Convegni

Diritto, Politica, Economia

La città come istituzione, entro e oltre lo Stato

a cura di

Giuseppe Allegri, Laura Frosina, Alessandro Guerra, Andrea Longo

University Press

Sapienza Università Editrice

Collana Convegni 65

La città come istituzione, entro e oltre lo Stato

a cura di

Giuseppe Allegri, Laura Frosina, Alessandro Guerra, Andrea Longo

SAPIENZA
UNIVERSITÀ EDITRICE
2023

Il presente volume è stato pubblicato grazie al Progetto di ricerca di Ateneo – Sapienza, Università di Roma, 2018, dal titolo *Il diritto alla città dalla modernità europea all'età digitale* (coordinato da Andrea Longo) e con il contributo del Progetto di ricerca di Ateneo – Sapienza, Università di Roma (SEED PNR 2021) dal titolo *Città e modelli di* governance *nel XXI secolo*. *Trasformazioni giuridiche*, *istituzionali e sociali della dimensione urbana in prospettiva comparata* (coordinato da Laura Frosina).

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420
Registry of Communication Workers registration n. 11420

ISBN: 978-88-9377-276-1

DOI: 10.13133/9788893772761

Pubblicato nel mese di giugno 2023 | *Published in June 2023*

In copertina | *Cover image*: *The Ideal City*, Walters Art Museum, https://art.thewalters.org/detail/37626/the-ideal-city/. "https://commons.wikimedia.org/wiki/File:Florentine_painter_-_The_Ideal_City_-_Walters_Art_Museum_-_Google_Art_Project.jpg. Fra Carnevale (attribuito), Public domain, via Wikimedia Commons"

Indice

7. *Social scoring* e città distopica: la profilazione del cittadino con finalità di *policy* urbana alla prova dei valori costituzionali

Ylenia Maria Citino

Sommario: 7.1. Profilazione urbana e profilazione del cittadino: sfaccettature di un fenomeno complesso. – 7.2. L'assegnazione di punteggi alla popolazione fra le pratiche potenzialmente scorrette. – 7.3. Confronto tra esperienze di sistemi di *social scoring* e meccanismi reputazionali. – 7.4. Il panottico digitale? – 7.5. *Data first* o *privacy first*: due approcci confliggenti.

7.1. Profilazione urbana e profilazione del cittadino: sfaccettature di un fenomeno complesso

Le potenzialità di Internet si sono dimostrate particolarmente vantaggiose durante la pandemia da COVID-19: gli strumenti di geolocalizzazione e di tracciamento individuale sono stati, infatti, dei preziosi alleati nelle politiche di gestione e contenimento della crisi sanitaria. Se le varie esperienze hanno portato a risultati promettenti sul piano globale e nazionale, non si è potuto fare a meno di trasporre alcune di esse sul piano urbano, il livello di maggiore prossimità col cittadino.

Al contempo, però, le nuove tecnologie hanno sollevato svariati dubbi in merito al rischio di "sorveglianza" da parte degli Stati e alla compatibilità con le necessità di tutela della riservatezza del singolo e dei suoi dati personali[1]. Le nuove iniziative prese a livello comunale

[1] Fra i tanti, cfr. Colapietro & Iannuzzi (2020); Bengio *et al.* (2020); Altmann *et al.* (2020); Sowmiya *et al.* (2021). In particolare, il caso di Singapore illustrato da Bengio (74 e ss.) è di notevole interesse: brevemente, si può dire che il governo ha introdotto l'*app TraceTogether* per contenere la diffusione del virus. Vari cittadini si sono uniti per protestare contro l'applicativo, temendo che Singapore diventasse un "*surveillance State*". Successivamente, l'uso dell'*app* è diventato obbligatorio affinché,

hanno, infatti, mostrato un'attitudine fortemente invasiva delle zone di protezione degli anzidetti diritti.

La dimensione locale, che pur non sfugge alle dinamiche di avanzamento tecnologico, risulta essere più trascurata rispetto ai corposi sforzi regolativi del legislatore europeo, orientati invece a cogliere le sfaccettature ubiquitarie del fenomeno di Internet (Christou & Simpson 2011). Esso, come è noto, si sviluppa sempre più ad un livello transfrontaliero, di difficile "afferrabilità". D'altro canto, esiste un parallelo rischio, che attività locali, lesive dei singoli e condotte sfruttando le nuove tecnologie, proliferino in maniera altrettanto indisturbata.

In questo capitolo, partendo dall'esame di due casi concreti, si affronterà il tema della profilazione urbana, inteso come quel processo di raccolta e analisi di dati in una certa area urbana, con finalità di politiche regolative locali, e del suo intreccio con la profilazione dell'individuo, attività che comporta rischi di interferenza con la riservatezza dei cittadini e la tutela della persona e della dignità umana.

