

Siamo davvero i nostri dati? I meccanismi distorsivi premianti di social scoring in Cina, Olanda e Italia

di Vanessa Previti

Abstract: *Are we really our data? The distorting rewarding mechanisms of social scoring in China, Holland and Italy* - The contribution analyses the difference between the image that the individual gives of himself through an input in the circuits of his personal data and what he actually is, focussing on the statement of the personalistic principle of data that cannot be split from the individual himself. By studying the use of the rewarding mechanisms of Social Scoring of Chinese Social Credit Systems compared with Siri and the Italian Projects: Pollicino, Grantee's Cardholder, Marvel and Protector, a possible positive use of AI will be investigated to encourage the input of data systems that mirrors the centrality of human beings.

Keywords: Social scoring; Data altruism; AI; Profiling; Chinese social credit system

1095

1. Introduzione: stato dell'arte, metodologia e scopo della ricerca

Nella relazione del Garante al Parlamento relativa all'anno 2001, il presidente Rodotà ha, brillantemente, affermato che "noi siamo le nostre informazioni", sottolineando che la nostra identità è «affidata al modo in cui queste informazioni vengono trattate, collegate, fatte circolare»¹. Nel 2001 questa affermazione è stata considerata avanguardista², in un momento di iniziale diffidenza nei confronti del nostro "corpo informatico", affermare che il dato si identifica con la persona, ha determinato l'inizio della circolazione di quel flusso di informazioni che ha raggiunto una tale celerità da impedire all'individuo di avere reale contezza del cammino dei propri dati.

Questa ricerca avrà origine dall'affermazione del Professore Rodotà, analizzando il momento in cui il dato si è scisso dalla persona attraverso la degradazione della medesima da soggetto ad oggetto³ sia tramite l'introduzione di meccanismi premianti - spesso con l'ausilio di tecniche di intelligenza artificiale - che hanno condotto ad una imprudente dazione dei dati a fronte del conferimento di un punteggio, sia attraverso l'affidamento della gestione dei dati ad algoritmi che in maniera poco trasparente hanno captato le informazioni e hanno generato comportamenti discriminatori, per arrivare al tentativo, mediante il distacco da atteggiamenti di *gamification*, di

¹ Discorso di presentazione della Relazione per l'anno 2001, doc. web n. 354/1955.

² F. Modafferi, *Privacy: noi siamo i nostri dati*, in *diritto.it*, 8 febbraio 2018.

³ Discorso di presentazione della Relazione, cit.

ricongiungere il dato alla persona servendosi di un utilizzo positivo dell'intelligenza artificiale, nel novero della spontaneità dell'altruismo dei dati e della c.d. spinta gentile o teoria del *nudge*⁴.

Per analizzare i casi pratici attraverso cui si studierà il processo di distacco del dato dalla persona, si utilizzerà un approccio metodologico analitico-comparativo.

Pertanto, dopo aver accennato al panorama normativo di riferimento e dopo brevi cenni di carattere definitorio, si analizzerà la genesi del cosiddetto *Reputation scoring*⁵ correlato all'*Information Technology* attraverso lo studio del Sistema dei crediti sociali cinesi (SCS), emblematico esempio di utilizzo di strumenti di intelligenza artificiale da parte del Governo finalizzato a carpire i dati dei cittadini a fronte della dazione di punteggi e premi, nel prosieguo si vaglierà il caso SyRI, ipotesi del tutto singolare in cui un algoritmo, in modo non conforme ai dettami della CEDU, ha captato i dati dei cittadini olandesi per segnalare coloro i quali, in base a dei criteri non rivelati, fossero considerati maggiormente inclini a commettere frodi e infine, si approfondiranno le ipotesi italiane – il Progetto Pollicino, lo *Smart Citizen Wallet*, la Carta dell'Assegnatario del Comune di Fidenza, le iniziative Marvel e Protector – già oggetto di istruttorie da parte dell'Autorità Garante della *Privacy* in cui si è paventato l'inserimento di un meccanismo di *gamification* malcelato dietro l'attuazione della c.d. cittadinanza a punti come espressione dell'evoluzione delle città in *smart cities*.

Attraverso l'analisi comparata di questi casi di studio, si vaglierà da plurime prospettive la cessione del dato da parte della persona non già in un'ottica di spontaneità, ma a fronte della dazione di qualcosa.

Nella fase conclusiva, si cercherà di proporre un utilizzo positivo dell'Intelligenza artificiale nel tentativo di dare una rilevanza giuridica alla qualità delle informazioni di carattere personale che ciascun individuo mette in circolo quotidianamente, in luogo della quantità, per non consentire all'utilizzo di tali strumenti di deteriorare il valore della persona umana «portatrice dei valori riconosciuti dall'art. 2 cost. sia come diritti soggettivi sia come principi oggettivi»⁶ ma di innalzarla a protagonista principale della società digitale.

2. Panorama giuridico di riferimento: art. 22 del GDPR e Regolamento sull'Intelligenza artificiale

Per molto tempo si sono susseguite teorie della cultura alternativa americana degli anni Sessanta e Settanta⁷ secondo le quali la comunità

⁴ La teoria dei Nudge è un concetto appartenente al campo dell'economia comportamentale, che si è diffuso negli ultimi anni grazie al libro del premio Nobel per l'Economia Richard Thaler e del giurista Cass Sunstein, "Nudge – La spinta gentile".

⁵E. Di Carpegna Brivio, *Il Reputation scoring e la quantificazione del valore sociale*, in *federalismi.it*, 18/2022, 123 ss.

⁶ L. Mengoni, *Fondata sul lavoro: la Repubblica tra diritti inviolabili e doveri inderogabili di solidarietà*, in *Jus*, 1/1998, 45 ss.

