove competenze utili per il loro presente e futuro, e possono offrire alla cittadinanza spazi per la condivisione di opinioni e visioni del presente e del futuro della città.

Un tema recentemente emerso e che futuri studi potrebbero approfondire riguarda il ruolo dei musei come spazi di curatela, interpretazione, creazione di significati e circolazione dei *big data* raccolti dalla *smart city* nei diversi ambiti (es. trasporti, popolazione, gestione dei rifiuti ecc.) al fine di rendere i cittadini e i visitatori partecipi e interpreti della città[46]. Attraverso un'interpre-

[46] N. GRINCHEVA, *City museums in the age of datafication: could museums be meaningful sites of data practice in smart cities?*, in *Museum Management and Curatorship*, 2022; J. BATES,

tazione narrativa da parte dei musei, e una chiamata all'azione rivolta a visitatori *online* o *offline* tramite attività di *audience engagement*, le *smart cities* potrebbero giovare degli spazi di dialogo museali per progettare al meglio politiche ed iniziative cittadine.

Data Cultures, Power and the City, in *Data and the City*, ed. by R. KITCHIN, T.P. LAURIAULT, G. MCARDLE, New York, 2017, pp. 189-199.

BREVI CONSIDERAZIONI SULLA COMPATIBILITÀ DEI SISTEMI DI INTELLIGENZA ARTIFICIALE CON LA TUTELA DEL DIRITTO ALLA RISERVATEZZA

di *Fabrizio Dall'Acqua*

L'intelligenza artificiale si impone con sempre maggiore insistenza nella vita quotidiana, trasformando e semplificando il nostro stesso modo di vivere.

È sempre più spesso a portata di mano di ciascuno di noi: quando usiamo un traduttore automatico online o una app sul nostro smartphone magari per ricevere semplici indicazioni stradali, o quando facciamo uso di un termostato intelligente che può far risparmiare nella propria abitazione fino al 25% sulle bollette energetiche, analizzando le abitudini di chi ci vive e regolando conseguentemente la temperatura.

Nell'ambito dell'assistenza sanitaria gli algoritmi possono aiutare i dermatologi nella diagnosi, ad esempio individuando il 95% dei tumori della pelle mediante l'apprendimento automatico da grandi quantità di immagini medicali.

Sempre più frequente è la realizzazione di software di apprendimento automatico avanzato che utilizzano algoritmi comportamentali, capaci di captare e registrare le preferenze del soggetto utilizzatore.

Chi di noi non conosce e non fa uso, per esempio, di assistenti virtuali intelligenti come Siri o Alexa in grado di apprendere mediante una serie di interazioni, di interagire con l'abitazione e di effettuare, mediante comandi vocali, anche acquisti nello *store* Amazon?

Come si evince dai risultati pubblicati dalla Commissione per lo sviluppo regionale del Parlamento Europeo a seguito di una ricerca sul tema *Intelligenza artificiale e sviluppo urbano*, i sistemi di intelligenza artificiale possono certamente contribuire:

– a semplificare l'amministrazione dei centri urbani (si pensi ai sistemi di intelligenza per la mobilità, per monitorare il livello di inquinamento, per rilevare eventuali anomalie informatiche, per attuare forme di "vigilanza cibernetica" per edifici pubblici/aree sensibili, basate su *Computer Vision* tramite *Deep Lear-*

ning (AI), con sistemi di vigilanza automatizzata per rilevare pacchi sospetti, automezzi in aree pedonali, litigi, persone con armi, e tanto altro ancora);

– a sostenere i decisori pubblici nel processo decisionale,

– a contribuire al miglioramento dei servizi per i cittadini, in armonia ai principi di efficienza efficacia, economicità, imparzialità, trasparenza, pubblicità e buon andamento previsti dalla legge n. 241/1990;

– a creare nuove occasioni di sviluppo economico.

La pandemia, insieme agli eventi drammatici che ha prodotto e di cui ancora oggi portiamo i segni, ha avuto il merito non solo di accelerare processi di digitalizzazione ma anche di implementare con crescente velocità il ricorso a sistemi via via più sofisticati di intelligenza artificiale che hanno consentito, per esempio, al mondo della pubblica amministrazione, di erogare servizi secondo modalità che sino a quel momento avevano stentato a decollare, contribuendo a determinare un significativo cambio culturale sia degli stessi operatori della pubblica amministrazione che dei cittadini che, in larga misura, ancorché in alcuni casi non particolarmente inclini se non addirittura del tutto restii all'uso della tecnologia per accedere ai servizi offerti dalla Pubblica amministrazione, hanno mutato almeno in parte il proprio approccio, comprendendo che il Digitale è essenziale per ottenere, anche a distanza, servizi fondamentali per la vita di ciascuno.

Grazie ai sistemi di intelligenza artificiale, anche nei periodi pandemici più terribili caratterizzati da forti limitazioni alla stessa circolazione delle persone, il Comune di Milano (come tante altre realtà) ha saputo prendersi cura dei bisogni della gente implementando l'uso di diverse applicazioni che hanno consentito a chiunque di accedere anche attraverso il proprio cellulare, e utilizzando lo SPID, ad una serie ampia di servizi per ottenere certificati, effettuare versamenti, chiedere libri in prestito, prenotare appuntamenti presso uffici comunali, inviare segnalazioni all'amministrazione per migliorare la qualità dei suoi servizi, contribuendo nei fatti a dare attuazione agli stessi principi di sussidiarietà verticale e orizzontale previsti dalla stessa Carta Costituzionale.

L'e-government, la cittadinanza digitale, gli open data, la smart e green mobility, dimostrano in maniera evidente «la capacità di usare le nuove tecnologie per aumentare la partecipazione dei cittadini al processo democratico», in perfetta sintonia con quanto affermato dall'Unione Europea.

Il tema oggetto dell'odierna giornata di studio rappresenta certamente, come correttamente messo in risalto dal titolo di questo evento, una opportunità e una sfida allo stesso tempo.

Opportunità di crescita, di cambiamento culturale – organizzativo – di lavoro – di gestione del tempo, di miglioramento nell'erogazione dei servizi e nel soddisfacimento dei bisogni dei cittadini, ragioni tutte per le quali il ricor-

so a sistemi di intelligenza artificiale è anche particolarmente sfidante.

E, tal riguardo, ritengo che la sfida non debba essere intesa solo come capacità di provare ad impiegare la tecnologia per soddisfare al meglio la cura e la realizzazione di interessi privati e pubblici, ma anche come sforzo, tentativo di ottimizzare l'impiego della tecnologia e dei sistemi di intelligenza artificiale in armonia a valori e beni fondamentali dell'essere umano, quale – primo tra tutti – quello della riservatezza dei dati personali.

I sistemi di intelligenza artificiale, infatti, per loro natura trattano anche dati personali (che poi utilizzano per ricavare ulteriori dati) e, proprio per questa ragione, è necessario che il relativo trattamento avvenga nel rispetto dei principi contenuti nel Regolamento Europeo sulla Protezione dei Dati (GDPR – *General Data Protection Regulation*).

Il ricorso sempre più frequente alla tecnologia e alla intelligenza artificiale pone anche problemi di natura etica: sino a che punto, cioè, è giusto che si spingano questi sistemi?

Come ha giustamente osservato lo stesso Presidente dell'Autorità Garante della Privacy, «*quanto più la tecnica da protesica diviene mimetica, imitando cioè la razionalità umana, tanto più è necessario stabilire fin quando questa mimesi possa accettarsi, senza comportare una vera e propria sostituzione dell'uomo*».

Può la macchina sostituirsi definitivamente all'intervento umano? È compatibile un simile risultato con:

– la previsione di cui all'art. *22* del GDPR che garantisce all'interessato il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona?

– la regola, prevista dal medesimo articolo 22, secondo cui le decisioni basate sui processi automatizzati non possono coinvolgere le particolari categorie di dati personali di cui all'art. 9 GDPR (ossia dati personali che rivelino l'origine razziale, o etnica le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici o biometrici, dati relativi alla vita sessuale o alla salute) salvo che non ricorrano le ipotesi previste dallo stesso articolo che ne autorizza il trattamento e siano state adottate le adeguate cautele nel trattamento?

– l'art. 6 del GDPR che ritiene lecito il trattamento solo nei casi ivi previsti?

Fermo l'indiscutibile beneficio che l'impiego di questi sistemi produce nella nostra vita, vale la pena porsi anche qualche interrogativo.

Siamo disposti a correre il rischio – come osservato in dottrina – di una so-

stituzione del lavoro umano con quello realizzato dalle macchine, dai sistemi di intelligenza artificiale, dai robot?

Se le macchine intelligenti, i robot, potranno decidere da soli al posto nostro, come dovranno farlo? Saranno in grado di aiutarci, per esempio, a superare la discriminazione o potranno invece comportare il rischio di ulteriori e più profonde forme discriminatorie, come insegna il caso del riconoscimento facciale errato, per l'incapacità dell'algoritmo di distinguere il tratto somatico del nero da quello del bianco o *il caso dell'algoritmo divenuto razzista in 24 ore a causa dell'esposizione a materiale razzista*?

La Commissione Europea, in una comunicazione del 2019, ha sostenuto che «*la tecnologia della intelligenza artificiale dovrebbe essere sviluppata in modo da porre al centro l'essere umano e permettere di conquistare la fiducia del pubblico. Di conseguenza, le applicazioni di I.A. dovrebbero non solo rispettare la legge ma anche osservare i principi etici*».

La fiducia nei sistemi di intelligenza artificiale dipenderà dalla sua affidabilità e, conseguentemente, dalla sua credibilità, ma anche da un suo impiego in chiave antropocentrica, capace di porre *le persone al centro dello sviluppo dell'Intelligenza artificiale* (IA).

L'uso degli algoritmi, se da un canto può migliorare la velocità e l'efficienza delle pubbliche amministrazioni, sarà in grado di offrire l'immagine di una amministrazione davvero affidabile e credibile nelle scelte effettuate?

La decisione affidata solo a sistemi di IA può aumentare o ridurre il rispetto di scelte giuste ed eticamente corrette?

Chi risponderà delle scelte errate effettuate dal sistema artificiale? Chi della eventuale violazione di dati personali commessa da un robot? Quale sarà il confine tra la responsabilità dell'essere umano che ricorre agli strumenti di intelligenza artificiale per erogare servizi e la tutela del cittadino nel caso in cui il prodotto del sistema artificialmente intelligente non fosse quello giusto o, magari, fosse addirittura lesivo dei suoi interessi e dei suoi diritti?

Chi sarà responsabile dell'eventuale uso malevolo delle informazioni, magari causato semplicemente dalla incapacità del sistema di utilizzare dati e informazioni unicamente per le finalità consentite e non anche per finalità diverse?

Quali potranno essere cioè le finalità ulteriori compatibili ai sensi dell'art. 6, par. 4 del GDPR al trattamento dei dati acquisiti dai sistemi di intelligenza artificiale?

Sarà possibile conciliare l'acquisizione, da parte dei sistemi di intelligenza artificiale (che peraltro devono essere sempre più interoperabili tra loro), di una enorme varietà di informazioni necessarie per arricchire il bacino decisionale con l'esigenza di tutelare dati personali nel rispetto delle regole contenute nel codice della privacy?

Tutti questi quesiti spingono oggi taluni a ritenere che il GDPR potrebbe apparire incompatibile con l'Intelligenza Artificiale (IA), dato che contiene principi quali, la limitazione delle finalità, la minimizzazione dei dati, il trattamento speciale dei "dati sensibili" e la limitazione delle decisioni automatizzate, che possono intaccare le proprie funzionalità principali.

Lo sforzo comune deve pertanto essere quello di provare ad attuare un'interpretazione del GDPR che sia in grado di conciliare le due necessità (apparentemente) contrastanti: proteggere i dati personali e consentire l'utilizzo dell'IA.

La efficace regolamentazione del diritto alla riservatezza rappresenta un punto chiave per consentire a tecnologie come l'intelligenza artificiale di aiutare a risolvere le più grandi sfide del mondo.

La privacy è un diritto umano fondamentale e un'efficace protezione della stessa è importante per consentire agli individui di fidarsi della tecnologia.

Fondamentale in questo contesto, dunque, il ruolo dell'Autorità Garante per la protezione dei dati personali, i cui rappresentanti non a caso oggi partecipano a questo interessante evento.

Tanti, dunque, gli spunti e le sollecitazioni. Sono convinto che l'odierna giornata di studio sarà l'occasione per esaminare i diversi problemi e le diverse implicazioni dell'uso dell'intelligenza artificiale, magari dando l'avvio (come auspico) ad un processo virtuoso di scambio di buone prassi e di elaborazione di linee guida, possibilmente con il contributo – che giudico essenziale – dell'Autorità garante per la protezione dei dati personali, affinché davvero si riesca a coniugare l'ottimizzazione del benessere collettivo e individuale attraverso l'uso di sistemi di intelligenza artificiale con l'irrinunciabile rispetto di beni fondamentali dell'Uomo che meritano di essere in ogni caso adeguatamente salvaguardati.

SMART CITIES, DIRITTO AMMINISTRATIVO E PNRR

di *Marco Macchia*

SOMMARIO: 1. Le tecnologie impiegate dalle municipalità a supporto dei servizi al pubblico. – 2. I finanziamenti e i vincoli del PNRR per le città intelligenti. – 3. Le nuove tecnologie sono il carburante delle *smart city*. – 4. Presupposti, modalità di impiego e limiti: la necessità di una strategia complessiva per le città intelligenti.

1. *Le tecnologie impiegate dalle municipalità a supporto dei servizi al pubblico*

Le nuove tecnologie permettono di progettare *ex novo* la mobilità urbana, in chiave di maggiore sostenibilità, così da permettere a chi abita in città una valida alternativa all'uso dell'autovettura che sia funzionale alle proprie esigenze. In Israele, è stata implementata una tecnologia per un uso più consapevole dei tram della capitale volto a migliorare il servizio mediante l'impiego di nuove tecnologie. Per mezzo del sistema di intelligenza artificiale, messo a punto da Axilion, start-up entrata in Borsa nel 2020, i convogli della Jerusalem Light Rail impiegano il 47% di tempo in meno per attraversare la città (mezz'ora invece di un'ora), mediante un dialogo elettronico tra videocamere Azure Kinect installate sui tram e sui semafori di linea in grado di creare "un'onda verde semaforica" per il mezzo pubblico. I dati raccolti dalle telecamere sull'andamento del traffico vengono analizzati al fine di creare una città gemella digitale ove l'intelligenza artificiale simula e decide con un algoritmo le migliori strategie di regolazione degli incroci. Il coordinamento degli impianti semaforici e la digitalizzazione degli orari dei trasporti pubblici consentono agli utenti di riscontrare l'itinerario da *app* e pianificare il viaggio nel pieno rispetto e sicurezza della *privacy* dei dati raccolti[1].

[1] Sul ruolo dell'intelligenza artificiale nella gestione del traffico, S. NEELAKANDAN, M.A. BERLIN *et al.*, *IoT-based Traffic Prediction and Traffic Signal Control System for Smart City*, in

Che si tratti del controllo del flusso di traffico, dell'accesso ai parcheggi, di polizia predittiva, di verifiche del corretto pagamento di tributi o contributi alla municipalità, oppure dell'individuazione di abusi di mercato a livello locale, non v'è dubbio che le città sotto la spinta dell'intelligenza artificiale si preparano a cambiare volto, digitalizzandosi e velocizzando molte prestazioni rese al pubblico. Raccogliendo e analizzando una numerosa mole di dati relativi al traffico, alle utenze, allo sviluppo metropolitano, la città può essere in grado di offrire servizi "intelligenti" ai cittadini. Numerosi esempi stranieri dimostrano che questo cambiamento è già in corso.

Stando alle stime dell'ONU, nel 2050 la popolazione mondiale sarà composta da 9,7 miliardi di persone. Attualmente di questa "solo" il 55% vive nei centri urbani, mentre si ritiene che per quella data tale percentuale aumenterà fino a raggiungere il 70%. Se ciò è vero, diviene evidente come la costruzione di *smart city* che, allo stato, appare essere solo una prospettiva di alcune realtà municipali più grandi, nei prossimi anni crescerà in modo esponenziale fino a diventare una stretta necessità [2].

Allo stesso modo, per la medesima ragione, mostra caratteri di indifferibilità la decarbonizzazione, la quale, muovendo proprio dal dato dell'incremento vertiginoso della popolazione mondiale, mira alla riduzione delle emissioni di gas serra di almeno il 55% entro il 2030 rispetto ai livelli del 1990 in modo da giungere alla neutralità climatica entro il 2050 [3].

La città intelligente sfrutta le applicazioni di intelligenza artificiale a supporto di servizi al pubblico. Queste ultime si alimentano di innumerevoli dati raccolti da sensori, apparecchiature e altri sistemi per creare sostenibilità ed efficienza. Ma ciò non basta, serve altresì una strategia complessiva. Un'azione spontanea e non codificata in alcune realtà non è soddisfacente perché la città

Soft Computing, 2021, p. 12241; R. BRAUNEIS, E.P. GOODMAN, *Algorithmic Transparency for the Smart City*, in *Yale Journal of Law & Technology*, 2018, p. 103.

[2] Come sottolinea F. COSTANTINO, *Brevi note su intelligenza artificiale e smart cities*, in *Intelligenza artificiale e amministrazione*, a cura di A. PAJNO, F. DONATI, A. PERRUCCI, vol. II, Bologna, 2022, p. 187 ss., «*L'Oliver Wyman Forum, che cura un rapporto che ha ad oggetto l'indice di preparazione all'intelligenza artificiale delle città globali, segnala in particolare che nessuna città è vicina ad essere pronta per le sfide future (anche se alcune sono meglio preparate di altre). Lo stesso studio ha messo in rilievo come, sebbene le dimensioni contino, piccole e medie città possono avere risultati buoni come quelli delle grandi città (5 delle 10 con le performance migliori del rapporto contano meno di 5 milioni di abitanti). Risulta interessante anche il rilievo, contenuto nello stesso rapporto, secondo cui la maggior parte delle città non affronta i principali cambiamenti sociali guidati dall'intelligenza artificiale e da altre tecnologie, perché si concentra sugli sviluppi delle smart cities e sulle opportunità, ignorando o minimizzando i rischi, di cui invece risultano essere più consapevoli gli abitanti stessi*».

[3] Così sancita in Europa dal pacchetto FIT for 55 della Commissione Europea.

intelligente deve essere integrata e interagente con le altre realtà urbane affinché garantisca convenienza ed efficienza [4].

Sebbene mediante il PNRR, come si vedrà, non manchi la certezza di disponibilità finanziarie per dare impulso e sviluppo ad un arcipelago di *smart cities*, allo stesso tempo ciò che sembra mancare è una chiara indicazione dei procedimenti interessati, delle tecnologie utilizzate, dei criteri in base ai quali è possibile rivolgersi al mercato invece di produrre internamente l'algoritmo, delle ragioni dell'utilizzo, nonché dell'impostazione di un monitoraggio tale da mostrarne il funzionamento e i relativi esiti.

2. *I finanziamenti e i vincoli del PNRR per le città intelligenti*

Dall'efficienza energetica alla mobilità, dalla sicurezza alla riqualificazione degli spazi urbani, fino alla digitalizzazione degli enti locali: il tema *smart city* permea in maniera trasversale gran parte del Piano Nazionale di Ripresa e Resilienza (PNRR) e delle sue missioni. Proprio perché gli ambiti applicativi che rientrano nella sfera di influenza delle città intelligenti sono molteplici, il po-

[4] E.E. JOB, *Policing the Smart City*, in *International Journal of Law in Context*, 2019, p. 177. Negli ultimi anni la letteratura su questo tema è notevolmente incrementata, si fa riferimento in particolare a A. CASINELLI, *Le città e le comunità intelligenti*, in *Giorn. dir. amm.*, 2013, p. 240; E. CARLONI, M. VAQUERO, *Le città intelligenti e l'Europa. Tendenze di fondo e nuove strategie di sviluppo urbano*, in *Smart cities e amministrazioni intelligenti*, in *Istituzioni del federalismo*, 2015, p. 880; R. FERRARA, *The Smart City and the Green Economy in Europe: a Critical Approach*, in *Energies*, 2015, p. 4724; E. FERRERO, *Le smart cities nell'ordinamento giuridico*, in *Foro amm.*, 2015, p. 1267; F. FRACCHIA, P. PANTALEONE, *Smart City: condividere per innovare (e con il rischio di escludere?)*, in *Federalismi.it*, 2015; A. PENSI, *L'inquadramento giuridico delle «città intelligenti»,* in *giustamm.it*, 2015; C. SCHEPISI, *Servizi della società dell'informazione, Unione europea e nuovi modelli economici: smart cities e sharing economy*, in G. OLIVIERI, V. FALCE (a cura di), *Smart Cities e Diritto dell'Innovazione*, Milano, 2016, p. 3; G. ANTONELLI, G. CAPPIELLO (a cura di), *Smart Development in Smart Communities*, London-New York, 2017; R.P. DAMIERI, *Smart City Implementation, Creating Economic and Public Value in Innovative Urban Systems*, Berlin, 2017, p. 23; G.F. FERRARI (a cura di), *La prossima città*, Milano, 2017; V. AGUADO, I CUDOLÀ, V. PARISIO *et al.* (a cura di), *El derecho a la ciudad: el reto de las smart cities*, Barcellona, 2018; F. GASPARI, *Città intelligenti e intervento pubblico*, in *Dir. econ.*, 2019, pp. 71-110; C. IAIONE, *Legal infrastructure and urban networks for just and democratic smart cities*, in *Ital. Journ. Pub. Law*, 2019, p. 747; C. NAPOLI, *La Smart City tra ambizioni europee e lacune italiane: la sfida della sostenibilità urbana*, in *Le Regioni*, 2019, p. 445; M. CAPORALE, *Dalle smart cities alla cittadinanza digitale*, in *Federalismi.it*, 2020; T. FAVARO, *Verso la smart city: sviluppo economico e rigenerazione urbana*, in *Riv. giur. ed.*, 2020, p. 87; S. PETTIROSSI, *Tra smart city e smart land: le agende urbane delle Regioni italiane*, in *Istituzioni del federalismo*, 2020, p. 207.

tenziale degli interventi previsti dal piano è molto alto. Eppure appare ancora da districare la trama delle misure di finanziamento di queste strategie di sviluppo urbano.