La profilazione trova una sua definizione legale nell'art. 4, comma 4 del Regolamento Generale sulla Protezione dei Dati (*General Data Protection Regulation* o, più comunemente, GDPR)[2], che la definisce come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

---

si giustificava il governo, si potesse passare alla fase di riapertura dalle restrizioni. Si rassicuravano i cittadini promettendo che l'*app* fosse sicura da attacchi di *hacker* e rispettosa della *privacy*: i dati sarebbero stati utilizzati solo per scopi momentanei di contrasto dell'epidemia e la *data retention policy* sarebbe stata breve. Nel gennaio 2021 si è scoperto che i dati dell'*app* venivano condivisi per fini criminal-preventivi e investigativi: il governo si è scusato, giustificandosi asserendo che il monitoraggio era utile per contrastare o reprimere i crimini più gravi ed efferati. Lo studio dimostra, sorprendentemente, che, nonostante i fatti, i cittadini di Singapore hanno dichiarato di fidarsi maggiormente degli enti statali piuttosto che delle *big corporations*. Sulla sorveglianza derivante da tecniche di riconoscimento facciale, v. Mobilio (2021).

[2] 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), in GU L 119/1, 4 maggio 2016.

La profilazione urbana può essere, innanzitutto, una grande opportunità e uno strumento fondamentale nello sviluppo delle *smart cities* del futuro in una chiave di sostenibilità e di miglioramento della qualità della vita che tenga conto dell'aumentato fabbisogno di servizi da parte dei cittadini[3]. Negli ultimi anni, infatti, le tecnologie di intelligenza artificiale che si avvalgono di analisi dei *big data* in combinazione con il *deep learning*[4] sono state applicate al contesto della profilazione urbana. Così, dunque, è stato possibile combinare visualizzazioni su mappe geografiche di dati diversi, qualitativi e quantitativi, attraverso la fusione di informazioni fra loro eterogenee e provenienti da fonti diverse con finalità predittive dei comportamenti umani. Si è trattato, per fare qualche esempio, di dati relativi al traffico e alla mobilità, all'uso delle infrastrutture urbane, alle previsioni meteorologiche; dati provenienti da sistemi di videosorveglianza urbana; persino dati che aiutino a mappare lo stato della criminalità locale.

Il tema degli algoritmi[5] si incastra sulla profilazione urbana poiché di essi ci si avvale al fine di estrarre dati utili dall'enorme mole di informazioni prodotte nel tessuto urbano (*mining*). Tali meccanismi, dunque, portano con sé i noti difetti collegati alla progettazione umana: gli algoritmi operano mediante esemplificazioni, standardizzazioni, operazioni sequenziali che, talvolta, non solo danno luogo a errori ma, soprattutto, riflettono le distorsioni cognitive e i pregiudizi di chi li ha impostati (*bias*)[6].

Il vero rischio, pertanto, si colloca nei processi a monte di raccolta dei dati, che diventano ancora più sensibili se estratti da sistemi di profilazione dell'individuo. Nel caso in cui, infatti, operino *software* applicativi installati su telefoni appartenenti a privati cittadini, rispetto ai quali il consenso risulta essere stato assente, non liberamente espresso o viziato da un'informativa inidonea o carente, possono emergere forti stridori con le tutele apportate dal diritto costituzionale (Casonato 2019) e, nello specifico, dalla disciplina che regolamenta la protezione

---

[3] Sul punto, si legga, ad esempio, lo studio di Foster & Iaione (2016) che promuove un'idea di città sostenibile attraverso una governance urbana collaborativa e nuove forme di "sperimentalismo costituzionale".

[4] Il *deep learning* è una tecnica di apprendimento delle macchine basate su tecnologie di intelligenza artificiale che si avvale di reti neuronali complesse per analizzare grandi quantità di dati in funzione predittiva. V. Koumetio Tekouabou *et al.* (2021).

[5] Fra i tanti, Simoncini (2019) e Nardocci (2021).

[6] Si veda, di recente, una riflessione di Aliprandi (2021).

dei dati personali. Ulteriore criticità deriva dall'assenza di trasparenza sui fornitori di tali servizi. Ancora una volta, va sottolineato che mentre è largamente attuale il tema dell'uso dei *consumer data* da parte delle piattaforme private (Midiri 2020), resta ancora sullo sfondo il risvolto che vede come soggetto collettore un ente pubblico.

Questi processi, come si vedrà, non possono restare in uno stato di anomia normativa, né essere regolati da un legislatore che prova a rincorrere gli avanzamenti tecnologici[7]. I possibili abusi derivanti dai servizi di profilazione del cittadino non possono, perciò, essere affrontati soltanto con un approccio casistico, poiché le infinite potenzialità di sviluppo e di progresso informatico rischiano di provocare nell'interprete un disorientamento giuridico derivante dalla mancanza di solidi appigli valoriali.

Alcuni casi attualmente al vaglio del Garante della Privacy offrono, dunque, l'occasione per illustrare certe dinamiche di *social scoring* nel contesto urbano e per riflettere sui rischi che tali sistemi di valutazione dei residenti producono, configurando una distopica "cittadinanza a punti" e facilitando dinamiche che paiono in netto contrasto con alcuni principi costituzionali fondamentali.

