# Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica?

Federica Paolucci - Oreste Pollicino


## Abstract

Parlare di città intelligente può sembrare un argomento di fantascienza. Eppure, dati, intelligenza artificiale e sensori sono strumenti che sempre di più fanno parte del panorama urbano. La presente analisi offre una panoramica dei principali interrogativi su cui può appuntarsi il contributo del diritto costituzionale. Difatti, è innegabile che la *smart city* pone delle sfide che concernono sicuramente il mercato, ma anche il nuovo assetto di poteri in ambito digitale.

Talking about a smart city may sound like science fiction. Yet, data, artificial intelligence, and sensors are tools that are increasingly part of the urban landscape. This analysis offers an overview of the main questions to which constitutional law can contribute. Undeniably, the smart city poses challenges that concern the market and the new order of powers in the digital sphere.


## Sommario




## Keywords

smart city - dati - protezione dati - privacy - digitalizzazione


* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". Il presente lavoro è frutto dell'attività di ricerca dei due autori. In particolare, i paragrafi 2 e 2.1 sono attribuibili interamente a Oreste Pollicino, mentre i paragrafi 3 e 3.1 a Federica Paolucci. I paragrafi 1 e 4 sono attribuibili a entrambi.

## 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 concentrarsi sull'*humus* che sta consentendo l'intersecazione tra spazio urbano e rete: i dati. Difatti, gli incessanti flussi di 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 questi 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

[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.

[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*, 56, 2017, 122 ss.

[4] Come è 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 particolare R. Kitchin - G. McArdle, *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets*, in *Big Data & Society*, 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,* 2 (1), 2016, 28 ss.

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 possono prescindere dall'esperienza fisica, sicché 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, sta venendo a formarsi un "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 normative del legislatore europeo. Quest'ultimo, 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

[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 & Technology*, 34 (3), 2020, 254 ss.

[10] J. Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation,* in *Philosophy & Technology*, 29 (3), 2016, 245 ss.

[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.

[12] 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).

[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.

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 stati previsti nel regolamento (UE) 2016/679[14], come la portabilità, e che, sulla base di determinati presupposti, riguarderanno sia i dati personali sia quelli non personali. La circolazione dei dati diviene, dunque, in questo contesto, la principale infrastruttura della città intelligente. D'altro canto, 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.

A partire, dunque, da una cornice generale ove si è cercherà di porre in evidenza come i diritti individuali vengono messi ulteriormente in discussione nell'assetto della città intelligente, l'analisi riguarderà nel particolare la sfida posta al sistema della privacy europeo. La tematica in esame verrà trattata considerando anche la diffusione di questo modello anche al di fuori dell'ambito comunitario. In secondo luogo, si evidenzierà 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.

## 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 ricorrendo ad una *governance* partecipativa[15]. È indubbio il fatto che l'innovazione e la tecnologia rappresentano degli importanti 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

[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.

[15] F. Toni, *Smart city: innovazione e sostenibilità*, in *EAI Energia, Ambiente, Innovazione*, 5, 2021, 35 ss.

[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 *AI 4 Good* consultato in data 25 marzo 2022.

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 considerabile 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]. Nonostante, 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 della comunità[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 rea-

[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,* 5 (3), 2016.

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

[19] A tal riguardo, si rimanda a L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2012*,* spec. 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. 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,* 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*, 2, 2021. Peraltro, la recente pronuncia nel

lizzano i diritti democratici dei cittadini, come nel caso della libertà di assemblea o di associazione. 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 espressione; il diritto alla cultura; il diritto all'identità e all'autonomia; il diritto all'autodeterminazione; il diritto alla privacy – vengono materialmente mediati dai soggetti privati. Si realizza, dunque, un'inscindibile unione tra la persona *offline* e *online*. 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 urbana[25]. In particolare, è necessario chiedersi: in una città che tutto vede, tutto processa, come può darsi il diritto all'identità, il diritto all'autodeterminazione, 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[26]. 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[27]. La sfida non ricade solamente sull'attore privato che deve avere chiaramente un ruolo prominente nel progettare sistemi tecnologici rispettosi dei diritti umani. Tuttavia, è altresì vero che il principale ruolo è rivestito dai pubblici poteri, che vengono chiamati a dotarsi di un nuovo sistema di *governance* ove le tradizionali risorse del diritto devono attagliarsi a scenari inediti, come si dirà nella seconda parte di questo contributo.