Questo impulso e sviluppo alle *smart cities* è il frutto dunque di un significativo accordo politico con le istituzioni europee, sebbene l'Unione non abbia in questa materia una competenza diretta. Al riguardo, pertanto, sono possibili unicamente interventi non rientranti nel diritto derivato, ma incorporati in atti di *soft law* e in comunicazioni non giuridicamente vincolanti propri di politiche comuni europee già consolidate con la finalità di orientare gli enti pubblici[5]. Oppure sono concepibili risoluzioni consistenti in azioni, incentivi e progetti di finanziamento collegati alla realizzazione di programmi riconducibili a competenze di settore oppure ad iniziative specifiche di partenariato pubblico-privato.

Le risorse stanziate per questo processo di innovazione sono di certo ingenti. Il PNRR destina in sostanza oltre 10 miliardi di euro per lo sviluppo ed il potenziamento delle realtà urbane.

Ad un primo sguardo, sono tre le missioni previste del PNRR in cui sono presenti elementi e obiettivi riconducibili al tema della *smart city*. In primo luogo, viene in evidenza la missione 5 relativa all'inclusione e coesione con investimenti in tema di rigenerazione urbana, tra cui merita attenzione la riforma dei piani urbani integrati. In secondo luogo, la Missione 1 di digitalizzazione mira a promuovere, tra le altre cose, progetti di *Mobility as a service* (MaaS). In terzo luogo, all'interno della Missione 2 dedicata alla rivoluzione verde e alla transizione ecologica si articolano diverse soluzioni ascrivibili, direttamente o indirettamente, nell'ambito della rete di interventi abilitati dalle *smart cities*.

Più in particolare, la Missione 5 sui piani urbani integrati per una città innovativa, inclusiva e sostenibile, contempla, tra i 9 miliardi di euro destinati alla rigenerazione urbana, intesa come novero di azioni complesse di contrasto al degrado urbano, incidenti non solo sull'ambito urbanistico ma anche sugli assetti socio-economici, culturali e occupazionali del territorio interessato, nonché sulla riduzione del consumo di suolo, circa 2,5 miliardi sono dedicati ai piani urbani integrati, che prevedono progetti di pianificazione e rigenerazione urbanistica partecipata, con l'obiettivo di trasformare territori vulnerabili in città *smart* e sostenibili.

Gli interventi avranno l'obiettivo di promuovere sinergie di pianificazione tra città metropolitane e comuni limitrofi più piccoli, per creare un tessuto

[5] Sul tema, *ec.europa.eu/info/euregional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en*.

urbano ed extra-urbano più omogeneo e colmare deficit infrastrutturali e di mobilità. Progetti di *smart land* o *smart city* condivisi semplificherebbero le interazioni e lo scambio di informazioni all'interno del network, aumentandone l'impatto sul territorio, livelli di innovazione e qualità di vita dei cittadini. L'auspicio è che, in tal modo, l'attenzione a questo processo di innovazione non riguardi solo le grandi città (principalmente Milano, Torino, Firenze, Genova, Trento, mentre Roma e Ferrara hanno avviato progetti pilota), ma sia un processo organico che interessa quasi ogni realtà urbana del Paese.

Oltre a ciò, sono stati stanziati altri fondi di rigenerazione urbana, pari a 2,8 miliardi di euro, per il programma innovativo della qualità dell'abitare, che ha tra i vari scopi anche quello di utilizzare modelli e strumenti innovativi per la gestione, l'inclusione e il benessere urbano.

Riguardo la Missione 1, ossia *Mobility as a Service* e sistemi integrati di trasporto urbano, tra i 2 miliardi di euro per i servizi digitali e la cittadinanza digitale troviamo altresì una nota dedicata al *Mobility as a Service* (MaaS) come nuova modalità di trasporto integrato da sperimentare nelle città metropolitane.

Mobility as a Service è un progetto volto a realizzare un sistema di mobilità sostenibile, che preveda l'integrazione di diverse modalità di trasporto attraverso un unico canale digitale, agevolando gli spostamenti nei centri urbani. A tal proposito, è già stato aperto un bando per presentare proposte progettuali, tramite cui sono state scelte città "*leader*" per realizzare i primi pilot, e città "*follower*", che implementeranno le soluzioni più innovative ed efficaci in un secondo step.

Infine, nell'ambito della Missione 2, dedicata alla rivoluzione verde e alla transizione ecologica nei centri urbani[6], si riscontrano risorse a supporto di interventi sul trasporto pubblico locale in chiave di sostenibilità, sul trasporto rapido di massa, nonché nel comparto delle infrastrutture di ricarica elettrica e della mobilità ciclistica. Sebbene i progetti in Missione 2 abbiano un respiro applicativo molto più ampio della dimensione urbana, alcuni interventi vedono le città protagoniste del cambiamento.

---

[6] Non vanno dimenticati poi gli interventi a favore di una rete idrica più digitale, con l'obiettivo di ridurre le perdite e ottimizzare i consumi. Oppure gli interventi di digitalizzazione delle infrastrutture, in cui si stanziano risorse (4 miliardi di euro) per *smart grid* e il rafforzamento della rete di distribuzione elettrica in chiave digitale e flessibile, in cui le città possono essere coinvolte abilitando la transizione dei consumi energetici verso l'elettrico. Il monitoraggio del territorio è un ulteriore ambito applicativo in cui c'è spazio per progetti urbani *smart*, in particolare per migliorare la capacità previsionale sul cambiamento climatico e prevenirne gli effetti sulla vulnerabilità del territorio, adottando misure tecnologiche e innovative per gestire i rischi e aumentando la resilienza dei Comuni ed efficientando il sistema idrico.

A tutto ciò devono essere aggiunti i finanziamenti ai progetti di *smart building* ossia i fondi stanziati per l'efficienza energetica e la riqualificazione di sedi giudiziarie, scuole e sistemi urbani intelligenti in generale. In sintesi, se non può essere messo in dubbio che i fondi e le risorse siano sufficienti, bisogna vedere se tutto ciò sia affiancato da un adeguato apparato di *governance* idoneo a cogliere queste opportunità con figure professionali a ciò dedicate. Le grandi città sembrano aver individuato all'interno della giunta competenze adeguate per queste attività, mentre i comuni al di sotto dei 15 mila abitanti non sembrano avere personale appropriato per cogliere questa sfida[7].

Le opportunità di intervento del PNRR per rendere le città più digitali e connesse sono quindi molteplici[8]. Il rischio è che, con le tempistiche ristrette per realizzare il Piano, le risorse non trovino l'impiego più efficace per raggiungere gli obiettivi iniziali. Allo stesso tempo, un'altra problematica da non sottovalutare è la mancanza di personale, amministrativo e tecnico, per seguire i progetti, dall'uscita del bando alla sua implementazione, la cui mancanza impatta negativamente su tempi di esecuzione e risultati degli interventi.

Sviluppare un'integrale visione di insieme degli interventi da porre in essere e delle scadenze imposte dal piano, così come riuscire a fare sistema con gli attori (anche privati) del mercato *smart city*, sono qualità quanto mai necessarie per sfruttare a pieno le opportunità per rendere "intelligenti" le città.

Questi rimangono nodi fondamentali. Anche perché, in base al Regolamento UE 2021/241 che istituisce il dispositivo per la ripresa e la resilienza, si evince come non sia possibile semplicemente ritardare il raggiungimento di alcuni obiettivi saltando temporaneamente una rata per poi ricominciare a raggiungere *milestones* e *target* per le scadenze successive. Il PNRR è uno strumento dove tutto si tiene ed è necessario, quindi, nel caso in cui non si raggiungano gli obiettivi a una determinata scadenza, raggiungerli in seguito il prima possibile per "rimettersi in pista" e poter continuare con l'attuazione del pia-

---

[7] Allo stato il 72% delle grandi città si è attrezzata in tal senso, mentre solo un comune di piccole dimensioni su tre ha predisposto competenze adeguate. Nei progetti di *smart building* rientrano anche 15 miliardi stanziati per l'efficienza energetica e la riqualificazione di edifici pubblici come scuole, sedi giudiziarie ed unità abitative pubbliche, in cui tecnologie intelligenti possono essere adottate per ridurre consumi e renderle più *green* ed efficienti.

[8] Al di là degli obiettivi conclamati, appare significativa la reale percezione del PNRR tra le città italiane. Una recente indagine del Tavolo di Lavoro *Smart City* ha intercettato l'interesse dei Comuni italiani (452 intervistati) verso il PNRR, rilevando che il 69% degli oltre 100 enti locali che investiranno nel prossimo triennio sono già sicuri di volersi appoggiare a questi fondi, mentre il 26% è in fase di valutazione. Spiccano, tra quelle che attraggono maggiore interesse, le missioni legate alla digitalizzazione, alla transizione ecologica, alle infrastrutture per la mobilità sostenibile e alla rigenerazione urbana.

no. Sempreché non si tenti un nuovo accordo politico con le istituzioni europee per la modifica del piano.

Per monitorare eventuali interventi disomogenei nel territorio è stato attivato lo strumento informatico ReGis della Ragioneria generale dello Stato. Con quest'ultimo si intende verificare in tempo reale gli stati di avanzamento degli interventi del piano, al fine di indicare la situazione dei dati relativi al cronoprogramma procedurale delle misure adottate o da adottare. In questo modo, eventuali disorganicità territoriali nella distribuzione degli investimenti in chiave di città intelligenti potranno essere messi subito in evidenza, il che renderà possibili correzioni in corso d'opera a favore di un piano organico diretto ad evitare zone di eccellenza, isole intelligenti in un deserto urbano né intelligente né integrato.

3. *Le nuove tecnologie sono il carburante delle* smart city

Per realizzare città intelligenti sono necessari ingenti finanziamenti. I Piani integrati permettono alle città metropolitane di sostenere progetti *smart* per i trasporti, il consumo energetico, la rivitalizzazione economica, nell'ambito del PNRR[9]. Appurato che un importante stimolo all'uso dell'intelligenza artificiale nell'azione amministrativa e nei servizi alla collettività offerti dalla municipalità è svolto dagli incentivi dell'Unione Europea di tipo economico (e non economico) che derivano dal confronto delle pratiche in sede internazionale ed europea, le nuove tecnologie sono pur sempre apportatrici di diversi vantaggi e presentare contestualmente rischi di errori, opacità e discriminazioni. Non solo, rimane pur sempre il problema di verificare la solidità del criterio distintivo fra ciò che è vietato e ciò che è consentito.

Gli usi di nuove tecnologie presentano, difatti, numerosi vantaggi per i pubblici poteri nell'ottica di un diritto ad una buona amministrazione, elencabili dalla possibilità di comprimere i tempi per decidere e di razionalizzare l'impegno di risorse umane, alla elaborazione di indicazioni anche prospettiche, alla possibilità di evitare errori umani e di limitare le occasioni di corruzione. I

[9] Si v. l'art. 21 del d.l. 6 novembre 2021, n. 152, nonché la legge 7 aprile 2014, n. 56 che affida alla città metropolitana le funzioni di area vasta, tra cui si riscontrano i compiti di programmazione dello sviluppo urbano nell'ottica di *smart city*. In particolare, sono di competenza della città metropolitana le funzioni di promozione e di gestione dei servizi, delle infrastrutture e delle reti di comunicazione (art. 1, comma 2) e quelle di indirizzo, di pianificazione e di supporto ai Comuni dell'area metropolitana, con particolare riguardo alla promozione e all'attuazione dei sistemi di informatizzazione e di digitalizzazione (art. 44, lett. f).

settori di intervento sono quelli della gestione del traffico, della sicurezza, dell'ottimizzazione dei consumi di energia, della gestione del territorio e della gestione dei rifiuti. In questi ambiti, l'intelligenza artificiale costituisce uno strumento per l'effettività dell'organizzazione e dell'azione amministrativa, ossia di un diritto amministrativo che sia osservato, attuato e foriero di risultati coerenti con gli obiettivi per cui è stato previsto.

Ai vantaggi connessi all'impiego delle nuove tecnologie sono affiancabili i rischi, che corrono dall'opacità, all'errore, alla discriminazione. L'intelligenza artificiale può essere il mezzo mediante il quale perpetrare storture e imperfezioni che caratterizzano tipicamente i processi cognitivi e le scelte compiute dagli esseri umani, secondo il modello *garbage in, garbage out*. Da un lato, gli algoritmi riducono la variabilità dei giudizi umani su situazioni identiche, da un altro però le alterazioni possono essere amplificate dalla scarsa qualità dei dati che alimentano l'intelligenza artificiale, ad esempio perché raccolti da soggetti in conflitto di interessi, oppure basati su presunzioni non validate dal diretto interessato o esclusivamente su dati storici, ovvero ancora su dati raccolti per scopi diversi oppure tratti da "tracce" lasciate in rete dalle persone [10].

Ciò solleva l'esigenza di un inquadramento normativo per gli usi dell'intelligenza artificiale basato sulla trasparenza, in termini di effettiva conoscibilità, come regola minima e comune a tutte le applicazioni, ed esteso ai presidi della motivazione (come effettiva spiegabilità) e verificabilità dei sistemi per gli usi da parte delle pubbliche amministrazioni nei processi decisionali pubblici.

Stando all'art. 20 del d.l. 18 ottobre 2012, n. 179, il riferimento all'inclusione intelligente consiste nella «*capacità, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di offrire informazioni nonché progettare ed erogare servizi fruibili senza discriminazioni dai soggetti appartenenti a categorie deboli o svantaggiate e funzionali alla partecipazione alle attività delle comunità intelligenti*». La comunità intelligente è «*quel luogo e/o contesto territoriale ove l'utilizzo pianificato e sapiente delle risorse umane e naturali, opportunamente gestite e integrate mediante le numerose tecnologie i.c.t. già disponibili, consente la creazione di un ecosistema capace di utilizzare al meglio le risorse e di fornire servizi integrati e sempre più intelligenti (cioè il cui valore è maggiore della somma dei valori delle parti che li compongono)*» [11].

Le *smart cities*, quale nuovo paradigma dello sviluppo urbano, sono altamente interconnesse e *technology-dependent*. Tale concetto non può essere li-

[10] R. BRAUNEIS, E.P. GOODMAN, *Algorithmic Transparency for the Smart City*, in *Yale Journal of Law & Technology*, 2018, p. 103.

[11] Secondo le linee guida pubblicate dall'AgID nel 2012.

mitato soltanto alla digitalizzazione o legato esclusivamente alle problematiche ambientali. Esso implica, al contrario, una vera e propria rivoluzione relativa al "come" concepire il rapporto tra uomo, ambiente e territorio [12]. L'intervento sulle città, sulla loro forma e sui principi che le governano è necessario, in quanto è atto ad assicurare il soddisfacimento pieno degli interessi della persona. Il miglioramento delle condizioni di vita, in qualunque parte del mondo, passa necessariamente per l'avanzamento delle città, perché la maggior parte dell'umanità vive all'interno di esse. È chiaro, dunque, che del tema dell'accessibilità urbana debba tenersi conto nel momento in cui si progettino le *smart cities*.

Proprio grazie agli algoritmi, può concretizzarsi l'attività più avanzata connessa ai *big data*, ovvero l'attività predittiva. Ciò permette di sfruttare al massimo il valore dei dati, consentendo alle amministrazioni di utilizzare le informazioni a disposizione per svolgere proiezioni future e ampliare così il proprio patrimonio informativo, sulla cui base prendere decisioni.

Una ricaduta di ciò è evidente nei sistemi di sicurezza e videosorveglianza mediante il riconoscimento facciale o altre tecniche di identificazione. Basti pensare, tra i molti esempi, al sistema denominato SyRI (*Systeem Risico Indicatie*) diretto ad accertare l'attitudine a commettere frodi o abusi da parte di cittadini, residenti in determinati quartieri, ai quali erano stati erogati sussidi o che beneficiavano di altre forme di assistenza pubblica. Questo algoritmo, impiegato dal governo olandese dal 2014 al febbraio 2020, rappresenta un'infrastruttura tecnologica funzionale a collegare e analizzare i dati in modo anonimo in un ambiente sicuro, in modo che possano essere generati rapporti sui rischi. Attraverso SyRI, gli enti pubblici erano in grado di condividere tra loro un ingente quantità di dati al fine di generare numerose informazioni nella ricerca di frodi a danno del sistema previdenziale o tributario [13].

---

[12] R. GIFFINGER, C. FERTNER *et al.*, *Smart Cities. Ranking of European Medium-sized Cities*, Wien, 2007, p. 13, «*A smart city is a city well performing in a forward-looking way in these six characteristics, built on the "smart" combination of endowments and activities of self-decisive, independent and aware citizens. (Smart Cities: smart economy; smart mobility; smart environment; smart people; smart living; smart governance)*».

[13] La Corte dell'Aia ha, successivamente, accertato l'illegittimità di SyRI sulla base del fatto che non sono state previste garanzie sufficienti per tutelare adeguatamente l'individuo di fronte ad un'interferenza pubblica la quale, sebbene sorretta da uno scopo legittimo, si caratterizza per essere particolarmente invasiva. Il tribunale non ha solo verificato la previsione di obblighi di pubblicità, trasparenza e partecipazione, ma si è spinto a conoscere della concreta afflittività dell'intervento in relazione al *vulnus* cagionato alle prerogative degli interessati. La decisione merita evidenza, altresì, per il metodo innovativo dei giudici sull'impatto che le nuove tecnologie producono sull'esercizio del potere da parte delle amministrazioni. L'evoluzione tecnologica viene infatti, vista, non quale mera variabile nelle modalità di azione dei pubblici poteri, che quindi richiede un semplice adattamento dell'esistente, ma come un (nuovo) presupposto sulla

Che il tema della videosorveglianza invasiva nei luoghi pubblici, del resto, sia particolarmente critico lo dimostra altresì il dibattito in corso presso il Parlamento europeo per l'approvazione del primo regolamento sull'intelligenza artificiale. Le Commissioni Giustizia e Mercato interno hanno difatti approvato il divieto di riconoscimento facciale indiscriminato nei luoghi pubblici, fatta eccezioni per ipotesi eccezionali che siano autorizzate dalla magistratura e che facciano riferimento al perseguimento di reati già commessi. Risulta essere, peraltro, vietato in ogni caso il riconoscimento biometrico in tempo reale [14].

Oltre ai tradizionali rischi che l'intelligenza artificiale è in grado di veicolare in generale (a cominciare dal fatto che un modello artificiale potrebbe risultare impreciso quando utilizzato nel mondo reale), vi sono poi problematiche specifiche sollevate proprio dagli usi che dell'intelligenza artificiale si fanno nel comparto della *smart city*, che attengono ai diversi momenti ed obiettivi per i quali i pubblici poteri fanno uso di questi sistemi tecnologici.

4. *Presupposti, modalità di impiego e limiti: la necessità di una strategia complessiva per le città intelligenti*

Ridefinire la sicurezza, la mobilità urbana, le reti energetiche, la gestione dei rifiuti richiede, innanzitutto, una nuova definizione dei confini geografici e dimensionali che sia funzionale alle esigenze delle infrastrutture. È evidente, infatti, che i servizi della città intelligente per funzionare hanno bisogno di appoggiarsi ad una significativa rete infrastrutturale, composta da sensori, telecamere, misuratori, strumenti di comunicazione, algoritmi di gestione, la cui efficienza è data da diversi elementi tra cui rileva la dimensione territoriale e il peso demografico di alcune aree ad alta intensità [15].

Come è stato messo in evidenza, «*le tecnologie smart city dipendono dalle reti di comunicazione digitale: c'è bisogno di reti cablate e wireless sicure, ridon-*

---

cui base ripensare i principi e ridefinire le garanzie nei confronti del potere al fine di affrontare i problemi posti dai processi di *decision making* mediante algoritmi.

[14] European Parliament, *AI Act: a step closer to the first rules on Artificial Intelligence*, 11 maggio 2023.