7.2. L'assegnazione di punteggi alla popolazione fra le pratiche potenzialmente scorrette

I casi appena evocati sono diffusi da un comunicato stampa del giugno 2022[8], con cui il Garante della Privacy annunciava l'apertura di tre istruttorie a carico di soggetti pubblici e privati che avrebbero avviato pratiche di profilazione sui propri cittadini. Nella specie, l'Autorità rilevava la problematicità di "iniziative basate su soluzioni di tipo premiale che fanno ricorso a meccanismi di *scoring* associati a comportamenti 'virtuosi' del cittadino in diversi settori (ambiente, fiscalità, cultura, mobilità, sport)": per il Garante, infatti, tali meccanismi comporterebbero l'instaurazione di "una sorta di 'cittadinanza a punti'" potenzialmente lesiva dei diritti e delle libertà degli interessati,

---

7 Su cui valga Costanzo (2012).

8 Garante della Privacy, "*'Cittadinanza a punti': Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini 'virtuosi'*", Comunicato stampa n. 9778361, 8 giugno 2022.

inclusi i soggetti più vulnerabili, poiché alla base di azioni pubbliche di discriminazione sostanziale[9].

La prima *app* sperimentale finita nel mirino del Garante è denominata *IoPollicino* ed è stata programmata nell'ambito del "Progetto Pollicino"[10]. Lanciato dalla Fondazione per lo sviluppo sostenibile, dal Ministero della transizione ecologica e dal Ministero delle infrastrutture e della mobilità sostenibili, l'esperimento ha coinvolto per primo il Comune di Bologna, anch'esso tra gli interpellati dal Garante. L'*app*, come spiega il sito del progetto, richiede una "collaborazione attiva di un campione rappresentativo di cittadini che condividono volontariamente e in forma anonima i dati sui propri spostamenti, lasciati cadere come briciole digitali, con una nuova consapevolezza sul ruolo dei dati e sul loro sfruttamento non commerciale, dedicato solo a finalità sociali e ambientali". Si tratta, con evidenza, di meccanismi premiali per quei cittadini che, almeno sedicenni, installino il software di tracciamento della posizione accettando di essere geolocalizzati. Come risulta dalla c.d. prima fase del progetto, il dispositivo ha raccolto i dati sugli spostamenti degli utenti così ottenuti per due settimane, trasmettendoli poi, in forma "volontaria e anonima" per consentire l'effettuazione di analisi sulla mobilità urbana.

Il Garante fa notare, anticipando in qualche modo la successiva istruttoria, che la modalità di cessione dei dati prodotti dai cittadini è di dubbia compatibilità con le regole sulla tutela dei dati personali. La disponibilità degli utenti ad essere tracciati per due settimane è stata, infatti, oggetto di retribuzione mediante premi messi in palio dai *partner* privati del Progetto. Così, dunque, il rischio di incorrere in sovrapposizioni fra soggetto pubblico e società privata fa sorgere vari interrogativi in capo all'Autorità, non essendo chiare le modalità di trattamento dei dati né, quantomeno, la base giuridica di tali operazioni. All'interno del meccanismo premiale, infatti, si annida l'eventualità di un condizionamento e di una "cattura" del consenso del cittadino, rispetto al quale andrebbe oculatamente valutato se la mera accettazione secondo la logica *take it or leave it* possa essere considerata una condizione legittimante sufficiente.

---

[9] Sul punto, vale la pena di citare lo studio di Caravita (1984), che richiama proprio il valore delle azioni pubbliche a contrasto delle diseguaglianze.

[10] Del Progetto Pollicino, attivato a partire dall'11 maggio 2022 per due settimane, si dà notizia sul sito del Comune di Bologna.

Una seconda iniziativa, sempre all'interno del piano di innovazione digitale del comune di Bologna, è lo "Smart Citizen Wallet"[11], che riprende l'analoga piattaforma "Citizen Wallet", attivata in via sperimentale dal Comune di Roma Capitale[12]. Come risulta dal sito istituzionale, il sistema capitolino è strutturato in maniera tale da incentivare due comportamenti c.d. virtuosi: "la compilazione del questionario sui servizi online di Roma Capitale; l'utilizzo del servizio *tap&go* di ATAC". Per ottenere la premialità, il cittadino, previa sottoscrizione di un'informativa, può iscriversi alla piattaforma con le credenziali del Sistema Pubblico di Identità Digitale (SPID) oppure con quelle della Carta d'Identità Elettronica (CIE) o della Carta Nazionale dei Servizi (CNS).

