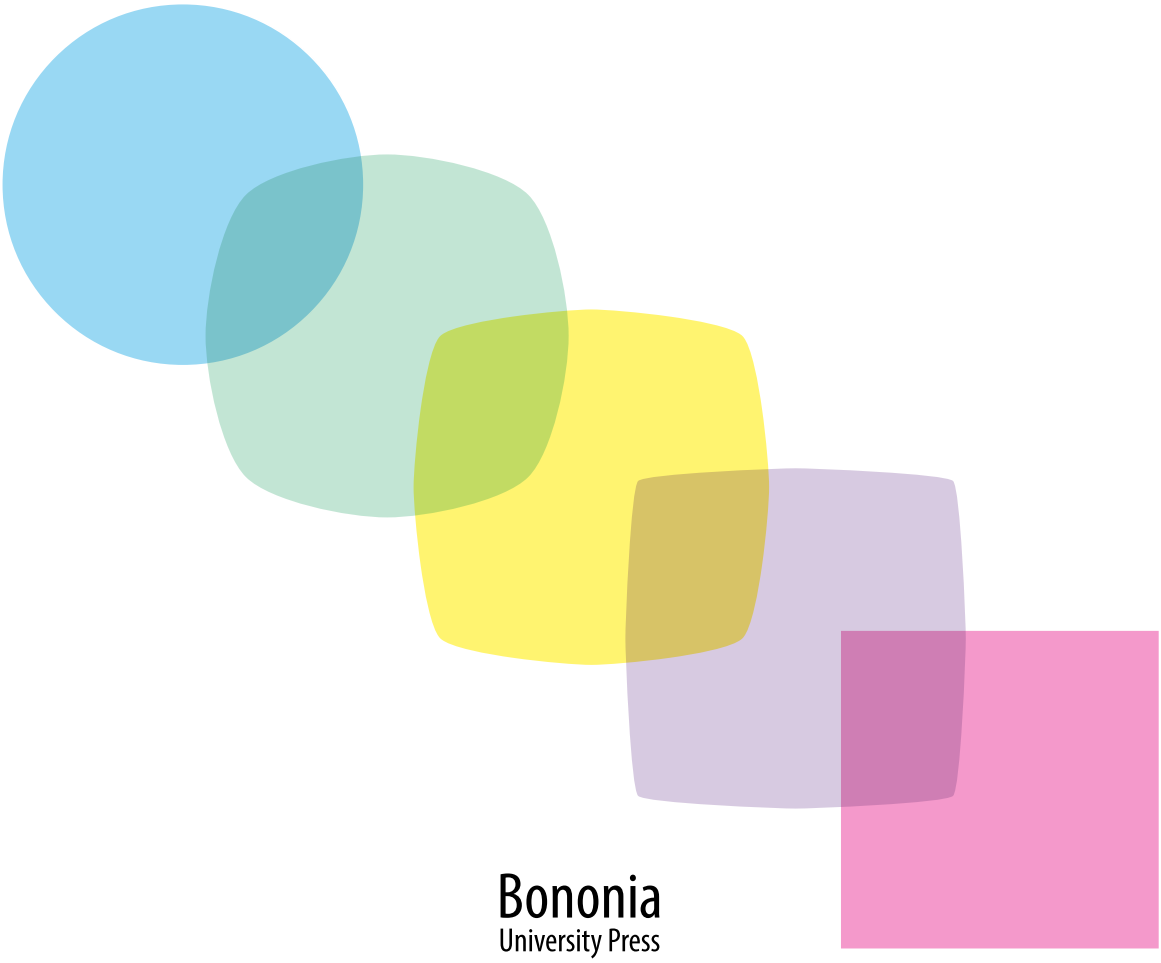
La mediazione interculturale

Strumento per le politiche di inclusione e di contrasto alle disuguaglianze

a cura di

Francesca Curi, Paolo Fasano,

Giampaolo Gentilucci, Giovanna Santandrea



Bononia
University Press

La mediazione interculturale

Strumento per le politiche di inclusione e di contrasto alle disuguaglianze

a cura di

Francesca Curi, Paolo Fasano,

Giampaolo Gentilucci, Giovanna Santandrea

Bononia
University Press

Bononia University Press
Via Foscolo 7
40123 Bologna
tel. (+39) 051 232882
fax (+39) 051 221019