⁷ S. A. Matei, *From Counterculture to Cyberculture: Virtual Community Discourse and the Dilemma of Modernity* in *Journal of Computer-Mediated Communication*, Vol. 10, Issue 3, 2005.

virtuale doveva essere considerata come una società più autentica, scevra dai condizionamenti sociali, ma questo ha comportato lo sviluppo di un «complesso universo mitopoietico di libertà e deregolamentazione»⁸ che ha collocato il diritto in una condizione di estraneità. Ad oggi, l'affermazione dell'identità digitale intesa come «moltiplicazione dei frammenti della personalità individuale che vengono lasciati in rete»⁹ ha reso l'intervento del diritto necessario, urgente e certamente innovativo¹⁰.

L'Unione europea ha, progressivamente, assunto una posizione regolatoria in materia, assecondando la prospettiva secondo la quale il sostegno all'innovazione tecnologica sia un elemento preponderante dello sviluppo economico-sociale dell'Unione ma anche «saldamente riannodato al portato civile e costituzionale dell'esperienza europea»¹¹, elaborando un'economia digitale sana e idonea ad assicurare un autentico miglioramento sociale¹². Nella materia del trattamento dei dati personali si è sviluppato il carattere innovativo della normazione eurounitaria¹³.

Il regolamento europeo 2016/679 UE, il GDPR-*General Data Protection Regulation* ha enucleato dei principi fondamentali a sostegno della centralità della persona a fronte dell'affermazione del potere computazionale.

L'art. 22 par. 1, sancisce che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona» ed è stato considerato il cardine normativo che ha garantito il c.d. «principio della conservazione dell'elemento umano»¹⁴ (*human in the loop*) in ogni circostanza in cui possano essere messi in discussione i diritti umani.

Inoltre, da questa previsione europea, ordinamenti nazionali – quali quello italiano – hanno sviluppato indirizzi della giurisprudenza amministrativa che ha tratto dal GDPR principi fondamentali¹⁵ quali «la piena conoscibilità dei criteri applicati dai modelli automatizzati»¹⁶ o «il diritto in capo all'organo titolare della decisione di verificare la logicità e la legittimità degli esiti prodotti dagli algoritmi»¹⁷.

Quanto ai rischi collegati alla profilazione, sebbene siano state individuate due basi giuridiche molto forti per limitarli – il «consenso

⁸ E. Di Carpegna Brivio, *Il Reputation scoring e la quantificazione del valore sociale*, op. cit.

⁹ S. Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *consultaonline*, 02/2021, 572.

¹⁰ S. Chesterman, *We the Robots? Regulating Artificial Intelligence and the Limits of the Law* in *Cambridge University Press*, 2021.

¹¹ E. Di Carpegna Brivio, *Il Reputation scoring e la quantificazione del valore sociale*, op. cit.

¹² Considerando n. 7 del regolamento 2016/679/UE.

¹³ F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 3 ss.

¹⁴ P. Benanti, *Human in the loop, Decisioni umane e intelligenze artificiali*, Milano, 2022, 161.

¹⁵ G. Cerrina Feroni, *LA nei processi decisionali della PA, il faro è la Costituzione*, in *Agenda Digitale UE*, 1-28.

¹⁶ Consiglio di Stato, sezione VI, 13 dicembre 2019, n. 8472.

¹⁷ Consiglio di Stato, sezione VI, 4 febbraio 2020, n. 881.

esplicito dell'interessato»¹⁸ e la «conoscibilità dell'utilizzo e del riutilizzo dei dati»¹⁹ – in dottrina²⁰ è stato evidenziato come la normativa non possa eliminare il pericolo, soprattutto se si considera che la disciplina è nata con l'intento di arginare la pervasività delle strategie di marketing²¹ mentre la potenzialità offensiva dell'intelligenza artificiale invade ogni sfera del privato, con lo scopo di ridurre l'individuo a numero.

Da ciò è conseguita la necessità e l'urgenza di predisporre una regolamentazione in materia.

La versione definitiva del Regolamento europeo sull'Intelligenza artificiale²² segue un approccio basato sul rischio, adattando la tipologia e le regole contenute all'intensità e alla portata del medesimo, vietando le pratiche inaccettabili e stabilendo requisiti specifici per i sistemi ad alto rischio con conseguenti obblighi per gli operatori, predisponendo un'innovazione digitale umano-centrica; il Titolo II elenca le attività che sono vietate dall'Unione europea in quanto lesive dei diritti fondamentali quali l'attribuzione di un punteggio sociale basato sull'IA per finalità generali da attori privati o pubbliche autorità, che, come chiarito dal Considerando 31, può generare risultati discriminatori, dal momento che la valutazione dell'affidabilità delle persone sulla base di un loro comportamento sociale, della personalità o di una caratteristica sociale lede i valori costituzionali della dignità umana, dell'uguaglianza e della non discriminazione.

Per quel che occupa questo studio, l'art. 5 alla lettera c) prevede che sia vietata «l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di un trattamento pregiudizievole che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità», mentre la lettera g) inserisce il divieto di «immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale». Sebbene si tratti di un rilevante passo in avanti, soprattutto con riferimento a quelle distorsioni che possono generare una discrasia tra intelligenza artificiale e rispetto dei principi fondamentali costituzionali, restano notevoli incertezze regolatorie

¹⁸ Art. 22 GDPR.

¹⁹ Art. 15 GDPR.

²⁰ R. Bond, *The EU E-Privacy Directive and Consent to Cookies* in *The Business Lawyer*, 1/2012, 215 ss.; I. Destri, A.M. Lotto, *La profilazione*, in G. Cassano, V. Colarocco, G.B. Gallus, F.P. Micozzi (a cura di), *Il processo di adeguamento al GDPR*, Milano, 2018, 133 ss.

²¹ Buzzacchi, *La politica europea per i big data e la logica del single market: prospettive di maggiore concorrenza?* in *Concorrenza e mercato*, 1/2016, 153 ss.