Con un'idea di sapore orwelliano, il comune di Bologna propone di monitorare il portafoglio "del cittadino virtuoso", il quale verrebbe premiato da agevolazioni monetarie e scontistiche di vario tipo. Questa "patente digitale" sarebbe in grado di identificare i cittadini più meritevoli tra gli utenti volontariamente registrati in un innovativo quanto potenzialmente pervasivo sistema computazionale di sorveglianza. Tramite i dati che l'utilizzatore fornisce periodicamente (e forse inconsapevolmente), si assegnerebbe un punteggio più alto agli utenti dalla condotta impeccabile per attribuire vantaggi economici da parte di soggetti terzi. Come spiegava un amministratore locale in un'intervista al Corriere della Sera, "il cittadino avrà un riconoscimento se differenzia i rifiuti, se usa i mezzi pubblici, se gestisce bene l'energia, se non prende sanzioni dalla municipale, se risulta attivo con la Card cultura" (Rosano 2022).

Infine, l'Autorità sottopone a scrutinio una terza iniziativa congegnata dal Comune di Fidenza, in provincia di Parma. Con delibera del 17 febbraio 2022 è stato, infatti, approvato un regolamento unico comunale in materia di edilizia residenziale pubblica (E.R.P.) – in seguito rimosso dai siti istituzionali, evidentemente come conseguenza dell'istruttoria in corso – istitutivo di un sistema di valutazione a punti dei comportamenti dei nuclei familiari e dei conduttori di alloggi E.R.P., denominato "carta dell'assegnatario". Nel volantino

---

[11] L'iniziativa non risulta attualmente resa pubblica su alcun sito istituzionale del Comune di Bologna, ma se ne trova una traccia, oltre che nel comunicato stampa del Garante Privacy, altresì in un'intervista rilasciata a Rosano (2022).

[12] Comune di Roma, *Citizen Wallet: la piattaforma che ti premia*: il riferimento era disponibile sul sito istituzionale del Comune (consultato: 27 luglio 2022), poi rimosso.

informativo diffuso dal Comune si spiegava che tale carta, attribuita a ciascuna famiglia, conteneva una base di 50 punti, che sarebbero aumentati di 5 punti ogni 3 anni "per chi rispetta le regole senza sanzioni", di qualche unità "per chi si attiva per sistemare un danno che ha provocato", nonché ulteriori punti extra a discrezione del Comune per chi pone in essere "comportamenti virtuosi nell'ambito di specifici progetti in favore della comunità condominiale". Al contrario, il mancato rispetto delle regole di convivenza avrebbe provocato, oltre a sanzioni pecuniarie, la decurtazione di punti dalla carta e, allo spirare del credito, la decadenza dall'assegnazione dell'alloggio.

La discussa patente per le residenze popolari, come riporta il comunicato del Garante, pare dunque finalizzata "al riconoscimento di benefici e sanzioni, inclusa la risoluzione e/o la decadenza del contratto di locazione, con possibili conseguenze pregiudizievoli in capo a categorie di soggetti vulnerabili".

In sostanza, si tratta di pratiche potenzialmente scorrette poste da enti locali per finalità di *policy* urbana ma connotate da una certa dose di lesività che il Garante non omette di sottolineare quando, a chiosa del comunicato, rivolge un monito a tutti gli enti locali affinché valutino "con la massima attenzione eventuali future adozioni di progetti di '*social scoring*' o sue derivazioni". È bene, infatti, che tali iniziative siano "anticipate da puntuali valutazioni di impatto e rispettino i principi fondamentali del Regolamento Ue".

7.3. Confronto tra esperienze di sistemi di *social scoring* e meccanismi reputazionali

L'idea di una cittadinanza "a punti" volta a profilare e suddividere i cittadini in base all'onestà dei loro comportamenti, avvalendosi di *big data* e sistemi computazionali automatizzati, non è senza precedenti[13]. Il caso forse più noto è quello dell'ordinamento cinese, che da tempo ha elaborato i c.d. *Social Credit Systems* (SCSs) arrivando a monitorare circa 210 milioni di abitanti[14]. Il programma di "sorveglianza sociale" del go-

[13] Per una ricostruzione dell'evoluzione del *reputation scoring*, a partire dal settore di erogazione del credito, v. Di Carpegna Brivio (2022).

[14] V. Liang *et al.* 2018; Mac Síthigh & Siems 2019; Liang & Chen 2022. Sugli effetti dei sistemi reputazionali e di *rating* sociale sulla mobilità dei cittadini nei contesti urbani, cfr. Raghunath (2020) Per un approfondimento delle risposte istituzionali cinesi rispetto alla tradizione politica, v. nuovamente Di Carpegna Brivio (2022, 129).

verno cinese si caratterizza per l'elevata interoperabilità fra piattaforme: le capacità di calcolo sono, infatti, potenziate dalla possibilità di ottenere dati aggregandoli da fattori diversi quali le transazioni commerciali online, i consumi, i rapporti bancari, gli spostamenti in autovettura, l'uso del telefono cellulare e l'area geografica di residenza, così come persino il grado di rispetto delle decisioni dell'autorità pubblica o giudiziaria. I cittadini "disonesti" possono, in ultima analisi, essere inseriti in *black list* compilate dai vari ministeri[15] o in un *Joint Punishment System*, istituito sulla base delle risultanze del diciottesimo congresso del partito cinese e dei valori ivi espressi dal Segretario generale Xi Jinping (innovazione, coordinamento, ecologia, apertura e sviluppo condiviso)[16]. Oltre a questo programma a livello nazionale, esistono in Cina più di quaranta progetti-pilota in varie città, volti al controllo della popolazione con la combinazione di sistemi di videosorveglianza, programmi di riconoscimento facciale, test del DNA obbligatori e aggregazione di dati ottenuti dall'Internet delle Cose[17]. Progetti utilizzati per favorire la "pace sociale" in aree turbolente come lo Xinjiang, o per prevenire le infrazioni pubbliche, come nello Shangdong[18].