ISBN 978-88-6923-780-5
ISBN online 978-88-6923-781-2

www.buponline.com
e-mail: info@buponline.com

Progetto di copertina e impaginazione: Design People (Bologna)

Prima edizione: aprile 2021

Sommario

SEZIONE II: GLI INTERVENTI

SEZIONE III: LA TAVOLA ROTONDA

La mediazione digitale e nuove forme tecnologiche di discriminazione

Monica Palmirani

Professore ordinario di Filosofia del diritto, Università di Bologna

1. Infosfera, Big Data e AI

Internet si è sviluppata presso le università californiane negli anni Settanta come infrastruttura di comunicazione e di condivisione libera, neutrale, globale[1]. Nel tempo tale tecnologia si è trasformata divenendo prima uno strumento anche di e-commerce[2] e dopo di socializzazione digitale[3], cambiando radicalmente la struttura della nostra società. Internet è divenuto così strumento costitutivo della realtà fino a plasmare il nucleo di una nuova collettività basata sull'informazione e i dati digitali, tanto che taluni autori definiscono questa trasformazione il centro di una più ampia rivoluzione industriale e culturale[4]. Successivamente il flusso e il volume dei *big data* prodotti dalle interazioni dell'uomo attraverso le diverse piattaforme digitali (c.d. *Big Tech* o *Over The Top* — OTT) ha consentito il fiorire di applicazioni di intelligenza artificiale in svariati ambiti delle attività umane (e.g., agricoltura, industria, sanità, turismo), ma anche di utilizzare tali dati per controllare meglio la sicurezza pubblica (e.g., riconoscimento facciale) o per attuare

[1] Il 29 ottobre 1969 i ricercatori dell'UCLA (University of California, Los Angeles) e l'Università di Stanford si scambiano il primo messaggio in Internet formato da due caratteri "Lo", il messaggio originale doveva essere *login*, ma la connessione cadde prima del compimento di tale invio.

[2] Il fenomeno dell'e-commerce trova il suo apice fra il 1999 e il 2000 quando il Web consente di utilizzare i portali digitali per promuovere le attività commerciali, superando così le barriere fisiche territoriali.

[3] Si assiste al c.d. Web 2.0 ossia scrivibile anche da coloro privi di conoscenze tecnologiche, ma in grado di utilizzare le competenze linguistiche e della comunicazione offerte dai social media, blog, bacheche virtuali, chat e finanche enciclopedie distribuite (e.g., Wikipedia).

[4] Si veda Floridi 2017; Rifkin 2011.

una super-sorveglianza[5] di massa (e.g., basti pensare al Datagate NSA negli Stati Uniti[6] e al Social Credit System in Cina[7]).

Questa trasformazione si realizza e si rafforza anche grazie alla nascita di nuovi modelli economici basati sulla *digital economy*. Se si osservano le analisi di Forbes[8] si vedrà una trasformazione negli ultimi vent'anni nell'assetto economico mondiale, posizionando ai primi posti aziende nel settore del digitale (Apple, Google, Microsoft), dei social media (Facebook), della vendita online (Amazon), scalzando imprese legate all'industria meccanica (General Motors), energetica (Exxon), delle telecomunicazioni (AT&T). Il digitale quindi diviene nuovo elemento fondante di un capitalismo immateriale[9] nel quale i dati personali, e non-personali, i comportamenti monitorati dai dispositivi (e.g., spostamenti), le attività svolte all'interno delle piattaforme online (e.g., acquisti), le azioni passive (e.g., visione di contenuti multimediali) nonché quelle attive (e.g., creazione di contenuti, creatori e consumatori nello stesso tempo – *prosumatori*[10]) e quelle osservate (e.g., traffico dati Wifi) divengono *big data*[11], ossia materia prima preziosa per alimentare molte applicazioni denominate generalmente di *intelligenza artificiale* (e.g., sistemi automatici

---

5 Si veda Clarke, Greenleaf 2017.

6 Le tecniche usate dalla National Security Agency americana, ed emersi nel noto "Datagate" del 2013, erano basate quasi esclusivamente sui metadati (e.g., *log file*, *digital footprint*), i quali rivelavano le attitudini, i comportamenti, gli interessi degli utenti sorvegliati.

7 Si veda Mac Síthigh, Siems 2019.

8 https://www.forbes.com/the-worlds-most-valuable-brands/#56c52d2b119c.