[15] Sul tema, G.C. RICCIARDI, A. VENTURI, *Investimenti e finanziamenti in infrastrutture digitali per le smart cities in una prospettiva comparata ed europea. Uno studio introduttivo*, in *Dir. pubb. comp. eur.*, 2020, p. 1095; C. BENETAZZO, *Appalti innovativi e smart cities: verso una nuova dimensione pubblico-privata?*, in *Federalismi.it*, 2021; G. DELLE CAVE, *«Comunità intelligenti», enti locali, mobilità sostenibile: le smart city al cospetto del potere pubblico*, in *Dir. econ.*, 2021, p. 385; C. LAURI, *Smart City*, in *Dig. disc. pub.*, Agg. VIII, Torino, 2021, p. 377.

danti e resilienti, una complessa rete di dispositivi e sensori interconnessi, connettività ad ampia larghezza di banda. Serve inoltre energia elettrica, in quanto, al di là del ruolo che possono assumere le smart cities nella gestione dell'energia, esse stesse ne hanno bisogno: senza di essa le città possono affrontare blackout, con enormi problemi al traffico, all'infrastruttura idrica, all'assistenza sanitaria, solo per fare alcuni esempi»[16].

Reti infrastrutturali di questo tipo – da realizzare per giunta nei tempi brevi imposti dal PNRR – impongono alle pubbliche autorità di fare ricorso alle esperienze e alle competenze tecnologiche delle imprese private. In quest'ottica, assume un ruolo centrale il partenariato pubblico privato, con l'obiettivo di stimolare investimenti in soluzioni energetiche integrate e innovative, nella gestione intelligente dei rifiuti, sempre in armonia con il principio dello sviluppo sostenibile.

Un cambiamento di questo tenore porta a scorgere il tramonto di una *governance* della città interamente pubblica, con l'inevitabile sostituzione degli strumenti di pianificazione tradizionale, espressione del modello di regolazione *top-down*, con l'idea del *market-led planning*[17]. Ossia modelli di rigenerazione integrata, i quali sottendono molteplici e innovative modalità di intervento, accomunate dal conseguimento del fine generale dello sviluppo socio-economico urbano, e giustificate da una gestione congiunta pubblico-privato ovvero che vede il decisore pubblico coordinare diversi operatori economici privati.

La necessità di supporto tecnico dei privati per veicolare le innovazioni tecnologiche nelle *smart city* dovrebbe trovare riscontro a monte negli appalti pubblici. Le gare ad evidenza pubblica possono fungere, difatti, da strumenti di *policy* per raggiungere specifiche finalità, diverse dalla mera competizione economica. Al riguardo, le pubbliche amministrazioni nell'approvvigionamento di tecnologie di riconoscimento facciale da parte di società private, decisive nel comparto *smart*, dovrebbero inserire nel bando e nelle specifiche tecniche requisiti funzionali connessi alla progettazione miranti alla protezione dei dati e alla non discriminazione nell'uso di questi dispositivi.

Non va dimenticato, infatti, che il ricorso a strumenti algoritmici e all'intelligenza artificiale, necessari per investimenti in progetti di rigenerazione urba-

---

[16] F. COSTANTINO, *Brevi note su intelligenza artificiale e smart cities*, cit., p. 194.

[17] Al riguardo, S. RANCHORDIS, *Law and Autonomous Systems Series: Cities as Corporations? The Privatization of Cities and the Automation of Local Law*, in *www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-cities-corporations-privatization*.

All'estero si diffondono anche forme di *popular planning*, ossia di pianificazione popolare rimessa in tutte le sue fasi al controllo diretto dei cittadini, tale insomma da coinvolgere i singoli cittadini e le comunità che insistono su quel territorio.

na, sebbene siano volti alla riduzione di fenomeni di marginalizzazione e degrado sociale, nonché al miglioramento della qualità del decoro urbano e del tessuto sociale ed ambientale, possono essere loro stessi fonte diretta di discriminazione e di sottrazione di spazi all'accessibilità. Mentre le città intelligenti devono essere socialmente inclusive e accessibili a tutti. Perciò la cultura tecnologica e digitale dovrebbe sempre accompagnarsi a soluzioni idonee al superamento del *digital divide*, ispirate di fatto al principio di solidarietà.

Del resto, *smartness* e *digitalization* non sono concetti pienamente assimilabili. Nella costruzione della nuova realtà urbana risultano centrali numerosi altri fattori, come quelli umani, sociali, istituzionali. In questo senso, una città non è intelligente in quanto è tecnologica, bensì è intelligente nel momento in cui, grazie al fatto di essere tecnologica, riesce a soddisfare meglio gli interessi e i diritti (o a facilitarne il soddisfacimento) di chi la vive [18].

Sotto questo profilo, le *smart cities* possono realizzare quelle condizioni di governo, infrastrutturali e tecnologiche, tali da generare anche innovazione sociale. Unicamente se davvero "sensibili" perché inclusive le città del futuro potranno essere definite effettivamente intelligenti [19]. Ciò implica riconoscere alle città un ruolo fondamentale sul piano locale nella promozione e protezione dei diritti fondamentali, riqualificando il patrimonio destinato all'edilizia residenziale sociale, rigenerando il tessuto socio-economico, incrementando l'accessibilità, la sicurezza dei luoghi e la rifunzionalizzazione di spazi e immobili pubblici. A questi obiettivi è rivolta, difatti, la rete delle *Città dei diritti umani*, in cui si concentra l'attenzione sull'individuazione di strumenti innovativi per l'incorporazione dei diritti fondamentali nei processi decisionali delle amministrazioni locali, ottimizzando la qualità dell'abitare.

Se l'obiettivo della *smart city* è migliorare la qualità della vita dei cittadini secondo il modello urbano della città intelligente, inclusiva e sostenibile, il prezzo da pagare è quello della riservatezza e della sicurezza dei dati. Il funzionamento dei dispositivi *smart* richiede una mole cospicua di informazioni di cui alimentarsi. È chiaro che, benché connessi con sistemi pubblici, permane il rischio di un uso improprio di questi dati. Le applicazioni e intersezioni spesso risultano complesse e macchinose, poco chiare all'occhio del cittadino.

---

[18] Dal che consegue un diverso significato da attribuire agli interventi di digitalizzazione funzionali alla trasformazione del tessuto urbano, prendendo atto che la rivoluzione tecnologica delle attività e dei servizi deve essere considerata uno strumento a disposizione e non un obiettivo da raggiungere.

[19] Tali necessità sono state messe in evidenza anche dalle Nazioni Unite, le quali, tra i principi per la implementazione della *New Urban Agenda* del 2016, hanno precisato che «*le città sono per la gente*», e hanno incluso il criterio di «*providing equal access for all to physical and social infrastructure and basic services*».

Per garantire trasparenza, tracciabilità e sicurezza del metodo (e della metodologia) informatica, tutelando i diritti fondamentali, serve una progettazione adeguata dei servizi intelligenti al pubblico. Per questa ragione, nella Proposta di regolamento sull'approccio europeo all'Intelligenza Artificiale (COM/2021/206 final) del 21 aprile 2021 la Commissione europea ha circondato di garanzie i sistemi di intelligenza artificiale "*ad alto rischio*" a protezione dei diritti essenziali maggiormente esposti [20].

Al riguardo, ad esempio, l'uso da parte delle pubbliche amministrazioni delle tecniche di riconoscimento facciale deve essere rispettoso del principio di proporzionalità, essere soggetto a garanzie procedimentali e sottoposto a controllo da parte di autorità indipendenti, per non compromettere il rapporto tra Stato e cittadino, secondo quanto messo in evidenza dall'Agenzia Europea per i diritti fondamentali [21].

---

[20] Come evidenziato in M. MACCHIA, A. MASCOLO, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in *Giorn. dir. amm.*, 2022, p. 556 ss., sono vietati in termini assoluti i sistemi che mirano a manipolare in base a tecniche subliminali la condotta delle persone oppure fanno leva sulle vulnerabilità di alcuni soggetti al fine di condizionarne la condotta e provocare un danno fisico o psicologico all'utente o ad un'altra persona (art. 5, lett. a e b). Vengono, invece, proibiti soltanto in linea di principio i sistemi di IA utilizzati «*da parte di autorità pubbliche o per loro conto*» per stabilire l'affidabilità delle persone in base alla loro condotta sociale o alle caratteristiche personali (art. 5, lett. c). Questi applicativi sono proibiti solo se esse determinano un trattamento pregiudizievole o, comunque, sfavorevole in un contesto scollegato a quello in cui i dati sono stati generati oppure ad un trattamento pregiudizievole che sia ingiustificato o sproporzionato rispetto alla condotta sociale e alla sua gravità. È infine vietato anche l'uso di sistemi di identificazione biometrica in modalità *real time* in spazi aperti al pubblico per finalità di polizia (art. 5, lett. d), salvo che non siano strettamente necessari per la ricerca mirata di potenziali vittime di azioni criminose, come bambini scomparsi, per la prevenzione di un pericolo specifico, sostanziale e imminente alla vita o alla sicurezza di una persona o di un attacco terroristico o, infine, per la individuazione, localizzazione o incriminazione di un soggetto sospetto di reati previsti dall'art. 2(2) della decisione quadro del Consiglio 2002/584 per i quali lo Stato membro interessato preveda una pena detentiva pari o superiore a tre anni. In tali ipotesi, l'autorità pubblica deve graduarne l'utilizzo tenendo conto della «gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema» nonché delle relative possibili implicazioni per i diritti e le libertà delle persone coinvolte.

[21] L'Agenzia ritiene necessario per regolamentare la diffusione e l'uso delle tecnologie di riconoscimento facciale un quadro giuridico chiaro e dettagliato, che stabilisca quando l'elaborazione delle immagini del volto è necessaria e quali presupposti devono sussistere affinché possa considerarsi proporzionata. Secondo l'Agenzia particolare importanza deve essere assunta dalla valutazione di impatto delle misure e delle norme adottate. Come si legge nel documento «*le autorità pubbliche devono ottenere dall'industria tutte le informazioni necessarie per effettuare una valutazione dell'impatto sui diritti fondamentali dell'applicazione delle tecnologie di riconoscimento facciale che intendono acquisire e utilizzare*». Inoltre, l'Agenzia fa una distinzione tra l'elaborazione delle immagini del volto a fini di verifica e quella ai fini di identificazione. Nel caso dell'identificazione, poiché il rischio di interferenze con i diritti fondamentali è maggiore,

Nei sistemi tecnologici delle *smart city* i temi dell'accesso e dell'uso dei dati privati sono amplificati. Per un verso, l'acquisizione dei dati avviene senza il consenso degli interessati, né soluzioni di prestazione del consenso sono immaginabili in questo settore. È innegabile per giunta, come sopra evidenziato, che vi sia il coinvolgimento delle società private nell'elaborazione dei *software* di intelligenza artificiale, a cui segue un rischio di privatizzazione dei dati dei cittadini o di affidamento degli stessi a terzi.

Per un altro verso, fatta eccezione per i sistemi di riconoscimento facciale, molti dati che servono ad alimentare le città intelligenti sono anonimi, come quelli rilevati dai sensori, il che potrebbe essere sufficiente a proteggere la riservatezza dei cittadini.

In conclusione, rispetto alle potenzialità delle nuove tecnologie e ai benefici che queste possono generare, l'uso degli strumenti di intelligenza artificiale, che le città *smart* fanno, non può implicare un deficit sulle garanzie imprescindibili nel rapporto tra Stato e cittadino. Né può dar luogo a squilibri autoritari tra pubblici poteri e individui. Per raggiungere questo obiettivo è necessaria anzitutto la trasparenza, in termini del diritto ad essere informati sulle modalità di raccolta dei dati (benché anonimi), sul loro accesso e sul loro eventuale impiego in altri contesti. L'opacità del funzionamento nel caso deve essere superata dalla previsione di misure di partecipazione funzionali a garantire agli interessati una consapevolezza in merito alla gestione dei propri dati, alla verificabilità del procedimento e alla comprensione della decisione finale.

Particolare attenzione deve essere posta, infine, alle garanzie procedimentali e ai controlli, soprattutto nella fase di monitoraggio da affidare ad organi quanto più possibile neutrali. Nel bilanciamento tra opposti interessi, la previsione di garanzie procedimentali rappresenta un efficace antidoto affinché nessun interesse debba essere eccessivamente sacrificato nel rispetto del principio di proporzionalità [22]. La partecipazione informata del privato riconfigura

il test di necessità e proporzionalità deve essere più rigoroso. In particolare, l'utilizzo di "tecnologie di riconoscimento facciale dal vivo" utilizzato dalle forze di sicurezza dovrebbe essere utilizzato solo in casi eccezionali, ad esempio per combattere il terrorismo o individuare persone scomparse e vittime di reato.

[22] Secondo l'art. 8 della Convenzione europea per i diritti dell'uomo, l'interferenza pubblica nella vita privata di un soggetto è ammessa solo se ricorre un interesse pubblico che la giustifichi. L'esistenza di un interesse pubblico è un presupposto necessario, ma non sufficiente a concludere per la legittimità dell'interferenza pubblica nella vita privata ai sensi della disciplina CEDU. In presenza di una delle esigenze imperative di carattere generale di cui al secondo comma dell'art. 8, la limitazione da parte di un'autorità pubblica all'esercizio del diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza è ammissibile purché la misura sia prevista dalla legge e costituisca «una misura necessaria in una società democratica». Il provvedimento adottato deve essere strettamente necessario e pro-

l'equilibrio oggetto del procedimento amministrativo, tra i diversi interessi pubblici e privati coinvolti, bilanciando la ricerca dell'efficienza dell'azione amministrativa con le esigenze di garanzia e imparzialità della decisione. Le amministrazioni devono dichiarare che la misura intrapresa è proporzionata in relazione allo scopo, e che nella stessa di faccia uso dei dati necessari per l'esecuzione delle analisi dei rischi, senza che sussista una misura meno invasiva per gli interessati, ugualmente idonea a soddisfare lo scopo. In questo senso, ogni aspetto del funzionamento della macchina algoritmica è rilevante e può giustificare la necessità di maggiori garanzie. Perciò, è innegabile che dalle esperienze straniere debba essere tratta linfa per individuare delle *best practice* sulla base delle informazioni e delle sperimentazioni condotte a livello nazionale.

porzionale allo scopo di modo che tra l'interesse generale perseguito e l'interesse dell'individuo alla tutela della propria vita privata e familiare sia garantito un "giusto equilibrio".

Ovviamente si chiede il rispetto anche dei principi del GDPR in materia di trattamento dei dati personali: dal principio del necessario consenso dell'interessato come base per l'elaborazione dei dati, a quelli di responsabilità, trasparenza, limitazione delle finalità e minimizzazione degli stessi, e la tutela dei diritti fondamentali, innanzitutto del diritto alla vita privata, in virtù del quale l'individuo dovrebbe avere la ragionevole aspettativa di essere in grado di dare seguito ai propri dati personali e di essere informato sul loro trattamento.

LA *SMART CITY* COME ECOSISTEMA DIGITALE. PROFILI DI *DATA GOVERNANCE*

di *Valentina Pagnanelli*[1]

SOMMARIO: 1. Introduzione: alla ricerca di un quadro regolatorio per le *smart cities*. – 2. Coordinate per la regolazione delle *smart cities*. La strategia europea declinata nelle città intelligenti. – 3. Le proposte di *Artificial Intelligence Act* e *Data Act*. – 4. Conclusioni: prospettive e criticità per lo sviluppo degli ecosistemi digitali urbani.

1. *Introduzione: alla ricerca di un quadro regolatorio per le* smart cities

Dietro al label "*smart city*" si sommano decine di diverse definizioni della Città intelligente. Alcune di esse si basano sugli obiettivi che la città si pone di raggiungere, altre sui servizi implementati, oppure sull'uso più o meno massiccio delle nuove tecnologie nella fase di elaborazione di nuove politiche o ancora sulla partecipazione dei cittadini alla vita della comunità. Effettivamente non esiste un modello i cui parametri siano condivisi in modo sufficientemente consolidato da poter consentire, sulla base di quegli stessi parametri, di svolgere una verifica del grado di realizzazione di una *smart city*.

Nel 2021 la Commissione per lo sviluppo regionale (REGI) del Parlamento Europeo ha pubblicato i risultati di una ricerca sull'utilizzo dell'Intelligenza Artificiale nello sviluppo urbano[2]. Lo studio esamina l'impatto dell'Intelligenza Artificiale sulla coesione socio-economica e territoriale all'interno delle aree urbane e tra di esse[3]. Dal report emerge chiaramente come l'enorme mole di

---

[1] Una versione più ampia di questo scritto è apparsa in *dirittifondamentali.it*, fascicolo 2/2023, 12 giugno 2023, p. 188 ss.

[2] L. COLNOT, L. DELPONTE J. PELLEGRIN, *Artificial Intelligence and Urban Development*, reperibile al link *https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690882/IPOL_STU(2021)690882_EN.pdf.*

[3] Cfr. V. PAGNANELLI, *Intelligenza artificiale e sviluppo urbano. Lo studio del Parlamento eu-*

dati prodotti nello svolgimento della vita cittadina[4] possa essere sfruttata al meglio attraverso l'applicazione ai *big data* di una combinazione di mezzi e tecnologie (*Artificial Intelligence*, infrastrutture telco, *cloud* …). Le applicazioni concrete spaziano dalla sanità, alla sicurezza, alla mobilità, all'energia, fino ad incidere sul miglioramento dei profili di gestione della città, sul *policy-making*, sullo sviluppo di nuovi servizi, sulla creazione di nuove opportunità economiche[5].

A questi ambiti "tradizionali" si sono aggiunte di recente numerose altre declinazioni delle c.d. soluzioni *smart*, diffusesi rapidamente per rispondere a esigenze e bisogni contingenti. La pandemia di Covid-19, e poi il riaffacciarsi prepotente degli scenari bellici alle porte dell'Unione Europea, hanno imposto cambiamenti repentini[6] e talvolta drastici di abitudini, prassi, equilibri consolidati per decenni, accelerando il percorso di ripensamento delle strategie globali e locali[7], sino ad intaccare la dimensione urbana e le modalità di erogazione dei servizi: la crisi energetica ad esempio ha richiesto una gestione "intelligente" dei consumi, in gran parte nelle mani delle amministrazioni locali[8].

---

ropeo, in *Laboratorio sulla Transizione Digitale, https://www.civiltadellemacchine.it/*, 15 dicembre 2021.

[4] Sull'utilizzo di *big data* e sistemi di intelligenza artificiale nella predisposizione dei servizi e nella elaborazione di politiche nei contesti urbani si veda S. RANCHORDAS, A. KLOP, *Data-driven regulation and governance in smart cities,* in *University of Groningen Faculty of Law Legal Studies Research Paper Series*, 7/2018, p. 1 ss.

[5] «*I dati sono la linfa vitale dello sviluppo economico: sono la base di molti nuovi prodotti e servizi e generano guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici, rendendo possibili prodotti e servizi più personalizzati, un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici. […] La disponibilità di dati è essenziale per l'allenamento dei sistemi di intelligenza artificiale […]*», cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - "Una strategia europea per i dati"*, COM(2020) 66 final, 19 febbraio 2020.

[6] Cfr. P. COSTANZO, *Lo "Stato digitale"*, in P. COSTANZO, P. MAGARÒ, L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, p. 13.

[7] Si vedano, per tutti, i volumi *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, a cura di A. PAJNO, L. VIOLANTE, Bologna, 2021; in particolare il contributo di A. PATANÈ, *Democrazia rappresentativa durante la pandemia: il ruolo dei consigli regionali*, vol. I, p. 269 ss.

[8] La trasformazione digitale della pubblica amministrazione ha modificato «*la struttura del sistema di produzione e distribuzione dell'energia, dando la stura a sistemi locali di produzione e di regolamentazione, "agevolando la gestione collettiva ed economica di produzione e di consumo attraverso reti intelligenti"*», cfr. F.F. PAGANO, *Pubblica amministrazione e innovazione tecnolo-*

Per ciò che più interessa ai fini della presente trattazione, il report della Commissione REGI ha evidenziato come l'azione strategica dell'Unione Europea non abbia posto una attenzione specifica allo sviluppo dell'Intelligenza Artificiale nelle *smart cities*, rispetto alle quali non esistono riferimenti normativi e regolamentari *ad hoc*[9].

L'assenza di un quadro normativo specifico può essere spiegata, a parere di chi scrive, in ragione della varietà di forme che la Città intelligente può assumere. L'aggettivo "*smart*" può essere attribuito ad un ventaglio amplissimo di applicazioni concrete, che spaziano dai sistemi di video-sorveglianza (anche biometrica), alle *smart grids* in grado di controllare i consumi e regolare l'utilizzo dell'energia elettrica, ai sensori che rilevano l'inquinamento atmosferico, ai sistemi integrati di *smart mobility*, sino alla prenotazione di prestazioni sanitarie[10].

Questo contributo vorrebbe ricondurre le *smart cities* entro una griglia di regole applicabili a fattispecie anche differenti – come differenti sono i "modelli" di Città intelligente[11] – ma accomunate dalla presenza di due caratteri-

---

gica, in P. COSTANZO, P. MAGARÒ, L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, pp. 301-311.