Oltre ai più discussi esempi asiatici della Cina e di Singapore[19], il mondo "democratico" non è da meno. Pionieri nel *social credit rating* sono, ad esempio, gli Stati Uniti, su cui non si può non fare rinvio al volume di O'Neil (2016), che dimostra come il negato accesso al credito e la persecuzione creditizia abbiano aumentato le diseguaglianze sociali, ad esempio precludendo l'accesso alle migliori università alla popolazione afroamericana.

Per restare in ambito europeo, poi, va almeno citata la vicenda degli algoritmi di SyRI (*Systeem Risico Indicatie*) nei Paesi Bassi. SyRI è stato uno strumento di monitoraggio predisposto dal governo olandese

---

15 Ha fatto scalpore, ad esempio, quella compilata dal Ministero della Cultura e del Turismo, per cui ai cittadini che ne fanno parte è negato l'accesso sui vettori aerei e sui treni ad alta velocità. (Fenwick Elliot 2018).

16 Per approfondire, si vedano i pareri del Consiglio di Stato cinese n. 33/2016 sull'istituzione del *Joint Punishment System*, tradotti da R. Cremeers.

17 V. Lucas & Feng (2018).

18 In questa provincia, in particolare, il *social scoring* prevede l'attribuzione a ciascun cittadino di un punteggio fino a mille e la categorizzazione dei residenti in cittadini di serie A, B, C o D, a seconda dei comportamenti tenuti (negativi, come infrazioni stradali, o positivi, come l'assistenza ai familiari anziani). V. la ricostruzione compiuta da Raphael & Xi (2019).

19 *Supra*, nota 1.

per individuare eventuali frodi dei cittadini aventi diritto a prestazioni sociali, esenzioni e benefici fiscali. La Corte distrettuale dell'Aia, però, con una sentenza senza precedenti, ha dichiarato il sistema illegale per violazione dell'articolo 8 CEDU, che presidia il diritto al rispetto per la vita privata e familiare, nonché dei principi di trasparenza e delle regole sul trattamento dei dati disposte dal GDPR[20].

Un ulteriore caso di discriminazione algoritmica da parte di soggetti governativi si è verificato in Spagna (Valdivia & de la Cueva 2022). Diverse pubbliche amministrazioni hanno fatto ricorso a un'applicazione messa a punto dal Governo, denominata BOSCO, e contenente algoritmi al fine di identificare in maniera efficace i cittadini in situazione di vulnerabilità a cui spettava il diritto a ricevere sussidi per il pagamento di bollette dei servizi di somministrazione dell'energia elettrica. Tuttavia, i criteri di selezione dei destinatari dei benefici sarebbero stati produttivi di effetti distorsivi tant'è che, al momento in cui si scrive, risulta essere ancora in corso il contenzioso giudiziario per l'accesso al codice sorgente, richiesto da Civio, un'associazione per la tutela dei cittadini.

Il quadro complessivo appena evocato ricorda la serie televisiva tecno-distopica *Blackmirror* e, in particolare, *Nosedive*, il primo episodio della terza stagione (Pandit & Lewis 2018). Ambientato in una realtà in cui il gradimento delle altre persone sulle piattaforme *social* influenza lo *status* socio-economico, tutto dipende da una tecnologia pervasiva, collocata nei telefoni di tutti i cittadini, che consente di attribuire punteggi alle persone identificate attraverso lenti biometriche. In uno scenario così immaginato, si ipotizzano relazioni umane falsate e ipocrite, in funzione dell'accrescimento della popolarità individuale. Chi, però, vede crollare il proprio punteggio al minimo subisce conseguenze incalcolabili. Relegato ai margini di una società manierata, si vede negati i servizi basilari, trasformandosi in un paria.

7.4. Il panottico digitale?

Il passo dalle piccole innovazioni urbane – mosse da buoni intenti ma condotte, come sottolinea il Garante, in assenza di valutazioni di

[20] Corte distrettuale dell'Aja, Decisione del 5 febbraio 2020 n. C/09/550982, resa nota il 6 marzo 2020 e disponibile nella versione inglese. Sulla distinzione fra gli artt. 7 e 8 CEDU, v. Bassini & Pollicino (2021).

impatto – al panottico digitale alla Bentham (1983) è, per fortuna, ancora lungo e le vicende in commento vanno giudicate senza toni allarmistici. Tuttavia, il progresso di tali tecnologie mette continuamente alla prova il diritto costituzionale. Siamo già abituati al c.d. *surveillance capitalism* e ai meccanismi di *social rating* sulle piattaforme private: non è difficile ipotizzare che chiunque avrà almeno una volta rilasciato una recensione o un punteggio ad un autista di *Uber*, a un venditore di *e-Bay*, a un ristorante su *Tripadvisor* o a un *host* di *AirBnB* senza porsi domande sulle conseguenze che tali giudizi possano avere sull'attività altrui (c.d. sorveglianza fra *peer users*)[21]. A maggior ragione, però, occorre riflettere quando le tecniche di profilazione non sono più sfruttate a meri fini commerciali bensì subentrano nei processi decisionali dei soggetti pubblici che si impegnano a fornire servizi o prestazioni al cittadino condizionandoli alle condotte migliori o peggiori.