²² Regolamento europeo sull'Intelligenza artificiale, approvato il 14 maggio 2024, per la consultazione <https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/it/pdf>,

in merito al rapporto uomo-tecnologie avanzate che tendono a sostituirsi ad esso.

2.1 Cenni di carattere definitorio

Il *social scoring* ispirato alla *gamification* che si ha quando «elementi divertenti simili a quelli di un gioco compaiono in diverse attività e tutto dipende dal punteggio quantificato»²³, è una delle possibili combinazioni tra la raccolta dei dati e sia gli algoritmi c.d. tradizionali che i meccanismi di intelligenza artificiale, costituendo «il portato del carattere pervasivo della tecnologia in qualsivoglia settore della società e della quotidianità che incide sul rapporto Stato e cittadino»²⁴.

La combinazione tra profilazione e reputazione sociale fonda le sue radici nel settore dell'erogazione del credito²⁵ quale elemento di valutazione sintetica del merito creditizio.

Negli USA, a causa dell'innalzamento della domanda di acquisto di beni e della conseguenziale richiesta di carte di credito, già negli anni Sessanta, le banche non riuscivano ad effettuare indagini approfondite su larga scala e procedevano al conferimento di punteggi di origine statistica che permettevano di suddividere i richiedenti credito in categorie, assegnando un ordine di merito²⁶. L'intelligenza artificiale ha comportato la reinterpretazione del *social scoring* in un'ottica di reputazione sociale, «attraverso gli algoritmi di profilazione è possibile raccogliere una serie di dati quali la propensione al consumo, i gusti, gli interessi, le amicizie, le frequentazioni, l'ambiente lavorativo»²⁷ che esulano dal settore bancario e che, invece, possono ricostruire l'affidabilità del soggetto. Infatti, ad oggi, il conferimento di un punteggio alla persona attiene alla sua generale affidabilità, venendo in rilievo l'insieme delle relazioni che l'individuo sviluppa nella società digitale quali pagamenti online, ricerche di beni e servizi e comportamenti social. Pertanto la potenzialità dell'incidenza di tali strumenti nelle attività quotidiane è evidente e la valutazione dell'impatto dei medesimi sui diritti umani ne esplica la pericolosità.

Di fatti, è agevole temere che tale combinazione possa comportare una cessione della sovranità dell'essere umano su se stesso in favore dell'avvicinamento «di un comportamento reale ad uno predeterminato»²⁸ per ottenere un vantaggio.

Da ciò deriva la categorizzazione dei soggetti a cui attribuire benefici o sanzioni che possano influenzare i comportamenti dei singoli, generando

²³ D. Lyon, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori* in *Luiss University Press*, 2020, 140.

²⁴ G. Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale di diritto amministrativo*, 3/2021, 318.

²⁵ *Ex multis*, F. Pasquale, *The black box society. The Secret algorithms that control money and information*, Boston, 2015, 22 ss.

²⁶ E. Di Carpegna Brivio, *Il Reputation scoring e la quantificazione del valore sociale*, op. cit.

²⁷ F. Mattasoglio, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore* in *Diritto della banca e del mercato finanziario*, 02/2020.

²⁸ J. Van Dijck, *Datification, dataism and dataveillance: Big Data between scientific paradigm and ideology* in *Big Data Surveillance* Vol. 12, Issue 2, 2014, 200.

forme di soggezione²⁹, come nel caso della Cina. Esattamente di segno opposto al concetto di *social scoring*, è il principio di altruismo dei dati che viene definito dall'art. 2, paragrafo 1, n. 16 del *Data Governance Act*³⁰ (DGA) e consta della volontarietà della dazione dei dati, l'assenza di compenso e la funzionalizzazione a obiettivi di interesse generale. Il meccanismo dell'altruismo dei dati potrebbe essere considerato una parte della teoria del *nudging*, secondo cui «i processi decisionali e i comportamenti di gruppi e individui possono essere influenzati attraverso suggerimenti e rinforzi “indiretti” con un'efficacia pari o superiore a quella che può essere ottenuta attraverso l'imposizione di regole, leggi o istruzioni dirette»³¹. Dunque la libera e conscia circolazione dei dati non avverrebbe sulla base di «tecniche subliminali»³² ma attraverso l'utilizzo del perseguimento di obiettivi di interesse generale quale condizionamento indiretto che influenza il comportamento individuale e sociale.

3. Il Sistema dei crediti sociali cinesi: ratio, casi pratici, criticità

Il sistema dei crediti sociali in Cina ha assunto un rilievo nella letteratura popolare e accademica grazie all'estensione del merito creditizio ai comportamenti sociali, basandosi su informazioni degli individui per determinare la credibilità degli stessi al fine di consentire alla società di avere contezza dei soggetti protagonisti delle interazioni economiche e civiche³³.

Nel contesto della Cina, le reti sociali assumono una particolare rilevanza assumendo la forma di *guanxi*³⁴ che è un reticolato di interazioni dirette tra individui al fine di generare familiarità e obblighi reciproci³⁵ strettamente legate al concetto di *xinyong* che si riferisce, invece, alle idee di credibilità e affidabilità; secondo autorevole dottrina³⁶, lo *xinyong* tra due soggetti potrà essere sviluppato solo in presenza di un *guanxi* sufficiente, per mitigare le situazioni di rischio e generare un alto livello di credibilità che permette di effettuare transazioni informali e di ottenere dei vantaggi quali l'avanzamento di carriera.

In una società in cui lo Stato ha conservato un forte ruolo di guida morale, elaborare un sistema di crediti sociali – in cui la parola “credito”

²⁹S. Eschholz, J. Djabbarpour, *Big data and scoring in the financial sector*, in T. Hoeren E. B. Kolany-Raiser (a cura di), *Big Data in Context. Legal, Social and Technological Insights*, Springer, 2016, 63 ss.; E. Hendricks, *Credit reports, credit checks, credit scores*, in *GPSolo*, 5/2011, 32 ss.

³⁰ Regolamento (UE) 2022/868.