9 Si veda Zuboff 2015.

10 Si veda Toffler 1980.

11 Esistono diverse definizioni di "big data" e pur non convergendo su un'unica formulazione, tutte concordano su alcuni parametri essenziali quali volume, velocità, varietà dei dati collezionati tali da costituire un valore per il soggetto, pubblico o privato, che li ha raccolti. Definizione dell'OCSE di De Mauro: «*Big Data is the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value*». Definizione delle Linee guida del Consiglio d'Europa 2017: «The term "Big Data" usually identifies extremely large data sets that may be analysed computationally to extract inferences about data patterns, trends, and correlations. According to the International Telecommunication Union, Big Data are "a paradigm for enabling the collection, storage, management, analysis and visualization, potentially under realtime constraints, of extensive datasets with heterogeneous characteristics" (ITU. 2015. Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities)». Dal glossario di Gartner IT, voce "Big data" http://www.gartner.com/it-glossary/big-data (visitato il 4 ottobre 2019), definizione poi ripresa da ICO «*high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making*». Si veda anche AGCOM 2019; ICO 2017.

di decisione, *profiling*, *advertising*, *marketing*, *clustering*, *predictive*, *analytics*, *microtargeting*, ecc.). La società quindi si è trasformata e siamo tutti coinvolti all'interno di un dialogo fra mondo degli atomi e mondo dei bit (*infosfera*) in una condizione che non ha più bisogno di una netta distinzione fra *online* e *offline* perché in continua comunicazione in uno spazio non spazio, quindi fluido, definito *onlife*.

2. Identità digitali, *prosumer*, cittadini digitali

I dati depositati in rete e nei nostri dispositivi elettronici (e.g., *smartphone*, *fitness tracker*, domotica intelligente, ecc.) determinano le nostre identità digitali, proiezione ed espansione della nostra identità personale[12] tramite i nostri comportamenti in rete e nel mondo analogico. Le identità digitali influenzano la vita materiale, non sono più confinati in un mondo parallelo. Il report *Work Trends Study 2019*[13] svela che le agenzie di reclutamento hanno scartato il 44,1% dei curriculum sulla base dei materiali pubblicati nei social media utilizzando la c.d. *Web reputation*. Il Garante europeo per la protezione dei dati personali già dal 2015 si è occupato di fornire riflessioni sull'utilizzo dei *big data* nel parere 7/2015[14] sottolineando come tali dati possono acuire «*discrimination, re-enforcement of existing stereotypes, social and cultural segregation and exclusion*». In aggiunta i meccanismi algoritmici orientati a una iper-personalizzazione del prodotto digitale creano isole informative volutamente parziali e filtrate attraverso le nostre stesse preferenze (*filter bubble*[15]) precludendoci finanche di accedere a un trasparente e unitario strato informativo, presupposto per alimentare il nostro pensiero critico (come è possibile accedere a tutte le differenti tesi?), il confronto dialettico (come è possibile dibattere se ciascuno di noi vede un solo frammento?), e conseguentemente definire il diritto a una consapevole auto-determinazione (come posso scegliere se non conosco che esi-

[12] Palmirani, Martoni 2019.

[13] Il *Work Trends Study 2019* è uno studio sulle modalità di reclutamento e di come offerta e domanda si incontrano. È condotto da Adecco in collaborazione con l'Università Cattolica del Sacro Cuore di Milano. L'indagine, giunta quest'anno alla sua quinta edizione, ha coinvolto 259 recruiter e 1.466 candidati in tutta Italia.

[14] https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en.

[15] Si veda Pariser 2012.

stono altre opzioni? Si pensi a Cambridge Analytica[16]). In questa struttura sociale nuove fragilità ed esistenti vulnerabilità vengono acuite dalle politiche di utilizzo delle tecnologie, non tanto perché le tecnologie siano dannose per sé, ma perché non accompagnate da una riflessione etico-giuridica che regoli il bilanciamento fra interesse legittimo delle piattaforme di accumulare dati, e sfruttarli per offrire servizi commerciali, e i diritti e le libertà degli individui[17][18].