Il problema, infatti, sta nella compatibilità di queste "fabbriche di decisioni automatizzate" (Bovens & Zouridis 2002) con il nostro sistema di diritti e principi fondamentali. Problema che si acutizza con riguardo ai sofisticati sistemi di profilazione che funzionano mediante sorveglianza attiva in abbinamento a meccanismi di premi o sanzioni che interferiscono con la cittadinanza. Indubbiamente il GDPR e il Codice della privacy rappresentano una efficace barriera di protezione contro le violazioni[22]. Ma non bisogna scordare, sullo sfondo, il compito del costituzionalismo che, in quanto "scienza chiamata a sindacare le finalità del potere e a stabilire le regole per il suo funzionamento", deve guidare le scelte legislative con dei solidi princìpi (Di Carpegna Brivio 2022, 131).

Il Garante già in passato ha riscontrato e sanzionato violazioni cagionate dalla profilazione psicologica di utenti *online* e, a cascata, dal trattamento dei dati così ottenuti. Tali condotte rischiano di dare luogo a fattispecie "inafferrabili" nel momento in cui le operazioni di cessione dei dati assumono, per di più, una dimensione transfrontaliera. In materia, ad esempio, è significativa l'ordinanza del Garante della

---

[21] Sul punto v. Resnick & Zeckhauser (2002).

[22] Decreto-legislativo del 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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", in GU n. 174 del 29 luglio 2003.

Privacy emessa il 14 giugno 2019 che ha pesantemente sanzionato Facebook Ireland Ltd e Facebook Italy s.r.l. a causa dell'illegittima condivisione di dati dei propri utenti con applicazioni terze che avrebbero effettuato attività di profilazione psicologica finalizzata all'elaborazione di "campagne promozionali altamente specializzate"[23]. Per di più, si è riconosciuta l'aggravante dell'entità del pregiudizio arrecato, per cui le violazioni risultano essere state compiute su "banche dati di particolare rilevanza e dimensioni"[24].

Per quanto riguarda, poi, le iniziative a livello europeo, va segnalata la proposta per la regolamentazione dell'intelligenza artificiale (*Artificial Intelligence Act*)[25], presentata dalla Commissione il 21 aprile 2021 e basata sul Libro bianco sull'IA del 2020.

La proposta suddivide le pratiche di IA vietate da quelle "ad alto rischio". In particolare, l'art. 5, comma 1, lett. c. vieterebbe "l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste".

Condizione per il divieto è che il punteggio sociale così ottenuto comporti "un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti", ovvero analogo trattamento "che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità". Qualora la proposta dovesse entrare in vigore, il divieto sembrerebbe ricalcare le tre fattispecie oggetto di istruttoria da parte del Garante che diventerebbero, pertanto, vietate[26]. Rispetto ai sistemi di IA ad alto rischio[27], che presentano forti implicazioni sulla salute,

---

[23] Autorità Garante della Privacy, Ordinanza di ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l., n. 134 del 14 giugno 2019.

[24] *Ibidem*.

[25] Commissione Europea, 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.

[26] Va detto che, al momento in cui si scrive, sono stati depositati molti emendamenti dai parlamentari europei e che la materia del *social scoring* è tra le più contestate (Bertuzzi 2022).

[27] V. Titolo III, "Sistemi di IA ad alto rischio" della proposta di legge sull'intelligenza

sulla sicurezza e sui diritti fondamentali delle persone e che, pertanto, richiedono l'applicazione di specifici criteri per la valutazione dei rischi *ex ante* e il rispetto di obblighi di sicurezza da parte dei fornitori dei sistemi stessi, le pratiche di cui all'art. 5 sono invece oggetto di divieto assoluto e nessun rischio può essere accettato rispetto ad esse. Pertanto, non si ammettono eccezioni.

Il coinvolgimento di pubbliche autorità esclude, poi, che in questi casi si possa invocare la "scusante" della profilazione a fini di *marketing*: il cittadino non può essere considerato alla stregua di un cliente o di un consumatore. Non può, quindi, essere oggetto di manipolazioni, fidelizzazioni e profilazioni che vedano, come risultato finale, l'esasperazione di quei profili discriminatori che probabilmente, nell'intenzione degli ideatori, ci si era proposti, forse ingenuamente, di combattere[28].