[9] Secondo E. SPILLER, «*la disciplina di settore spesso consiste in una sorta di* patchwork *in cui si tenta di assemblare gli istituti necessari alla realizzazione di diversi progetti*», cfr. *Citizens in the loop? Partecipazione e Smart city*, in F. PIZZOLATO, A. SCALONE, F. CORVAJA (a cura di), *La città e la partecipazione tra diritto e politica*, Torino, 2019, p. 289. La recente pubblicazione dello studio *Social approach to the transition to smart cities* (che può essere consultato al link *https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2023)737128*) da parte del Parlamento europeo – Panel for the Future of Science and Technology (STOA), conferma che il tema tende ad essere affrontato principalmente attraverso studi tematici, finalizzati alla elaborazione e condivisione di buone pratiche e alla proposta di *policy options* (si vedano a proposito i capitoli 3 e 4 dello studio, p. 30 ss.).

[10] Nel tempo si sono susseguiti numerosi tentativi di definizione. Alcuni autori sostenevano, già alcuni anni fa, che il termine *smart city* sarebbe ben presto incorso in obsolescenza: «*Smart city is still an evolving field, with many projects still alive; however, it is expected that the term itself will soon lose its relevance and will be superseded by a new label with new agendas, interests and technologies*», cfr. K.S. WILLIS, A. AURIGI, *Digital and Smart cities*, London-New York, 2018, p. 16.

[11] Uno degli approcci definitori descrive la *smart city* come «*un sistema di sviluppo che si caratterizza per un insieme di strategie di pianificazione urbanistica tese all'ottimizzazione e all'innovazione dei servizi pubblici allo scopo di mettere in relazione le infrastrutture materiali delle città con il capitale umano, intellettuale e sociale di chi le abita in ragione del ricorso diffuso alle nuove tecnologie della comunicazione, della mobilità e dell'efficienza energetica*», v. F.F. PAGANO, *Pubblica amministrazione e innovazione tecnologica*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, pp. 311-312. A parere di chi scrive, sebbene la descrizione proposta sia condivisibile, una impostazione incentrata sulle finalità o sui settori di svi-

stiche essenziali, cioè la digitalizzazione e l'uso delle nuove tecnologie, in particolare l'Intelligenza Artificiale [12]. La città "funziona" in quanto le persone che la popolano [13], gli enti pubblici, le società private, in diversa misura si fanno attori e fruitori di un ecosistema digitale [14].

La componente datificata della Città, insieme ai sistemi di Intelligenza Artificiale utilizzati per estrarne conoscenza, saranno dunque i due riferimenti rispetto ai quali nei prossimi paragrafi si cercherà di individuare, senza pretesa di esaustività, le coordinate normative imprescindibili a partire dalle quali ogni *smart city* è chiamata a definire il proprio modello di *data governance.* Basandosi sul combinato disposto delle norme, principalmente di matrice europea, che disciplinano la raccolta, l'utilizzo, il riutilizzo, la condivisione e la conservazione dei dati, personali e non personali, infatti ogni Città [15], più o meno "intelligente" è tenuta a organizzare i flussi di dati nel modo più adeguato al conseguimento dei propri fini, garantendo al contempo il rispetto dei diritti e delle libertà di tutti gli attori che popolano l'ecosistema digitale urbano.

---

luppo della Città intelligente rischia di escluderne *a priori* alcune declinazioni non appartenenti alla casistica dei primi "prototipi" di *smart city* ma invece oggetto di implementazione grazie al progredire dei progetti.

[12] Lo sviluppo di una *smart city* dipende infatti dalla disponibilità di ingenti quantità di dati, costantemente aggiornati e provenienti da diverse fonti, insieme alla capacità di elaborazione di tali dati attraverso tecniche di *data mining* oltre che dalla possibilità di utilizzo della stessa "materia prima" per addestrare sistemi di apprendimento automatico, anche ad un livello "profondo" (*deep-learning*), basato su interconnessioni che riproducono le reti neurali del cervello umano. J. BURREL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & Society* 3 (2016), 1, pp. 1-12.

[13] Non solo cittadini ma anche turisti, pendolari, *city-users*.

[14] La Commissione Europea nella Comunicazione "*Costruire un'economia dei dati europea*" afferma che i dati sono diventati una risorsa essenziale, e l'analisi dei dati offre potenzialità enormi in vari campi, tra cui lo sviluppo delle *smart cities*, cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - "Costruire un'economia dei dati europea"*, COM(2017) 9 final, 10 gennaio 2017.

[15] Tutti i richiami alla Città o alla *smart city* contenuti in questo elaborato devono intendersi come riferiti alla dimensione territoriale e alla definizione giuridica del Comune come risultanti dal Testo Unico degli Enti Locali, d.lgs. n. 267/2000.

2. *Coordinate per la regolazione delle* smart cities*. La strategia europea declinata nelle città intelligenti*

Nel *Libro bianco sull'Intelligenza artificiale* [16] pubblicato nel febbraio 2020, la Commissione Europea ha chiarito che la massima valorizzazione del patrimonio informativo [17] e un deciso investimento sullo sviluppo dei sistemi di Intelligenza Artificiale sono gli ingredienti fondamentali per garantire all'Unione di giocare un ruolo da protagonista nel *Global market*.

Il primo dei due obiettivi rappresenta la condizione necessaria al raggiungimento del secondo [18], poiché i risultati raggiunti nel campo dell'Intelligenza Artificiale negli ultimi decenni sono dovuti, in gran parte, alla disponibilità dei *big data* [19], necessari per sviluppare, allenare, verificare il funzionamento di *software* di IA sempre più sofisticati.

Il percorso per assicurare, entro lo spazio giuridico europeo la circolazione

---

[16] COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale – "Un approccio europeo all'eccellenza e alla fiducia"*, COM(2020) 65 final, 19 febbraio 2020.

[17] «*Iniziano solo ora ad emergere sia l'enorme diversità delle fonti e dei tipi di dati, sia la ricchezza di possibilità di sfruttamento di quei dati in tutta una serie di settori, anche per l'elaborazione di politiche pubbliche. Per trarre vantaggio da tali opportunità, i soggetti attivi pubblici e privati del mercato dei dati devono poter accedere a insiemi di dati vasti e diversificati*», cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Costruire un'economia dei dati europea"*, 10 gennaio 2017, COM(2017) 9 final, 4.

[18] «*Il valore dei dati risiede nel loro utilizzo e riutilizzo. I dati attualmente disponibili non sono sufficienti per un riutilizzo innovativo, ed esempio per lo sviluppo dell'intelligenza artificiale*», cfr. *Comunicazione 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, 7.

[19] Sui *big data*, *ex plurimis*: AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, giugno 2018; S. BAROCAS, A.D. SELBST, *Big data's disparate impact*, in *California Law Review*, 104 (2016), 3, pp. 671-732; G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 447 ss.; F. DI PORTO (a cura di), *Big data e concorrenza,* in *Concorrenza e mercato*, n. spec. 23/2016, p. 5 ss.; M. DELMATRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019; S. FARO, N. LETTIERI, *Big Data: una lettura informatico-giuridica*, in *Scritti per Luigi Lombardi Vallauri*, vol. 1, Padova, 2016, p. 503 ss.; R. KITCHIN, G. MCARDLE, *What makes Big Data, Big Data?,* in *Big Data & Society*, 2016; A. MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, 34 (2018), 4, pp. 754-772; F. PASQUALE, *The black box society. The Secret Algorithms that control money and information*, Cambridge, 2015.

dei dati personali e non personali [20] e l'apertura e il riutilizzo dei dati del settore pubblico sempre più incisivi ed efficaci si era già avviato ben prima della capillare diffusione sulla scena mondiale dei sistemi di Intelligenza Artificiale [21]. Questi testi normativi, che di seguito richiameremo, costituiscono il nocciolo duro incomprimibile sulla base del quale le Città debbono costruire il loro modello di governo dei dati; si tratta adempimenti di non poco conto, data la mole e la varietà di dati – non solo personali – che vengono raccolti e trattati nei Comuni [22], con i conseguenti gravi rischi che potrebbero derivare da una loro perdita, modifica, o da un loro uso malevolo o criminoso.

***

Le norme fondamentali in materia di trattamento dei dati personali sono contenute nel Regolamento 2016/679 [23], il cui scopo è di agevolare la libera

[20] Sulla libera circolazione dei dati: M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza regole*, 2/2019, p. 293 ss.; R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019; S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Rivista critica di diritto privato*, 1984.

[21] Cfr. V. PAGNANELLI, *Il settore pubblico alla sfida dell'Intelligenza artificiale*, in C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021*, Milano, 2022, p. 159 ss.

[22] L'art. 3 del Testo Unico degli Enti Locali, d.lgs. n. 267/2000, affida ai Comuni, il compito di curare gli interessi e promuovere lo sviluppo della comunità, e i successivi artt. 13 e 14 elencano le funzioni proprie («*Spettano al comune tutte le funzioni amministrative che riguardano la popolazione ed il territorio comunale, precipuamente nei settori organici dei servizi alla persona e alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico*») e delegate dallo Stato («*Il comune gestisce i servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica*»), v. M. CLARICH, *Manuale di diritto amministrativo*, Bologna, 2013, p. 333. Sulla scelta da parte del legislatore costituzionale di una «*tendenziale competenza amministrativa generale dei Comuni*» cfr. P. CARETTI, U. DE SIERVO (a cura di), *Diritto costituzionale e pubblico*, Torino, 2020, p. 411.

[23] *Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*. Per una introduzione: G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Torino, 2019, p. 1 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, p. 106 ss.

circolazione dei dati personali, garantendo al contempo la tutela dei diritti e delle libertà delle persone. Il GDPR predispone un apparato di principi e regole applicabili a persone fisiche o giuridiche, soggetti pubblici o privati, senza significative differenze nella quantità di requisiti di adeguamento richiesti, , salvo che per casi particolari [24].

Il principio dell'*accountability*, introdotto agli artt. 5 e 24 [25], responsabilizza il Titolare del trattamento, che, effettuata una analisi del rischio, dovrà predisporre tutte le misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare il rispetto dei principi in materia di protezione dati. I principi della *privacy by design* e per impostazione predefinita [26] anticipano

---

[24] Quali la nomina del Responsabile per la Protezione dei Dati, obbligatoria solo per i soggetti pubblici, oppure nel caso in cui le attività principali svolte dal titolare o dal responsabile comportino il monitoraggio regolare e sistematico degli interessati su larga scala, o le attività principali consistano in trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali e reati, v. art. 37, par. 1; si vedano, *ex plurimis*, A. AVITABILE, *Il responsabile della protezione dei dati*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, Torino, 2019, p. 355 ss.; L. FEROLA, *La "nuova" figura del Responsabile della Protezione dei Dati personali e le sue caratteristiche*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, p. 347 ss.; oppure la tenuta di un Registro dei trattamenti, obbligatoria per titolari del trattamento con più di duecentocinquanta dipendenti, «*a meno che il trattamento che esse effettuano non possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati […] o i dati personali relativi a condanne penali e a reati […]*», v. L. BOLOGNINI, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, p. 226 ss.

[25] Sul principio di *accountability* v. G. MALGIERI, *Art. 5*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, pp. 189-190; F. PIZZETTI, L. GRECO, *Art. 24*, *ivi*, p. 405 ss.; G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Torino, 2019, p. 1 ss.; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, 2017, p. 128 ss.

[26] GDPR, «Art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita – 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garan-

l'intervento del *Data controller* ad una fase anteriore al trattamento dei dati personali, cioè al momento della progettazione di un nuovo servizio. Questi brevi cenni sui principi e gli obblighi di *compliance* imposti dal GDPR, confermano quanto la normativa sulla *data protection* possa incidere nella realizzazione – progressiva – di servizi basati sull'utilizzo dei dati all'interno di un Comune.

Infatti il Regolamento UE 2016/679 assegna al Comune in qualità di Titolare del trattamento[27], e, a norma dell'art. 107 del TUEL, ai dirigenti dell'ente, la responsabilità di regolare i flussi di dati personali garantendone la riservatezza e la sicurezza, e assegna a questi soggetti il compito di individuare all'uopo misure adeguate a ridurre i rischi (misure che non sono indicate *a priori* dal legislatore[28]).

Nell'ecosistema digitale urbano una rigorosa suddivisione delle responsabilità relative al trattamento dei dati personali è di cruciale importanza. Infatti, sebbene il *Data controller* sia il primo responsabile per la tutela dei diritti e delle libertà degli individui i cui dati sono oggetto di trattamento, in misura differente saranno responsabili anche il *Data processor*, i contitolari e le persone autorizzate al trattamento dei dati personali[29]. Il reticolo delle relazioni tra i soggetti appena menzionati richiede di essere cristallizzato in atti giuridici dai quali emerga con chiarezza il criterio di imputazione di ogni attività di trattamento ad un soggetto giuridico identificato. Ciò significa che all'interno

---

tire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica […]». Per un commento si veda D. FARACE, *Privacy by design e privacy by default*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 485 ss.

[27] Cfr. GDPR, art. 4 par. 1 n. 7: Il Titolare del trattamento è la persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

[28] Come avveniva invece in vigenza del Codice privacy, prima che fosse modificato dal d. lgs. n. 101/2018, quando le misure *minime* di sicurezza erano indicate nell'*Allegato B*

[29] Sui c.d. Ruoli privacy si vedano: A. D'OTTAVIO, *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, p. 143 ss.; L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Torino, 2019, p. 321 ss.; N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data protection officer*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 115 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 196 ss.

di un Comune tutte le mansioni attribuite a ciascun dipendente dovranno essere periodicamente riesaminate per verificare quali siano i trattamenti effettuati da ciascun soggetto e procedere di conseguenza all'atto formale di nomina, contenente istruzioni dettagliate per il corretto trattamento dei dati personali.

Di più. Tali adempimenti valgono per l'organizzazione interna del Titolare ma anche nei rapporti del Titolare con soggetti esterni.

Gli esempi di trattamenti che, nella *smart city*, vedono coinvolti attori interni ed esterni all'organizzazione dell'ente, e soggetti pubblici e privati, sono molteplici. Si pensi a tutte le attività per le quali il Comune necessita dei servizi di aziende IT per fornire le proprie prestazioni; oppure a molti altri servizi, dalla mobilità agli asili nido, che sono forniti da società partecipate o cooperative, con flussi di dati anche particolarmente sensibili (quali quelli di minori, o persone con disabilità), che impongono al Titolare di cristallizzare il riparto delle responsabilità e di effettuare controlli ed audit sulle misure di sicurezza applicate. Nell'ecosistema digitale a ciascun soggetto coinvolto nella realizzazione dei servizi (aziende private, professionisti, società partecipate, società *in-house*, Comuni limitrofi …) sarà attribuito un *ruolo privacy*, con i conseguenti obblighi di *compliance*.

Non potendo in questa sede addentrarci in dettagli tecnici, sia consentito solo brevemente evidenziare come all'interno dell'ecosistema digitale urbano uno stesso attore, quale ad esempio una società fornitrice di servizi IT, rivestirà con ogni probabilità il doppio ruolo di titolare del trattamento e di responsabile del trattamento nei confronti del Comune, per i servizi ad esso erogati (e dunque per il trattamento dei dati svolto "per conto" del Comune medesimo[30]).

La circolazione dei non-personal data è garantita dal Regolamento 2018/1807[31], c.d. FFD (*Free Flow Data Regulation*). Per assicurare il libero scambio transfrontaliero di dati, l'articolo 4 vieta agli Stati membri di imporre al proprio interno obblighi di localizzazione, fatte salve le necessità di sicurezza pubblica. L'indicazione di maggior rilievo in merito alla *data governance* dell'ecosistema digitale urbano è contenuta nell'art. 2 par. 2, ove vengono delineate le regole di gestione degli insiemi di dati misti. La norma stabilisce che ove all'interno di uno stesso insieme non sia possibile scindere i dati personali da

[30] GDPR, art. 4, n. 8, Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

[31] *Regolamento UE 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*. Si veda S. TORREGIANI, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in *Federalismi.it*, 10 giugno 2020.

quelli non personali, in quanto indissolubilmente legati, all'intero *dataset* verrà applicata la disciplina più tutelante per le persone fisiche, quella contenuta nel GDPR.

Gli insiemi di dati misti peraltro rappresentano la stragrande maggioranza dei *set* di dati[32], e con ogni probabilità rappresentano anche la maggioranza dei flussi di dati che alimentano le *smart cities.* Ad esempio, in un sistema integrato di mobilità, dati aggregati relativi al trasporto pubblico urbano (i dati sull'accesso dei viaggiatori alla rete tramviaria) potrebbero essere analizzati congiuntamente a dati relativi all'utilizzo del *bike-sharing*. In questa seconda ipotesi il processo di identificazione dell'interessato-fruitore del servizio risulterebbe molto meno complesso rispetto al primo[33].

***

L'esempio della mobilità urbana torna utile anche per evidenziare l'importanza delle politiche di apertura del patrimonio informativo del settore pubblico. Invero la disponibilità di dati relativi agli spostamenti che avvengono nell'area cittadina, corredati da informazioni su orari, tipologia di viaggiatori e destinazioni, potrebbe consentire a imprese private di sviluppare e proporre nuovi servizi e nuove soluzioni per una mobilità intelligente. Negli anni si è consolidata la filosofia degli *Open data*[34], che ha consentito al settore privato di accedere a molti dati che non presentano caratteristiche critiche che ne ostacolino la condivisione[35].

La Direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico[36] è stata emanata proprio al fine di «*sfruttare*

---

[32] Cfr. COMMISSIONE EUROPEA*, Comunicazione della Commissione al Parlamento europeo e al Consiglio – "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union"*, COM(2019) 250 final, p. 8 ss.

[33] Sul tema della reidentificazione v. Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 5/2014 sulle tecniche di anonimizzazione*, 10 aprile 2014.

[34] V. R. MARZO, *Dati e Open Data: polifunzionalità e rilevanza costituzionale?*, in P. COSTANZO, P. MAGARÒ, L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022., p. 447 ss.; C. ROMANO, *Open data e riutilizzo nel decreto trasparenza: propulsore per la democrazia e lo sviluppo o sfida ulteriore per i diritti fondamentali?*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2017, p. 263 ss.; V. PAGNANELLI, *Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, in *Giornale di storia costituzionale*, 31/2016, p. 205 ss.

[35] Dati personali, dati protetti da diritto d'autore, dati secretati…

[36] *Direttiva UE 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.*

appieno il potenziale dell'informazione del settore pubblico a vantaggio dell'economia e della società europee»[37]. Il patrimonio informativo pubblico viene considerato «*una fonte straordinaria di dati in grado di contribuire a migliorare il mercato interno e lo sviluppo di nuove applicazioni*» mentre l'utilizzo dei dati attraverso sistemi di Intelligenza Artificiale «*può trasformare tutti i settori dell'economia*[38]».

Nelle *smart cities* l'accesso ai *big data* pubblici e la possibilità di riutilizzo di molte informazioni rappresenta un fattore abilitante per le imprese ed i singoli. Infatti il cittadino e l'imprenditore possono, grazie alla conoscenza, agire direttamente nella gestione della *res publica*[39], in ossequio all'art. 118 IV comma della Costituzione italiana[40] e al principio di sussidiarietà orizzontale in esso promosso.

Con il fine di allargare il bacino dei dati pubblici accessibili e utilizzabili, il *Data Governance Act*[41] integra oggi la Direttiva 2019/1024, stabilendo regole per il riutilizzo, a determinate condizioni, dei dati detenuti da enti pubblici che siano soggetti a diritti di terzi[42].

Il *Data Governance Act* mira a promuovere la disponibilità ed il migliore utilizzo dei dati[43] in favore di nuovi soggetti economici e attori pubblici. L'obiettivo è quello di contrastare le *Big Tech* in ottica pro-concorrenziale, e al contempo consentire la definizione degli indirizzi politici sulla base – anche – di quelle informazioni[44]. Questo scopo può essere ottenuto attraverso diversi

---

[37] Direttiva 2019/1024, Considerando 4.

[38] Direttiva 2019/1024, Considerando 9. La varietà di informazioni che il settore pubblico raccoglie, produce, riproduce e diffonde è richiamata nel Considerando 8. Si tratta di «*informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione*».

[39] G. URBANO, *Le "Città intelligenti" alla luce del principio di sussidiarietà*, in *Istituzioni del federalismo*, 2019, p. 474.

[40] C. CLARICH, *Manuale di diritto amministrativo*, Bologna, 2013, pp. 156-157; B. DI GIACOMO RUSSO, *Il principio di sussidiarietà orizzontale nell'ordinamento italiano: analisi e prospettive*, Lecce, 2022.

[41] *Regolamento UE 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento UE 2018/1724 (Data Governance Act).*

[42] Si tratta dei dati protetti per motivi di riservatezza commerciale, riservatezza statistica, protezione della proprietà intellettuale, protezione dei dati personali. Cfr. *Data Governance Act*, art. 3, par. 1.

[43] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale,* in *Studi parlamentari e di politica costituzionale*, 209, 1° semestre 2021, p. 40.

[44] S. SCAGLIARINI, *Identità digitale e tutela della privacy*, in P. COSTANZO, P. MAGARÒ, L.

meccanismi tra i quali la condivisione tra imprese dietro compenso, i servizi di intermediazione, la donazione dei dati da parte degli interessati su base volontaria con finalità altruistica [45].

Merita soffermarsi sull'ultima ipotesi di *data sharing* citata, il c.d. altruismo dei dati.