Vi è un ulteriore passaggio che rende ancora più rilevante la questione finora posta: non solo le *Big Tech* accumulano dati, ma anche i governi in autonomia o imponendo agli stessi colossi del digitale di contribuire con i propri *big data* alla costituzione di banche dati di sorveglianza. I servizi online erogati dalle pubbliche amministrazioni spesso includono la condivisione di pagine con i maggiori social media che mediante i *cookies* o i metadati di autenticazione dirottano i dati verso i datacenter oltreoceano[19]. In questo modo le amministrazioni, inconsapevolmente ma anche colposamente, forniscono il tassello mancante per una mappatura del cittadino da parte delle *Big Tech* le quale possono unire i dati della sfera privata dell'individuo con le molte relazioni offerte dalla sfera pubblicistica. Fortunatamente il regolamento GDPR si preoccupa di definire limiti di giurisdizione o di sovranità dei dati[20], rafforzati anche dalle recenti sentenze della Corte di Giustizia Europea *Schrems I*[21] e *II*[22] le quali mettono in luce come la sovranità dei dati sia un punto essenziale per tutelare le libertà e i diritti dei propri cittadini secondo la giurisdizione europea e ben precise misure di sicurezza.

Il CEPD (Comitato Europeo per la Protezione dei Dati)[23] ha sviluppato un

---

[16] Si veda il report della Federal Trade Commission, *In the Matter of Cambridge Analytica, LLC, a Corporation*, Complaint Docket No. 9383, July 2019, https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf (accessed 25 October 2019).

[17] Si veda Pagallo 2014; Frosini *et al.* 2017.

[18] Si veda O'Neil 2016.

[19] Il recente Google-down del 14 dicembre 2020 ha messo in luce come un guasto dei data center americani di Google abbia di fatto compromesso i servizi in parte dell'Europa, fra cui l'Italia. Questo denota non solo la dipendenza rispetto a politiche e strategie d'oltreoceano, ma anche la raccolta dei dati di molti servizi essenziali di natura pubblica (e.g., didattica a distanza delle scuole pubbliche) fuori dai confini europei.

[20] Si veda Frosini *et al.* 2017.

[21] Sent. ECLI:EU:C:2015:650, c.d. Schrems I.

[22] Sent. ECLI:EU:C:2020:559, c.d. Schrems II.

[23] European Data Protection Board, *Initial legal assessment of the impact of the US CLOUD Act on the*

report dettagliato sui rischi del CLOUD US Act[24] in relazione ai dati contribuiti dai cittadini e dalle imprese europee e archiviati presso gestori di *cloud computing* statunitensi. Secondo il CLOUD US Act il governo americano può richiedere, per contrastare gravi crimini (e.g., terrorismo), i dati agli operatori di *cloud computing* assoggettati alla legge statunitense anche se i server sono collocati in Europa (e.g., si veda il caso Microsoft). Per questi motivi la Commissione Europea nella comunicazione "Una strategia europea per i dati"[25] sottolinea il pieno sostegno a iniziative volte a rafforzare «la sovranità tecnologica dell'Europa per quanto riguarda le tecnologie e le infrastrutture abilitanti fondamentali per l'economia dei dati» e a sviluppare «sinergie tra il lavoro sulla federazione europea del cloud e le iniziative degli Stati membri quali Gaia-X[26]». Il *cloud* tuttavia, e di conseguenza i *big data*, non è la sola vulnerabilità nella strategia digitale europea che necessita di essere colmata e lo evidenzia il secondo importante report sulla *Strategia dell'AI* che completa il pacchetto della Commissione EU[27]. In questo documento la Commissione EU sottolinea come «la cooperazione internazionale sulle questioni riguardanti l'IA debba basarsi su un approccio che promuova il rispetto dei diritti fondamentali, tra cui la dignità umana, il pluralismo, l'inclusione, la non discriminazione e la protezione della privacy e dei dati personali, e si adopererà

EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, July 2019, in edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

[24] Clarifying Lawful Overseas Use of Data (CLOUD) Act (in https://www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf) il quale statuisce che «A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States».

[25] Bruxelles, 19.2.2020 COM(2020) 66 final, *Una strategia europea per i dati*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

[26] La piattaforma è denominata Gaia-X ed è inclusa nelle strategie della governance dei dati della Commissione Europea anche per creare uno spazio condiviso dei dati sanitari per combattere la pandemia. Gaia-X sarà anche il luogo dove sviluppare forme di intelligenza artificiale che siano conformi a valori etico-giuridici definiti secondo la regolazione europea. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[27] Bruxelles, 19.2.2020 COM(2020) 65 final, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1603192201335&uri=CELEX:52020DC0065.

per esportare i suoi valori nel mondo» o piuttosto, quando possibile, rendersi autonoma da altre giurisdizioni non in linea con tali principi e valori.