7.5. *Data first* o *privacy first*: due approcci confliggenti

Si è appena avuto modo di vedere, sotto varie angolazioni, il ventaglio di criticità che la combinazione di profilazione urbana e individuale può sollevare sulla riservatezza del singolo e dei suoi dati personali. Sulla base di queste brevi considerazioni, va sottolineato come, da un punto di vista strettamente costituzionalistico, un argine fondamentale debba restare, immancabilmente, l'art. 3 della Costituzione che svetta come principale presidio a tutela della uguaglianza e della pari dignità umana e sociale. Tale combinazione di valori che da endiadi ha poi costituito, nel solco tracciato dalla giurisprudenza della Corte costituzionale, "una visione unitaria o monolitica del medesimo [articolo], dove la pari dignità sociale parrebbe operare o quale matrice dell'eguaglianza finale o come risultato dell'applicazione di quest'ultima" (Camerlengo 2022, 35), non può che essere valorizzata

artificiale.

[28] Rimarchevole è anche il fatto che negli Stati Uniti, l'approccio europeo stia cominciando a fare presa e il "modello GDPR" stia riverberando i suoi effetti in materia di *targeting*, *citizenship surveillance* e *social scoring*. Recente è, infatti, il deposito di un *American Data Privacy and Protection Act* (ADPPA), la cui approvazione creerebbe un quadro federale completo sulla privacy dei consumatori, identificando entità titolari di grandi quantità di dati (*large data holders*) e richiedendo loro l'obbligo di ottenere un previo consenso "volontario e informato". Sul punto, si consulti il rapporto di studio del Congressional Research Service, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, disponibile online.

come "copertura" ultima di tutte le possibili fattispecie che emergono dal progresso tecnologico e informatico.

La selezione del "buon cittadino" con logiche performative e tecniche di incentivazione subliminale che si avvicinano pericolosamente a quelle di mercato, rende gli attori pubblici permeabili alle trappole degli operatori privati, allontanandoli dai compiti tradizionali dello stato verso lidi ancora poco esplorati[29]. Il rischio, allargando il campo visivo, è che tali processi vadano a detrimento di quelle categorie della società più sfavorite, marginalizzate dagli esiti di processi algoritmici poco trasparenti e distorsivi. Queste pratiche di fornitura di servizi alla "cittadinanza digitale" sono, pertanto, suscettibili di enfatizzare discriminazioni già esistenti, sottorappresentando alcuni gruppi sociali a favore di altri, imponendo svantaggi ingiustificati a carico di specifiche categorie di cittadini, persino trasgredendo i più elementari principi costituzionali, con l'aggravante, però, dell'assenza di una responsabilità "umana" diretta[30].

Se, dunque, per cogliere le opportunità dell'intelligenza artificiale applicata al tessuto urbano per fini di *policy* sarebbe meglio non ostacolare del tutto lo sviluppo di applicativi basati su *scoring* e profilazione, questi devono nondimeno essere progettati in modo da non dare luogo a più mali di quelli che sono chiamati a curare. Si impone, dunque, al regolatore di contemperare due approcci potenzialmente confliggenti: *data first* oppure *privacy first*[31]. Non è detto che l'uno debba per forza escludere l'altro, a patto che si riesca a trovare una cornice regolativa dei nuovi fenomeni di Internet che consenta di sfruttare i dati in maniera trasparente, informata, procedimentalizzata. Su questo, dunque, vanno attesi i prossimi risvolti dell'attività dell'Autorità Garante della privacy, che potranno certamente fornire nuovi e interessanti spunti di riflessione.

---

[29] Evocando le nuove frontiere del potere di Zuboff (2019).

[30] Per un interessante commento sulla *accountability* degli algoritmi nei processi decisionali della pubblica amministrazione, v. Busuioc (2021).

[31] Sul punto, si veda l'interessante studio sulla "regolazione algoritmica" di Yeung (2018).

Bibliografia

Aliprandi, S. (2021), *La proprietà intellettuale sui modelli di previsione e di profilazione*, in "Ragion pratica", 2, pp. 365–382.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, Nosenzo, F. D., Toussaert, S., Abeler, J. (2020), *Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study*, in "JMIR mHealth and uHealth" VIII, 8, pp. e19857.

Bassini, M., Pollicino O. (2021), *Art. 8: Protezione dei dati di carattere personale*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, G. De Gregorio (a cura di), *Codice della privacy e data protection. Le fonti del diritto italiano*, Giuffré, Milano 2021.

Bengio, Y., Janda, R., Yu, Y.W., Ippolito, D., Jarvie, M., Pilat, D. Struck, B., Krastev, S., Sharma, A. (2020), *The need for privacy with public digital contact tracing during the COVID-19 pandemic*, in "The Lancet Digital Health" II, 7, pp. e342–e344.

Bentham, J. (1983), *Panopticon, ovvero la casa d'ispezione*, Marsilio, Venezia.

Bertuzzi, L. (2022), *AI regulation filled with thousands of amendments in the European Parliament*, in "www.euractiv.com", 2 giugno.