È bene ricordare infatti che in quelli che abbiamo definito ecosistemi digitali urbani, attori pubblici e privati interagiscono valorizzando le informazioni prodotte e condivise sul territorio [46], anche con il contributo, più o meno consapevole, dei cittadini [47].

Il Considerando 45 del DGA recita: «*L'utilizzo per obiettivi di interesse generale di dati messi a disposizione su base volontaria dagli interessati […] presenta grandi potenzialità. Tali obiettivi di interesse generale comprendono l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche europee, il miglioramento della fornitura dei servizi pubblici, o delle politiche pubbliche. […]*».

I cittadini potrebbero quindi decidere, consapevolmente, di partecipare attivamente alla costruzione dell'ecosistema digitale urbano mettendo a disposizione i propri dati senza richiedere alcun corrispettivo [48] per fini di interesse

---

TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, p. 365.

[45] *Ivi*, p. 366.

[46] Ad esempio il c.d. *Gemello Digitale* della città consente di monitorare e governare una città e i suoi servizi correlando informazioni raccolte sul territorio in tempo reale.

[47] Sulla scarsa consapevolezza degli individui rispetto al trattamento dei propri dati personali, *ex plurimis*, A. FONZI, *Il principio di autodeterminazione dell'utente al cospetto delle nuove tecnologie*, in *dirittifondamentali.it*, 3/2021, 20 dicembre 2021, p. 570 ss.; C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, fascicolo speciale, maggio 2019, p. 107; V. PAGNANELLI, *Una "valutazione d'impatto" della privacy sulle Big Tech. Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, p. 19 ss. Si veda anche l'Interim report sui Big Data di Agcom ove si legge che le sorgenti di dati digitali strettamente legate agli individui (connessione in rete, utilizzo della posta elettronica, uso dei servizi di telecomunicazioni mobili, sensori e sistemi di sensori) producono un costante flusso di dati di cui una parte sempre più rilevante viene raccolta senza il consenso esplicito degli utenti, in maniera passiva (i c.d. passive data), cfr. Autorità per le garanzie nelle comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 37.

[48] A. MORETTI, *Il Valore dei dati nell'European Data Strategy: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, p. 106.

generale, tra cui l'assistenza sanitaria, il miglioramento della mobilità e dei servizi pubblici.

L'art. 15 lascia agli Stati membri l'iniziativa e l'individuazione delle politiche nazionali per l'altruismo dei dati, scelta questa che sembra depotenziare l'impatto che il nuovo istituto potrebbe avere nel sistema di condivisione e governo dei dati a livello europeo.

Chiudono la rassegna dei principali atti normativi che più incidono nella configurazione del sistema di governo dei dati delle Città intelligenti due Regolamenti europei che si trovano ancora nello stadio di proposta. Si tratta del Regolamento sull'Intelligenza Artificiale e del *Data Act*, su cui ci soffermeremo nel prossimo paragrafo.

3. *Le proposte di* Artificial Intelligence Act *e* Data Act

Il Regolamento sull'utilizzo dell'Intelligenza Artificiale [49] contribuirà senza dubbio a delineare le regole del funzionamento delle *smart cities*, in ragione dei numerosi obblighi e divieti cui i soggetti pubblici, spesso più dei privati, dovranno sottostare [50].

L'Artificial Intelligence Act rileverà però anche, più specificamente, nel reticolo delle norme che serviranno a delineare il modello di *data governance* dei contesti urbani. L'articolato contiene infatti alcune disposizioni finalizzate a

---

[49] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM(2021) 206 final, 21 aprile 2021; si vedano, *ex plurimis*, C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021*, Milano, 2022; G. CERRINA FERONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, Bologna 2022; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di Intelligenza Artificiale*, in *Biolaw Journal - Rivista di BioDiritto*, 3/2021, p. 415 ss.; A. MANTELERO, *Sulle regole AI l'Europa sceglie approccio "industriale": luci e ombre*, in *AgendaDigitale*, 27 aprile 2021; A. SIMONCINI, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, in *BioLaw Journal - Rivista di BioDiritto*, 2, 2021.

[50] Non è possibile in questa sede approfondire il tema della applicazione delle regole di utilizzo dei sistemi di Intelligenza artificiale che incideranno in particolare nel settore pubblico. Questi aspetti sono stati trattati dall'A. nel contributo *Il settore pubblico alla sfida dell'Intelligenza artificiale*, in C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021*, Milano, 2022, p. 157 ss., al quale si rimanda.

regolare il trattamento dei dati utilizzati per alimentare i sistemi di IA.

L'art. 10 ad esempio pone regole di *data governance* per garantire la qualità dei dati. La norma richiede che i sistemi di IA vengano utilizzati con set di dati di addestramento, convalida e prova che siano pertinenti, rappresentativi, esenti da errori e completi [51]. Quello che potrebbe essere definito in sintesi come "principio di esattezza" è però in realtà solo apparentemente sovrapponibile a quello omonimo, enunciato nel GDPR.

Il principio di esattezza enunciato nell'AIA e quello presente nel GDPR sembrerebbero infatti non sovrapponibili. Nel Regolamento 2016/679 invero il principio di esattezza è [52] strettamente collegato alla tutela dei diritti dell'interessato – persona fisica (è proprio all'interessato che viene riconosciuto il diritto di chiedere la rettifica, l'aggiornamento, o, a determinate condizioni, la cancellazione dei dati personali che lo riguardano) [53]. È da notare come invece nell'art. 10 dell'AIA si faccia riferimento alla esattezza *tecnica* del dato. Il legislatore ha adottato in questo caso un linguaggio che attinge al lessico industriale, per riferirsi ad operazioni da compiere materialmente sui dati (*annotazione, etichettatura, pulizia, arricchimento, aggregazione*) [54] piuttosto che all'esattezza giuridica degli stessi, intesa come perfetta corrispondenza tra l'elemento informativo espresso nel dato e l'identità della persona a cui il dato si riferisce [55].

---

[51] Il paragrafo 3 richiede inoltre che i *dataset* di addestramento, convalida e prova posseggano «*proprietà statistiche appropriate*» anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema di Intelligenza Artificiale ad alto rischio è destinato ad essere usato.

[52] Il riferimento è al principio enunciato nell'articolo 5 del GDPR, *Principi applicabili al trattamento di dati personali:*

«1. I dati personali sono: […] d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»)», v. *ex plurimis* G. MALGIERI, *Articolo 5*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, p. 176 ss.; L. BOLOGNINI, E. PELINO (a cura di), *Codice della disciplina privacy*, Milano, 2019, p. 85 ss. Sul rispetto del principio di esattezza e sui diritti dell'interessato nel contesto della profilazione si vedano anche le *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679*, *WP* 251 rev.01, 2018, (Gruppo di lavoro Art. 29).

[53] Cfr. gli articoli 5, par. 1, lett. d) (principio di esattezza), 13, par. 2, lett. b) (informazione all'interessato sul diritto di rettifica), 16 (diritto di rettifica), (diritto di cancellazione) del Reg. 2016/679.

[54] G. D'ACQUISTO, *Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 265 ss.

[55] L'esattezza dei dati richiesta dalla normativa privacy è uno dei presidi posti a tutela dell'autodeterminazione informativa, su cui v. *ex plurimis*, V. ZENO-ZENCOVICH, *Il consenso in-*

L'individuazione delle catene di responsabilità nel trattamento dei dati e nell'utilizzo dei sistemi di IA potrebbe introdurre negli ecosistemi digitali urbani un ulteriore elemento di complessità. L'applicazione congiunta delle norme sui dati e sui sistemi di IA dovrebbe comportare infatti l'attribuzione dei ruoli privacy (quindi delle responsabilità per il trattamento dei dati personali) e al contempo un riparto delle responsabilità tra le figure individuate nell'AIA e coinvolte nell'utilizzo dei sistemi di Intelligenza Artificiale: produttori, fornitori, distributori, utenti.

Affinché la responsabilità per il trattamento dei flussi di dati attraverso sistemi di IA sia correttamente suddivisa tra gli attori dell'ecosistema digitale (cioè della *smart city*) la filiera dei ruoli privacy (titolari, responsabili, incaricati, oltre che DPO) dovrà dunque essere coordinata con quella i cui ruoli sono definiti nell'AIA. L'utilizzo di algoritmi di *machine-learning* e *deep-learning* potrebbe rendere ancora più difficoltosa l'individuazione dei centri di imputazione di singole attività di trattamento dati che vengono svolte. In questi casi, infatti, sono gli stessi sistemi di IA a manifestare la loro opacità rispetto ai singoli passaggi logici svolti e alle modalità del loro funzionamento [56].

***

La proposta di *Data Act* [57], ove dovesse essere approvata definitivamente nella forma attuale, avrebbe un significativo impatto sulla quantità di dati a disposizione del settore pubblico. La Legge sui dati potrebbe infatti dare la possibilità ai soggetti pubblici, anche se solo in casi limitati ed eccezionali, di

---

formato e l'autodeterminazione informativa, in *Corr. giur.*, 1997, p. 915 ss.; S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014; ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, pp. 588-589; S. NIGER, *Le nuove dimensioni della privacy: dalla riservatezza alla protezione dei dati personali*, Padova, 2006; G. VETTORI, *Privacy: un primo bilancio*, in *Riv. dir. priv.*, 1998, n. 4, p. 673 ss.

[56] Cfr. COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES (MSI-NET), Council of Europe study DGI(2017)12, *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications,* p. 38. V. anche A. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 295.

[57] *Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act)*, COM(2022) 68 final, 23 febbraio 2022.

accedere a dati detenuti dal settore privato, garantendo a questi ultimi solamente il compenso per i costi tecnici e organizzativi sostenuti per soddisfare la richiesta dell'attore pubblico [58].

Questa innovazione avrebbe certamente un effetto nello sviluppo delle *smart cities*. Occorre infatti evidenziare che nella prospettiva di crescita dei servizi di una *smart city* è di assoluta rilevanza la circostanza che vi siano sufficienti dati a disposizione della Amministrazione locale. Invero le normative volte alla apertura dei dati sono state sinora principalmente volte ad agevolare una condivisione G2B (*Government to Business*), mentre l'aspetto dei flussi digitali B2G (*Business to Government*) è rimasto in secondo piano, anche per ragioni di tutela del valore economico del patrimonio informativo detenuto dalle aziende private, compresa la protezione di segreti industriali e proprietà intellettuale [59]. La proposta di *Data Act* mira a riequilibrare la ripartizione del valore dei dati [60].

Nella Comunicazione *Una strategia europea per i dati* [61] la Commissione Europea aveva posto l'attenzione sulla necessità di elaborare un quadro normativo per disciplinare il riutilizzo da parte del settore pubblico di dati detenuti dai privati, evidenziando come i dati a disposizione del settore pubblico fossero insufficienti sia per migliorare l'elaborazione di nuove politiche e di servizi pubblici che per potenziare la tempestività e la rilevanza delle statistiche ufficiali [62].

Il *Data Act* sembrerebbe ora poter incidere su questo aspetto con l'introduzione di un obbligo di "messa a disposizione" dei dati detenuti da soggetti privati in favore di soggetti pubblici, nei soli casi in cui sia dimostrata una necessità eccezionale di utilizzare tali dati [63]. Circostanza questa che potreb-

---

[58] Cfr. Proposta di Data Act, art. 20, par. 2.

[59] «*I dati ottenuti da tali entità [imprese titolari di dati, N.d.A.] possono essere commercialmente sensibili*», Proposta di Data Act, Considerando 62.

[60] *Proposta di Regolamento del Parlamento europeo e del Consiglio relative a norme armonizzate sull'accesso e l'uso equo dei dati, Nota esplicativa.*

[61] Per un commento v. A. MORETTI, *Il Valore dei dati nell'European Data Strategy: sviluppo della persona, dinamiche di mercato e benessere sociale*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, p. 93 ss.

[62] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - "Una strategia europea per i dati"*, pp. 8-9.

[63] Cfr. Proposta di Data Act: «*Articolo 14 – Obbligo di mettere a disposizione i dati sulla base di necessità eccezionali*

1. Su richiesta, il titolare dei dati mette i dati a disposizione di un ente pubblico o di un'istitu-

be verificarsi solo in casi eccezionali [64], per motivazioni specifiche, descritte nell'art. 15 e riassumibili nella necessità di rispondere ad una emergenza attraverso l'utilizzo per un periodo di tempo limitato di dati appartenenti a titolari privati, al fine di poter svolgere compiti di interesse pubblico previsti dalla legge, nel caso in cui il soggetto pubblico non abbia reperito i dati sul mercato o tramite altri obblighi di legge, e la procedura di "espropriazione temporanea" riduca sostanzialmente l'onere amministrativo per i titolari dei dati o altre imprese.

Le procedure di messa a disposizione e di utilizzo dei dati sono definite nel dettaglio [65], anche per quanto attiene all'eventuale risarcimento riconosciuto al titolare per i soli costi tecnici e organizzativi legati al soddisfacimento della richiesta [66].

4. *Conclusioni: prospettive e criticità per lo sviluppo degli ecosistemi digitali urbani*

Occorrerà attendere l'approvazione definitiva dei due Regolamenti appena richiamati, oltre che le prime applicazioni concrete delle regole ivi descritte per poterne valutare l'efficacia e la funzionalità per gli scopi rispetto ai quali sono state elaborate. Certamente le disposizioni che abbiamo richiamato nel paragrafo precedente sono destinate ad incidere sulla *governance* dei dati degli enti locali perché da una parte richiederanno procedure molto bene congegnate per evitare problemi di coordinamento con altre norme pure applicabili (mi riferisco qui al coordinato disposto delle disposizioni dell'AIA con tutte le norme relative ai flussi di dati).

Per quanto attiene al *Data Act* invece, all'aspetto procedurale, sicuramente

---

zione, un'agenzia o un organismo dell'Unione che dimostri la necessità eccezionale di utilizzare i dati richiesti. […]».

[64] «*In caso di emergenze pubbliche, come le emergenze sanitarie, le emergenze derivanti dal degrado ambientale e da gravi calamità naturali, comprese quelle aggravate dai cambiamenti climatici, nonché le gravi catastrofi provocate dall'uomo, come i gravi incidenti di cibersicurezza, l'interesse pubblico derivante dall'utilizzo dei dati prevale sugli interessi dei titolari dei dati a disporre liberamente dei dati in loro possesso. In tal caso è opportuno che ai titolari dei dati sia imposto l'obbligo di mettere i dati a disposizione di enti pubblici o di istituzioni, agenzie o organismi dell'Unione su loro richiesta. […]*», Proposta di Data Act, Considerando 57.

[65] Agli artt. da 17 a 20 della Proposta di Data Act.

[66] Parrebbe forse più opportuno fare riferimento ad un indennizzo.

da tenere in considerazione, si affiancheranno le considerazioni di merito rispetto alla valutazione dello stato di necessità. Ci si chiede ad esempio se tale valutazione rimarrà totale appannaggio dei vertici dell'ente locale o se invece sarà sottoposta a parametri elaborati a livello centrale.

***

Il tentativo di analisi della *smart city* nella sua componente digitale svolto in questo contributo ci ha consentito di individuare una serie di norme che, regolando le modalità di trattamento e condivisione dei dati, rappresentano l'intelaiatura dei sistemi di governo dei dati che gli enti locali debbono progressivamente costruire. Non sfugge però come la *governance* dei dati non possa definire il profilo di una *smart city* se non negli aspetti "tecnici" e latamente costituzionali.

Vero è che le regole poste dal GDPR e dalle altre normative citate sono tutte orientate alla realizzazione di principi e diritti fondamentali riconosciuti dall'Unione Europea. Ciononostante, pare fondamentale, in conclusione, ricordare come il sistema valoriale che una città esprime non potrà essere individuato solamente tramite il rimando ai diritti fondamentali, quanto piuttosto attraverso l'espressione degli indirizzi politici da parte del corpo elettorale, e degli indirizzi politico-amministrativi da parte dell'organo consiliare [67].

A parere di chi scrive gli organi di governo degli enti locali costituiscono l'ideale centro di raccordo dell'azione di tutti i soggetti che partecipano alla costruzione di un ecosistema digitale urbano. Tra di essi sicuramente vi sono gli attori privati, il cui apporto in alcuni settori è con ogni probabilità insostituibile. Ciononostante dovrebbero essere i cittadini, attraverso i loro rappresentanti eletti con metodo democratico, a definire le modalità con cui la tecnologia può essere impiegata per perseguire il bene pubblico, in tal modo scongiurando il rischio che squilibri di potere economico e tecnologico provochino slittamenti verso modelli di Smart city considerevolmente plasmati dagli interessi privati [68].

Detto altrimenti, i Comuni dovrebbero mantenere saldamente un ruolo

---

[67] M CLARICH, *Manuale di diritto amministrativo*, Bologna, 2013, p. 332.

[68] «*The risk of corporate capture of public powers arises in this context since there is the significant risk that private companies will shape the way in which public bodies employ technology to pursue the public good*», S. RANCHORDAS, A. KLOP, *Data-Driven Regulation and Governance in Smart Cities*, in *University of Groningen Faculty of Law Legal Studies Research Paper Series*, 7/2018, p. 33.

centrale nelle scelte di indirizzo. Solo in questo modo essi potranno gradualmente trasformarsi in ecosistemi digitali virtuosi, in Città intelligenti in cui la politica, seppure *data-driven*, sia autenticamente costituzionale, e sia capace di orientare la realtà, piuttosto che inseguirla [69].

[69] M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in P. COSTANZO, P. MAGARÒ, L. TRUCCO (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Napoli, 2022, p. 65.

LE *SMART CITIES* E IL RILIEVO SOCIALE DEI DATI

di *Giorgio Resta* [*]

1. Smart cities *e governo dei dati*

Fra i vari temi dibattuti nell'ambito della già ampia letteratura sulle *smart cities*, quello relativo al modello di *governance* dei dati ha senza dubbio un rilievo centrale [1]. Tuttavia, l'accento è stato sin qui prevalentemente posto sul tema delle libertà individuali e della sorveglianza. Si tratta com'è ovvio di un profilo essenziale, anche se non è l'unico che merita di essere affrontato. Una questione non meno rilevante, ad esempio, è quella del regime di appartenenza e/o amministrazione dei dati (usando tali espressioni in maniera molto ampia e flessibile). Molti autori prospettano, almeno in termini generali, un'alternativa tra tre principali modelli organizzativi [2]: *a*) quello della proprietà pubblica; *b*) quello della titolarità individuale; *c*) quello della appartenenza comune o collettiva con connotazioni fiduciarie. Questo contributo non intende portare argomenti pro o contro un determinato modello, quanto indagare le recenti trasformazioni del diritto europeo dei dati. L'obiettivo è quello di illustrare quan-

[*] Una versione più ampia di questo scritto è apparsa nella *Rivista trimestrale di diritto pubblico*, 2022, p. 971 ss.

[1] S. RANCHORDÁS, A. KLOP, *Data-driven regulation and governance in smart cities*, in A. BERLEE, V. MAK *et al.*, *Research Handbook in Data-science and law*, Cheltenham, 2018, p. 245 ss.; T. SCASSA, *Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto*, in *Techn. & Reg.,* 2020, p. 44 ss.

[2] M. MICHELI *et al.*, *Emerging models of data governance in the age of datafication*, in *Big Data & Society,* July-December 2020, p. 1 ss.

to le alternative in oggetto siano più di facciata che di sostanza, atteso che qualsiasi moderno diritto dei dati è chiamato a bilanciare le tre dimensioni in oggetto – pubblico, privato, collettivo – assicurandone la coesistenza e il reciproco intreccio. Il quadro che si tratteggerà, prevalentemente incentrato sull'analisi del pacchetto digitale UE, potrà risultare utile per una più specifica riflessione sul regime di governo dei dati nel contesto delle *smart cities*.

2. *Le trasformazioni del diritto europeo dei dati*

Il sistema europeo di governo dei dati è stato a lungo connotato da un particolare equilibrio. Questo ha visto in una posizione culturalmente e assiologicamente sovraordinata il compendio normativo concernente il trattamento dei dati personali, mentre un ruolo comparativamente minore è stato svolto da altri segmenti di disciplina, come quello relativo all'accesso ai dati, al riutilizzo delle informazioni del settore pubblico, o alla stessa proprietà intellettuale (con le specifiche propaggini delle discipline sulla tutela delle banche di dati e del segreto industriale)[3]. Si potrebbe parlare, con qualche semplificazione, di un modello unipolare. Le ragioni sono agevolmente comprensibili e risiedono in larga parte nell'antecedenza storica della normativa in materia di trattamento dei dati personali, sviluppatasi sin dagli anni '70 prima in seno agli ordinamenti nazionali e poi gradualmente penetrata nel sistema del Consiglio d'Europa (Convenzione n. 108/1981) e dell'Unione Europea (a partire dalla Direttiva 95/46/CE)[4]. I circa cinquant'anni di applicazione della normativa in oggetto, che peraltro ha implicato la creazione di apposite istituzioni deputate a assicurarne la supervisione e ha prodotto il sorgere di una comunità scientifica di specialisti della materia, hanno restituito ad essa caratteri di sistematicità, organicità e completezza che non è dato rinvenire nelle altre normative in tema di controllo delle informazioni. A ciò si aggiunga che sul piano dei principi, la disciplina della protezione dei dati personali si colloca senza dubbio ai vertici del sistema, in coerenza con un discorso pubblico che ha da sempre enfatizzato il legame di tali garanzie con il costituzionalismo post-bellico, sorto sulle macerie delle esperienze totalitarie novecentesche[5]. Ne è ora limpida te-

[3] T. STREINZ, *The Evolution of European Data Law*, in P. CRAIG, G. DE BÚRCA (a cura di), *The Evolution of EU Law*, III ed., Oxford, 2021, p. 902 ss., p. 915; e ora P.C. JOHANNES, *Europäisches Datenrecht – ein Spickzettel*, in *ZD – Aktuell,* 2022, p. 1166.