³¹R. Viale, *Nudging*, Milano, 2022.

³²S. Orlando, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, in *Persona e mercato*, 2022/3, 362.

³³M. Meissner, *China's social credit system: A big-data enabled approach to market regulation with broad implications for doing business in China*, in *chinafile.com*, 24 maggio 2017.

³⁴Per approfondimenti, M. Zhang, J. L., Hartley, et al., *Informal interorganizational business relationships and customer loyalty: Comparing Guanxi, Yongo, and Wasta*, in *International Business Review*, 30/2021.

³⁵Y. Bian et al, *Bringing strong ties back in: Indirecties, network bridges, and job searches in China* in *Social Network*, 40/2015, 129-138.

³⁶Tong, C. K., & Yong, P. K. *Guanxi bases, xinyong and Chinese business networks* in *The British Journal of Sociology*, 49/1998, 75-96.

assume la duplice valenza economica finanziaria e ispirata a logiche di rettitudine interiore degli individui³⁷ – ha comportato la necessità di interrogarsi circa il rapporto del medesimo con la rete di *guanxi*.

Sebbene si tratti di un argomento tutt'oggi oggetto di disamine, una parte di dottrina³⁸ ritiene che questi due sistemi possano lavorare insieme per agevolare il raggiungimento occupazionale e la mobilità sociale, influenzandosi e contribuendo, in collaborazione, alla realizzazione della «cultura della sincerità»³⁹. Nel 2007 il Consiglio di Stato cinese ha pubblicato delle «Linee guida riguardanti la costruzione di un sistema dei crediti sociali» con l'obiettivo di coinvolgere tutte le aree della vita economica e personale, in virtù del principio fondamentale secondo cui «se la fiducia è rotta da una parte, le restrizioni si applicano ovunque».

Con la diffusione dell'intelligenza artificiale e dei *Big Data*, attraverso la combinazione dei «meccanismi di responsabilità individuale e metodologie del controllo sociale»⁴⁰, il progetto si eleva ad una «profilazione dei comportamenti *on line* e *offline* dei cittadini, definizione di un sistema di *Reputation Scoring* che assegna punteggi ai comportamenti profilati e ad un preciso progetto di ingegneria sociale che rappresenta l'ideale a cui occorre avvicinare la società reale»⁴¹.

I *Big Data* costituiscono quell'insieme di informazioni necessarie per sviluppare analisi che possano soddisfare coloro i quali hanno l'autorità per stabilire i parametri comportamentali e l'intelligenza artificiale fornisce il mezzo attraverso il quale vaste quantità di dati potranno essere incorporate in modelli che possono correggersi e adattare gli algoritmi⁴².

Con riguardo al fenomeno della profilazione, negli anni 2000 era stato attribuito a ciascuna persona fisica un numero identificativo di 18 cifre che, a seguito dell'elaborazione del Sistema dei crediti sociali, è divenuto uno strumento di monitoraggio delle attività effettuate dagli individui da parte dello Stato.

Infatti, con riferimento alle attività *online*, è stata prevista l'obbligatoria registrazione con il proprio nome al fine dell'immediata riconducibilità di ogni pagamento digitale, social, ricerca ad una persona fisica⁴³, mentre con riguardo alle attività *offline*, si è registrato un incremento

³⁷F. Liang, V. Das, N. Kostyuk, M.M. Hussain, *Constructing a Data-Driven Society: China's social credit System as a State Surveillance Infrastructure*, in *Policy and Internet*, 4/2018, 424; R. Creemers, *China's Social Credit System: An Evolving Practice of Control*, 9 maggio 2018.

³⁸N. Raghunath, *A Sociological Review of China's Social Credit Systems and Guanxi Opportunities for Social Mobility*, in *Sociology Compass*, 5/2020, 1-11.

³⁹Linee programmatiche tracciate nel documento Pianificazione di un sistema dei crediti sociali (2014-2020) approvato dal Consiglio di Stato nel luglio del 2014.

⁴⁰S. Hoffman, *Managing the State: Social credit surveillance and the CCP'S Plan for China*, in *China Brief*, 11/2017, 24.

⁴¹P.F. Langer, *Lessons from China – The formation of a Social Credit System: Profiling, Reputation Scoring, Social Engineering*, The 21° Annual international Conference of Digital Government Research, Seul, 15-19 giugno 2020.

⁴²L. Catá Backer, *China's Social Credit System: Data-Driven Governance for a 'New Era'*, *Current History* 118/2019, 209-214.

⁴³R. Creemers, *China's social credit System: an evolving practice of control*, op. cit.

di telecamere a riconoscimento facciale nella pubblica via per realizzare banche dati aventi ad oggetto i dati biometrici dei cittadini⁴⁴.

Per quel che concerne il c.d. *Reputation Scoring*, ad oggi non esiste un sistema unificato ed esteso a tutto il territorio cinese che assegna punteggi univoci a cui corrispondono premialità o sanzioni, ma plurimi progetti pilota⁴⁵.

Tra i più discussi vi è quello della città di *Suining* in cui ad ogni cittadino veniva assegnato un ammontare di 1.000 crediti e ogni violazione di legge, di prescrizioni amministrative o di precetti morali comportava una decurtazione che incideva in ogni ambito della vita personale; vi era una classificazione in quattro categorie, da A a D a cui corrispondevano stili di vita differenti⁴⁶.

Se ai cittadini di classe A era garantita la possibilità di accedere ai migliori servizi disponibili e a plurime agevolazioni, per i soggetti inseriti nelle categorie inferiori qualsiasi attività era subordinata allo scrutinio governativo con conseguente difficoltà anche nel recupero di punteggi persi. Inoltre era previsto un sistema di pubblicazione dei nomi degli individui che alimentava lo stigma e l'isolamento sociale⁴⁷. Questo sistema è stato fortemente criticato e pertanto è stato interrotto, di fatti anche l'Agenzia di stampa statale Xinhua ha paragonato tale sistema alla «carta del buon cittadino» adottata dal Giappone durante la Seconda Guerra Mondiale⁴⁸.