In merito, dunque, alla tutela dell'identità di ognuno nello spazio intelligente, un note-

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 opionin* 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*".

[23] D. Mac Sithigh, *Virtual walls? The law of pseudo-public spaces*, in *International Journal of Law in Context*, 8 (3) 2012, 394 ss.

[24] Cfr. J. Danaher, *he Threat of Algocracy,* cit.

[25] C. Ratti, *La città di domani. Come le reti stanno cambiando il futuro urbano,* cit.

[26] 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.

[27] 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, 5.

vole valore deve essere dato alla *privacy*. È proprio nella facoltà di aggirarsi liberamente per lo spazio urbano, senza il rischio di eccessive intrusioni nella sfera privata[28], che si sostanzia l'ancillare concezione della *privacy*, così come venne intesa da Warren e Brandeis[29].

Giova rammentare, a tal proposito, che in ambito europeo il percorso di costituzionalizzazione ha compiuto un ulteriore passo con l'adozione del GDPR. 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 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»[30]. 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[31]. 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 su *cloud* sono solo alcuni degli elementi che si crede possano mettere in crisi il sistema del GDPR all'interno della città intelligente[32].

Sebbene vi siano delle proposte su come creare un bilanciamento tra esposizione e riservatezza, tra intrusione e *privacy*[33], queste non appaiono del 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

---

[28] M. Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review*, 49 (5), 2017, 1591.

[29] S. D. Warren - L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review,* 4, 1890.

[30] GDPR, considerando 4.

[31] 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».

[32] 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,* Berlino, 2021.

[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 (MA), 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.

qualitativa della città intelligente. Al contrario, è importante sottolineare 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, si 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 Primo Emendamento europeo. 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, 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

[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, 493 ss.

[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*, 25(2), 2019, 140 ss.

[36] Art. 7 e art. 8 Carta dei diritti fondamentali dell'Unione europea (2000/C 364/01).

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].

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. L'ambiente intelligente, come si diceva nel paragrafo precedente, creano le condizioni perché si possa pienamente parlare di sistema *onlife*: vale a dire l'esperienza di una realtà iper-connessa ove è impossibile scindere tra identità analogica e digitale[40].

La tutela, dunque, di questo spazio, almeno in Europa, pare essere ancorata 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. 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[41].

---

[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*, 26, 2015.

[39] Come si vedrà, non sorreggono, peraltro, nemmeno i limiti imposti dal GDPR 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, e 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 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] Detto termine, è un neologismo coniato dal filosofo Luciano Floridi, di cui viene data ampia descrizione e spiegazione nel volume *The onlife manifesto: Being human in a hyperconnected era*, Berlino, 2015.

[41] Y. Ivanova, *The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World,*

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*; le domande su cui il costituzionalista deve interrogarsi riguardano altresì l'interazione degli utenti-cittadini con gli strumenti tecnologici che fisicamente consentiranno alla città intelligente di materializzarsi. A tal riguardo, emerge un rilevante problema riguardante l'accompagnamento e l'educazione all'utilizzo di questi ultimi, giacché è inimmaginabile delegare tale aspetto alla maieutica. Non essendo, tuttavia, la sede per affrontare questo aspetto, la presente analisi si interrogherà in merito alla scelta dello standard cui elevare la tutela della riservatezza pare rilevante se si pensa sia alla programmazione *ex ante* sia all'interazione uomo-tecnologica *ex post*.

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 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[42]. L'equivalenza nel grado di protezione è richiesta, secondo la Corte, in virtù di un'interpretazione della direttiva 95/46/CE alla luce della Carta di Nizza.

in *SSRN,* 2020.

[42] Si vedano in tal senso anche le Conclusioni dell'Avvocato Generale in *Maximillian Schrems c Data Protection Commissioner (Schrems I)*. In particolare, al § 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 § 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».

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 Corte di giustizia 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 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*[43] e *Schrems I*[44], ove la Corte di giustizia 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[45]. Similmente, in *Schrems I*, la valutazione effettuata dalla Corte di giustizia 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[46], resa prima che la Corte di giustizia, in *Google c. CNIL*[47], 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 a sito che web accusato di violare i diritti di proprietà

[43] CGUE, C-131/12 *Google Spain SL e Google Inc c Agencia Española de Protección de Datos, Mario Costeja González* (2014).