[4] S. RODOTÀ, *Tecnologie e diritti*, II ed., Bologna, 2021.

[5] F. BIGNAMI, *European versus American Liberty: A Comparative Analysis of Antiterrorism Data Mining*, in 48 *B.C. L. Rev.* 609 (2007).

stimonianza la scelta, compiuta dalla Carta dei Diritti Fondamentali UE, di prevedere in aggiunta al diritto al rispetto della vita privata una specifica disposizione sul diritto alla protezione dei dati personali (art. 8). Tutto ciò si è tradotto in una posizione di primazia, sia sul piano della gerarchia delle fonti, sia su quello della compiutezza dell'elaborazione scientifica, della disciplina del trattamento dei dati personali rispetto agli altri campi del diritto preordinati a regolare la circolazione delle informazioni.

Non è forse azzardato prevedere che tale primazia sia destinata gradualmente ad incrinarsi sino a cedere il passo, per le ragioni che saranno di seguito illustrate, a un modello multipolare, nel quale le istanze di protezione dei dati coesisteranno con pari dignità con quelle di libero accesso e riuso dei dati medesimi. A fianco a un *Datenschutzrecht* sembra emergere e acquistare giuridica consistenza un *Datenwirtschaftsrecht*[6].

La strategia europea dei dati[7] sembra preludere proprio a un siffatto percorso. Le scelte compiute con il *Data Governance Act*, destinate a essere ulteriormente integrate e sistematizzate con il *Data Act* (ancora allo stato di proposta della Commissione), rappresentano un primo passo in questa direzione. Non è quindi un caso che il DGA opti per una definizione autonoma di "*dati*" quali "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva …*" (art. 2, n. 1). Tale formula segna un distacco netto dalla pregressa impostazione da un lato perché delinea un *Oberbegriff* atto a ricomprendere al suo interno sia dati personali sia dati non personali; dall'altro perché mette in esponente la dimensione sintattica (per riprendere il linguaggio della scienza dei dati) dei dati[8]. In altri termini, mentre la nozione di dato personale si incentra sul carattere della riferibilità di una specifica informazione a un determinato individuo, esaltando così nella costruzione della fattispecie la dimensione semantica del dato quale latore di un'informazione, la formula accolta dal DGA prescinde da tale aspetto e accentua l'idea della "*codifica*" di stati del mondo tramite rappresentazione digitale. Si coglie in ciò un sottile scivolamento della logica sottesa alla disciplina in oggetto: questa

---

[6] B. STEINRÖTTER, *Das 'Datenwirtschaftsrecht' als neues Teilrechtsgebiet im Recht der Daten,* in *ZD,* 2021, p. 543; D. STAUDENMAYER, *Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz. Auf dem Weg zum Privatrecht der Datenwirtschaft,* in *EuZW,* 2022, p. 596.

[7] Comunicazione della Commissione del 19 febbraio 2020, COM(2020) 66 final, *A European Strategy for Data.*

[8] Per questa distinzione v. H. ZECH, *Besitz an Daten?*, in T. PERTOT (a cura di), *Rechte an Daten,* cit., pp. 21, 91; J. DREXL, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access,* in *JIPITEC,* 8 (2017), p. 257.

non è più volta a precostituire un meccanismo di salvaguardia di determinati beni incorporali in ragione del potenziale di conoscenza che essi possono sprigionare in relazione ad una persona. Prevale, invece, l'intento di prefissare un sistema di regole concernenti la circolazione e l'uso di dati in relazione alla loro strutturazione formale (e in particolare la leggibilità da un sistema automatico), indipendentemente dal tipo di significati che questi siano atti a veicolare[9]. Sul piano teleologico, questo mutamento di impianto si riflette nel passaggio da una normativa essenzialmente limitativa ad una di stampo promozionale circa l'uso dei dati.

La nuova "strategia dei dati" segna quindi una forte discontinuità nel sistema di governo dei dati. L'approccio preesistente, posto a confronto con la nuova realtà tecnologica dei *big data* e dell'intelligenza artificiale, si è mostrato deficitario sotto molteplici punti di vista, ma soprattutto sotto i due profili dell'assenza di incentivi alla condivisione dei dati (personali e non personali) e dell'inefficacia dell'apparato di tutela rispetto alla realtà dell'*informational capitalism.*

Come osservato da Viktor Mayer Schönberger, le risultanze statistiche mostrano che circa l'85% dei dati raccolti in Europa non viene riutilizzato[10]. Tale circostanza è comune sia al settore dei dati personali, che, come ha mostrato l'esperienza pandemica, potrebbero essere reimpiegati con più efficacia per finalità di interesse pubblico, come la promozione della ricerca scientifica e il supporto alle politiche sanitarie; sia a quello dei dati non personali, quali ad esempio i dati industriali e i dati in possesso delle pubbliche amministrazioni. Ciò rappresenta di fatto un fattore frenante sul piano dell'innovazione, atteso che questa – e il riferimento non è limitato al settore industriale – è oggi in larga parte *data-driven.*

D'altro canto, anche nell'ambito normativo nel quale l'istanza preponderante è quella del controllo e non della condivisione, e segnatamente dei dati personali, il meccanismo di disciplina messo a punto dal legislatore europeo si è rivelato sotto alcuni aspetti inefficace al cospetto delle prassi organizzative e di mercato affermatesi nel contesto dell'economia digitale. In particolare, l'enfasi posta sin dalla Direttiva 95/46/CE sul meccanismo del consenso informato quale base normativa atta a legittimare il trattamento dei dati – al

---

[9] B. STEINRÖTTER, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts,* in *RDi,* 2021, p. 480, alla p. 481; F. ROSENKRANZ, M. SCHEUFEN, *Die Lizenzierung von nicht-personenbezogenen Daten. Eine rechtliche und rechtsökonomische Analyse,* in *ZfDR,* 2022, p. 159, alla p. 168.

[10] T. RAMGE, V. MAYER SCHÖNBERGER, *Fuori i dati! Rompere i monopoli delle informazioni per rilanciare il progresso*, Milano, 2021, p. 39; v. inoltre per una dettagliata descrizione delle criticità dell'attuale sistema di governo dei dati, la già citata Comunicazione *A European Strategy for Data,* alla p. 6 ss.

fianco di altri meccanismi legittimanti, compiutamente elencati negli artt. 6 e 9 del Regolamento 2016/679 – ha innescato un processo di burocratizzazione del consenso sia nei rapporti con i soggetti privati sia in quelli con i soggetti pubblici [11]. Soprattutto, nel contesto dei rapporti *online* il consenso si è tradotto in quella famosa "foglia di fico" a cui accennavano già molti anni addietro Guido Calabresi e Stefano Rodotà, atta a mascherare una realtà fortemente asimmetrica e in cui l'idea dell'autodeterminazione dell'interessato si è rivelata poco più che un'etichetta priva di riscontri operazionali [12].

Sono molteplici gli studi empirici che dimostrano come le c.d. *privacy policies (*informative nel linguaggio del legislatore) siano redatte in maniera talmente complessa e articolata che nella stragrande maggioranza dei casi (alcune indagini indicano il 75% dei casi) esse non vengono neanche lette [13]. E ciò peraltro è una scelta razionale, atteso che le *chances* di negoziazione dei termini del trattamento dei dati sono comunque molto basse, stante l'inclusione del consenso in moduli predeterminati unilateralmente (spesso volti a disciplinare anche altri aspetti del rapporto contrattuale, come il servizio di *social network* o la gestione di una casella di posta elettronica) e non suscettibili di modifica se non per aspetti marginali [14]. Inoltre, si è fatto notare che anche qualora il soggetto sia in grado di esprimere una consapevole determinazione di volontà nel rapporto con il primo titolare del trattamento (mercati primari), massima è l'opacità che regna sul resto della catena del valore e dunque sui successivi riutilizzi dei dati (mercati secondari) [15]. D'altronde è sotto gli occhi di tutti che i grandi oligopoli digitali hanno acquisito le loro sconfinate quote di mercato proprio grazie alle strategie di estrazione di valore dai dati delle persone, riguardati come risorse liberamente appropriabili [16]. Dunque, fra le critiche che più frequentemente vengono rivolte al modello europeo di protezione dei dati

---

[11] Sul punto v. C. WENDEHORST,S. SCHWAMBERGER, J. GRINZINGER*, Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, in T. PERTOT (a cura di), *Rechte an Daten*, cit., p. 103 ss.

[12] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 47 ss., p. 133; ID., *Protezione dei dati e circolazione delle informazioni,* ora in *Tecnologie e diritti*, cit., p. 79 ss.

[13] T.J. GERPOTT, *Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO. Empirischer Forschungsstand und Verbesserungsfelder*, in *MMR,* 2020, p. 739.

[14] M. KAMP, M. ROST, *Kritik an der Einwilligung. Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen*, in *DuD,* 2013, p. 80 ss.

[15] C. WENDEHORST, S. SCHWAMBERGER, J. GRINZINGER, *Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, cit., 103 ss.; V. ZENO-ZENCOVICH, *Do, Data Markets' Exist?*, in *MediaLaws*, 2019, p. 22 ss.

[16] In luogo di molti si veda l'approfondita indagine di J.E. COHEN, *Between Truth and Power: The Legal Construction of Informational Capitalism*, Oxford, 2019.

v'è quella per cui la normativa in oggetto mentre ha reso in certi casi più complicato il riutilizzo dei dati per finalità di pubblico interesse (si pensi unicamente al settore della ricerca biomedica, che soffre sia la mancanza di coordinamento a livello europeo del regime di riutilizzo dei dati, frammentato alla luce dell'art. 89 GDPR su scala nazionale [17], sia di insufficienti garanzie a livello locale [18]), al contempo non è riuscita ad opporre un argine robusto alle operazioni di parassitismo commerciale poste in essere a partire da risorse consustanziali alla sfera identitaria della persona.

3. *Il* Data Governance Act *e le tre dimensioni di governo dei dati*

Si comprende quindi che la già citata Comunicazione della Commissione sulla Strategia europea dei dati [19] indichi la necessità di un cambio di rotta sotto ciascuno dei profili evidenziati, con l'obiettivo di non disperdere le opportunità create dalle tecniche dell'intelligenza artificiale e promuovere – a tutti i livelli – una maggiore circolazione e condivisione dei dati [20]. Il *Data Governance Act* raccoglie questa sfida operando su tre fronti principali: *a*) quello del riutilizzo dei dati in mano pubblica; *b*) quello dei servizi di intermediazione per lo scambio dei dati; *c*) quello della destinazione dei dati per finalità altruistiche.

4. *Pubblico e privato*

Le disposizioni che operano sul primo punto si muovono in una linea di continuità rispetto al *corpus* normativo preesistente, allargando la portata dei principi stabiliti dalle direttive su *open data* e riutilizzo delle informazioni del settore pubblico [21], sulla base della premessa che «*i dati generati o raccolti da*

---

[17] C. WIESE SVANBERG, *sub § 89*, in C. KUNER, L. BYGRAVE *et al.* (eds.), *The EU General Data Protection Regulation*, Oxford, 2020, p. 1240.

[18] G. COMANDÈ, *Ricerca in sanità e data protection, un puzzle… risolvibile*, in *Riv. it. med. leg.*, 2019, p. 187.

[19] COM(2020) 66 final.

[20] B. STEINRÖTTER, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts,* cit., p. 483 ss.

[21] V. in particolare la Direttiva 2019/1024. In tema R. SCHILDBACH, *Zugang zu Daten der öf-*

enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società» (Considerando 6). Il DGA estende l'ambito di operatività di tali principi a determinate categorie di dati, e segnatamente quelli protetti per motivi di riservatezza commerciale, riservatezza statistica, tutela dei diritti di proprietà intellettuale o tutela dei dati personali (art. 3, comma 1). Il limite principale di tale modello è che non vengono prefissati specifici obblighi o garantiti diritti azionabili in ordine all'accesso ai dati pubblici per finalità di riutilizzazione, bensì sono semplicemente disciplinate agli artt. 4-8 le modalità con le quali può essere concesso il riutilizzo (divieto di accordi di esclusiva, requisiti inerenti il formato dei dati e la messa a disposizione, limite al trasferimento extra-UE, canoni concessori, sportelli unici) [22].

Si tratta di una linea giuspolitica coerente con l'impianto preesistente [23], ma probabilmente non tanto innovativa quanto quella perseguita dalla Proposta di *Data Act*, che piuttosto che insistere sul flusso dei dati *Government to Business*, sposta l'asse di incidenza normativo sull'opposto registro *Business to Government* [24]. Prendendo le mosse da una realtà operativa spesso connotata da una rilevante asimmetria tra i patrimoni informativi goduti da alcuni soggetti privati, granulari e continuamente aggiornati, e il patrimonio informativo pubblico, frequentemente disperso in silos informativi non comunicanti, la Proposta mette a sistema una serie di indici normativi già esistenti a livello nazionale (in particolare nel diritto francese) [25] ed europeo [26] e raccoglie alcune istanze emerse a livello di società civile soprattutto nell'ambito dei dibattiti sulle *smart cities* [27]. Essa

---

fentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes, in *ZD,* 2022, p. 148.

[22] Sul punto D. TOLKS, *Die finale Fassung des Data Governance Act. Erste Schritte in Richtung einer europäischen Datenwirtschaft*, in *MMR*, 2022, pp. 444, 445-446.

[23] A. HARTL, A. LUDIN, *Recht der Datenzugänge. Was die Datenstrategie der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen*, in *MMR*, 2021, p. 534.

[24] D. TOLKS, *Die finale Fassung des Data Governance Act*, cit., p. 449.

[25] Cfr. art. 17 ss. della *Loi pour une république numérique* del 7 ottobre 2016.

[26] Sul punto debbono confrontarsi soprattutto gli studi di H. RICHTER, *Zugang des Staates zu Daten der Privatwirtschaft*, in *ZRP*, 2020, p. 245; ID., *The Law and Policy of Government Access to Private Sector Data (B2G Data Sharing)*, in BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ, MAX-PLANCK-INSTITUT FÜR INNOVATION UND WETTBEWERB (hrsg. v.), *Data Access, Consumer Interests and Public Welfare*, 2021, p. 529 *https://doi.org/10.5771/9783748924999-529*; nonché A. VIGORITO, *Government Access to Privately Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models*, in 20 *Eur. J. Comp. L. & Governance* 1 (2022); e in prospettiva comparatistica F. CATE, J. DEMPSEY (a cura di), *Bulk Collection*, Oxford, 2017.

[27] V. ad es. E. MOROZOV, F. BRIA, *Rethinking the Smart City. Democratizing Urban Technology,* New York, 2018*,* p. 25 ss.

codifica quindi il modello noto in letteratura come "*reverse PSI*" [28], delineando una fattispecie generale di trasferimento dei dati – sia non personali, sia personali previa pseudonimizzazione (art. 17, comma 2, lett. d; art. 18, comma 5) – dal settore privato al settore pubblico [29].

Ciò segna una rilevante innovazione, almeno sul piano delle formule legislative, perché sinora si era sempre data la preferenza ad un modello di *data transfer* volontario [30]. Ove la Proposta dovesse essere approvata nei termini auspicati dalla Commissione, nelle ipotesi di "*eccezionale necessità*", puntualmente disciplinate all'art. 15, le pubbliche amministrazioni potranno far ricorso a un meccanismo autoritativo di accesso ai datasets privati, salva la corresponsione di un indennizzo – non dovuto soltanto nei casi di emergenza pubblica – comprensivo dei costi di duplicazione e trasferimento, nonché di un "*margine ragionevole*". La particolare rilevanza di questa norma si coglie dal fatto che tra le ipotesi di eccezionale necessità rientrano non soltanto i casi di prevenzione o gestione di un'emergenza pubblica, ma anche la circostanza per cui «*l'assenza di dati disponibili osti all'attuazione di un compito di interesse pubblico stabilito per legge, i dati non siano reperibili sul mercato e l'adozione della procedura prevista dalla norma riduca significativamente gli oneri burocratici per i detentori dei dati*». È evidente che in tal modo sono di fatto poste le premesse – sia pure in linea teorica – per una sorta di trasferimento coattivo dei dati per pubblico interesse, che potrebbe rappresentare il succedaneo dell'*eminent domain* nella società digitale. Non a caso è proprio su questa norma che si sono appuntate le prime notazioni critiche circa la Proposta [31].

5. *La dimensione collettiva*

Sul secondo profilo si sofferma invece il capitolo III del DGA. Questo stabilisce i requisiti per i servizi di intermediazione dei dati, prescrivendo oneri procedurali di notifica (art. 11), condizioni sostanziali per la fornitura del ser-

---

[28] Y. POULLET, *From* open data *to* reverse PSI – *A new European policy facing GDPR,* in *Eur. Public Mosaic,* 11, 2020.

[29] R. PODSZUN, C. PFEIFER, *Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission*, in *GRUR*, 2022, pp. 952, 958.

[30] A. VIGORITO, *Government Access to Privately Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models,* cit., p. 14.

[31] R. PODSZUN, C. PFEIFER, *Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission*, cit., p. 958.

vizio (art. 12), meccanismi pubblici di supervisione (artt. 13-14). È importante notare che, secondo la nuova definizione proposta nell'art. 2, n. 11, si intende per servizio di intermediazione dei dati un «*servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali*». È significativo che siano espressamente esclusi dal perimetro della nozione i servizi che rappresentano il cuore del modello del capitalismo informazionale contemporaneo, come Google o Facebook, che raccolgono dati dagli utenti offrendo servizi formalmente gratuiti per poi conseguire profitti extra tramite la licenza a terzi dei dati aggregati, analizzati e organizzati in formato leggibile dalle macchine [32]. Ai sensi dell'art. 2, n. 11, lett. a), infatti, non rientrano tra i servizi di intermediazione i servizi che «*ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati*». Sottesa alla disciplina del DGA, come si osservava, è una finalità promozionale. Attraverso la predisposizione di un quadro giuridico certo e trasparente ci si propone di stimolare una maggiore condivisione dei dati, anche in continuità con la politica volta alla creazione dei nuovi specifici 'spazi europei dei dati' connotato ciascuno da proprie caratteristiche funzionali e regolamentari [33]. Uno dei presupposti fondamentali per conseguire tali obiettivi è aumentare la fiducia dei 'titolari' dei dati nella neutralità e nell'affidabilità del servizio di intermediazione (cfr. Considerando 5 e 32). Si comprende quindi che già sul piano definitorio siano stati esclusi i servizi che si basano sul modello dello sfruttamento industriale dei dati; e che il principio della neutralità sia stato formulato come primo tra i requisiti sostanziali da osservare per la fornitura del servizio [34]. L'art. 12, comma 1, lett. a), prescrive infatti che il fornitore del servizio di intermediazione «*non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione attraverso una persona giuridica distinta*». Del pari, la lett. m) della medesima disposizione stabilisce uno specifico ob-

[32] In tema M. HENNEMANN, L. V. DITFURTH, *Datenintermediäre und Data Governance Act,* in *NJW,* 2022, pp. 1905, 1908.

[33] Cfr. il Considerando 27 e v. D. TOLKS, *Die finale Fassung des Data Governance Act,* cit., p. 446.

[34] Sul principio di neutralità M. HENNEMANN, L. V. DITFURTH, *Datenintermediäre und Data Governance Act,* in *NJW,* 2022, pp. 1905, 1906.

bligo di natura fiduciaria per l'ipotesi in cui il servizio di intermediazione abbia ad oggetto dati personali, nell'intento di rafforzare ulteriormente la trasparenza e l'affidabilità del servizio: «*il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso*».