Il Governo cinese ha estrapolato da questo esperimento l'elaborazione di un Meccanismo unificato di premi e sanzioni, rendendo il sistema delle *blacklists* e delle *redlists* un «elemento strutturale per la costruzione del sistema nazionale dei crediti sociali»⁴⁹.

L'inserimento di un soggetto all'interno di una *blacklist* da parte di una pubblica amministrazione comporta il verificarsi di conseguenze negative in tutti i settori quali «il diniego di accesso a sussidi statali o percorsi professionali ovvero l'impossibilità di acquistare biglietti aerei o ferroviari, di andare in vacanza all'estero, di comprare casa o avere accesso a mutui e prestiti o di iscrivere i figli a scuole prestigiose»⁵⁰.

Inoltre, in dottrina⁵¹ è stata evidenziata un'asimmetria informativa in merito alla determinazione dei criteri di inserimento nelle liste c.d. rosse o

⁴⁴G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, par. 6.4.

⁴⁵M. Ohlberg, S. Ahmed, B. Lang, *Central Planning, Local experiments: The complex implementation of China's Social Credit System*, *Merics China monitor* n. 43/2017, 11.

⁴⁶E. Consiglio, G. Sartor, *Il sistema di credito sociale cinese: una "nuova" regolazione sociotecnica mediante sorveglianza, valutazione e sanzione*, in *Rivista di scienze della comunicazione e di argomentazione giuridica*, 2/2021, 139-161.

⁴⁷R. Creemers, *China's social credit System: an evolving practice of control*, op. cit.

⁴⁸E. Di Carpegna Brivio, *Il Reputation scoring e la quantificazione del valore sociale*, op. cit.

⁴⁹A. Trauth-Goik, A. Bernot., *Decentralising Data Collection and Centralising Information in the People's Republic of China: Decentralise, Manage, and Service Reforms in Surveillance & Society*, Vol.19, Issue 4, 2021, 518-536.

⁵⁰L. Biamonti, *Il sistema di credito sociale cinese e la sua implementazione a livello pratico in Fiscalità e commercio internazionale*, n. 6/2021, 65-70.

⁵¹S. Engelmann, M. Chen, F. Fischer et al, *Clear sanctions, vague rewards: how China's Social Credit System Currently defines "good" and "bad" behavior*, *Conference on Fairness, Accountability and Transparency*, Atalanta, 29-31 gennaio 2019.

nere, mentre è noto che l'inserimento nelle *blacklist* consegue alla violazione di prescrizioni, l'inclusione nelle *redlist* è, invece, discrezionale, il più delle volte collegato al sistema di *guanxi*.

La mancanza di trasparenza e l'incertezza in merito alle conseguenze dei propri comportamenti determina il superamento del Sistema dei crediti sociali inteso nell'accezione del raggiungimento della cultura della fiducia, di fatti, inserendo anche dei meccanismi tipici della *gamification*, emerge la pervasività del controllo del Governo centrale cinese a discapito delle libertà dei cittadini.

Sebbene dall'analisi della dottrina maggioritaria emerga un atteggiamento di timore nei confronti dell'utilizzo che la Cina possa fare dei meccanismi di *social scoring* con l'utilizzo dell'intelligenza artificiale, l'attenzione rivolta negli ultimi anni alla protezione dei dati personali culminata nell'adozione della PIPL⁵² il 20 agosto 2021, in direzione diametralmente opposta a quella occidentale in cui la riservatezza è un diritto "congenito", è espressione di un cambiamento in atto da parte dell'Estremo oriente⁵³.

Nonostante originariamente la Cina avesse adottato un sistema "statunitense" di privacy che annoverava nel «*genus* della tutela della riservatezza la *species* della protezione delle informazioni e dei dati personali»⁵⁴, a seguito del riconoscimento dei dati come «fattore di produzione»⁵⁵ e il collegamento con la Legge sulla cybersicurezza del 2017, è stato elaborato un sistema duale che tutela sia il diritto alla non intrusione nell'altrui vita privata sia il diritto alla protezione delle informazioni personali⁵⁶. La PIPL, allontanandosi dal modello americano, ha quindi cercato di emulare il GDPR, ad esempio, attraverso la limitazione dell'utilizzo di algoritmi decisionali per finalità di profilazione, mantenendo però delle caratteristiche distintive quali la mancata applicazione della normativa sul trattamento anche alle autorità statali⁵⁷ ovvero l'inesistenza di un corrispettivo del diritto all'oblio⁵⁸ che la rendono un «GDPR con caratteristiche cinesi»⁵⁹.

4. Il Caso SyRI: il primo caso in cui il Tribunale dell'Aja ha sanzionato un algoritmo di deep learning per aver violato l'art. 8 della CEDU

⁵² Legge sulla protezione delle informazioni personali.

⁵³ *Ex multis*, D. Clementi, *La legge sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?* in *diritticomparati.it*, 1/2022, 189-216.

⁵⁴ *Ibidem*.

⁵⁵ Pareri del Comitato Centrale del Partito comunista cinese e del Consiglio di Stato sulla costruzione di un sistema e un meccanismo più completi per l'allocazione di fattori basata sul mercato.

⁵⁶ W. Liming, *Sulla protezione legale dei diritti sulle informazioni personali*, in *Modern law science*, 4/2014.

⁵⁷ Capo II, Sez. III della PIPL.

⁵⁸ Sentenza Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd, (2015).