Le stesse pubbliche amministrazioni o autorità si dotano oggi di strumenti di intelligenza artificiale per controllare meglio le frontiere, per monitorare lo spostamento degli immigrati, per combattere il terrorismo, per predire eventuali potenziali crimini. Tali strumenti tuttavia, frutto ad oggi per la maggior parte della ricerca tecnologica di base condotta negli Stati Uniti e in Cina, risentono fortemente delle scelte valoriali di altre giurisdizioni e includono pregiudizi e *bias* cognitivi derivanti da un tessuto sociale diverso da quello europeo[28].

Per questi motivi si può assistere alla nascita di possibili nuove discriminazioni veicolate dalle tecnologie come mezzo di propagazione indiretta di strategie, metodologie, valori estranei al nostro impianto valoriale che devono essere prontamente attenzionate e isolate da una regolazione basata sui diritti fondamentali[29]. In tal senso il GDPR è una barriera importante per definire non solo regole tecnico-procedurali (e.g., registro dei procedimenti, DPIA, DPO, ecc.) di *accountability*, ma per porre come fondamento dell'uso delle tecnologie nelle nostre società la dignità umana e i diritti fondamentali, specie a tutela delle categorie vulnerabili[30][31][32]. La recente proposta della Commissione Europea del

---

[28] Si veda Zuiderveen Borgesius 2018. Si veda Directorate-General for Justice and Consumers 2017; Commissione Europea 2018; Committee of experts on Internet Intermediaries (MSI-NET), 2018.

[29] Si veda Palmirani, Martoni 2019 e Palmirani 2019.

[30] Il Considerando 75 del GDPR cita espressamente come rischiosi i trattamenti dei dati che possono cagionare discriminazione e pregiudizio a persone vulnerabili: «(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, [*omissis*]; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; [*omissis*]; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; [*omissis*]».

[31] Per integrare la definizione di categorie vulnerabili si veda: allegato 1, del provvedimento del Garante Privacy italiano "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018" che elenca così i «soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)».

[32] Altra definizione di persone vulnerabili la troviamo nell'art. 8 comma 1, d.lgs 140/2005, «persone vulnerabili quali minori, disabili, anziani, donne in stato di gravidanza, genitori singoli con figli

"Data Governance Act"[33] introduce nuove forme di condivisione dei dati, veicolate anche da intermediari qualificati, e includendo un concetto nuovo, a ben vedere piuttosto insidioso, di contribuzione dei dati personali «a fini altruistici» per finalità di «interesse generale». Le definizioni di "fini altruistici" e di "interesse generale"[34] sono da ben delineare, specie in un quadro nazionale dove ogni stato membro ha margini rilevanti di regolazione di diritto pubblico, come già lo stesso regolamento GDPR ha evidenziato in molti punti[35]. Questi regolamenti vanno poi integrati con la Direttiva 680/2016[36] e il Regolamento UE 603/2013[37] per l'uso dei dati personali per le finalità di polizia, da organi, uffici e comandi di polizia e con il DPR 15/2018[38].

3. Nuove forme tecnologiche di discriminazione

Molte sono le applicazioni tecnologiche che vengono in soccorso delle categorie vulnerabili quali gli immigranti fornendo strumenti *app* o siti web per agevolare la

---

minori, persone per le quali è stato accertato che hanno subito torture, stupri o altre forme gravi di violenza psicologica, fisica o sessuale».

[33] Proposta di Data Governance Act (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767).

[34] Si veda COM(2011) 900 final, *Una disciplina di qualità per i servizi di interesse generale in Europa* dove si evidenziano le difficoltà di giungere a una definizione certa di "interesse generale".

[35] Ci sono molti punti nei quali il regolamento GDPR lascia ampi margini di normazione ai legislatori nazionali quali l'art. 6 comma 2, con particolare riguardo al trattamento «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» e ancora l'art. 8 per la definizione dell'età minima per i minori di accedere in autonomia ai servizi dell'informazione, art. 9, comma 3, per i dati genetici, biometrici o relativi alla salute, art. 84 sulle sanzioni non amministrative, art. 85 per la libertà di espressione e di informazione coordinata con i singoli ordinamenti e costituzioni, art. 88 per la regolazione dei dati personali in ambito lavorativo, art. 89 per definire deroghe specifiche per il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, art. 90 in merito agli obblighi di segretezza.

[36] Direttiva 680/2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione (https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L0680).

[37] https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:32013R0603.