Quest'ultimo rilievo induce a soffermarsi sulla tassonomia dei servizi di intermediazione proposta dal DGA e sul significato che essa assume nella prassi. L'art. 10, comma 1, contempla tre tipologie di servizi di intermediazione tra loro molto diversi.

i) La prima è quella incentrata sulla condivisione dei dati tra attori di mercato, per il tramite dell'interscambio o della costituzione di *data pools*. Nel linguaggio normativo si tratta di servizi di intermediazione tra "*titolari dei dati*" e "*potenziali utenti*" di essi, i quali «*possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati*». Nella valutazione della Commissione, lo scambio B2B è ancora a un livello insoddisfacente e, se adeguatamente supportato, potrebbe ingenerare effetti positivi in termini di innovazione e offerta di servizi a valore aggiunto. Il problema fondamentale è che, in assenza di un diritto di esclusiva sullo sfruttamento dei dati industriali, sin qui opportunamente rigettato dal legislatore europeo [35], l'unico strumento di tutela è rappresentato dalla disponibilità materiale, e dunque dal potere di fatto vantato su tali risorse. Di conseguenza, sussiste una comprensibile ritrosia degli operatori economici a scambiare o mettere direttamente in condivisione i *datasets* più rilevanti, a meno che non siano assicurate idonee garanzie in punto di sicurezza della conservazione, limiti all'uso dei dati, assenza di conflitti di interesse, ecc. Le condizioni stabilite all'art. 12 (in part. alle lett. b, f-h, l), sono mirate proprio a creare un terreno propizio alla messa in comune dei dati tramite una riduzione dei costi di transazione derivanti dalle asimmetrie informative [36]. In-

[35] F. ROSENKRANZ, M. SCHEUFEN, *Die Lizenzierung von nicht-personenbezogenen Daten. Eine rechtliche und rechtsökonomische Analyse*, cit., p. 168; B. STEINRÖTTER, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts*, cit., p. 482; per ulteriori riferimenti al dibattito decennale sulla proprietà dei dati sia consentito rinviare a G. RESTA, *Towards a unified regime of data-rights? Rapport de synthèse*, cit., p. 242.

[36] H. RICHTER, *Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance"*, cit., p. 643.

termediari qualificati e dotati di adeguato capitale reputazionale, anche al di là delle esperienze esistenti dei *marketplaces* globali e delle piattaforme industriali di dati [37] – potrebbero favorire l'incontro tra domanda e offerta, contribuendo alla messa a punto di formati interoperabili e assicurando almeno indirettamente una forma di supervisione sull'uso dei dati [38].

ii) La seconda tipologia è quella consistente nei «*servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679*» [39]. Se nell'ipotesi precedente la preoccupazione principale è quella di stimolare la condivisione dei dati, in questo caso concorre l'esigenza di rafforzare l'esercizio consapevole del diritto di autodeterminazione informativa. Come si è osservato in precedenza, le caratteristiche più comuni dei mercati dei dati tendono a esaltare il divario di potere reale tra il singolo e le controparti professionali, rendendo la manifestazione del consenso poco più che un atto formale privo di reale valore decisionale [40]. Del pari, i diritti di cui agli art. 15 ss. GDPR non sempre hanno un effettivo riscontro operazionale, o perché mancano gli incentivi necessari al superamento dei costi di inerzia coinvolti nell'esercizio del diritto o perché le stesse possibilità di supervisione circa le modalità di uso dei dati sono limitate. Di qui l'idea, da tempo avanzata, per cui il coinvolgimento di soggetti collettivi – come associazioni in tema di libertà civili, sindacati, ecc. – in funzione di assistenza e supporti dei singoli interessati possa contribuire a rafforzare l'effettività dei rimedi in tema di trattamento dei dati [41]. Il DGA sembra muoversi su questa linea, prefigurando forme più o meno avanzate di supporto ai singoli individui sia nella fase antecedente alla manifestazione del consenso (art. 12, comma 1, lett. m; Considerando 30) sia in quella dell'esercizio dei diritti dell'interessato e dell'esperimento dei relativi rimedi (art. 2, comma 1, n.

---

[37] Per una descrizione dettagliata M. HENNEMANN, L. V. DITFURTH, *Datenintermediäre und Data Governance Act,* cit., p. 1906.

[38] M. HENNEMANN, L. V. DITFURTH, *Datenintermediäre und Data Governance Act*, cit., pp. 1906, 1910.

[39] In tema F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, p. 199 ss.

[40] Cfr. *supra*, par. 2.

[41] V. EDPS, *Opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data* (2016); C. WENDEHORST, S. SCHWAMBERGER, J. GRINZINGER*, Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?,* cit.

11; art. 10, comma 1, lett. b). Se lo schema è chiaro in termini generali, rimane da capire come si sposino tali regole con le forme organizzative riscontrabili nella prassi.

È opportuno distinguere a tal riguardo almeno due diverse ipotesi, connotate da caratteristiche funzionali profondamente differenti. La prima è riconducibile alla categoria nota come «*personal information management services*»[42], consistente nell'offerta al pubblico, per fini lucrativi, di servizi di gestione professionale dei dati (un esempio, recentemente portato all'attenzione del Garante per la protezione dei dati, è Weople)[43]. Questi possono comprendere strumenti tecnici per la personalizzazione delle dichiarazioni di consenso in ordine a specifici settori o trattamenti, attività preordinate alla negoziazione collettiva dei diritti al fine della monetizzazione dei dati personali, assistenza nell'esercizio dei diritti dell'interessato (si pensi tipicamente all'esercizio del diritto alla portabilità, di cui all'art. 20 GDPR). Nelle forme più avanzate, questa forma organizzativa potrebbe ricalcare il modello delle *collecting societies* del diritto d'autore[44]. La seconda è quella dell'amministrazione dei dati per finalità e in ambiti essenzialmente non lucrativi, come quelli della ricerca scientifica o delle politiche sanitarie. Molto diffusa a questo proposito, nei discorsi pubblici e nella letteratura scientifica, è la formula del *data trust* (o nella sua trasposizione tedesca *Datentreuhand*), che a sua volta può essere disarticolata in diverse tipologie operative, tutte connotate dal carattere fiduciario dei poteri ascritti al gestore e dalla segregazione del patrimonio informativo oggetto del *trust*[45].

iii) La terza tipologia è costituita dai servizi di cooperative dei dati[46]. Questi vengono definiti dall'art. 2, comma 1, n. 11 come servizi di intermediazione

---

[42] B. FALKHOFEN, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X*, in *EuZW*, 2021, p. 787, alla p. 790.

[43] *https://weople.space*. Per approfondimenti su questo caso v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 216.

[44] L. SPECHT-RIEMENSCHNEIDER *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung*, in *MMR-Beil.*, 2021, 25, alla p. 27.

[45] Su questa figura si v. in particolare L. SPECHT-RIEMENSCHNEIDER *et al.*, *Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung*, cit., p. 25 ss.; C. WENDEHORST, S. SCHWAMBERGER, J. GRINZINGER, *Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, in T. PERTOT (hrsg. v.), *Rechte an Daten*, cit., p. 103 ss.

[46] In generale v. H. BAARS, A. TANK *et al., Cooperative Approaches to Data Sharing and Analysis for Industrial Internet of Things Ecosystems*, in *App. Sc.*, n. 11, 2021, p. 7547; M. MICHELI *et al., Emerging models of data governance in the age of datafication,* in *Big Data & Society,* July-

«*offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali*». Prevalente, in questa fattispecie, è la finalità mutualistica, in base all'assunto per cui creando una struttura collettiva e di coordinamento volta a socializzare il valore dei dati, i singoli membri di essa ne ricaverebbero un guadagno non soltanto in termini monetari, ma anche e soprattutto sul piano del controllo sulle modalità di trattamento e utilizzo secondario dei dati. Alcuni esempi emersi nella prassi, come quello delle cooperative dei dati create da conducenti di taxi (Driver's seat), da pazienti (salus.coop), o da pescatori (PescaData), mostrano come le cooperative di dati possano rappresentare, soprattutto a livello locale, un sistema interessante di gestione dei dati con carattere imprenditoriale ma alternativo rispetto agli schemi caratteristici del capitalismo estrattivo [47]. Non a caso, proprio all'interno del dibattito sulle *smart cities* si è più volte fatto riferimento al modello delle cooperative, assieme a quello del *data trust,* come alternativa organizzativa preferibile rispetto a quella dell'impresa lucrativa [48].

6. *L'altruismo dei dati*

L'art. 15 sottrae alla disciplina procedurale e sostanziale dei servizi di intermediazione le «*organizzazioni per l'altruismo dei dati riconosciute*», non-

December, 2020, 1, p. 7; S. DELACROIX, N.D. LAWRENCE, *Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance*, in 9 *International Data Privacy Law* 236 (2019).

[47] Per un'attenta indagine sociologico-giuridica, v. E. BIETTI, A. ETXEBERRIA *et al., Data Cooperatives in Europe: A Legal and Empirical Investigation,* White Paper created as part of *The New School's Platform Cooperativism Consortium* and *Harvard University's Berkman Klein Center for Internet & Society* Research Sprint (Dec. 2021), accessibile all'indirizzo *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*.

[48] M. PETRAS, *Demokratischer Datenschutz. Kooperative Privatheit in der 'Smart City'*, in *MMR*, 2021, pp. 862, 864.

ché le «*altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati*». L'intento è quello di ritagliare un complesso di regole di favore per enti collettivi che, operando senza scopi di lucro, si propongano di stimolare la raccolta di dati personali e non personali e la loro destinazione a finalità di interesse generale[49]. Qui si innesta il terzo cardine su cui ruota l'impianto del DGA.

L'altruismo dei dati è definito dall'art. 2, comma 1, n. 16 come «*la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale*»[50]. Siamo fuori, evidentemente, dallo schema dell'intermediazione di mercato preordinata a stabilire modelli coordinati di sfruttamento (come nei data pools) o sistemi di monetizzazione dei dati collegati al loro reimpiego per scopi commerciali. Non siamo lontani, invece, dall'ipotesi del data trust – e le organizzazioni dell'altruismo dei dati ne rappresentano un chiaro esempio applicativo[51] – ferma restando la predeterminazione legislativa del tipo di finalità sottese all'intero schema negoziale, le quali debbono essere congruenti con l'interesse generale. L'esperienza della pandemia da Covid-19 ha avuto da questo punto di vista un rilievo centrale, perché ha fatto emergere l'importanza della condivisione dei dati, mostrando peraltro alcuni limiti del modello del GDPR[52]. Si noti, ad esempio, che in Germania – dove il consenso dell'interessato è stato ritenuto base giu-

[49] In tema P. v. HAGEN, L. VÖLZMANN, *Datenaltruismus aus datenschutzrechtlicher Perspektive. Wechselwirkung zwischen DGA und DS-GVO*, in *MMR*, 2022, p. 176.

[50] La disciplina dell'altruismo dei dati del DGA dà spessore normativo a un fenomeno ampiamente indagato in letteratura negli ultimi anni: v. tra i molti studi M. TADDEO, *Data Philantropy and Individual Rights*, in 27 *Minds and Machines* 1 (2017); B. PRAINSACK, *Data Donation: How to Resist the iLeviathan*, in J. KRUTZINNA, L. FLORIDI, *The Ethics of Medical Data Donation*, Cham, 2019, p. 9.

[51] S. KEMPNY, H. KRÜGER, M. SPINDLER, *Rechtliche Gestaltung von Datentreuhändern. Ein interdisziplinärer Blick auf ‚Data Trusts'*, in *NJW*, 2022, pp. 1646, 1648.

[52] K. KUNER, *Data Crossing Borders*, in *Verfassungsblog.de*, 15 aprile 2020.

ridica adeguata per il trattamento dei dati attraverso tracing app [53] – il Robert Koch-Institut ha promosso un'applicazione (*Corona-Datenspende*) volta a permettere la donazione da parte dei cittadini dei dati personali raccolti dai dispositivi intelligenti, quali ad. es. gli *smart watch*, per finalità epidemiologiche e di contrasto alla pandemia [54]. Del pari, diverse organizzazioni come Google o Facebook, hanno messo a disposizione dei governi i dati aggregati relativi alla mobilità della popolazione per individuare i cluster e seguire la diffusione del virus. Generalizzando tale modello, il DGA assegna uno specifico ruolo alle organizzazioni non lucrative impegnate sul fronte della raccolta e successiva destinazione dei dati per finalità di interesse generale, predisponendo un minuto apparato regolamentare che assicuri la trasparenza e l'indipendenza di tali organizzazioni, evitando la creazione di incentivi disallineati. Si prevede quindi innanzitutto un onere di iscrizione presso il registro pubblico delle organizzazioni di altruismo dei dati stabilito dall'art. 19 DGA. Questo è subordinato al possesso di una serie di requisiti specificati all'art. 18 (tra i quali lo scopo di lucro, la struttura funzionalmente separata per le attività in oggetto, il rispetto del codice contemplato all'art. 22). In secondo luogo, l'art. 20 impone il mantenimento di registri aggiornati, mentre l'art. 21 fissa una serie di obblighi e principi a tutela dei titolari dei dati, tra i quali l'obbligo di informazione (relativi agli obiettivi di interesse generale e alle successive vicende del dato), il rispetto della finalità nell'utilizzo dei dati, l'assistenza tecnica nella fase della prestazione o della revoca del consenso, la sicurezza nella conservazione dei dati. L'intento di fondo, coerentemente con quanto già osservato in merito ai servizi di intermediazione dei dati, è quello di corroborare la fiducia del pubblico nell'affidabilità di tali organizzazioni (cfr. Considerando 46), permettendo così alle altre forme di *nudging* che sostengono le motivazioni altruistiche (ad es. le campagne pubbliche di sensibilizzazione) di trovare un valido sistema di instradamento. Da notare inoltre la previsione, all'art. 25, di un modulo europeo di altruismo dei dati volto a permettere la raccolta del consenso in un formato uniforme presso tutti gli stati membri [55]; tema che solleva la grande questione – ampiamente dibattuta soprattutto nel contesto della ricerca scientifica e malauguratamente lasciata irrisolta dal DGA

[53] V. a questo riguardo D. SAMARDZIC, T. BECKER, *Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps*, in *EuZW*, 2020, p. 646.

[54] J. KÜHLING, R. SCHILDBACH, *Corona-Apps. Daten– und Grundrechtsschutz in Krisenzeiten,* in *NJW,* 2020, p. 1545, alla p. 1546; v. per informazioni attuali *https://corona-datenspende.de*.

[55] Sul punto, e per i problemi di rapporti con il GDPR, P. V. HAGEN, L. VÖLZMANN, *Datenaltruismus aus datenschutzrechtlicher Perspektive. Wechselwirkung zwischen DGA und DS-GVO*, cit., p. 177 ss.

(v. Considerando 50) – dei limiti di ammissibilità del c.d. *broad consent*[56].

Qui si arresta la portata dell'intervento europeo, sia perché non sono previste disposizioni puntuali né sui rapporti tra il "donante" dei dati e le organizzazioni di altruismo, né su quelli intercorrenti tra tali organizzazioni e i terzi destinatari finali dei dati[57]; sia perché l'art. 16 è univoco nel rimettere agli stati membri l'adozione di politiche mirate di supporto all'altruismo dei dati, anche attraverso l'adozione di specifiche misure organizzative o tecniche.

7. *Luci e ombre del modello europeo*

Nel proporre una valutazione conclusiva dell'itinerario intrapreso con il DGA si deve necessariamente tratteggiare un quadro connotato da luci e da ombre.

Dal primo punto di vista, merita indubbio apprezzamento la linea di politica del diritto che sorregge il nucleo embrionale del nuovo diritto europeo dei dati, costituito dal DGA e destinato ad essere ulteriormente arricchito dal Data Act. Come si è illustrato in precedenza, questo non è più unicamente improntato a un'attitudine difensiva, ma persegue un intento di apertura dei silos informativi e messa a frutto del valore dei dati – personali e non personali – presenti in Europa attraverso la costituzione di spazi comuni di dati rimessi alla libera circolazione intracomunitaria. Tale progetto – che non va visto in autonomia, bensì in connessione con quello non meno importante concernente le infrastrutture digitali europee[58] – è cruciale sia sul piano della politica industriale, poiché nel medio periodo potrebbe contribuire alla riduzione della dipendenza strategica delle nostre imprese dalle grandi piattaforme di dati transnazionali[59], sia su quello delle politiche sociali, atteso che qualsiasi processo di innovazione volto a sfruttare le opportunità dischiuse dalle tecniche di intelligenza artificiale richiede inevitabilmente la disponibilità di parchi di dati strutturati in formato leggibile dalle macchine e interoperabili. Ovviamente la specifica curvatura impressa al nuovo sistema eu-

---

[56] R. SCHILDBACH, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes*, cit., p. 151.

[57] *Ibidem*.

[58] B. FALKHOFEN, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X*, cit., p. 791.

[59] In generale v. M. DENGA, *Digitale Souveranität durch Datenprivatrecht?*, in *GRUR*, 2022, p. 1113.

ropeo di governo dei dati non può implicare la radicale eliminazione delle garanzie – in particolare con riferimento al trattamento dei dati personali – costruite con fatica nel corso di un lungo processo di interazione tra diritto interno e diritto sovranazionale [60], ma richiede una delicata operazione di adattamento del quadro giuridico preesistente alla nuova realtà definita dalla transizione digitale.

È proprio in relazione a tale profilo che emergono alcune ombre dell'impianto regolatorio europeo. Un primo rilievo critico attiene all'eccessivo appesantimento burocratico e all'idea che la predisposizione di una cornice istituzionale adeguata possa di per sé condurre agli esiti auspicati dal legislatore. Complice il limite delle competenze unionali, non può certo ignorarsi che la semplice definizione di una nuova forma giuridica per i servizi di intermediazione o per le organizzazioni di altruismo dei dati non sia di per sé garanzia dell'attrattività sul piano costi/benefici di tali attività e dunque della loro effettiva intrapresa [61]. In assenza di adeguate politiche di incentivazione, in primo luogo di carattere fiscale, e in presenza di un fitto reticolato di obblighi procedurali e sostanziali che generano non irrilevanti oneri di compliance, non è remoto il rischio che l'impatto reale di tale disciplina risulti meno soddisfacente di quanto auspicato [62], anche perché per contendere il primato delle piattaforme transnazionali i nuovi soggetti dovrebbero fare scala e raggiungere livelli dimensionali e organizzativi elevati. Un secondo ordine di considerazioni, di tenore opposto, attiene alla difficoltà del sistema di coordinamento con il quadro normativo preesistente e alla portata ancora troppo limitata delle sue modifiche [63]. Uno dei problemi fondamentali da questo punto di vista è costituito dalla tensione intrinseca tra il GDPR e la normativa volta a incoraggiare la condivisione dei dati. La scelta del legislatore è stata quella di riaffermare, in caso di contrasto, la prevalenza del GDPR e di escludere che il DGA possa costituire una valida base giuridica per il trattamento, nonché influire su diritti e obblighi previsti dalla normativa sulla protezione dei dati (art. 1, comma 3). Il prevedibile effetto di un siffatto modello di interazione è quello di depotenziare gli strumenti messi in campo dal DGA per promuovere una maggiore circolazione dei dati.

---

[60] A. ROßNAGEL, *Grundrechtsschutz in der Datenwirtschaft. Vorsorgeflichten in der Data-Governance,* in *ZRP*, 2021, p. 173.

[61] H. RICHTER, *Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance",* cit., p. 646 ss.

[62] Così M. HENNEMANN, L. v. DITFURTH, *Datenintermediäre und Data Governance Act*, cit., p. 1910.

[63] B. FALKHOFEN, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X*, cit., p. 790.

Basterà considerare soltanto tre esempi, che appaiono particolarmente significativi.

Al primo si è già fatto cenno in precedenza, trattando delle organizzazioni di altruismo dei dati [64]. L'idea della "donazione" dei dati per determinate finalità di interesse generale è di per sé interessante e atta a colmare il divario tra la disciplina del corpo (incentrata sul modello del dono solidaristico) e quella dei dati [65]. Tuttavia, in assenza di disposizioni di natura sostanziale che circoscrivano il requisito della specificità del consenso e ammettano la possibilità di destinare dati personali per scopi altruistici a ambiti o linee di ricerca o altre politiche sociali, con effetto di armonizzazione sovranazionale, l'altruismo dei dati rischia di tradursi in una mera formula di facciata, un dispositivo di marketing normativo privo di significativo impatto operazionale [66].

Il secondo esempio concerne il rapporto tra intermediari dei dati e esercizio dei diritti dell'interessato (lo stesso tema emerge in relazione all'autorizzazione al trattamento dei dati, ma verrà trattato di seguito). Perché i fiduciari possano adempiere efficacemente i compiti loro assegnati parrebbe importante riconoscere in capo a costoro la facoltà di sostituirsi all'interessato nell'esercizio dei diritti *ex* artt. 15 ss. GDPR [67]. Tuttavia, è dubbio che tale soluzione sia praticabile alla luce del diritto vigente. Da un lato il DGA usa espressioni ambigue, che riflettono una malcelata incertezza circa la natura dei poteri vantati dai fiduciari. L'art. 2, comma 1, n. 11, nel definire i servizi di intermediazione dei dati, fa riferimento a una funzione strumentale all'instaurazione di rapporti commerciali tra gli interessati e gli utenti dei dati «*anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali*». Il Considerando n. 30, dopo aver premesso che il ricorso a servizi di intermediazione potrebbe permettere di «*rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano*», prospetta un mero ruolo di assistenza. Si afferma infatti che gli intermediari «*assisterebbero i singoli individui nell'esercizio dei loro diritti a norma del regolamento (UE) 2016/679, in particolare gestendone la concessione e la revoca del consenso al trattamento dei dati, il diritto all'accesso ai propri dati, il diritto alla rettifica dei dati personali inesatti, il diritto alla cancellazione o "diritto all'oblio", il diritto alla limitazione del trattamento e il diritto alla portabilità dei da-*

---

[64] Cfr. *supra,* par. 4.3.

[65] G. RESTA, voce *Contratto e diritti fondamentali*, in *Enc. dir. – I tematici*, I, *Contratto*, Milano, 2021, p. 291 ss., pp. 302, 306.