⁵⁹ D. Clementi, *op. cit.*

Nel novero dell'analisi dei casi pratici, si è ritenuto interessante analizzare il controverso caso “SyRI”⁶⁰, in cui il Tribunale dell’Aja ha sanzionato⁶¹ un algoritmo di *deep learning* – creato per verificare la correttezza delle domande di sussidi pubblici da parte di persone che versano in stato di bisogno – per aver violato l’art. 8.2 della CEDU, ritenuto preminente rispetto all’art. 22 del GDPR, in considerazione del fatto che la raccolta della massa dei dati personali e la conseguente compromissione della vita privata è stata posta a fondamento del ragionamento giuridico della decisione a discapito del funzionamento logico dell’algoritmo che integrerebbe la profilazione ai sensi dell’art. 4, par. 4 del GDPR.

La vicenda riguarda SyRI, un sistema che avrebbe analizzato considerevoli quantità di dati ottenendo come risultato un “marcatore” di rischio, emesso nei confronti persona fisica o giuridica considerata sospetta con riferimento a frodi, usi illeciti o non conformi alla normativa che regola il beneficio richiesto. Per quanto concerne la presente ricerca, i profili problematici sono ravvisabili nella carenza di trasparenza da parte dello Stato in merito alla creazione e allo sviluppo del progetto⁶² e nella focalizzazione della raccolta in determinati luoghi – Rotterdam, Haarlem e Capelle aan den IJssel – dove, secondo le autorità, le frodi sui benefici fiscali, sociali e previdenziali sarebbero state più probabili in considerazione della presenza nella banca dati di “indirizzi già indagati dal team di intervento per aver commesso frodi”⁶³.

La raccolta dei dati avveniva aggregando qualsiasi informazione – di lavoro, fiscale, pensionistica, giudiziaria, esposizione debitoria e financo l’assicurazione sanitaria⁶⁴ – e fornendo un codice-pseudonimo, che, attraverso la comparazione con il modello fornito dagli indicatori, individuava il nome della persona a cui appartenevano quei dati sensibili che erano stati pseudonomizzati ma mai anonimizzati; successivamente, tali informazioni venivano trasmesse al Ministero per la seconda fase di analisi.

Infatti, sebbene la normativa che ha previsto la realizzazione dell’algoritmo abbia autorizzato una «pesca a strascico indiscriminata dei dati personali dei soggetti coinvolti»⁶⁵, questa non soddisfa i requisiti ex art. 8.2 CEDU, dal momento che «l’interferenza esercitata dallo Stato nella vita privata non è proporzionata allo scopo perseguito in una società democratica [...] non essendovi conformità con il “giusto equilibrio” che deve esistere

⁶⁰ *Ex multis*, S. Bekker, *Fundamental rights in digital welfare states: The case of SyRI in the Netherlands*, in *Netherlands Yearbook of International Law* 2019, 2020, 289-307; M. Vetzo, *The Netherlands-algorithmic fraud detection system violates human rights- the case of SyRI in public law*, 2021, 650 ss.

⁶¹ Rechtbank Deen Haag, 05/02/2020, C-09-550982- HA 18-388, Tribunale dell’Aja.

⁶² «Il tribunale ritiene di non poter verificare l’accuratezza della posizione dello Stato su cosa sia esattamente SyRI, in quanto non è stato reso pubblico il modello di rischio e gli indicatori che compongono o possono consistere nel modello di rischio, non avendo fornito informazioni verificabili oggettivamente al tribunale al fine di consentire di verificare» Rechtbank Deen Haag, 05/02/2020.

⁶³ E. Falletti, *Discriminazione algoritmica: una prospettiva comparata*, op. cit.

⁶⁴ V. Gantchev, *Data protection in the age of welfare conditionally: Respect for basic rights or a race to the bottom?* In *European Journal of Social Security*, Vol 21, Issue 1, 2019, 16 ss.

⁶⁵ E. Falletti, *Discriminazione algoritmica: una prospettiva comparata*, op. cit.

tra l'interesse sociale perseguito dalla legge e la violazione della vita privata provocata dall'implementazione della legislazione stessa»⁶⁶.

Nonostante la Corte olandese abbia considerato rilevante solo l'art. 8.2 della CEDU, in quanto «sebbene indubbiamente il sistema SyRI integrasse la profilazione ai sensi dell'art. 4, par. 4 del GDPR, tuttavia non si configurerebbe un processo decisionale individuale automatizzato indicato e vietato dall'art. 22 GDPR»⁶⁷, autorevole dottrina⁶⁸ ritiene, invece, che in tale circostanza sussista un'ipotesi di profilazione, essendo SyRI un algoritmo di *deep learning* e non un sistema esperto, acquisendo i dati e inserendoli nelle *blackbox* ha generato l'elaborazione di una decisione individuale automatizzata che produce effetti discriminatori nella sfera giuridica del destinatario e lo priva, di fatto, del c.d. “diritto alla spiegazione” e alla contestazione, oltre che del sussidio in oggetto, senza avere possibilità di contraddittorio.

5. I Progetti “Pollicino”, “Smart Citizen Wallet”, “La carta dell'assegnatario”, “Marvel” e “Protector”: quando i meccanismi di gamification si celano dietro la digitalizzazione delle città

Il connubio tra altruismo dei dati e *social scoring* si è manifestato in talune iniziative italiane che sono state oggetto di istruttoria da parte del Garante⁶⁹. L'intervento dell'Autorità ha avuto come fine quello di prevenire «rischi connessi a meccanismi di profilazione che comportino una sorta di “cittadinanza a punti” e dai quali possano derivare conseguenze giuridiche negative sui diritti e le libertà degli interessati, inclusi i soggetti più vulnerabili»⁷⁰ e di intervenire, anche in un'ottica collaborativa, su progetti che, attraverso l'uso delle nuove tecnologie, «possano modificare il comportamento delle persone e condizionare anche l'esercizio delle libertà democratiche»⁷¹.

È d'uopo sottolineare che le problematiche sottese alla sorveglianza e le conseguenze della stessa sono di rilevante interesse giuridico perché effettuata dalle pubbliche amministrazioni.