[38] https://www.gazzettaufficiale.it/eli/id/2018/03/14/18G00040/sg.

ricerca del lavoro (*Workeen*[39]), l'aggregazione, le conoscenze linguistiche (*MyGrants*[40]), l'accesso ai servizi della pubblica amministrazione (*Migreat*[41]). Tuttavia, si riscontrano anche grandi violazioni dei diritti umani, qualche esempio lo vediamo qui di seguito. *Salaat First* è un'app per smartphone che ricorda quando praticare la preghiera mussulmana e i luoghi di culto nelle vicinanze: nella versione Android rintraccia la posizione delle persone (geolocalizzazione) e la trasmette a terze parti. Lo stesso avveniva per *Muslim Pro*. I dati se trasmessi ad agenzie di intelligence possono creare un forte pregiudizio rispetto all'istituto della presunzione di innocenza relativamente al reato di terrorismo o discriminare in altri diritti fondamentali (e.g., libertà di culto). L'inchiesta del *The Washington Post*[42] ha rilevato che l'app *Ovaia* condivide i dati relativi alla gestione della fertilità delle donne con datori di lavori e assicuratori. Un report *Invading Refugees' Phones: Digital Forms of Migration Control*[43] ha rivelato che vi sono diverse aree dove le tecnologie di intelligenza artificiale in particolare falliscono a causa di errate selezione dei dati nella fase di apprendimento da parte degli algoritmi: i) strumenti linguistici automatici (traduttori, assistenti vocali) che discriminano determinate lingue o dialetti in base alla pronuncia delle persone (e.g., *TraLitA*[44]); ii) riconoscimento facciale che discrimina a seconda del colore della pelle o del genere (e.g., *iBorderCtrl* progetto europeo sperimentato in modo fallimentare nella frontiera fra Serbia e Ungheria); iii) algoritmi predittivi e di profilazione (e.g., sulla base dell'orientamento religioso); iv) estrazione dei dati dai cellulari mediante *spyware*. La maggiore lacuna di questi sistemi si deve all'incorretta scelta dei dati per addestrare gli algoritmi di AI. Dati che risentono del tessuto sociale che li ha raccolti, selezionati e classificati, includendo così nei sistemi software gli stessi pregiudizi che affliggono tali società, invece di agire secondo principi di neutralità. Il progetto

[39] https://sea.unipr.it/it/notizie/workeen-la-nuova-app-che-aiuta-immigrati-e-rifugiati-ad-entrare-nel-mercato-del-lavoro.

[40] https://mygrants.it.

[41] https://play.google.com/store/apps/details?id=com.mi.great.

[42] https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

[43] Il report è curato da Gesellschaft für Freiheitsrechte e.V. (GFF, Society for Civil Rights). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf.

[44] TraLitA è un sistema utilizzato in Germania per riconoscere chi mente sulle proprie origini utilizzando la pronuncia. Siriani e iracheni sono riconosciuti correttamente nell'85-90%, coloro che provengono dalla regione del Maghreb vengono riconosciuti solo nel 35%.

Gender Shades del MIT[45] ha evidenziato per esempio che i tre maggiori produttori di riconoscimento facciale (Microsoft, IBM, Face++[46]) registrano un errore fino al 34,4% nelle donne di colore rispetto agli uomini bianchi. Google il 6 aprile 2020[47] ha modificato i suoi algoritmi di classificazione delle immagini perché accusata di razzismo nei confronti di soggetti con la pelle nera poiché identificavano una mano nera impugnare una pistola invece che un termoscanner, quando la medesima foto con una mano bianca era classificata con un monocolo.

Il report dell'Alto Commissario per i Diritti Umani (OHCHR) *Racial discrimination and emerging digital technologies: a human rights analysis*[48], approvato presso l'assemblea generale delle Nazioni Unite, fornisce delle raccomandazioni finali dopo aver lungamente esposto i pericoli delle tecnologie nell'accentuare le disuguaglianze, il razzismo e la discriminazione: i) fare in modo che gli stati introducano norme che prevengano tali situazioni e che combattano quelli esistenti; ii) fornire ai costruttori di applicazioni informatiche delle linee guida per lo sviluppo etico e in linea con i diritti fondamentali. Per questo motivo è nato il progetto B-Tech[49] che promuove questi due aspetti. Anche la Commissione Europea si è espressa in tal senso in diverse occasioni, in modo specifico nella comunicazione *A Union of equality: EU anti-racism action plan 2020-2025*[50] nella quale si sottolinea come «the use of algorithms can perpetuate or even stimulate racial bias if data to train algorithms does not reflect the diversity of EU society». Ed è proprio nella diversità valoriale dell'Europa che si incuneano i ragionamenti sopra esposti volti a tutelare le categorie vulnerabili riprendendo i principi sanciti dalla Carta dei diritti fondamentali dell'Unione europea e applicandoli anche alle fasi di lavorazione dei dati di training, di sviluppo, di testing e finanche statistici che spesso mascherano la visibilità palese di violazioni nella sfera religiosa, filosofica, culturale[51].