Bovens, M., Zouridis, S. (2002), *From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control*, in "Public Administration Review", LXII, 2, pp. 174–184.

Busuioc, M. (2021), *Accountable Artificial Intelligence: Holding Algorithms to Account*, in "Public Administration Review", LXXXI, 5, pp. 825–836.

Camerlengo, Q. (2022), *Per una interpretazione costituzionalmente sostenibile del merito*, in "Federalismi.it", 13, pp. 1–41.

Caravita, B. (1984), *Oltre l'eguaglianza formale*, Cedam, Padova.

Casonato C. (2019), *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in "BioLaw Journal", pp. 711–725.

Christou, G., Simpson, S. (2011), *The European Union, multilateralism and the global governance of the Internet*, in "Journal of European Public Policy", XVIII, 2, pp. 241–257.

Colapietro, C., Iannuzzi A. (2020), *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in "Dirittifondamentali.it", 2, pp. 1–32.

Costanzo, P. (2012), *Il fattore tecnologico e le sue conseguenze*, in "Convegno annuale AIC, Salerno, 23-24 novembre 2012 'Costituzionalismo e globalizzazione'", pp. 1–29.

Di Carpegna Brivio, E. (2022), *Il Reputation scoring e la quantificazione del valore sociale*, in "Federalismi.it", 18, pp. 119–147.

Fenwick Elliot, A. (2018), *China is banning people with «bad social credit» from using plans and trains*, in "The Telegraph", 19 marzo.

Foster, S.R., Iaione, C. (2016), *The City as a Commons*, in "Yale Law and Policy Review", 34, pp. 281–349.

Koumetio Tekouabou, S.C., Diop, E.B., Azmi, R., Jaligot, R., Chenal, J. (2021), *Reviewing the application of machine learning methods to model urban form indicators in planning decision support systems: Potential, issues and challenges*, in "Journal of King Saud University", pp. 1–25.

Liang, F., Das, V., Kostyuk, N., Hussain, M.M. (2018), *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in "Policy & Internet", X, 4, pp. 415–453.

Liang, F., Chen, Y. (2022), *The making of "good" citizens: China's Social Credit Systems and infrastructures of social quantification*, in "Policy & Internet", XIV, 1, pp. 114–135.

Lucas, L. Feng E. (2018), *Inside China's surveillance state. From schoolchildren to political dissidents: how technology is tracking a nation*, in «Financial Times», 20 luglio.

Mac Síthigh, D., Siems, M. (2019), *The Chinese Social Credit System: A Model for Other Countries?*, in "The Modern Law Review", LXXXII, 6, pp. 1034–1071.

Midiri, M. (2020), Privacy *e* Antitrust*: una risposta ordinamentale ai* Tech Giant, in T. Cerruti, C. Bertolino, M. Orofino, A. Poggi (a cura di), *Scritti in onore di Franco Pizzetti*, II, Edizioni Scientifiche Italiane, Napoli-Torino 2020.

Mobilio, G. (2021), *Tecnologie di riconoscimento facciale: rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, Napoli.

Nardocci C. (2021), *Quando "manca" il giudice... il Garante della Privacy, l'algoritmo e la profilazione*, in "Forum di Quaderni Costituzionali", 4, pp. 30–35.

O'Neil C. (2016), *Weapons of math destruction: how big data increases inequality and threatens democracy*, Crown, New York.

Pandit, H.J., Lewis, D. (2018), *Ease and Ethics of User Profiling in Black Mirror*, in Companion of 'The Web Conference 2018', Lyon.

N. Raghunath (2020), *A Sociological Review of China's Social Credit Systems and Guanxi Opportunities for Social Mobility*, in «Sociology Compass» XIV, 5.

Raphael, R., Xi, L. (2019), *China's rewards and punishments*, in "Le Monde Diplomatique», gennaio.

Resnick, P., Zeckhauser, R. (2002), *Trust among strangers in internet transactions: Empirical analysis of eBay' s reputation system*, in "Advances in Applied Microeconomics", 11, pp. 127–157.

Rosano, F. (2022), *Bologna, la «patente digitale» per i cittadini virtuosi: punti e premi. E un'app con tutti i servizi*, in "Corriere della Sera", marzo 29.

Simoncini, A. (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", pp. 63–89.

Sowmiya, B., Abhijith, V.S., Sudersan, S., Sakthi Jaya Sundar, R., Thangavel, M., Varalakshmi, P. (2021), *A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19*, in "SN Computer Science", II, 3, pp. 136 e ss.

Valdivia, A., de la Cueva, J. (2022), *The Paradox of Efficiency: Frictions Between Law and Algorithms*, in "Verfassungsblog", 2 aprile.

Yeung, K. (2018), *Algorithmic regulation: A critical interrogation: Algorithmic Regulation*, in "Regulation & Governance", XII, 4, pp. 505–523.

Zuboff, S. (2019), *The age of surveillance capitalism: the fight for the future at the new frontier of power*, Profile Books, London.