La prima iniziativa oggetto di istruttoria è il “Progetto Pollicino”, essa prevede dei meccanismi premiali per i cittadini che, almeno sedicenni, scarichino sul proprio *smartphone* l'applicazione *IoPollicino* affinché consenta loro di lasciare le proprie “briciole digitali” attraverso il tracciamento della posizione; il *software* trasmette in forma “volontaria e anonima” i dati sugli spostamenti degli utenti al fine di consentire un'analisi della mobilità urbana.

⁶⁶ Rechtbank Deen Haag, 05/02/2020 par. 6.7.

⁶⁷ Rechtbank Deen Haag, 05/02/2020, cit.

⁶⁸E. Falletti, *Discriminazione algoritmica: una prospettiva comparata*, op. cit.

⁶⁹A. Vigorito, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *medialaws.it*, 1/2023.

⁷⁰ Comunicato stampa del Garante della Privacy dell'8 giugno 2022- Doc-Web 9778361.

⁷¹ Comunicato stampa del Garante della Privacy del 25 gennaio 2024- Doc-Web 9977299.

Oggetto della preoccupazione del Garante è la “moneta”⁷² con cui i cittadini saranno retribuiti e cioè i premi messi in palio dai soggetti privati, per questa ragione lo stesso ha richiesto ai soggetti pubblici e privati coinvolti «la base giuridica del trattamento, le modalità del funzionamento del sistema dell'app e i trattamenti ad essa connessi»⁷³.

La seconda iniziativa, invece, è lo “*Smart Citizen Wallet*”, nell'ambito della stessa, la pubblica amministrazione propone di attivare una “patente digitale” che permetta di identificare i cittadini più virtuosi tra coloro che si registrino, sempre su base volontaria, «in un innovativo quanto pervasivo sistema computazionale di sorveglianza e *tracking*»⁷⁴ a fronte di una serie di premi e incentivi messi a disposizione dal Comune e dai partner accreditati; in tale progetto, il cittadino sarà tenuto a rilasciare un consenso all'utilizzo dei propri dati che verranno poi utilizzati dall'applicazione dedicata. Emergono delle preoccupazioni con riferimento alla tipologia delle informazioni utilizzate, le finalità e i mezzi individuati in merito all'effettiva tutela dei diritti e delle libertà dei singoli interessati.

Con riguardo alla terza iniziativa oggetto di istruttoria, il Comune di Fidenza ha approvato un regolamento unico comunale in materia di edilizia residenziale pubblica (E.R.P.) che, ai sensi dell'articolo 8, Titolo III, Parte II dello stesso, introduce un sistema che attribuisce ad ogni nucleo familiare la “Carta dell'Assegnatario”, riportante un punteggio iniziale di 50 punti. All'interno del documento vengono riportate le tabelle “dei divieti e degli obblighi legati all'alloggio e agli spazi accessori” tra cui figurano “l'utilizzo di barbecue e griglie sul balcone” o l'ospitare “persone estranee al nucleo senza la preventiva autorizzazione del Comune e/o dell'Ente gestore” comportamento a cui farebbe seguito una multa di 50 euro e una decurtazione di 25 punti. Inoltre, in caso di segnalazioni di comportamenti illeciti è previsto l'intervento di un “agente accertatore” di ACER⁷⁵ che potrà ispezionare gli alloggi e sanzionare i nuclei familiari. Infine, nel caso di mancata commissione di illeciti nell'arco di tre anni è prevista la dazione di una premialità, mentre a fronte della decurtazione dei punti, si rischierà «la risoluzione e/o la decadenza dal contratto di locazione, con possibili conseguenze pregiudizievoli in capo a categorie di soggetti già vulnerabili»⁷⁶.

Nel caso di studio appena menzionato, si paventa che l'introduzione di *software* di intelligenza artificiale – quali i droni – possa determinare un controllo pervasivo delle pubbliche autorità sui domicili dei soggetti beneficiari degli alloggi popolari, pertanto il Garante ha ritenuto necessario fare chiarezza sui meccanismi di attribuzione di punti e sull'impatto della tecnologia su questa iniziativa. Infine, i progetti Marvel (*Multimodal Extreme Scale Data Analytics for Smart Cities Environments*) e Protector (*PROTECTing places of wORship*), entrambi finanziati con fondi europei, sono stati elaborati

⁷² Y. Citino, *Cittadinanza “a punti” e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, in *diritticomparati.it*, 22 giugno 2022.

⁷³ Comunicato stampa del Garante della Privacy dell'8 giugno 2022.

⁷⁴ Y. Citino, *Cittadinanza “a punti” e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, cit.

⁷⁵ L'Azienda Casa Emilia-Romagna (ACER) gestisce il patrimonio immobiliare di Edilizia Residenziale pubblica e provvede alla loro manutenzione.

⁷⁶ Comunicato stampa cit.

con lo scopo di sviluppare soluzioni tecnologicamente avanzate per migliorare la sicurezza urbana nel novero delle *smart cities*.

La prima iniziativa prevedeva l'acquisizione dei filmati delle telecamere di videosorveglianza e dell'audio dai microfoni installati nelle vie del Comune di Trento per vigilare sulla sicurezza urbana per individuare, tramite tecniche di intelligenza artificiale, eventi di rischio.

La seconda, invece, aveva ad oggetto la captazione dei filmati senza audio e la rilevazione di messaggi d'odio o emozioni negative attraverso i post pubblicati sui *social network* per arginare eventuali minacce di natura religiosa. Secondo il Garante, nel caso di specie, mancava una base giuridica sufficiente, trattandosi di dati estremamente sensibili, inoltre, il livello di trasparenza era carente, non essendo chiarita nella cartellonistica stradale la finalità di trattamento dei dati; sul piano delle misure di prevenzione, «le tecniche di anonimizzazione erano deficitarie e non era stata effettuata la valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali»⁷⁷, inoltre le informazioni erano cedute a *partner* internazionali⁷⁸.