[66] R. SCHILDBACH, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes*, cit., p. 152 ss.

[67] C. BEISE, *Datensouvernaität und Datentreuhand*, in *RDi*, 2021, p. 597.

ti». Benché la terminologia impiegata sia tutt'altro che inappuntabile, sembrerebbe che le formule utilizzate evochino l'idea di una amministrazione meramente tecnica di determinazioni di volontà riferibili all'interessato (il modello sembra essere quello dei "*personal information management services*"), così confermando l'idea dell'assenza di autonomo potere decisionale in capo al fiduciario. Dall'altro lato, un'interpretazione diffusa dell'art. 80 GDPR, enfatizzando la lettera del primo comma, limita la possibilità di conferire mandato a enti e organizzazioni collettive soltanto in ordine alla proposizione del reclamo e all'esperimento dei rimedi giurisdizionali di cui agli artt. 77 ss. GDPR, escludendo invece l'ipotesi dell'esercizio dei diritti di cui agli artt. 15 ss.[68] Premesso che a chi scrive una siffatta interpretazione non appare né obbligata né persuasiva – l'apparente lacuna può essere ragionevolmente colmata attraverso un'applicazione analogica dell'art. 80, comma 1[69] – è innegabile che una più coraggiosa formulazione del DGA avrebbe contributo a rimuovere tale incertezza e legittimare una soluzione più funzionale agli scopi perseguiti (peraltro perfettamente in linea con le stesse indicazioni della legge 675/1996 che all'art. 13 prevedeva espressamente il diritto di conferire mandato a enti collettivi per l'esercizio dei diritti dell'interessato).

L'ultimo esempio concerne le cooperative di dati. Qui si deve innanzitutto osservare che, sul punto dell'esercizio dei diritti dell'interessato *ex* art. 15 ss. GDPR, il testo finale del DGA segna un progresso significativo rispetto all'originaria Proposta della Commissione. Difatti, il Considerando 24 della Proposta, specificamente concernente le cooperative, affermava: «*è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati*»[70]. Il riferimento al "conferimento" e alla "delega" è scomparso dal testo finale del Regolamento. Nel corrispondente Considerando 31 si legge ora, invece, che «*i diritti a norma del Regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunziarvi*». Sebbene gli esercizi di esegesi delle norme di matrice europea sulla base delle categorie del diritto interno debbano sempre essere condotti con grande prudenza, sembrerebbe ragionevole ritenere che mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento

[68] Si registrano però alcune aperture sul punto da parte dell'EDPB, *Guidelines 01/2022 on data subject rights – Right of access*, 18 january 2022, p. 27.

[69] L. SPECHT-RIEMENSCHNEIDER *et al.*, *Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung*, cit., p. 43.

[70] EDPB-GEPD, *Parere congiunto sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati*, 2021, p. 35.

in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria. Sembrerebbe quindi aprirsi un più ampio spazio operativo quanto meno per la tutela esterna dei diritti degli interessati da parte di una cooperativa di dati che operi come rappresentante dei suoi membri [71]. Ciò detto, si apre un secondo problema, che attiene non tanto al profilo negativo della tutela, quanto a quello positivo dello sfruttamento mediante attività negoziale con terzi. La logica stessa di una compagine con scopo mutualistico suggerirebbe l'opportunità di riconoscere un conferimento dei dati con correlativi poteri dispositivi in capo alla società. Tuttavia le formule legislative sembrano escludere una siffatta possibilità, sia perché tra gli obblighi imposti ai servizi di intermediazione v'è quello della neutralità (art. 12, comma 1, lett. a), così da escludere qualsiasi attività di *data analytics* prodromica ad un'efficace attività negoziale con terzi (questa ad esempio è la logica organizzativa di Drivers' seat e di altre cooperative nel settore della mobilità) [72]; sia perché il DGA in diversi punti sembra espressamente limitare il ruolo delle cooperative – e a maggior ragione degli altri intermediari dei dati – a un'attività di consulenza precedente alla manifestazione del consenso, o al massimo a quella di trasmissione a terzi della manifestazione di volontà dell'interessato [73]. Il consenso, in altri termini, figura nell'impianto del DGA come atto personale non delegabile a terzi. Nel Considerando 31 è contemplato tra gli obiettivi della cooperativa quello di «*rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di* acconsentire all'utilizzo dei dati*, influenzando i termini e le condizioni stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo*»; nell'art. 12, comma 1, lett. m*,* nel delineare il contenuto fiduciario dei doveri gravanti sugli intermediari di dati personali (tra i quali rientrano le cooperative), contempla specifici compiti di consulenza, in modo tale da fornire agli interessati adeguate informazioni sulle proposte negoziali dei terzi «*prima che gli interessati diano il loro consenso*». D'altronde già sul piano della teoria generale del consenso al trattamento dei dati, è prevalente – ma non unanime – l'opinione che esclude la possibilità di rappresentanza, riconoscendo a tale atto natura personalissima [74]. Non c'è quindi da stupirsi per la timidezza mostra-

[71] L. SPECHT-RIEMENSCHNEIDER *et al.*, *Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung*, cit., p. 41 ss.

[72] Sul punto E. BIETTI, A. ETXEBERRIA *et al.*, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., pp. 17-18.

[73] Così, criticamente, M. DENGA, *Digitale Souveranität durch Datenprivatrecht?*, cit., p. 1118.

[74] S. ERNST, *Die Einwilligung nach der Datenschutzgrundverordnung*, in *ZD*, 2017, p. 110, alla p. 111.

ta dal legislatore del DGA, anche se bisognerebbe riconoscere che lo strumento della cooperativa dei dati, per conseguire efficacemente i propri scopi sociali e per contendere il primato del modello imprenditoriale lucrativo, necessita un più ampio margine di azione e un quadro giuridico abilitativo[75]. È per questa ragione che lo stesso totem della natura personale del consenso, che pure costituisce un baluardo dell'autodeterminazione nell'ambito dei rapporti di mercato, trasposto alla sfera dei rapporti fiduciari e ai sistemi di imprenditoria sociale, meriterebbe forse di essere superato. D'altronde l'intera esperienza della negoziazione dei diritti della personalità ha fatto emergere, nelle pieghe delle declamazioni dottrinarie, spazi inaspettati di esercizio dell'autonomia privata (si pensi alla concessione di licenze con effetti reali)[76], che richiedono di essere opportunamente valorizzati, sì da riconoscere la possibilità di rappresentanza nell'espressione del consenso al trattamento dei dati, con il solo limite della soggezione della procura dei requisiti fissati dall'art. 7 GDPR, e in particolare a quello della specificità[77]. D'altronde l'art. 8 GDPR prevede espressamente che gli esercenti la potestà genitoriale possano validamente esprimere un consenso per il minore d'età, e il mero silenzio in ordine all'ipotesi della rappresentanza volontaria non può essere di per sé inteso come un divieto[78].

In conclusione, l'itinerario intrapreso a livello europeo merita nel complesso apprezzamento, ma si deve auspicare un ulteriore sforzo nel valorizzare la dimensione relazionale e collettiva del trattamento dei dati[79], anche aprendo con più decisione all'autonomia contrattuale, oltre le strettoie imposte da una lettura eccessivamente individualistica del sistema delineato dal GDPR. Se non si compie un passo più deciso in questa direzione, non si vede come si possa sciogliere la contraddizione di fondo derivante dal fatto che il DGA e il Data Act intendono creare un mercato dei dati, mentre la normativa di *Datenschutz* è mirata a sottrarre i dati al mercato.

---

[75] E. BIETTI, A. ETXEBERRIA *et al.*, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 18.

[76] G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 320 ss.; V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, p. 545.

[77] L. SPECHT-RIEMENSCHNEIDER *et al.*, *Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung*, cit., pp. 41-42.

[78] *Ibidem.*

[79] S. VILJOEN, *A Relational Theory of Data Governance*, in 131 *Yale L.J.* 573 (2021).

CONCLUSIONI

INTELLIGENZA ARTIFICIALE E *SMART CITIES*. SFIDE E OPPORTUNITÀ

di *Pasquale Stanzione*

Il fenomeno delle *smart cities* è così peculiare da poter essere assunto, in un certo senso, a paradigma della società digitale nella sua fase attuale, dell'internet di ogni cosa e dell'algocrazia. Queste espressioni sottolineano i profondi mutamenti sociali, antropologici, culturali, determinati dalla diffusione dell'intelligenza artificiale nelle nostre vite e dall'autonoma interazione di tutto, sì che oggetti di utilizzo quotidiano, dispositivi di mobilità, finanche il territorio, divengono snodi attraverso i quali si producono e si veicolano ingenti quantità di dati, naturalmente anche e soprattutto personali.

Ad essere connesse e inserite in un flusso informativo continuo sono, così, le nostre case, le nostre relazioni sociali, persino le nostre città, nella loro duplice dimensione di strutture urbanistiche e di comunità di persone, di nucleo ad un tempo territoriale e sociale.

Riconoscimento facciale e telecamere intelligenti divengono sempre più strumenti ordinari di *governance* urbana. Le implicazioni di ordine culturale, giuridico, politico e simbolico che derivano dalla delega alla tecnica della gestione dello spazio urbano sono determinanti e forse neppure integralmente prevedibili, nel loro straordinario impatto trasformativo, nel loro configurare una vera e propria rivoluzione di senso, non "soltanto" del determinismo tecnologico e dell'architettura sociale.

Il digitale, in questo modo, da mezzo diviene ecosistema in cui si sviluppa, nella sua duplice componente, individuale e collettiva, la vita della persona.

La *smart city* è, in questo senso, figura paradigmatica sia di questa linea di tendenza sia della sua ambivalenza. Le città connesse sono, infatti, soluzioni all'avanguardia ideate per promuovere una mobilità (definita appunto "intelligente", ma anche "sostenibile") il più possibile efficiente e regolare, migliorando la qualità dei servizi offerti ai cittadini; garantendo anche, in caso di incidenti o comunque di illeciti, la possibilità di ricostruirne la dinamica, favorendo così l'accertamento delle relative responsabilità, come in una grande *black box*.

Le città connesse si avvalgono di reti stradali intelligenti progettate in modo da poter consentire l'analisi dei flussi di traffico, con sistemi di segnaletica stradale, semafori, videocamere connessi tra loro e al *web*. La *smart city* è, quindi, un esempio di progettazione urbanistica (e in questa misura sociale, oltre che territoriale), fondata sullo sfruttamento di *big data* per l'ottimizzazione della mobilità ma, più in generale, dei servizi pubblici e, nelle esperienze (o, forse, intenzioni) migliori, per la democratizzazione dell'accesso ad essi.

La *smart city* dovrebbe dunque, almeno nella sua migliore concezione, non limitarsi alla c.d. "*uberizzazione*" dei servizi pubblici e della mobilità, ma promuovere il ripensamento dello spazio urbano in funzione delle esigenze dei cittadini, oltre che dell'ambiente, integrando vicendevolmente spazio fisico e virtuale, così da realizzare una nuova dimensione urbana.

In questo senso, si attribuisce alla città intelligente un'accezione anche valoriale che la distingue dalla mera società digitale, per la sua finalità di incidenza pure sulla dimensione sociale e democratica. La città intelligente dovrebbe, quindi, definirsi tale per come si relaziona con il cittadino e ne favorisce la qualità della vita, promuovendone anche condizioni migliori per le minoranze più vulnerabili o svantaggiate (si pensi alle specifiche funzionalità progettate per consentire ai disabili una migliore fruizione dei servizi urbanistici).

Smart, in altri termini, dovrebbe ritenersi la città non soltanto ecosostenibile, "del benessere e della conoscenza", ma quella in cui l'innovazione è funzionale alla migliore allocazione delle risorse e alla corretta erogazione dei servizi, in ragione delle necessità degli utenti. Ciò presuppone, dunque, non soltanto un ambiente, ma un governo intelligente degli spazi urbani, che si avvalga della crescente disponibilità di dati ricavati dalla connessione delle infrastrutture urbane digitalizzate, per promuoverne un'analisi e un utilizzo funzionale non già al controllo, ma alla libertà, all'eguaglianza, al superamento delle discriminazioni, alla promozione delle minoranze.

Come tutte le espressioni della tecnica (prima ancora che della tecnologia), anche le *smart cities*, la mobilità intelligente, presentano infatti una forte ambivalenza e possono, in ragione dell'utilizzo cui siano sottoposte, avere implicazioni estremamente positive o, per converso, altrettanto negative. Così, in particolare, l'intelligenza urbana può ridisegnare la morfologia del territorio, ma anche del controllo, favorendo, in ragione della sua applicazione, l'espansione o, per converso, la contrazione delle libertà.

Il flusso di dati utile al governo intelligente delle città può, infatti, in assenza di limiti e di requisiti stringenti, alimentare una forma di sorveglianza ubiquitaria e costante, capillarmente diffusa sul territorio. Ne sono un esempio alcune delle più avveniristiche città cinesi, disseminate di videocamere e di sistemi di riconoscimento facciale.

Quella al controllo permanente e senza limiti è, peraltro, nella realtà cinese, una tendenza inevitabilmente espansiva e come tale non circoscritta al solo ambito urbano, con cui inevitabilmente dovrà fare i conti la nuova legge sulla protezione dei dati, recentemente approvata sul modello del GDPR.

Del resto, la tendenza all'espansione del controllo è uno dei rischi impliciti nell'uso non adeguatamente regolato e lungimirante della tecnologia, che, come ogni forma di potenza, può, in assenza di una "visione", degenerare in eccesso acritico.

È significativo, in questo senso, che il recente *draft* di regolamento europeo sull'IA sia fondato su di una tassonomia di limiti e di condizioni per le varie fattispecie di ricorso a questa tecnica, fondate proprio sui rischi sociali suscettibili di verificarsi. In cima alla "piramide" di rischiosità dei vari usi dell'IA vi sono, significativamente, quelli fondati su tecniche subliminali tali da condizionare il comportamento altrui o da sfruttare le vulnerabilità di gruppi sociali, nonché sistemi di *social scoring* basati sul monitoraggio del comportamento individuale. È un limite importante, che contrasta non solo derive simili a quelle del modello cinese, ma anche quell'"*automating poverty*" propria del ricorso ad algoritmi potenzialmente (ancorché non intenzionalmente) discriminatori, per l'erogazione di prestazioni di *welfare*.

Ne è un esempio il sistema olandese di verifica antifrode (SyRI) ritenuto illegittimo dalle corti interne e definito strumento al servizio dello *Stato di sorveglianza per i poveri* dall'alto rappresentante ONU per i diritti umani, in quanto capace di individuare, con un monitoraggio socialmente selettivo, proprio le fasce più svantaggiate della popolazione. E tra gli usi tendenzialmente vietati, salve esigenze imperative socialmente rilevanti e normativamente definite, vi è anche il riconoscimento facciale a fini di contrasto, oggetto da noi di un recente divieto generale e di limiti stringenti per l'uso in ambito giudiziario penale e di polizia. Si tratta di previsioni necessarie per un governo antropocentrico dell'innovazione, che ne eviti eccessi socialmente regressivi.

Questo vale anche per la "rivoluzione" dei *big data*, di cui le *smart cities* e l'*IoT* sono espressione.

L'apparente "innocuità" di oggetti o di servizi di uso quotidiano connessi però al *web*, induce, infatti, a sottovalutare le loro potenzialità anche nel rivelare, mediante l'uso secondario dei dati raccolti, stili di vita, capacità economica, finanche patologie o dipendenze (per la *smart home*) e relazioni, spostamenti, frequentazioni (per la *smart city*).

A causa delle elevate capacità di reidentificazione delle attuali tecnologie e, quindi, della loro suscettibilità di favorire forme di monitoraggio pervasive, le maggiori garanzie per le libertà dell'utente s'inscrivono nella disciplina di protezione dei dati, che incide sulle condizioni e sui limiti di circolazione e di

sfruttamento di quel bene giuridico (sempre più economicamente appetibile) che sono i dati personali. Contribuendo, anche, a minimizzare il rischio, inaccettabile anzitutto sul piano culturale, di intendere la cessione dei propri dati, quale tributo necessario alla fruizione dei vantaggi offerti, solo apparentemente *priceless,* dal pianeta connesso.

Pur informandosi al principio di neutralità tecnologica – per evitare di cristallizzare le norme in un determinato contesto tecnico, suscettibile di veloce obsolescenza –, il GDPR contiene, infatti, alcune norme e garanzie di particolare interesse per i trattamenti su larga scala come quelli realizzati su *big data*.

Anzitutto, il criterio di applicabilità del Regolamento stesso anche a trattamenti svolti da imprese situate all'estero, ma i cui servizi siano destinati a (o profilino) persone che si trovino nell'Unione Europea. Si tratta di un'innovazione importante, che consente di attrarre nella giurisdizione europea i *big player* dell'economia digitale, situati prevalentemente oltreoceano e che accentrano nelle proprie mani la pressoché totalità dei *big data*. Con la limitazione, che necessariamente ne consegue, delle garanzie dei cittadini rispetto all'uso dei loro dati e con gli squilibri e le asimmetrie nei rapporti di forza che inevitabilmente ne derivano, sul piano geopolitico. Del resto, in una realtà, quella digitale, per sua stessa natura refrattaria ai confini di leggi e di giurisdizioni, la tutela dei cittadini rispetto a un diritto fondamentale, quello alla protezione dati, non può che essere uniforme e ugualmente garantita a prescindere da stabilimenti più o meno di comodo del titolare.

Come scelte di merito rilevano, in particolare, l'anticipazione della soglia di tutela dei dati alla fase della progettazione dei sistemi, inscrivendo così nelle stesse tecnologie le garanzie per gli utenti e la tutela rafforzata accordata, tra gli altri, ai dati biometrici sui quali, ad esempio, si fonda il riconoscimento facciale.

Rilevante anche il principio di responsabilizzazione del titolare su cui si fonda l'intero Regolamento e che impone, ad imprese (o professionisti), di adottare strategie aziendali che garantiscano un livello di tutela dei dati personali adeguato al livello di rischio proprio del trattamento e idonee misure preventive.

Rilevantissima, inoltre, la *privacy by design* e *by default*, volta a incorporare negli stessi sistemi e dispositivi misure di minimizzazione. Il generale innalzamento dei livelli di sicurezza e di resilienza dei sistemi, promosso dal GDPR, è poi strategico nel contrasto delle minacce cibernetiche, che sempre più si avvalgono delle vulnerabilità dei dispositivi IoT e delle infrastrutture digitali poco protette delle *smart cities*, con effetti, soprattutto in quest'ultimo caso, paralizzanti per l'intera collettività.

Innovative sono poi le garanzie adottate rispetto ai processi decisionali au-

tomatizzati, sui quali si basa l'economia dei *big data*, assicurandone la contestabilità e la trasparenza della logica, dei criteri e delle sue conseguenze ed esigendo, almeno in ultima istanza, il filtro dell'uomo, per contrastare la delega incondizionata al determinismo dell'algoritmo.

La protezione dei dati, del resto, è funzionale anche alla stessa correttezza del processo analitico fondato su *big data*, ove le scelte algoritmiche sono rese possibili dall'auto-apprendimento di cui è capace la macchina a partire dai dati immessi e di cui va quindi garantita la qualità. Dall'esattezza dei dati utilizzati nella configurazione degli algoritmi dipende l'"intelligenza" delle loro scelte. Se è errata la classificazione delle casistiche di riferimento fornita all'algoritmo per assumere determinate decisioni operative, anche queste saranno inevitabilmente viziate, spesso con danni incalcolabili, non solo nel settore sanitario o militare.

La protezione dei dati, dunque, tutt'altro che un ostacolo, è invece un presupposto di efficacia della *big data analytics* e, quindi, della funzionalità di case, lavoro, città intelligenti. Che saranno tali, se renderanno la tecnologia funzionale all'espansione dei diritti e delle libertà e non alla loro contrazione, per una malintesa idea di sicurezza o, peggio, per fini di profitto. In questa strategia di "umanizzazione" e funzionalizzazione della tecnica alla libertà, la disciplina di protezione dei dati è destinata a giocare un ruolo primario: di limite e di orizzonte di senso. Contribuiamo quindi tutti, con il rispetto delle sue norme e la consapevolezza della sua rilevanza, a promuoverne il valore.

Finito di stampare nel mese di ottobre 2023
nella Stampatre s.r.l. di Torino
Via Bologna, 220

DIMENSIONE GIURIDICA | LEGAL DIMENSION

Studi per il Dottorato in Scienze Giuridiche dell'Università di Firenze

Volumi pubblicati:

1. D. Bianchi-M. Rizzuti (a cura di), *Funzioni punitive e funzioni ripristinatorie. Combinazioni e contaminazioni tra sistemi*, 2020.
2. S. Cocchi-A. Simoni (eds), *Freedom v. Risk. Social Control and the Idea of Law in the Covid-19 Emergency*, 2022.
3. D. Bianchi (a cura di), *Distribuzione del rischio sanitario tra responsabilità dell'organizzazione e responsabilità individuali*, 2021.
4. E. Cremona-F. Laviola-V. Pagnanelli (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, 2022.
5. M. Giannelli-V. Pagnanelli (a cura di), Smart cities*. Diritti, libertà e governance*, 2023.