[44] CGUE, C-362/14, *Maximillian Schrems c Data Protection Commissioner (Schrems I)* (2015), § 38.

[45] Sulle conseguenze di queste decisioni si veda C. Docksay, *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, *Human Rights Challenges in the Digital Age: Judicial Perspectives*, Strasburg, 2020, 47 ss.

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

[47] CGUE, C-507/17, *Google c CNIL* (2019).

intellettuale dell'attore stesso. Google aveva obbedito all'ordine, anche se la rimozione aveva riguardato soltanto la versione canadese del motore 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 connessa alla natura locale delle giurisdizioni impegnate nell'applicazione dei diritti fondamentali in gioco[48].

La Corte d'Appello della Columbia Britannica rigettò l'appello di Google, sostenendo che la Corte aveva giurisdizione territoriale nel pronunciare quella decisione non solo in Canada, ma altresì al di fuori del suo territorio[49].

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[50]. Secondo la Corte la soluzione adottata da Google era del tutto insoddisfacente dal punto di vista degli attori[51]. 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]. 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.

---

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

[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. Si vedano §§ 47-48 e 50

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

[51] 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.

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

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[54]. Tuttavia, poiché l'ambiente digitale difficilmente riesce a imporsi con barriere e confini, giacché il suo habitat naturale è globale, il caso in esame ha avuto il pregio di dimostrare la necessaria interlocuzione, anche per il tramite delle corti di merito e di legittimità nella scelta e applicazione dello standard di tutela più garantista. Difatti, la Corte canadese comprese che 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[55]. 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].

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 tentavi della Corte digiustizia di assicurare un'effettiva protezione per i diritti dei propri cittadini sotto il profilo transnazionale. In particolare, l'art. 3, par. 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, par. 2, GDPR saranno soggetti alla giurisdizione dell'Unione. Questo approccio permette di superare la dottrina dello stabilimento elaborata dalla Corte di giustizia in *Google Spain*, in quanto persino quegli enti che non siano stabiliti in UE potranno essere soggetti al GDPR. Ancora più importante

[53] Ivi, § 148.

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

[55] 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.

[56] Ivi, §§ 47-48.

[57] In particolare, l'art. 3, par. 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».

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 Corte di giustizia 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]

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. 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 conclusioni, 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.

Orbene, 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.

---

[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 europea 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.*

## 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[59]. 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[60]. Sebbene in un contesto pubblico, sussiste una zona di interazione dei cittadini con gli altri, nella quale si estrinseca un'aspettativa alla *privacy*[61]. 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[62], già ripresa da diverse Corti americane[63], le quali hanno avuto modo di chiarire che «*advances in technology can increase the potential for unreasonable intrusions into personal privacy*»[64].

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

[59] *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.

[60] Si vedano, tra altri precedenti, CEDU, *Botta c. Italia*, ric. 21439/93 (1998)*;* CEDU, *Barbulescu c. Romania*, ric. 61496/08 (2017).

[61] Si vedano, tra altri precedenti, CEDU, *Peck c. Regno Unito*, ric. 44647/98 (2003); CEDU, *Von Hannover c. Germania*, ric. 40660/08 e 60641/08 (2012); CEDU, *Uzun c. Germania*, ric. 35623/05 (2010); CEDU, *Altay c. Turchia*, ric. 11236/09 (2019).

[62] 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), 350.

[63] In particolare, ci si riferisce a diverse importati 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).

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

persone[65].

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 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 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[66], l'attuale esercizio di questa libertà 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. La commercializzazione e la diffusione di sistemi automatizzati non hanno delle ricadute solamente sull'esercizio passivo della libertà d'espressione, 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[67], è possibile evincere che la dimensione attiva abbia un'immensa centralità, non solo in rispetto al *medium* tecnologico, ma anche nella sua dimensione atomica[68]. Proprio in questo contesto, dunque, il paci-

[65] 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».

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

[67] Si veda, ad esempio, la decisione della Corte EDU, *Stern Taulats and Roura Capellera c. Spagna,* ric. 51168/15 e 51186/15 (2018); *Z.B. c. Francia,* ric. 46883/15 (2021).

[68] Questo concetto emerge nella pronuncia *Stern Tautlas c. Spagna* ove al § 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».*

fico 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 per l'impiego di 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 dell'arte, l'educazione alla digitalizzazione è ancora un problema parzialmente irrisolto, così come l'accesso alle stesse e a Internet[69]. 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[70] 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 dalla 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*[71]: 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 delineata e che finora ha riguardato la privacy, la protezione dei dati personali, e la libertà d'espressione, si evince 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 della città intelligente con

[69] 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.