Dunque, è evidente come all'istituto della cittadinanza intelligente si stiano affiancando delle «logiche di mercato che targettizzano la popolazione con l'obiettivo di estrarre dati»⁷⁹, agli strumenti tradizionali si stanno sostituendo dei meccanismi che con l'ausilio dell'intelligenza artificiale minacciano l'impianto regolatorio della *Privacy* e questo ha indotto la dottrina⁸⁰ a chiedersi quale sia la direzione assunta dalle pubbliche amministrazioni per rendere gli enti locali "intelligenti", il fondamento scientifico di tali strumenti di sorveglianza di massa e se sussista un diritto, in capo al cittadino, di conoscere la logica giuridica alla base della nuova pervasività tecnologica.

6. Conclusioni attraverso l'analisi comparata dei casi di studio: Siamo davvero i nostri dati?

Nei paragrafi precedenti, sono state analizzati i casi di studio oggetto della ricerca e nel prosieguo si procederà ad una valutazione comparata dei medesimi.

Il vaglio del Sistema dei Crediti sociali ha fatto emergere un rilevante livello di pervasività degli strumenti di intelligenza artificiale nella vita dei cittadini cinesi in nome della creazione della società della fiducia di confuciana memoria in cui tutti i rapporti umani costituiscono un reticolato che cede sovranità a favore del Governo cinese nell'auspicio della concessione di premialità da conferire a seguito dell'attività di monitoraggio e controllo sui comportamenti della popolazione.

D'altro canto, però, il meccanismo – di senso opposto a quello occidentale – di tutelare attraverso una Legge sulla Protezione delle informazioni personali, per la prima volta nel 2021 il diritto alla riservatezza,

⁷⁷ Provvedimento del Garante della Privacy dell'11 gennaio 2024 doc. web 9977020.

⁷⁸ Nel progetto PROTECTOR i dati erano condivisi con la Polizia di Anversa e con il Ministero dell'Interno della Bulgaria.

⁷⁹S. Zuboff, *The Age of Surveillance Capitalism, The Fight for a Human Future at the New Frontier of Power*, in *PublicAffairs*, 2019.

⁸⁰R. Caso, *L'equilibrio tra privacy e sicurezza* in *L'Adige*, 3 febbraio 2024.

permette di aderire a quella dottrina minoritaria⁸¹ che rifugge dalla rappresentazione del progetto cinese come una «distopia orwelliana», sottolineando sia la frammentarietà dei vari sistemi di credito sociale sia la nuova centralità della *privacy*, a discapito di una sorveglianza di massa. Dall'analisi del caso SyRI è emerso che, in maniera non trasparente, un algoritmo di *deep learning* abbia captato i dati, anche sensibili, dei soggetti residenti in diverse zone considerate svantaggiate in assenza di base giuridica, ingerendosi prepotentemente nella vita privata dei singoli individui.

Lo studio dei casi italiani, invece, ha evidenziato come, mal celandosi dietro il principio delle *smart cities*, le pubbliche autorità hanno iniziato ad acquisire i dati dei cittadini a fronte di un corrispettivo, facendo venire meno il principio della gratuità, punto fermo del concetto di altruismo dei dati con meccanismi poco trasparenti, servendosi di *software* quali «assistenti virtuali, strumenti di analisi di immagini, motori di ricerca, sistemi di riconoscimento facciale e vocale»⁸² che possono violare i principi costituzionali.

Si evidenzia la preoccupazione in merito all'uso di *software* di intelligenza artificiale e di algoritmi con riferimento all'utilizzo dei dati in quanto il rischio è che la quantità delle informazioni di carattere personale che circolano determini un deterioramento della qualità in aperto contrasto con il fine promozionale che l'ordinamento giuridico deve avere nei confronti della società, secondo i dettami della Costituzione.

Infatti, nell'eventualità in cui si propendesse verso un percorso di senso opposto a quello intrapreso, pur mantenendo l'ausilio della strumentazione tecnologica "intelligente", attraverso un ritorno alla centralità della persona, si potrebbe addivenire ad una concezione di *privacy* e protezione dei dati che sia improntata al rispetto dei diritti umani per allontanarsi dal paradigma secondo cui "noi siamo i nostri dati"⁸³.

Di fatti, se a fronte di un beneficio di carattere individuale che non abbia caratteristiche premianti, il soggetto consapevolmente decida di servirsi di *software* di intelligenza artificiale per trarre giovamento nella propria quotidianità, non si configura più una logica pubblicitica di sorveglianza, controllo e intrusività dei pubblici poteri sull'uomo e sui suoi dati, ma è la persona che riacquisisce padronanza di sé e decide di immettere in circolo i suoi dati. Ad esempio, con riferimento ai dati di carattere sanitario, sarà possibile acconsentire alla cessione della propria anamnesi per permettere ai sistemi che già analizzano grandi quantità di dati medici di individuare relazioni e modelli specifici per migliorare le diagnosi o la profilassi, suggerendo esami strumentali necessari.

In conclusione, analizzando la normativa relativa al trattamento dei dati personali, alla luce del mutato contesto giuridico di riferimento, non già in un'ottica conservativa ma in una prospettiva propriamente assiologica, teleologicamente orientata ad un utilizzo proattivo delle nuove tecnologie, sarà possibile prevedere ulteriori, benefiche, finalità di trattamento dei dati

⁸¹*Ex multis*, M. Infantino, W. Wang, *Armonia sotto controllo: la regolazione del credito sociale nelle 'città modello' cinesi*, MLR, Vol. 1, Issue 2, 2020, 4-43.

⁸²Dossier n. 57 del 12 novembre 2021- Legge sull'intelligenza artificiale.

⁸³E. M. Renieris, *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, 2023, Massachusetts.

che siano conformi alla tutela di valori anche costituzionalmente garantiti quali il diritto alla salute, alla vita e al lavoro.

Vanessa Previti
Dipartimento
Università degli Studi di Messina
vanessa.previti@studenti.unime.it