---

[45] Il progetto condotto da Joy Buolamwiniha ha confrontato tre fra i più noti sistemi di riconoscimento facciale con foto di parlamentari di tutto il mondo: http://gendershades.org/.

[46] https://www.faceplusplus.com/.

[47] https://algorithmwatch.org/en/story/google-vision-racism/.

[48] https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/Info-Technologies-And-Racial-Equality.aspx

[49] https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

[50] Brussels, 18.9.2020 COM(2020) 565 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0565&qid=1610663034003.

[51] Si veda Durante 2019.

4. La mediazione digitale per una società umanamente sostenibile

Quanto qui esposto evidenzia come, oltre alla mediazione culturale, emerga l'esigenza urgente di un'altra competenza capace di esercitare la mediazione digitale attraverso i principi di cittadinanza digitale e non solo limitata all'alfabetizzazione informatica. La cittadinanza digitale è definita nel nostro ordinamento per la prima volta nel d.lgs. n. 217 del 13 dicembre 2017, apportando modifiche al CAD (Codice dell'amministrazione digitale d.lgs. 82 del 2005) al fine di creare il diritto di poter dialogare con la pubblica amministrazione in modalità digitale e utilizzando i servizi online. Successivamente una definizione viene fornita dalla legge 92 del 20 agosto 2019 per introdurre nel sistema di istruzione italiano un insegnamento trasversale e interdisciplinare volto a creare competenze per essere cittadini dell'*infosfera*. Segue il d.m. 35 del 22 giugno 2020, *Linee guida per l'insegnamento dell'educazione civica*. Tale orientamento è il recepimento di un'azione che nasce nel 2013 a cura del Joint Research Centre (JRC) della Commissione Europea che pubblica un compendio delle competenze digitali per affrontare la società dell'informazione (DigComp) ora arrivato alla sua versione 2.1 (2019). Il DigiComp prevede cinque aree di competenza (analisi dei dati, comunicazione, sicurezza, creazione multimediale, *problem solving*), 21 competenze specifiche declinate in tre livelli (base, intermedio, avanzato). L'intento è di rendere tutti i cittadini in grado di accedere alle medesime opportunità offerte dall'*infosfera*, sviluppando capacità critica, consapevolezza dei rischi e delle opportunità, abilità e attitudini corrette e rispettose dei diritti fondamentali.

Il 12,7% degli studenti nella prima ondata di lockdown ha perso l'occasione di formarsi adeguatamente avvicinandosi pericolosamente all'abbandono scolastico. Questo è il segno che il *digital divide* può minare il diritto costituzionale all'istruzione oggi, ma creare un *vulnus* ancora più grande nel cittadino di domani (si pensi alla capacità di riconoscere le *fake news*). Un programma più particolareggiato è rivolto agli educatori e insegnanti (Digital Competence Framework for Educators – DigCompEdu[52]). In Italia l'insegnamento di questi contenuti è stato inserito a partire dall'anno scolastico 2020 in programmazione didattica.

[52] https://ec.europa.eu/jrc/en/digcompedu.

In sintesi, la mediazione digitale è essenziale per non accentuare le disuguaglianze sociali e rendere tutti i cittadini capaci di autodeterminarsi. Per questi motivi tale mediazione digitale deve essere rivolta con particolare riguardo a fasce vulnerabili quali minori, immigrati, donne, persone che hanno perso il lavoro. Se è vero che l'accesso a Internet è un diritto fondamentale (Rodotà 2015[53], UN OHCHR 2012[54], UN OHCHR 2016[55]) o un bene essenziale (UK House of Lords, Report of Session 2014–15[56]), o un servizio essenziale (US code Title 42, §5189e[57]), sicuramente possedere le competenze tecnologiche di base è condizione necessaria per accedere sostanzialmente alle molte opportunità offerte dall'infosfera senza rimanere ai margini o schiacciati dalle dinamiche di data-personificazione della *digital economy*[58]. Per non accentuare il divario digitale e acuire la discriminazione sociale occorre istruire alla lettura dei dati, all'analisi critica dei processi messi in campo dai social media e dalla *digital economy*, riconoscere le violazioni di diritti e libertà individuali ad opera di algoritmi, poter opporre argomentazioni controfattuali. In una parola essere un cittadino digitale per costruire una società inclusiva, innovativa, creativa.