[70] F. Pasquale, *The Black Box Society,* Cambridge (MA), 2015.

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

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 dato avvio a delle iniziative anche in tal senso. Una di queste è il regolamento sui mercati digitali, o *Digital Markets Act* (DMA), la cui proposta è stata presentata insieme al *Digital Services Act*[72]. 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[73].

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.*[74] D'altro canto, però, i medesimi possono rafforzare situazione di 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[75] 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[76]. Difatti, uno dei principali aspetti della *smart city* riguarda proprio la gestione del traffico[77], 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, il 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[78].

---

[72] 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).

[73] Si veda considerando 28 e 32.

[74] Tale aspetto è chiaramente riconosciuto nel DMA al considerando 36.

[75] M. Polo - A. Sassano, *Dma: Digital Markets Act o Digital Markets Armistice?,* in *Mercato Concorrenza Regole*, 3, 2021.

[76] H. Olufowobi - G. Bloom, *Connected cars: Automotive cybersecurity and privacy for smart cities,* in *Smart cities cybersecurity and privacy*, in D. B. Rawat – K. Z. Ghafoor (a cura di) *Smart Cities Cybersecurity and Privacy,* Amsterdam, 2019, 227 ss.

[77] 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.

[78] 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*, 9 (3), 2019, come pure a M. Polo - A. Sassano, *Dma: Digital Markets Act or Digital Markets Armistice?*, cit.

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 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[79], 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[80]. Pertanto, la sfida si situa nella costruzione di una cornice normativa che sia in grado di sostenere gli obbiettivi del mercato unico e, d'altro canto, 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

[79] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 19 (1), 2020, 41 ss.; 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.

[80] L. Floridi, *The European Legislation on AI: A brief analysis of its philosophical approach*, in *Philosophy & Technology,* 34 (2), 2021, 215 ss.

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 [81].

Accanto alla collaborazione e alla *policy* «*by education*», 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 che consentono il funzionamento delle *smart city* saranno stati sviluppati con la collaborazione dei privati, ci saranno maggiori difficoltà nel mantenere una visione della *policy* urbana tutelante le posizioni dei singoli[82]. Si ritiene, in conclusione, che la *data driven regulation*[83] debba essere continuamente assistita da un'analisi di impatto che abbia il suo fondamento nei diritti fondamentali dei cittadini[84]. Una realtà la cui concretizzazione si auspica 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 esposte nell'ambito della digitalizzazione. Considerando le sfide poste alla riservatezza degli individui, nel corso della trattazione si sono indagati elementi di complementarità tra la città di domani e la città di oggi nell'ottica di delineare varchi in cui possano essere garantiti i diritti fondamentali di ciascuno anche nella città progredita dalla tecnologia e dalla diffusione delle reti.

Si tratta di uno "stress test" resosi necessario dall'annessione di sensori e tecnologie intelligenti nell'ambiente urbano: uno spazio in cui pubblico e privato sono necessariamente posti su piani inediti.

A ben vedere, sono argomenti che si inquadrano nel più ampio spettro delle proble-

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

[82] E. Joh, *Policing the smart city*, in *International Journal of Law in Context,* 15(2), 2019, 177-182.

[83] S. Ranchordas - A. Klop, *Data-Driven Regulation and Governance in Smart Cities*, in A. Berlee - V. Mak - E. Tjong Tjin Tai (eds.), *Research Handbook on Data Science and Law*, Groningen, 2018.

[84] 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 uncertainty about the direct and indirect effects of the system on users and the broader environments in which these systems are intended to operate».*

matiche provocate dalla digitalizzazione e con cui il diritto ha avuto a che fare negli ultimi dieci anni. In quest'ottica, la *smart city,* se 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 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[85].
«Siamo chiamati a essere costruttori non vittime del futuro», scriveva Fuller.[86] 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[87], non solo con riguardo al tema della *smart city*, e 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.

[85] F. Toni, *Smart city: innovazione e sostenibilità,* cit.

[86] R. Buckminster Fuller - K. Kuromiya, *Cosmography. A posthumous scenario for the future of humanity,* New York, 1992, 8.

[87] 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.