---

53 Art. 2 della *Dichiarazione dei Diritti di Internet*, Commissione Camera dei Deputati.

54 Alto commissariato delle Nazioni Unite per i diritti umani, L. 13, del 5 luglio 2012, *The promotion, protection and enjoyment of human rights on the Internet*, «5. *Decides* to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work», http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/20/L.13&Lang=E.

55 A/HRC/32/L.20.

56 *Make or Break: The UK's Digital Future*, ordered to be printed 4 February 2015 and published 17 February 2015.

57 «§5189e. Essential service providers. (a) Definition
In this section, the term "essential service provider" means an entity that-
(1)(A) provides
(i) wireline or mobile telephone service, Internet access service, radio or television broadcasting, cable service, or direct broadcast satellite service;».

58 Si veda Van Dijck 2014.

Riferimenti bibliografici

Agcom, Agcm, Garante privacy, 2019, *Big Data. Linee guida e raccomandazioni di policy*. *Indagine conoscitiva congiunta*, pp. 12.

Clarke R., Greenleaf G., 2017, *Dataveillance Regulation: A Research Framework*, in "Journal of Law, Information and Science", 25, 1, pp. 104-122.

Commissione Europea, 2018, COM(2018) 237 final Brussels, *Artificial Intelligence for Europe*.

Committee of experts on Internet Intermediaries (MSI-NET), 2018, *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Council of Europe, pp. 60.

De Mauro A., Greco M., Grimaldi M., 2016, *A Formal Definition of Big Data Based on its Essential Features*, in "Library Review", 65, 3, pp. 122-135.

Directorate-General for Justice and Consumers, 2017, European Commission, *A comparative analysis of non-discrimination law in Europe*, doi:10.2838/52129, pp. 153.

Durante M., 2019, *Potere computazionale: l'impatto delle ICT su diritto, società, sapere*, Meltemi, Milano.

Floridi L., 2017, *Quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano.

Frosini T. E., Pollicino O., Apa E., Bassini M. (a cura di), 2017, *Diritti e libertà in Internet*, Le Monnier, Firenze, pp. XIII-464.

ICO (Information Commissioner's Office), 2017, *Big data, artificial intelligence, machine learning and data protection*.

Mac Síthigh D., Siems M., 2019, *The Chinese social credit system: A model for other countries?*, European University Institute, Working Paper LAW 2019/01, pp. 30.

O'Neil C., 2016, *Weapons of Math Destruction*, Crown Books, New York, pp. 272.

Pagallo U., 2014, *Il diritto nell'età dell'informazione*, Giappichelli Editore, Torino.

Palmirani M., 2019, *Big data e sistemi automatici di decisione nello spazio pubblico*, in *Vulnerabilità di fronte alle istituzioni e vulnerabilità delle istituzioni*, Giappichelli Editore, Torino, pp. 23-38.

Palmirani M., Martoni M., 2019, *Big data, governance dei dati e nuove vulnerabilità*, in "Notizie di Politeia", 136, pp. 9-22.

Pariser E., 2012, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Books, New York, pp. 294.

Rifkin J., 2011, *La terza rivoluzione industriale: come il "potere laterale" sta trasformando l'energia, l'economia e il mondo*, Arnoldo Mondadori Editore, Milano.

Rodotà S., 2018, *Vivere la democrazia*, Laterza, Bari-Roma, pp. 160.

Toffler A., 1980, *The Third Wave*, Bantam Books, New York.

Van Dijck J., 2014, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, "Surveillance and Society", 12, 2, pp. 197-208.

Zuboff S., 2015, *Big other: surveillance capitalism and the prospects of an information civilization*, "Journal of Information Technology", 30, 1, pp. 75-89.

Zuiderveen Borgesius F., 2018, *Discrimination, artificial intelligence, and algorithmic decision-making*, Council of Europe, Anti-discrimination Department, pp. 51.